Special Conference Edition n. 7

CEPOL
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

EUROPEAN LAW ENFORCEMENT RESEARCH BULLETIN

Tackling the World of High-Risk Criminal Networks (HRCN)

Conference in cooperation with
Economic and Financial Police School
of the Italian Guardia di Finanza.

25-27 March 2025, Ostia, Rome (Italy)

CEPOL is an agency
of the European Union

Manuscript completed in February 2026

EUROPEAN LAW ENFORCEMENT RESEARCH BULLETIN

Previously published as and continuing from the *European Police Science and Research Bulletin*.

Luxembourg: Publications Office of the European Union, 2026

doi: https://doi.org/10.3013/39j9my77

Print ISSN 2599-5855 QR-01-25-007-EN-C
PDF ISSN 2599-5863 QR-01-25-007-EN-N

Content

Jan Pecháček

Executive Director

https://doi.org/10.3013/85m0p576

The European Union Agency for Law Enforcement Training (CEPOL) research and science conferences have, over the years, evolved into a recognised European platform where law enforcement practitioners, researchers, academic scholars and policy experts meet to exchange research findings, operational insights and forward-looking perspectives. They embody our conviction that effective law enforcement in Europe must be grounded in evidence, strengthened by interdisciplinary dialogue and inspired by innovation.

The conference 'Tackling the world of high-risk criminal networks', held last year in Ostia (Italy), once again confirmed the value of this approach. Bringing together experts from academia, law enforcement authorities, EU institutions and international partners, the event provided a timely and in-depth exploration of how criminal networks evolve, adapt and entrench themselves within our societies. The presentations and debates demonstrated that high-risk criminal networks (HRCNs) are neither static nor confined to one domain; rather, they operate across borders and sectors, and increasingly across physical and digital environments.

This special conference edition of the *European Law Enforcement Research Bulletin* captures the richness and diversity of those discussions. The contributions presented here reflect the complexity of today's organised crime landscape and underline the necessity of holistic, research-informed responses.

Taken together, the contributions in this edition demonstrate that HRCNs are adaptive, multilayered and increasingly embedded within legitimate economic and digital systems. They require responses that are equally adaptive, rooted in research and supported by strong cooperation at the national, European and international levels.

For CEPOL, fostering this dialogue between research and practice remains a core mission. By providing a platform for the dissemination of empirical findings and innovative approaches, we aim to strengthen the professional development of law enforcement officials and to support a more predictive, agile and resilient European law enforcement community.

I warmly invite you to engage with the articles presented in this edition. They offer not only analytical depth but also practical insights that can inform strategy, training and operational work.

We hope this publication inspires further research, strengthens cross-border cooperation and contributes to our shared commitment to protecting the security and integrity of our societies.

Jan Pecháček
Executive Director, CEPOL

Maria João Guia

Research and Knowledge Management Officer, Editor-in-Chief

https://doi.org/10.3013/dxmpxz16

This editorial foreword introduces the seventh issue of the conference bulletin of the *European Law Enforcement Research Bulletin* (Bulletin), marking a further milestone in a series dedicated to advancing rigorous, practice-oriented scholarship on police science, contemporary crime and security challenges. This issue draws on the proceedings of the 2024/2025 Research & Science Conference held in March 2025 in Ostia (Italy), devoted to the analysis of high-risk criminal networks (HRCNs). The Bulletin continues its core mission: to provide a credible forum where empirical research, theoretical development and operational insight intersect, offering value to scholars, practitioners and policy communities alike.

The conference proved to be a substantive and timely success. Bringing together researchers, policymakers, EU officials, analysts and law enforcement professionals from diverse jurisdictions, it nurtured sustained dialogue on the structure, resilience and adaptive capacity of HRCNs. Contributions addressed methodological innovation, cross-border cooperation and the implications of technological change for both criminal organisation and investigative response. The quality and diversity of the exchanges confirmed the relevance of the conference series as a stable platform for informed, evidence-based debate.

As Editor-in-Chief and, together with the Editorial Board members, I remain committed to maintaining the Bulletin's academic integrity, editorial independence and relevance to applied research. This role entails not only coordinating and reviewing contributions of the highest scholarly standard, but also ensuring coherence across disciplines and perspectives represented in each issue. The present volume reflects that commitment, offering carefully selected papers that combine analytical depth with operational relevance and that collectively advance understanding in this complex field.

This issue would not have been possible without the sustained dedication of the Editorial Board members and the editors' assistants, whose expertise, diligence and commitment continue to set a high benchmark for the publication.

I also extend my sincere appreciation to the authors for their rigorous and original contributions, and to the reviewers for their thorough, constructive and timely assessments. Their collective efforts underpin the scientific quality of this bulletin and reinforce its standing as a trusted reference within the law enforcement research community.

In the pages that follow, each chapter is introduced through a concise analytical synopsis designed to guide the reader through its core arguments, methodological approach and principal findings. These summaries are intended not merely as descriptive short abstracts, but as structured points of entry that situate each contribution within the broader thematic framework of HRCNs addressed in this issue. By foregrounding conceptual focus and empirical relevance, the chapter synopses aim to facilitate an informed and coherent reading of the volume as a whole, while allowing readers to identify points of convergence, complementarity and critical dialogue across contributions.

The opening article, awarded the best paper recognition, authored by Patricia Faraldo Cabana, offers a rigorous and critical examination of how the European Union has progressively framed the trafficking of cultural goods as a form of organised crime within its policy architecture. Drawing on a systematic qualitative content analysis of EU policy documents published between 1993 and 2023, the article traces the historical emergence, consolidation and transformation of this narrative, with particular attention to its increasing association with terrorism, terrorist financing and money laundering. The author demonstrates that, despite the growing policy emphasis on these links, EU approaches remain conceptually fragile and often rely on unsubstantiated assumptions regarding the organised and transnational nature of cultural property crime. The article persuasively argues that this lack of conceptual clarity risks generating misguided policy responses, while also identifying a significant policy shift of potential value: the incorporation of art market actors into the EU anti-money-laundering (AML) framework. By situating trafficking in cultural goods at the intersection of organised crime control, white-collar crime regulation and cultural heritage protection, the contribution provides an empirically grounded and theoretically informed critique that sets a strong analytical tone for the volume.

Gabriela Boneva, Luke Bates and Babak Akhgar authored the second chapter. In short, it maps the current EU landscape of new psychoactive substances (NPS) as a rapidly evolving drug phenomenon that strains both public health systems and law enforcement capacity. The article explains how NPS markets exploit legal fragmentation and chemical 'micro-innovation', producing substances that mimic controlled drugs while remaining difficult to schedule, identify and detect. Building on a two-stage design – an extensive review of academic and official sources complemented by structured consultations with practitioners from law enforcement agencies and postal services involved in the ARIEN project – the chapter reconstructs how NPS circulate through hybrid online–offline supply chains, frequently using Surface Web and Dark Web retail and relying heavily on postal and courier logistics. Boneva et al. synthesise evidence on prevalence (notably synthetic cathinones and synthetic cannabinoids), concealment and distribution tactics (including prison-focused methods such as paper impregnation), and the broader risk environment shaped by inconsistent forensic tools, limited automated online investigative capabilities and patchwork national control models (generic, substance-by-substance or hybrid). The chapter closes by identifying concrete capability gaps – particularly in detection technologies, cross-border intelligence integration and legislative harmonisation – and proposes a forward agenda that aligns regulatory coordination with operational realities and the escalating health harms associated with unknown potency and polysubstance exposure.

The third contribution, produced by Aleksandar Atanasov, provides an in-depth, operationally grounded analysis of HRCNs involved in migrant smuggling in Bulgaria, examined through criminological, law enforcement and intelligence lenses. Focusing on developments observed over the last three years, the chapter reconstructs the organisational logic and modus operandi of these networks by integrating open-source materials with analytically framed professional insight. Central to the analysis is the identification of five interrelated drivers – geosocial, local, foreign, criminal and non-criminal, and geopolitical factors – that together shape the structure, adaptability and resilience of smuggling networks operating along the Western Balkan and Eastern Mediterranean routes. The study details how Bulgarian-based criminal infrastructures interact with foreign facilitators, exploit challenging border terrain, deploy layered transport tactics and rely on a differentiated division of labour ranging from drivers and guides to field captains and network leaders. Beyond operational patterns, the chapter situates migrant smuggling within a broader security context, highlighting points of convergence with corruption, poly-criminality and, in specific cases, terrorism-related risks. By systematically mapping roles, routes and enabling environments, the article offers policy-relevant insights into how these networks function as service-oriented criminal enterprises and underscores the need for integrated, cross-border responses that address both immediate operational threats and the wider structural conditions sustaining them.

In Article 4, Hanna-Mari Lahtinen and five colleagues tackle a central problem in combating online child sexual abuse and exploitation: the evidential and behavioural 'blind spot' created by the fact that most child sexual abuse material (CSAM) users are never detected. Rather than relying on clinical or forensic cohorts, the authors describe and evaluate a replicable Dark Web data collection model that intercepts CSAM-related search activity on a Tor search engine and redirects users to an anonymous, multi-language survey alongside links to support services. Using responses from a large pool of self-identified CSAM searchers (with a final analytic sample exceeding 2 000 after exclusions), the study compares three self-reported groups – those reporting prior charges for sexual crimes against children, those reporting charges against adults and those reporting no charges – across motivational, behavioural and situational indicators. The findings underline meaningful heterogeneity within this offending population: variables such as prior violent charges, seeking material depicting the abuse of very young children, grooming behaviours and physical contact with children are associated with elevated likelihood of belonging to the 'charged' groups, while a substantial subgroup reports no charges and appears more receptive to preventive engagement. The chapter's contribution is therefore twofold: it demonstrates a practical method for accessing otherwise hidden offender data at scale, and it translates the resulting risk-relevant patterns into implications for law enforcement and prevention – particularly the value of integrating CSAM screening into wider sexual and violent crime investigations and of using online 'choice points' (search interfaces) to divert users toward disruption and help pathways.

The following article is authored by Victoria Koutsoupia, and it examines how confiscation, whistleblowing and technological innovation can be combined to disrupt the structural resilience of HRCNs across the EU. Rather than approaching organised crime solely through prosecution, the article reframes the problem as an economic and systemic one, arguing that criminal networks are most effectively weakened by depriving them of illicit profits and informational advantages. Through a qualitative, multi-method analysis of EU legislation, policy instruments and selected case studies, the chapter shows how asset confiscation targets the financial core of organised crime, while whistleblowing functions as a critical catalyst for detection and evidentiary development – particularly in complex, transnational cases. The analysis situates these tools within an increasingly digital criminal environment, where

encryption, crypto-assets and online platforms both facilitate criminal activity and open new avenues for enforcement through blockchain analytics, interoperable databases and secure reporting technologies. By assessing recent legal developments such as Directive 2024/1260 ([1]) and EU whistleblower protection frameworks alongside technological enforcement practices, the article demonstrates that no single instrument is sufficient in isolation. Its central contribution lies in articulating an integrated strategy in which confiscation, protected insider reporting and advanced technologies operate synergistically, offering a policy-relevant roadmap for dismantling HRCNs while safeguarding fundamental rights and reinforcing cross-border cooperation.

Article 6, written by Mari-Liis Tohvelmann and co-authored by three other authors, evaluates whether a serious-game, avatar-based training tool for investigative interviewing (with adult witness avatars) produces skills that generalise beyond the simulated setting to interviews with human witnesses. Using a pre-registered, between-groups experiment with 58 novice interviewers (feedback versus no-feedback control), participants completed four avatar interviews followed by a live online interview with a mock adult witness who had viewed a short crime video about a week earlier. The study operationalises interview quality through a widely used distinction between recommended question types (free recall, cued recall, open questions) and non-recommended types (closed, forced-choice, suggestive, misleading), and further examines whether questioning style translates into more accurate witness accounts. Results indicate that process feedback during avatar practice reliably reduced non-recommended questioning styles and increased the proportion of recommended questions during training; crucially, this pattern transferred to the subsequent mock-witness interview, where the feedback group again used fewer non-recommended questions and a higher recommended-question proportion. However, the intervention did not yield measurable gains in the amount or proportion of correct details elicited from the mock witnesses, suggesting that the improving question form alone may be insufficient – at least for novices, brief training doses, short stimulus events and relatively high baseline adult accuracy. The authors interpret these findings as evidence that avatar training with immediate feedback can shift interviewer behaviour in a direction consistent with best-practice guidelines, while also highlighting the need for future work (e.g. modelling components, AI-assisted coding, practitioner samples and designs that better test evidential yields) to translate improved interviewing style into consistently better investigative outcomes.

Denis Solodov is the author of Article 7, which examines how Poland's approach to cooperating witnesses in organised crime cases can be strengthened through the adoption of the UN Méndez Principles on Effective Interviewing. It argues that while cooperating witnesses are often crucial sources of insider evidence, their testimony is inherently exposed to bias, strategic self-interest and procedural vulnerabilities, particularly given incentive structures such as leniency or immunity and shifts in procedural status. By analysing Polish witness categories and recurring practical challenges – including corroboration deficits, limited defence participation and the sophistication of organised-crime actors – the chapter shows how traditional, confirmatory interviewing practices and reliance on written protocols may undermine evidential reliability. It concludes that integrating non-coercive, rapport-based interviewing, supported by mandatory audiovisual recording, targeted training and clearer procedural safeguards, would enhance both the quality of evidence and the legitimacy of organised crime investigations.

([1]) Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation, OJ L, 2024/1260, 2.5.2024, ELI: http://data.europa.eu/eli/dir/2024/1260/oj.

Article 8, authored by Zaur Gouliev, conceptualises 'disinformation as a service' as a maturing form of organised cybercrime in which influence operations are commodified, modular and sold to state and non-state clients through the same market logic that underpins crime-as-a-service ecosystems. Drawing on a case study of the 'Doppelganger' campaign, a systematic review of Surface Web and Dark Web marketplaces and a macro-analysis of foreign information manipulation around elections, the article shows how cloned media sites, automated amplification, ad-tech tools and bulletproof hosting are combined into resilient influence pipelines. These capabilities are traded alongside malware and access brokerage, evidencing a convergence between disinformation and cybercrime that lowers barriers to entry, frustrates attribution and enables rapid reconstitution after takedowns. The study concludes that disinformation as a service represents an HRCN model whose disruption requires law enforcement responses that target both market supply chains and campaign infrastructure through coordinated, cross-border and technologically integrated strategies.

Luna Filipović is the author of Article 9. She demonstrates how forensic linguistics can materially strengthen the investigation of international and organised crime by improving both evidence elicitation and intelligence analysis in multilingual contexts. Drawing on a large body of authentic police–suspect interactions from the United Kingdom and the United States, the chapter shows how questioning style, translation practices and unexamined linguistic and cultural assumptions can generate miscommunication, distort meaning and weaken evidential value – particularly in cross-language interviews. Beyond face-to-face policing, the article extends forensic linguistic insight to Dark Web communications, illustrating how systematic features of non-native English can reveal offenders' linguistic backgrounds and collaborative patterns within transnational criminal networks. By integrating empirical linguistic research, applied language typology and real investigative data, the chapter argues that forensic linguistics remains an underused yet scientifically robust resource for law enforcement, offering concrete benefits for accuracy, fairness and effectiveness in complex, multilingual criminal investigations.

Article 10, written by Pasquale Danese, argues that VAT (value added tax) fraud and false invoicing have become central mechanisms through which organised crime now generates and launders proceeds inside the legal economy, forcing a rethink of the classic 'placement–layering–integration' model. Building on European and Italian threat reporting, the chapter proposes that laundering dynamics vary systematically with the type and sophistication of criminal activity: low-complexity predatory crime still yields cash and fits the traditional model, whereas financial-crime networks increasingly produce 'already-banked' illicit revenues (and cybercriminal groups produce crypto-denominated proceeds), making 'placement' less decisive and shifting the operational problem toward separating funds from their origin under high traceability conditions. To capture this transition, the author introduces an AI-assisted 'declining sigmoid' function linking criminal sophistication to the share of cash proceeds, and advances a new phase – 'dissociation' – to describe strategies such as cross-border transfers to non-cooperative jurisdictions, monetisation/cash-out through intermediaries and crypto-based obfuscation (e.g. mixers, chain-hopping, DeFi (decentralised finance) mechanisms). The core contribution is a three-level framework (cash, traditional finance, DeFi/crypto) that treats laundering as context-dependent rather than linear, with implications for investigative training, asset tracing and EU cooperation against financially embedded criminal networks.

We then find Murat Tina's Article 11, which examines how foreign terrorist fighters (and returnees) intensify the convergence between organised crime and terrorism, arguing that recent conflict dynamics – especially those linked to Syria and broader governance collapse in the Levant – have accelerated a shift from occasional, transactional

cooperation to more durable, mutually reinforcing relationships. Drawing on desk-based analysis of scholarship, policy reporting and open-source data, the chapter traces how terrorist groups increasingly adopt profit-driven criminal practices (smuggling, trafficking, document fraud and money laundering), while criminal networks benefit from the operational reach, skills and ideological cover that foreign terrorist organisations can provide. The author treats foreign terrorist fighters as 'bridging actors' who move between milieus, connect local illicit markets to transnational extremist infrastructures and help standardise shared methods (routes, facilitators, informal finance, crypto channels), with illustrative discussion of patterns linked to the Islamic State in Iraq and Syria (ISIS) and the Kurdistan Workers' Party (PKK). The main implication is strategic: threat assessment and enforcement models that rigidly separate 'crime' from 'terrorism' understate hybrid risk, so responses should integrate cross-border intelligence, financial disruption, database interoperability and prevention measures (including prison-focused de-radicalisation and post-return monitoring) to target the combined ecosystem rather than its components in isolation.

Article 12, authored by Wendy Schreurs and two co-authors, argues that Dutch efforts against HRCNs are increasingly shaped by data-driven policing built around the operational exploitation of digital traces – especially encrypted communications once lawfully accessed – while stressing that technical capability alone is insufficient without organisational and ethical governance. Using interviews with strategic actors in the Dutch National Police, the authors describe how decrypted datasets from platforms such as EncroChat / Sky ECC / ANOM can produce actionable intelligence and arrests, but only when fused with other sources (e.g. automatic number plate recognition, open-source intelligence, video, seized devices) and translated into interventions through multidisciplinary work. The analysis frames data-driven policing as an evolution of intelligence-led policing, operationalised through models that integrate behavioural, technical and quantitative layers (e.g. the collect, store, analyse, engage – CSAE – model), yet repeatedly highlights 'human-in-the-loop' necessities: contextual interpretation, professional discretion and leadership that can bridge analysts and investigators. Implementation barriers are mapped across four domains – outdated ICT and storage, data quality and bias ('garbage in, garbage out'), cultural reluctance to share information and the legal–ethical friction created by surveillance technologies and opaque algorithms – leading to a central conclusion that effectiveness against adaptive HRCNs depends on sustained investment in infrastructure, skills, flexible team structures, clear authorisation/oversight mechanisms and continuous ethical review alongside technical innovation.

Article 13 is written by Jasmin Saarijärvi and nine co-authors, and it synthesises findings from the EU-funded Poseidon project, mainly on how corruption operates as an enabling condition for organised crime within EU seaport supply chains, especially in containerised trade. Drawing on desk research, interviews, focus groups, surveys and six case studies (Rotterdam, Antwerp-Bruges, Piraeus, Algeciras, Cartagena and Venice), the study maps where and why ports become vulnerable: high-throughput logistics, time-sensitive cargo (notably perishables) and complex documentation workflows create pressure points that organised crime groups exploit through bribery, information leakage and manipulation of inspections. The analysis distinguishes step-specific risks (e.g. 'rip-on/rip-off' insertion in terminals, compromised customs risk-selection, PIN-code abuse for container pickup, corruption of transporters and ship personnel) from structural drivers that cut across the chain, such as extensive human involvement in key tasks, uneven digitalisation and access controls, close-knit port labour communities, procurement and political exposure and friction in public–private information-sharing under legal constraints. Poseidon identifies early countermeasures – digitalisation, integrity screening, training and awareness and stronger public–private cooperation – while building an EU stakeholder network and an interactive dashboard to support transferability

assessment and, ultimately, make recommendations toward an EU port supply chain integrity standard, emphasising that effective responses must be tailored to port-specific conditions yet coordinated at the EU level to reduce displacement ('waterbed') effects.

Article 14 is presented by Halima Guelai, continuing the seaport topic as it examines how anti-corruption policy in the Port of Antwerp-Bruges has evolved alongside surging cocaine flows, violence and insider-enabled infiltration, arguing that corruption should be treated not simply as a facilitating factor but as a constitutive element of organised drug crime within port ecosystems. Using a 2013 port assessment, a targeted literature review (2013–2025) and 23 expert interviews, the study evaluates measures introduced over the last decade through five governance pillars – role clarity in multidisciplinary cooperation, political backing, evidence-based design, long-term orientation and adaptive capacity – and finds a persistent tilt toward 'visible' deterrence (screening, port bans, surveillance and access-control technologies) rather than the social, administrative and political conditions that sustain corrupt opportunity structures. It shows how fragmented mandates across police, customs, prosecutors, port authorities and private operators – combined with capacity constraints, legal barriers to information sharing, reliance on temporary labour and shifting modus operandi revealed by cases like Sky ECC – limit proactive prevention and encourage displacement rather than durable risk reduction. Technological fixes such as blockchain-based container pickup can harden specific vulnerabilities, but the article stresses that they may relocate pressure onto other roles unless these fixes are embedded in integrity governance, cybersecurity, reporting protections (e.g. PortWatch), sustained training and organisational change. The recommended trajectory is an integrity-based strategy grounded in shared responsibility, trust and continuous monitoring – accepting that 'zero corruption' is neither realistic nor efficiency-neutral – while pointing to policy windows such as Belgium's push to expand the International Ship and Port Facility Security Code and the coordinating potential of a national drugs agency to move from episodic securitisation toward a more integrated, evaluable and resilient anti-corruption architecture.

Kristin Weber is the author of Article 15 and she argues that social network analysis (SNA) – when anchored in legally validated evidence – can materially strengthen counterterrorism investigations by converting fragmented case material into an interpretable map of covert, high-risk networks. Drawing on 36 final court cases (2014–2017) involving ISIS-linked offences in Germany (excluding Al-Qaeda), the study combines qualitative file coding with SNA to reconstruct a network of 255 individuals and 650+ ties, distinguishing roles such as recruiters, preachers, propagandists, facilitators and foreign terrorist fighters. Using Gephi visualisation and standard centrality measures (degree, betweenness, closeness), the analysis shows how operational capacity depends not only on visible leaders but also on brokers and bridging nodes that connect peripheral clusters to core actors and sustain information, resource and mobilisation flows. A detailed subnetwork example (SR49–SR52) illustrates how a small set of peripheral yet well-positioned recruiters – reinforced by kinship ties – can drive departures to conflict zones and maintain linkage to a central preacher node, implying that targeted disruption of such connectors could fragment network functionality and prevent recruitment cascades. The article concludes that SNA is most valuable as a police training and investigative decision-support tool – improving risk assessment, prioritisation and inter-agency coordination – while warning that network adaptation, data incompleteness and overreliance on first-degree ties require longitudinal monitoring and higher-order network perspectives to detect reconfiguration after interventions and to anticipate renewed mobilisation.

Marco Garofalo and colleagues present Article 16, reporting on a European multidisciplinary platform against criminal threats (Empact) HRCN operational action led by Italy's Central Operations Service, which pilots a prevention-oriented methodology to index the risk of Italian mafia infiltration in foreign economies by shifting attention from classic 'sentinel crimes' toward business, ownership and contextual indicators that signal reinvestment, market distortion and corrupt access to procurement or regulated sectors. Built through collaboration among the State Police, Guardia di Finanza, Direzione Investigativa Antimafia, the European Union Agency for Law Enforcement Cooperation (Europol) and the Università Cattolica del Sacro Cuore of Milan's Transcrime research centre, the project operationalises Italy's anti-mafia experience (including the organisational logic associated with Article 416-bis) into a two-track assessment: (i) investigative profiling of managers / beneficial owners using structured intelligence and open-source criteria (relationships, judicial history, professional/financial traces), and (ii) a data-driven corporate risk model derived from Orbis data that compresses hundreds of candidate variables into a calibrated set of indicators spanning ownership opacity, territorial clustering, anomalous officer profiles, financial irregularities, adverse events and political exposure. From 59 nominated firms across catering, earth-moving/construction and gaming/betting, Transcrime could reliably identify 42 and classified most as high risk, highlighting patterns such as complex multilayer ownership, shareholders just below beneficial ownership disclosure thresholds, unusually elderly beneficial owners, high co-location of firms at the same address and creditor-payment anomalies – features that are more prevalent than in a matched control group. The combined analyses suggest that infiltration risk concentrates differently by sector and geography, that low-profile sectors may function as quieter vehicles for reinvestment and that convergence between policing assessments (including links to suspicious transaction reports and prior mafia-related records) and statistical scoring can improve targeting; the paper's core implication is that stable cross-border information exchange and shared analytical standards are necessary to turn such hybrid, indicator-based scoring into a durable tool for early detection and coordinated disruption of mafia economic penetration abroad.

The authors of Article 17, Ana Isabel Barros and colleagues, then argue that illicit markets should be analysed as adaptive 'business systems' rather than only as logistics chains or social graphs, and propose an exploratory, computational approach that links a criminal organisation's value chain (financial, logistical and social) to the time-dependent effects of law enforcement interventions. Using cocaine trafficking as the illustrative domain, Barros et al. frame criminal networks as complex adaptive systems whose profit incentives, embeddedness in legitimate economies and capacity to change modus operandi generate resilience and unintended intervention effects (e.g. displacement, violence escalation, corruption). The paper operationalises 'criminal business modelling' through stakeholder / value-network analysis, business model canvas mapping and cost–benefit quantification under uncertainty, then translates these insights into an agent-based simulation designed less for prediction than for learning and strategy design. Three stylised business models (smuggling via a Dutch port, routing via an alternative EU port and 'cocaine laundry' impregnation/extraction) are parameterised with differing cost structures, and simulated policing strategies shift relative profitability by raising targeted costs (with particular sensitivity in corruption and specialised nodes). The model's core contribution is pedagogical and organisational: by visualising how focused enforcement can leave profits intact (e.g. easily replaced extractors), trigger a waterbed effect (route switching) or create rapid cycling among business models, it supports double-loop learning – forcing decision-makers to revisit assumptions, anticipate adaptation and consider sustained, system-wide interventions that reduce overall attractiveness rather than merely reallocating pressure.

Article 18, by Sónia Morgado and Sérgio Felgueiras, examines *Ozark* (Season 1) as a criminological text, using mixed-method content analysis (thematic coding plus discourse analysis, supported by frequency counts) to map how the series depicts recruitment into organised crime and how closely those portrayals align with established frameworks. The authors treat recruitment as a multi-causal process shaped by structural strain, social learning and differential association and rational choice calculations, showing how characters are drawn in through a combination of economic precarity, social and familial obligations, opportunity structures and progressive moral disengagement; recruitment is portrayed less as a single 'moment' than as an incremental entanglement where coercion, manipulation and perceived necessity recalibrate actors' cost–benefit judgements over time. The analysis also situates these depictions within scholarship on media effects, arguing that serialised crime narratives can both reflect real recruitment tactics (e.g. exploiting vulnerability, leveraging trust networks, normalising deviance) and distort public understanding via simplification, stereotyping and glamorisation, with downstream implications for attitudes toward punishment, policing and prevention. By focusing on the season that establishes core relationships and motivations, the study claims a methodologically 'clean' window into early-stage criminal immersion, and it concludes that *Ozark* offers a plausible – though dramatised – representation of recruitment dynamics that can be used pedagogically (e.g. for media literacy or practitioner training) if interpreted critically and without treating fiction as direct empirical evidence.

Jasmin Saarijärvi and Mark Worth, authors of Article 19, situate corruption in the EU's financial sector as a two-way phenomenon – where institutions can be simultaneously exploited by and complicit in illicit finance – and frame it as a priority domain within the EU's emerging anti-corruption strategy, informed by a European Commission mapping exercise that flags finance (alongside procurement, construction, healthcare, defence/security and sports) as a high-risk area requiring stronger regulation, oversight, investigation and enforcement. The authors argue that the sector's decentralisation, digitisation and sheer transactional volume create 'black holes' for monitoring, while organised crime groups leverage professional enablers (lawyers, notaries, accountants, real-estate actors) and offshore structures to build parallel criminal economies that blur upperworld/underworld boundaries and complicate attribution of responsibility. Money laundering and tax evasion are treated as the most consequential corruption-linked crimes, intertwined with fraud, sanctions / terrorism-financing risks and cyber-enabled victimisation, with low asset recovery rates and under-investigation amplifying perceived impunity; the piece further highlights operational obstacles such as divergent national predicate-offence regimes, beneficial ownership opacity (shell entities, layered structures) and the growing misuse of fintech, crypto, DeFi, virtual IBANs (international bank account numbers) and neobanks. In societal terms, the analysis links financial corruption to macro-level harms – reduced growth, weakened public trust and the reinforcement of underground governance by criminal networks – while emphasising that effective countermeasures will require closing regulatory and data gaps, improving cross-border cooperation and targeting the enabling ecosystems that reduce criminals' transaction costs and shield illicit flows from scrutiny.

The author of Article 20 is Ioannis Vlassis and he analyses why police forces and prosecution services across the six countries of the Western Balkans ([2]) continue to struggle with integrity and operational independence despite extensive EU-aligned reforms, using a comparative research design (2023–2024) that triangulates legal/institutional review, case studies and expert interviews. The core finding is that informal political leverage – exerted through

([2]) Albania, Bosnia and Herzegovina, Kosovo (*), Montenegro, North Macedonia and Serbia. (*) This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

appointments, disciplinary tools and opaque case allocation – interacts with organised crime influence to produce selective enforcement, downgraded or delayed sensitive investigations and persistently low public trust. The paper further shows how fragmented oversight architectures and weak coordination among internal control units, prosecutors, parliaments, ombuds bodies, civil society and international partners limit prevention and learning, while resource constraints, outdated digital infrastructure and uneven specialised skills (e.g. financial investigations, cyber-enabled evidence) reduce prosecutorial and investigative effectiveness. Illustrative cases (e.g. Albania's 2023 assault episode, North Macedonia's post-wiretapping accountability efforts, Montenegro's 2023 court-evidence 'tunnel and Serbia's Sky ECC leak case) are used to demonstrate the gap between formal compliance and practical resilience. Finally, the article treats gender imbalance as both an integrity risk and a performance issue – especially where merit-based progression is undermined – arguing that sustainable rule-of-law gains require enforceable safeguards against interference, stronger accountability mechanisms, professional capacity building and gender-sensitive leadership pathways rather than further purely technocratic legal reforms.

Article 21, authored by Alp Cenk Arslan, conceptualises high-risk cybercriminal networks as industrialised, transnational ecosystems whose resilience is reinforced by a variable 'state–cybercrime nexus' (state-operated, state-enabled, state-tolerated) and argues that this alignment increasingly sits within contemporary geopolitical security doctrines. Using qualitative comparative analysis and structured documentary coding, the study systematically contrasts the US National Cybersecurity Strategy (2023) and the EU cybersecurity strategy for the digital decade (2020) across three analytic nodes – operational disruption, regulatory resilience and diplomatic attribution – while drawing on illustrative cases linked to China, North Korea and Russia, to show how state protection, tolerance or direct tasking amplifies criminal capability. The comparative findings indicate a strategic divergence: the United States prioritises persistent engagement, cost imposition and infrastructure/finance takedowns ('defend forward'), whereas the EU emphasises harmonised governance, 'secure-by-design' obligations and cross-border preparedness to strengthen guardianship and reduce opportunity structures. In parallel, the article identifies enduring transatlantic 'grey zones' created by mismatched legal thresholds, evidentiary timelines and jurisdictional fragmentation that allow networks to reconstitute faster than institutions can coordinate attribution, seizures and prosecutions. The paper concludes by proposing an integrated response that couples advanced technologies (e.g. AI-enabled detection, readiness for quantum-era risks) with tighter public–private operational integration, interoperable legal frameworks and structured inter-agency partnerships – particularly to support EU law enforcement in evidence production, disruption coordination with the European Cybercrime Centre within Europol and sustained cross-border investigations.

The last article of this conference volume 1 is Article 22, written by Kreseda Smith, who demonstrates that contemporary agricultural victimisation in Britain is increasingly experienced as organised and persistent rather than incidental, with significant implications for farmers' well-being and sector stability. Drawing on survey data from 239 farmers affected by crime in the preceding year, the analysis shows that organised agricultural criminality functions as a salient stressor – closely associated with psychological distress indicators such as anxiety, insomnia, feelings of vulnerability, loss of confidence, suicidal thoughts and considerations of exiting farming – particularly among women, younger farmers and those exposed to repeat offences. A central empirical insight concerns the disjunction between farmers' strong perception that organised crime groups are intensifying their activities in rural areas and the widespread belief that policing bodies neither recognise agricultural crime as organised nor respond effectively to reported incidents, contributing to eroded trust and perceived abandonment. Extending beyond

individual mental health effects, the article situates these experiences within broader secondary and tertiary consequences, including weakened farm viability, social withdrawal, under-reporting and longer-term risks to rural resilience and food security. On this basis, it calls for a reframing of organised agricultural crime as both a policing and public health concern, supported by improved crime classification, rural-sensitive police training, closer collaboration with farming communities and expanded comparative research capable of informing internationally relevant prevention and enforcement responses.

We hope that this volume 1 issue will be actively used as a research, training and reference resource, contributing to greater conceptual clarity and operational understanding of the complex phenomena examined across its contributions. A second volume arising from this conference will be issued immediately after this one, with more reflections around the same discussed topic: high-risk criminal networks. By bringing together empirical research, comparative analysis and practice-oriented reflection, the volume is designed not only to advance scholarly debate but also to support those engaged in professional education, policy development and operational training. I reaffirm, as the Research and Knowledge Management Officer and also Editor-in-Chief of this bulletin, a strong commitment to research-led training and to fostering dialogue between academia and practice, particularly in areas where HRCNs challenge existing institutional responses. I am confident that the insights gathered in this issue will meaningfully support the work of researchers, trainers and practitioners alike, and will serve as a durable foundation for informed analysis, effective capacity-building and future collaborative inquiry ([3]).

([3]) Generative-AI-assisted content drafted/amended.

Part I
Academic research

Exploring the EU perspective on the organised nature of the trafficking in cultural goods

Patricia Faraldo Cabana

https://doi.org/10.3013/645j0d93

Abstract

In recent years, the characterisation of the trafficking of cultural property as a form of organised crime has gained prominence in EU policies on the protection of cultural heritage. This article analyses how the EU has conceptualised and operationalised this link in terms of describing the phenomenon and designing countermeasures. Through a content analysis, we evaluate this connection in EU policy documents published from 1993 to 2023 that include both 'organised crime' and 'trafficking of cultural property' or similar terms (n = 59). The analysis demonstrates conceptual deficits and a correspondingly weak foundation for EU policy, since misunderstandings relating to the organised nature of trafficking of cultural property and its overlaps with other forms of organised crime, particularly terrorist financing, may result in misguided policies with the potential to undermine law enforcement efforts. We also address the addition of persons trading or acting as intermediaries in the trade of cultural goods to the list of obliged entities and persons in the anti-money-laundering (AML) framework, because it opens new opportunities to disrupt the illicit financial flow in the art market. This paper is one of the results of the EU project on research, intelligence and technology for heritage and market security.

Keywords: organised crime, cultural property crime, terrorist financing, EU crime control policy, money laundering.

Introduction

Since the 2000s, supranational bodies, policymakers, law enforcement actors and advocacy groups have highlighted the organised nature of the illicit trafficking of cultural goods (TCG) (UNESCO, 2018; Chechi, 2019; Blake, 2020; Interpol, 2021, 2022; Clooney Foundation for Justice, 2022). This perspective gained prominence in the early to mid 2010s, coinciding with heightened global awareness of the nexus between TCG and the financing of terrorist

activities in conflict zones across the Middle East (FATF, 2015, 2016; Jones, 2018). The alleged link between terrorist financing, money laundering, sanctions evasion and tax fraud has served to reinforce the characterisation of TCG as a form of organised serious crime (Ulph, 2011; Van Duyne et al., 2015; Yates, 2016; Mackenzie, 2020; US Senate, 2020; Baranello, 2021; Yates and Mackenzie, 2021).

The EU has wholly embraced this perspective on the organised nature of cultural property crime. The current EU action plan against trafficking in cultural goods was purportedly adopted as part of the EU strategy on organised crime (European Commission, 2022, p. 1), with TCG being regarded as one of the EU's primary priorities in this endeavour. Notwithstanding this association, some voices caution that there is no inherent relationship between organised crime and TCG (Howard et al., 2016; Brodie et al., 2019), and that an exclusive focus on the organised crime aspect of TCG may result in the formulation of a misguided legislation that fails to acknowledge the diversity of trafficking scenarios (Balcells, 2016), which in turn obscures the complexities of a market that is neither entirely licit nor illicit (a 'grey' market, see Mackenzie and Yates, 2017; Oosterman et al., 2021). A significant number of scholars have also expressed concern regarding the securitisation of the protection of cultural heritage, with worrying implications for efforts to combat TCG (Foradori et al., 2018; Puskás, 2019; Russo and Giusti, 2019; Lostal, 2020). Furthermore, the potential links to other forms of trafficking, corruption, money laundering, terrorism and terrorist financing remain understudied or highly contested (Eber et al., 2022).

The aims of this paper are twofold: (i) to pinpoint the origin and development of the association of TCG with organised crime; and (ii) to assess whether EU policymakers have identified the intersections between organised crime and cultural property crime with sufficient rigour to facilitate a common understanding of the issue and to inform the development of effective measures to enhance European policy on the protection of cultural heritage. To answer these questions, the paper proceeds as follows. The next section presents the research design. The third section shows the results of the content analysis. The fourth section discusses these findings. The fifth and final section offers concluding remarks.

Methodology

The present study surveys EU policy documents published since the foundation of the EU in 1993 through to 2023. The following types of documents and sources were considered: treaties, directives, decisions, framework decisions, regulations, formal policy statements (such as communications and conclusions), reports and reviews of the European Parliament, the Council, the European Commission, the European Public Prosecutor's Office (EPPO), the European Border and Coast Guard Agency (Frontex), the European Union Agency for Criminal Justice Cooperation (Eurojust) and the European Union Agency for Law Enforcement Cooperation (Europol). The policy documents of the seven EU bodies provide a complementary perspective on the substantive issues under consideration.

To identify relevant documents, we conducted searches using EUR-Lex ([4]) and the bodies' websites. We used a range of combinations of terms relating to organised crime: 'transnational organised crime', 'organised and serious international crime', 'serious organised crime', 'serious organised cross-border crime', 'serious international organised crime', 'serious forms of organised crime', 'serious and organised crime', 'serious crime activities' and 'organised property crime'. In the found documents (n = 238), we conducted a search for references to the following terms:

([4]) https://eur-lex.europa.eu/homepage.html?locale=en.

'cultural property crime', 'trafficking' of or 'illicit trade' in 'cultural goods', 'cultural property', 'cultural heritage', 'works of art', 'antiques' or 'antiquities' and 'heritage crime'. These terms were found in 58 documents. We then conducted a qualitative content analysis of the documents, exploring linkages to archetypical forms of organised crime, such as conspiracy and participation in an organised criminal group, terrorism, terrorist financing, corruption, smuggling, tax offences, sanctions evasion, money laundering, forgery and fraud. Our purpose was to study how the EU bodies define the nature of TCG and its relationship to other forms of organised crime, exploring the growing identification of the former as a particularly hideous form of serious organised transnational crime, to calibrate whether the foundations of EU policy regarding TCG are solid.

Results

Table 1.1 presents a list of the offences most frequently referenced in EU policy documents as crimes relating to TCG. Terrorist financing is the most frequently mentioned offence, appearing in 18 documents, closely followed by money laundering, in 13. The umbrella category of organised crime ranks third. Terrorism occupies the fourth position. The blocks of crimes ranking fifth to ninth largely cover offences typically considered as forms of organised crime. As we will see in the next sections, there is no adoption of specific measures regarding most of these nexuses, except for the anti-money-laundering (AML) framework, which is explicitly directed against terrorist financing.

Table 1.1. Top categories of crime most frequently referenced as crimes relating to the TCG in EU policy documents mentioning organised or serious crimes

Rank	Crime	No of documents
1	Terrorist financing	18
2	Money laundering	13
3	Organised crime	10
4	Terrorism	6
5	Other forms of illicit trafficking (drugs, persons, arms, oil, cigarettes, wildlife, counterfeit goods)	5 5
6	Corruption	4
7	Extortion Fraud Sanctions evasion	3 3 3
8	Financing of criminal organisations Forgery Tax evasion	2 2 2
9	Racketeering War crimes	1 1

The 'career' of TCG as a serious organised transnational crime in EU policy began in the 1990s, in the area devoted to police and judicial cooperation. The term 'illicit trafficking in cultural goods' was first used in an EU policy document in 1995 to describe a 'serious form of international crime'. The annex to the Europol Convention (Council

of the European Union, 1995) provided a list of 18 'serious forms of international crime which Europol could deal with in addition to those already provided for in Article 2(2)'. One of them was the 'illicit trafficking in cultural goods, including antiquities and works of art'. In the following years, the EU legal framework regarding police and judicial cooperation in criminal matters consistently referred to the illicit TCG and related offences (participation in a criminal organisation, corruption, money laundering, other illicit forms of trafficking) in all lists regarding the adoption of special procedures to facilitate police and judicial cooperation in criminal matters ([5]), including the creation of special agencies, such as Eurojust ([6]), explicitly addressing TCG as a form of organised crime.

Despite the relevance of the fight against organised crime during this period, the majority of EU policy documents outlining the EU strategy against organised crime made only perfunctory references to TCG or none at all, while references to overlaps between TCG and other forms of serious organised cross-border crime were totally absent (Council of the European Union, 1998; European Council, 2000, 2010). This is also evidenced by the limited attention given by EPPO, Frontex, Eurojust and Europol in the reviewed documents ([7]). The '2005 EU Organised Crime Report – Public version' (Europol, 2005, p. 22) was the only document to recognise that the criminal interest in cultural property encompasses a wide range of illicit activities, including theft and receiving, illicit trafficking, forgery and fraud, extortion and money laundering. It also acknowledged the involvement of organised criminals in the trade to meet rising demand of cultural objects. This finding was not followed up further until the mid 2010s, when the link between organised crime and TCG became a hot topic due to the connections with terrorism and terrorist financing.

The European Parliament publicly expressed its concerns regarding the use of TCG to finance terrorist activities in 2015. The resolution on the destruction of cultural sites perpetrated by ISIS/Daesh (Islamic State in Iraq and the Levant) claimed that 'illicit trade in cultural goods is now the third most significant illegal trade after drugs and arms' (European Parliament, 2015). In the same year, the European Commission announced its intention to explore the necessity and potential advantages of supplementary measures against terrorist financing and money laundering, including those related to TCG, because the same vulnerabilities in financial systems that allow for anonymity and opacity in transactions that facilitate terrorist financing also exist in the art market (European Commission, 2015, p. 14). Other policy documents emphasised the importance of enhancing international police collaboration and collaboration with customs authorities to disrupt the sources of terrorist funding, including measures relating to the freezing of terrorist assets and the control of the illicit trade in cultural goods (Council of the European Union, 2015, p. 2; European Commission, 2016, p. 12; Council of the European Union, 2023, p. 7) and other types of goods,

([5]) See the joint action on making it a criminal offence to participate in a criminal organisation (Council of the European Union, 1998), along with the legal instruments on the European Arrest Warrant (Council of the European Union, 2002), the execution in the EU of orders freezing property or evidence (Council of the European Union, 2003), the mutual recognition of custodial sentences or measures involving deprivation of liberty (Council of the European Union, 2008a), probation decisions and alternative sanctions (Council of the European Union, 2008b), supervision measures (Council of the European Union, 2009b), the European Investigation Order in criminal matters (European Parliament and Council, 2014), the use of passenger name records (Parliament and Council, 2016), the mutual recognition of freezing and confiscation orders (Parliament and Council of the European Union, 2018b), the facilitation of cross-border hot pursuits and cross-border surveillance (Council of the European Union, 2022) and the European Production Orders and European Preservation Orders (European Parliament and Council of the European Union, 2023a).

([6]) Initially, the competence of Eurojust covered the types of crime and the offences in respect of which Europol is at all times competent to act, set out in Article 2(1) of the Europol Convention and the annex thereto. Once the Council decision establishing Europol entered into force (Council of the European Union, 2009a), the competence of Eurojust was set up in Article 4(1) of that decision and in the annex thereto. Both annexes mention trafficking in cultural property, antiquities and works of art.

([7]) The serious and organised crime threat assessment (SOCTA) methodology, which initiates the first full policy cycle on serious international and organised crime, merely mentions illicit TCG, without identifying any overlap with other forms of serious organised international crime (Council of the European Union, 2012). Something similar happens in Eurojust's reports, in which the new methodology applied to mobile organised group classification identifies illicit TCG as one of the core offences in the category 'organised property crime', without giving it any additional thought (Eurojust, 2014, p. 30). In fact, as recently as 2021, TCG only merits a short subsection in the chapter on organised property crime in Europol's SOCTA report (Europol, 2021, pp. 88–89). Frontex's general reports and risk analyses and EPPO's reports do not mention the topic.

such as firearms, oil, drugs and wildlife, along with the smuggling of migrants, cigarettes and counterfeit goods by organised crime networks (European Commission, 2016, pp. 12–13; European Parliament, 2016, p. 108; European Parliament and Council of the European Union, 2018a, Article 1). In 2017, the Directive on Combating Terrorism characterised illicit TCG, along with other forms of trafficking, racketeering and extortion, as 'lucrative ways for terrorist groups to obtain funding' (European Parliament and Council of the European Union, 2017, recital 13).

In response to these concerns, the AML legal framework began to address as obliged entities and persons those trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, and persons storing, trading or acting as intermediaries in the trade of works of art when this is carried out by free ports, in both cases only where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more (European Parliament and Council of the European Union, 2018a). Transactions relating to cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, were listed as potentially being at higher risk of money laundering.

Other responses to these concerns regarding the link between terrorist financing, money laundering and TCG were the regulation on the introduction and import of cultural goods (European Parliament and Council of the European Union, 2019) and the resolution on cross-border restitution claims of works of art and cultural goods looted in armed conflicts and wars (European Parliament, 2019). The latter introduced specific provisions requiring importers to exercise due diligence regarding the licit provenance of the cultural goods imported, encouraging compliance through the provision of penalties for infringements. As further steps to adopt, the European Commission (2020) suggested the improvement of the online and offline traceability of cultural goods in the internal market and the cooperation with third countries where cultural goods are looted, along with the provision of active support to law enforcement and academic communities. By then, EU bodies were convinced that TCG was 'one of the most lucrative criminal activities, a source of funding for terrorists as well as organised crime and it is on the rise' (European Commission, 2020, p. 19). They stressed the fact that the illegal excavation, looting and trafficking of cultural property are not only linked to serious security threats, as they provide means for financing organised criminal and terrorist activities, but also instrumental in money laundering (Council of the European Union, 2020, 2023; European Commission, 2021). Explicitly, the Council of the European Union (2021, p. 10) set as one of the priorities on organised property crime the disruption of criminal networks involved in the illegal trade in cultural goods, with a special focus on those that are highly mobile and operating across the EU.

The EU action plan against trafficking in cultural goods (European Commission, 2022) is the first policy document to encompass a description of additional cultural property crimes beyond trafficking, including theft, robbery, looting and forgery. The scope of the action plan also includes other related crimes, such as fraud, disposal of stolen goods, smuggling, corruption, money laundering, sanctions evasion, tax evasion and terrorist financing. The action plan identifies the detection of illicit financial flows as a critical element in the fight against TCG. It acknowledges the need to pay particular attention to the prevalence of money laundering and terrorism financing with legally acquired cultural goods, identifying the business culture in the art market as the main facilitating factor of cultural property crime and one of the most probable explanations of its relative impunity.

Subsequent EU policy documents concentrate on the overlap between TCG and specific criminal activities, such as money laundering (Council of the European Union, 2023) and corruption (European Commission, 2023; European

Parliament and Council of the European Union, 2023b). Corruption is regarded as a crucial instrument for organised crime, as it enables a multitude of illicit operations, including TCG. However, no concrete action is taken to address this connection.

In sum, EU policy documents on TCG and organised crime demonstrate a distinct progression. Earlier documents lack any mention of this link, whereas more recent ones acknowledge that organised crime satisfies a demand for goods and services, including antiquities and works of art, but rarely incorporate specific measures to address it (but see Council of the European Union, 2023, with up to 36 recommended actions). Throughout the whole period, reports and reviews from EPPO, Frontex, Eurojust and Europol did not allude to the topic. A remarkable exception is the relationship between TCG and terrorist financing and money laundering.

Discussion

EU policy documents acknowledge that organised crime groups are involved in various forms of cultural property crime: 'theft and receiving, illicit trafficking, forgery and fraud, extortion, money laundering' (Europol, 2005, p. 22). This view has been repeatedly confirmed in case-law and police operations. However, the extent and nature of this involvement have not been fully investigated, apart from looting, damage and destruction in conflict zones. The literature consistently emphasises the disorganised nature of the illicit market in cultural goods, dominated by small groups and actors that are 'local at all points' (Hobbs, 1998, p. 419). This implies that the organisation of cultural property crime entails ever-mutating interlocking networks of mainly locally based criminality (Campbell, 2013; Brodie and Yates, 2019). Most existing networks are relatively small, opportunistic and highly decentralised, comprising members who are not necessarily full-time criminals (Nistri, 2009; Sargent et al., 2020). These findings are at odds with the stance taken by EU bodies, which consistently characterise cultural property crime as a serious organised cross-border crime.

Since 2017, there has been a notable focus on the areas of overlap between terrorism, illicit excavation and removal, illegal importation and exportation, acquisition, destruction and damage of cultural property in the context of armed conflicts. But the policy instruments that establish the connection appear to lack clarity regarding its extent and importance, sometimes acknowledging, quite cautiously, that illicit trade in pillaged cultural goods may serve as a source of terrorist financing and money laundering activities (European Parliament and Council of the European Union, 2019, recital 11 and p. 126), on other occasions affirming that terrorist groups are generating income from the illicit trafficking of cultural property (Council of the European Union, 2020, p. 8), to the point that it has 'become one of the most lucrative criminal activities' for terrorists and organised crime (European Commission, 2020, p. 19). These contradictory appreciations – it may be a source of funding, it is a source of funding, it is the most lucrative source of funding – touch on another contentious issue, namely the lack of evidence to support any of these claims. The documents in question did not delve further in their exploration, uncritically repeating unsubstantiated facts – or 'factoids' (Yates and Brodie, 2023). The assertion that the illicit trade in cultural property fuels terrorist activities is not based on research by any academic or professional expert, nor is it drawn from crime statistics or any relevant organisation within or outside the EU conducting field research. As a result, it has not been verified. It has been in place since the 2010s, supporting a narrative that equates terrorism with stricter measures against 'serious organised international' activities. In the absence of reliable evidence, the reception of this narrative by EU policymakers can only be considered as problematic (Sargent et al., 2019). It calls into question the foundation of EU policy on the illicit trade in art and antiquities on empirical evidence. Furthermore, the alignment of the fight against TCG with

the existing, ideologically charged narrative regarding the 'war on terror' comes at the cost of the former taking a back seat in that war (Puskás, 2019; Rosén, 2023).

However, there are some positive outcomes. The focus on terrorism has enabled archaeologists and art historians to gain political support for their efforts to combat the international trafficking of looted objects. It has helped to place the protection of cultural heritage on political agendas. It has also increased public awareness of the cultural, historical and economic value of cultural heritage and the urgent need to reduce the illicit activities threatening it. And, more importantly, it has paved the way for the inclusion of the art market in the AML framework.

Approaching cultural property crime from the AML framework aligns with a significant body of specialised literature, which posits that TCG should be examined not only or not principally as a form of organised crime, but as a white-collar crime. This perspective views cultural property crime as an unlawful form of entrepreneurship, governed by profit goals and business rationales, vocabularies and rules that normalise illicit behaviour while minimising the harmful consequences (Balcells, 2014; Mackenzie, 2019; Oosterman et al., 2021). It could be argued that TCG is not *per se* a white-collar crime, but it typically ends up as such at the final stage. In any case, precisely this final phase has been identified by the EU as a priority area for intervention, given the similarities between the art market and the financial sector. Imposing due diligence obligations and preventive regulatory requirements on market professionals, creating an effective supervisory framework and improving traceability and reliable information on the object's origin and history mark a significant turning point in the pursuit of robust protection for cultural heritage.

Conclusion

The growing interest of EU policymakers in TCG, evident since the mid 2010s, is closely linked to the fight against terrorism and terrorist financing. This development has undoubtedly provided a new impetus for combating the illicit trade and exploring the intersections with other organised crime typologies, particularly money laundering and corruption. It has increased public awareness of the true extent and impact of TCG activities, including among art market participants and law enforcement agencies that may not be fully aware of the harm this crime can cause (Brodie et al., 2019). Yet, the topic is becoming increasingly securitised. The fight against these crimes has increasingly become a matter of global governance, attracting the attention not only of the EU but also of other international organisations with a political and military alliance and collective defence mandate, such as NATO (Rosén, 2023). This approach places the protection of cultural property in a secondary position to the objective of preventing and combating terrorism. It fails to provide a robust foundation for policy discussions and demonstrates a significant shortcoming in the understanding of the illicit market among EU policymakers. It does, however, contribute to the identification of key areas for improvement, namely the need to control the art market and reduce its vulnerabilities. This seems a promising strategy. By imposing obligations on key players, the EU can foster a legal environment that facilitates the sharing of information among relevant parties, thereby enhancing our ability to combat the TCG. One could say that the existing AML framework presents several significant challenges regarding the obligations imposed on those engaged in the art and antiquities trade, including the scope of these obligations and the likelihood of their effective enforcement. However, given the lack of interest from art dealers and auction houses in implementing self-regulatory measures, the optimal course of action for the EU is to induce behavioural change and create an environment more conducive to the public interest in protecting cultural heritage (Baranello, 2021). In this line, the Council of the European Union (2023) encourages Member States to identify, assess and understand the risks of

TCG in the context of money laundering and terrorism financing as part of their risk assessment under the AML legislation and to adopt adequate measures to mitigate these risks, along with raising awareness and issuing guidance to the private sector on how best to comply with their obligations to prevent money laundering and terrorism financing in cooperation with the competent authorities.

References

Balcells, M. (2014), 'Art crime as white-collar crime', in: Kila, J. D. and Balcells, M. (eds), *Cultural Property Crime – An overview and analysis of contemporary perspectives and trends*, Brill, Leiden, pp. 96–110.

Balcells, M. (2016), 'Go research an art thief: The importance of empirical research on the art theft', in: Tompkins, A. (ed.), *Art Crime and Its Prevention*, Lund Humphries, London, pp. 31–44.

Baranello, A. M. (2021), 'Money laundering and the art market: Closing the regulatory gap', *Seton Hall Legislative Journal*, Vol. 45, No 3, pp. 695–737, https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1195andcontext=shlj.

Blake, J. (2020), 'Trafficking in cultural property: Where cultural heritage law and the international fight against transnational organized crime coincide', in Carstens, A. M. and Varner, E. (eds), *Intersections in International Cultural Heritage Law*, Oxford University Press, Oxford, pp. 157–180.

Brodie, N., Yates, D., Slot, B., Batura, O., van Wanrooij, N., et al. (2019), *Illicit Trade in Cultural Goods in Europe: Characteristics, criminal justice responses and an analysis of the applicability of technologies in the combat against the trade*, European Commission: Directorate-General for Education, Youth, Sport and Culture, ECORYS and Trafficking Culture, Brussels, https://data.europa.eu/doi/10.2766/183649.

Campbell, P. B. (2013), 'The illicit antiquities trade as a transnational criminal network: Characterizing and anticipating trafficking of cultural heritage', *International Journal of Cultural Property*, Vol. 20, No 2, pp. 113–153, https://www.cambridge.org/core/journals/international-journal-of-cultural-property/article/abs/illicit-antiquities-trade-as-a-transnational-criminal-network-characterizing-and-anticipating-trafficking-of-cultural-heritage/47EFDD1CF26E676A77BFD5D89A493DB7.

Chechi, A. (2019), *Fighting and Preventing Offences Relating to Cultural Property: Existing rules and proposals for functioning regulatory systems*, Council of Europe, https://rm.coe.int/fighting-and-preventing-offences-relating-to-cultural-property-existin/1680980d4ecultural-property-existin/1680980d4e.

Clooney Foundation for Justice (2022), *Conflict Antiquities – The docket: The need for prosecuting participants in the illegal antiquities trade for complicity in international crimes*, https://cfj.org/report/the-need-for-prosecuting-participants-in-the-illegal-antiquities-trade/need-for-prosecuting-participants-in-the-illegal-antiquities-trade/.

European Commission (2015), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European agenda on security, COM(2015) 0185 final of 28 April 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0185.

European Commission (2016), Communication from the Commission to the European Parliament and the Council on an action plan for strengthening the fight against terrorist financing, COM(2016) 50 final of 2 February 2016, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52016DC0050.

European Commission (2017), Communication from the Commission to the European Parliament, the European Council and the Council – Ninth progress report towards an effective and genuine security union, COM(2017) 407 final of 26 July 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017DC0407.

European Commission (2020), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU security union strategy, COM(2020) 605 final of 24 July 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0605.

European Commission (2021), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU strategy to tackle organised crime 2021–2025, COM(2021) 170 final of 14 April 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0170.

European Commission (2022), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU action plan against trafficking in cultural goods, COM(2022) 800 final of 13 December 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022DC0800.

European Commission (2023), Joint communication to the European Parliament, the Council and the European Economic and Social Committee on the fight against corruption, JOIN(2023) 12 final of 3 May 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023JC0012.

Council of the European Union (1995), Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention) (OJ C 316, 27.11.1995, p. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_1995_316_R_0001_01).

Council of the European Union (1997), Action plan to combat organized crime, OJ C 251, 15.8.1997, pp. 1–18, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:51997XG0815.

Council of the European Union (1998), Joint action of 21 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union, OJ L 351, 29.12.1998, pp. 1-3.

European Council (2000), The prevention and control of organised crime: a European Union strategy for the beginning of the new millennium, (OJ C 124, 3.5.2000, pp. 1–33, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000F0503).

Council of the European Union (2002), Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1, ELI: http://data.europa.eu/eli/dec_framw/2002/584/oj).

Council of the European Union (2003), Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196, 2.8.2003, p. 45, ELI: http://data.europa.eu/eli/dec_framw/2003/577/oj).

Council of the European Union (2008a), Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union (OJ L 327, 5.12.2008, p. 27, ELI: http://data.europa.eu/eli/dec_framw/2008/909/oj).

Council of the European Union (2008b), Council Framework Decision 2008/947/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions (OJ L 337, 16.12.2008, p. 102, ELI: http://data.europa.eu/eli/dec_framw/2008/947/oj).

Council of the European Union (2009a), Council Decision of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37, ELI: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009D0371).

Council of the European Union (2009b), Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention (OJ L 294, 11.11.2009, p. 20, ELI: http://data.europa.eu/eli/dec_framw/2009/829/oj).

European Council (2010), The Stockholm programme – An open and secure Europe serving and protecting citizens (OJ C 115, 4.5.2010, p. 1, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF).

Council of the European Union (2012), Serious and organised crime threat assessment (SOCTA) – Methodology, 12159/12, 4 July 2012, https://data.consilium.europa.eu/doc/document/ST-12159-2012-INIT/en/pdf.

Council of the European Union (2015), 'Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism', Council of the European Union and the European Council website, 20 November 2015, https://www.consilium.europa.eu/en/press/press-releases/2015/11/20/jha-conclusions-counter-terrorism/releases/2015/11/20/jha-conclusions-counter-terrorism/.

Council of the European Union (2020), Council conclusions on EU external action on preventing and countering terrorism and violent extremism, 8868/20, 16 June 2020, https://data.consilium.europa.eu/doc/document/ST-8868-2020-INIT/en/pdf.

Council (2021), Council conclusions setting the EU's priorities for the fight against serious and organised crime for EMPACT 2022–2025, 8665/21, 12 May 2021, https://data.consilium.europa.eu/doc/document/ST-8665-2021-INIT/en/pdf2021-INIT/en/pdf.

Council of the European Union (2022), Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation (OJ L 158, 13.6.2022, p. 53, ELI: http://data.europa.eu/eli/reco/2022/915/oj).

Council of the European Union (2023), Council conclusions on the fight against trafficking in cultural goods, 10249/23, 8 June 2023, https://data.consilium.europa.eu/doc/document/ST-10249-2023-INIT/en/pdf.

Eber, A., Leggett, T. and Yee, S. (2022), False Trades: Uncovering the scale and scope of trafficking in cultural property – Knowledge gaps and future directions for research United Nations Office on Drugs and Crime, https://www.unodc.org/documents/data-and-analysis/briefs/Trafficking_in_cultural_properties_brief.pdf.

Eurojust (2014), Eurojust *Annual Report 2013*, The Hague, https://www.eurojust.europa.eu/publication/eurojust-annual-report-2013.

Europol (2005), *2005 EU Organised Crime Report*, The Hague, https://www.europol.europa.eu/cms/sites/default/files/documents/eu-organisedcrimereport2005.pdf.

Europol (2021), *European Union Serious and Organised Crime Threat Assessment – A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime,* Publications Office of the European Union, Luxembourg, https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf.

FATF (Financial Action Task Force) (2015), Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL) Paris, https://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf.

FATF (2016), 'Consolidated FATF strategy on combatting terrorist financing', https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/FATF-Terrorist-Financing-Strategy.pdf.

Foradori, P., Giusti, S. and Lamonica, A. G. (2018), 'Reshaping cultural heritage protection policies at a time of securitisation: France, Italy, and the United Kingdom', *The International Spectator, Italian Journal of International Affairs*, Vol. 53, No 3, pp. 86–101, https://www.iai.it/sites/default/files/foradori-giusti-lamonica.pdf.

Hobbs, D. (1998), 'Going down to the glocal: The local context of organised crime', *The Howard Journal of Criminal Justice*, Vol. 37, No 4, pp. 407–422, https://onlinelibrary.wiley.com/doi/10.1111/1468-2311.00109.

Howard, R. D., Elliot, M. D. and Prohov, J. R. (2016), *IS and Cultural Genocide: Antiquities trafficking in the terrorist state*, Joint Special Operations University Press, Tampa, https://theantiquitiescoalition.org/wp-content/uploads/2017/01/IS-and-Cultural-Genocide-Antiquities-Trafficking-in-the-Terrorist-State.pdf.

Interpol (2021), 'Assessing Crimes Against Cultural Property 2020', https://www.interpol.int/content/download/16751/file/2020%20Assessing%20Crimes%20Against%20Cultural%20Property.pdf.

Interpol (2022), 'Assessing Crimes Against Cultural Property 2021', https://www.interpol.int/en/content/download/18513/file/Assessement%20Crime%20against%20cultural%20property%202021_Brochure-EN.pdf.

Jones, C. W. (2018), 'Understanding ISIS's destruction of antiquities as a rejection of nationalism', *Journal of Eastern Mediterranean Archaeology and Heritage Studies*, Vol. 6, Nos 1–2, pp. 31–58, https://muse.jhu.edu/pub/2/article/697782/pdf.

Lostal, M. (2020), 'Islamic State and the illicit traffic of cultural property', in: Jørgensen, N. H. B. (ed.), *The International Criminal Responsibility of War's Funders and Profiteers*, Cambridge University Press, Cambridge, pp. 122–147.

Mackenzie, S. (2019), 'White-collar crime, organised crime and the challenges of doing research on art crime', in: Hufnagel, S. and Chappell, D. (eds), *The Palgrave Handbook on Art Crime*, Palgrave, London, pp. 839–853.

Mackenzie, S. (2020), *Transnational Criminology: Trafficking and global criminal markets*, Bristol University Press, Bristol.

Mackenzie, S. and Yates, D. (2017), 'What is grey about the 'grey market' in antiquities?', in: Beckert, J. and Dewey, M. (eds), *The Architecture of Illegal Markets*, Oxford University Press, Oxford, pp. 70–86.

Nistri, G. (2009), 'The experience of the Italian Cultural Heritage Protection Unit', in: Manacorda, S. (ed.), *Organized Crime in Art and Antiquities*, International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme, pp. 95–108.

Oosterman, N., Mackenzie, S. and Yates, D. (2021), 'Regulating the Wild West: Symbolic Security bubbles and white collar crime in the art market ', *Journal of White Collar and Corporate Crime*, Vol. 3, No 1, pp. 7–15, https://www.researchgate.net/publication/353806258_Regulating_the_Wild_West_Symbolic_Security_Bubbles_and_White_Collar_Crime_in_the_Art_Market.

European Parliament (2015), European Parliament resolution of 30 April 2015 on the destruction of cultural sites perpetrated by ISIS/Da'esh (2015/2649 (RSP) (OJ C 346, 21.9.2016, p. 55, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2016_346_R_0010).

European Parliament (2016), European Parliament resolution of 25 October 2016 on the fight against corruption and follow-up of the CRIM resolution (2015/2110(INI)) (OJ C 215, 19.6.2018, p. 96, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2018_215_R_0020).

European Parliament (2019), European Parliament resolution of 17 January 2019 on cross-border restitution claims of works of art and cultural goods looted in armed conflicts and wars (2017/2023(INI)) (OJ C 411, 27.11.2020, p. 125, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2020_411_R_0017).

European Parliament and Council of the European Union (2014), Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p. 1, ELI: http://data.europa.eu/eli/dir/2014/41/oj).

European Parliament and Council of the European Union (2016), Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4.5.2016, p. 132, ELI: http://data.europa.eu/eli/dir/2016/681/oj).

European Parliament and Council of the European Union (2017), Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6, ELI: http://data.europa.eu/eli/dir/2017/541/oj).

European Parliament and Council of the European Union (2018a), Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (OJ L 156, 19.6.2018, p. 43, ELI: http://data.europa.eu/eli/dir/2018/843/oj).

European Parliament and Council of the European Union (2018b), Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders (OJ L 303, 28.11.2018, p. 1, ELI: http://data.europa.eu/eli/reg/2018/1805/oj).

European Parliament and Council of the European Union (2019), Regulation (EU) 2019/880 of the European Parliament and of the Council of 17 April 2019 on the introduction and the import of cultural goods (OJ L 151, 7.6.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/880/oj).

European Parliament and Council of the European Union (2023a), Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

European Parliament and Council of the European Union (2023b), Proposal for a directive of the European Parliament and of the Council on combating corruption, replacing Council Framework Decision 2003/568/JHA and the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union and amending Directive (EU) 2017/1371 of the European Parliament and of the Council, COM(2023) 234 final of 3 May 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A234%3AFIN.

Puskás, A. (2019), 'The securitization of cultural heritage protection in international political discussion through the example of attacks of ISIL/Daesh', *Security and Future*, Vol. 3, No 3, pp. 96–100, https://stumejournals.com/journals/confsec/2019/3/97.

Rosén, F. (2023), *'NATO and cultural property – A hybrid threat perspective', Prism, Vol. 10, No 3, pp. 45–58,* https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_10-3/prism_10-3_44-58_Rosen.pdf?ver=nvFxlxvmN1A8o8nORMAz_g==58_Rosen.pdf?ver=nvFxlxvmN1A8o8nORMAz_g%3d%3d.

Russo, A. and Giusti, S. (2019), 'The securitisation of cultural heritage', *International Journal of Cultural Policy*, Vol. 25, No 7, pp. 843–857, https://www.tandfonline.com/doi/full/10.1080/10286632.2018.1518979#abstract.

Sargent, M., Marrone, J. V., Evans, A., Lilly, B., Nemeth, E. et al., (2020), *Tracking and disrupting the illicit antiquities trade with open-source data*, RAND Corporation, Santa Monica, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2706/RAND_RR2706.pdf.

Ulph, J. (2011), 'The impact of the criminal law and money laundering measures upon the illicit trade in art and antiquities', *Art Antiquity and Law*, Vol. 16, No 1, pp. 39–52, https://www.obs-traffic.museum/sites/default/files/ressources/files/Ulph_impact_criminal_law.pdf.

UNESCO (United Nations Educational, Scientific and Cultural Organization) (2018), *Fighting the Illicit Trafficking of Cultural Property: A toolkit for European judiciary and law enforcement*, Paris, https://unesdoc.unesco.org/ark:/48223/pf0000266098?posInSet=1andqueryId=69eeca8c-383e-4b4f-b795-0e3dad58dab50e3dad58dab5.

United States Senate: Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs (2020), *The Art Industry and U.S. Policies that Undermine Sanctions*, https://permanent.fdlp.gov/gpo142344/20200729PSIStaffReportTheArtIndustryandUSPoliciesthatUndermine Sanctions.pdf.

Van Duyne, P. C., Louwe, L. and Soudijn, M. (2014), 'Money, art, and laundering: Coming to grips with the risks', in: Kila, J. D. and Balcells, M. (eds), *Cultural Property Crime*, Brill, Leiden, pp. 79–95.

Yates, D. (2016), 'Museums, collectors, and value manipulation: Tax fraud through donation of antiquities', *Journal of Financial Crime*, Vol. 23, No 1, pp. 173–186, https://www.scirp.org/reference/referencespapers?referenceid=2705542.

Yates, D. and Brodie, N. (2023), 'The illicit trade in antiquities is not the world's third-largest illicit trade: A critical evaluation of a factoid', *Antiquity*, Vol. 97, No 394, pp. 991–1003, https://doi.org/10.15184/aqy.2023.90.

Yates, D. and Mackenzie, S. (2021), 'Crime, material and meaning in art world desirescapes', in: Oosterman, N. and Yates, D. (eds), *Crime and Art – Sociological and criminological perspectives of crimes in the art world*, Springer, Cham, pp. 119–134.

New psychoactive substances: The current EU landscape

Gabriela Boneva, Luke Bates, Babak Akhgar

https://doi.org/10.3013/5mqec306

Abstract

New psychoactive substances (NPS) pose a growing global public health threat and an ever-changing and complex challenge for law enforcement efforts. Due to their ambiguous legal status across Europe and beyond, they are designed to replace traditional controlled drugs while evading detection measures. Each year, hundreds of new substances are detected and monitored by the EU Early Warning System. Nevertheless, there remains a limited knowledge base available for NPS. The current understanding of the public health threats posed by NPS is limited, predominantly due to their continually changing chemical composition. Due to these chemical modifications, traditional detection methods are unlikely to detect NPS, further challenging their tracking and control by law enforcement agencies. In this paper, we review the available literature on the current criminological landscape for NPS, including their prevalence, detection-resistance concealment methods, criminal modus operandi, presence online and potential health impacts on society. This work is supplemented by data collected through consultations with subject-matter experts as part of a European project that attempts to combat the illicit drug trafficking chain. On this basis, we identify gaps related to the knowledge and capability needs of law enforcement agencies in relation to NPS and formulate recommendations for future work.

Keywords: new psychoactive substances (NPS), drugs, EU landscape, NPS prevalence, organised crime.

Introduction

New psychoactive substances (NPS) reported on global markets are on the rise. According to the United Nations Office on Drugs and Crime (UNODC) definition, NPS are 'substances of abuse, either in pure form or a preparation, that are not controlled by the 1961 Single Convention on Narcotic Drugs or the 1971 Convention on Psychotropic Substances, but which may pose a public health threat'. The market for NPS began to rapidly expand in 2008 (EMCDDA, 2022), and since then around 1 200 NPS have been identified on the global drug market by the end of

2023 (EMCDDA and Europol, 2024a). However, due to control disparities, the estimation of the NPS market volume and the efforts to tackle it are greatly challenged, posing a significant risk to public health and obstructing drug policy (UNODC, 2020; UNODC, n.d.).

The adaptable nature of NPS enables the individuals producing, trafficking, dealing and using them to avoid controls and evade legal restrictions. NPS producers exploit the adaptability of the substances, leading to the continuous emergence of NPS achieved through minor chemical structural modifications. This facilitates the evasion of regulatory controls and places NPS in a legal grey area, enabling their production and relatively risk-free transportation and dealing (Lin et al. 2023). Although the overall number of NPS appearing for the first time in Europe has decreased in recent years, a record of over 30 tonnes of NPS was seized in 2022, consisting of a relatively small number of large-quantity seizures. However, detection capabilities are not consistent across the continent, which leads to under-reporting. The NPS market in Europe is dynamic, with hundreds of substances being added and monitored annually by the EU Early Warning System (EWS). The variations in national drug controls allow criminals to exploit this caveat, leading to the re-emergence of certain NPS after extended periods of absence (EMCDDA and Europol, 2024b). The majority of NPS are sold online and are reportedly often distributed to end users via postal or courier services, making digitalisation a strong NPS facilitator and stressing the need for effective and efficient measures to monitor and control online sales. Although most of the NPS on the European market are shipped from China and India, there is also some synthetic cathinone production observed domestically, and recent reports suggest that synthetic cannabinoids could also be actively produced in Europe (EMCDDA and Europol, 2024a). Threats of increased European production of NPS arise due to the limited control over the majority of NPS precursors, escalating the public health threats (EMCDDA and Europol, 2024b). Criminals use legal loopholes to obtain the chemicals needed to produce NPS, as these chemicals often have legitimate uses, such as pharmaceutical or industrial applications, but are usually scheduled and subject to national or international controls. For example, Regulation (EC) No 273/2004 (European Parliament and Council of the European Union, 2004) sets out provisions on the licences, labels and customer declarations needed for the control and monitoring of scheduled substances, enabling the control of precursors' presence on the market for legitimate uses and the limitation of their illicit diversion. Alternatively, to avoid the use of scheduled chemicals, criminals may attempt to use non-scheduled chemicals to produce NPS and controlled drugs; however, this may also increase their risks of detection due to the greater amounts of waste generated (EMCDDA and Europol, 2024b).

There is generally a limited intelligence picture of NPS due to the lack of systematic global control. Nevertheless, this paper indicates the role of NPS in the wider drug trafficking chain using the latest available data, along with the challenges this poses for law enforcement. These findings are further supported by primary data from consultations with subject-matter experts.

Research methodology

In order to promote a more extensive understanding of the complex EU NPS landscape, this research embraces a twofold approach, consisting of an expansive desk-based literature review and detailed written expert consultations.

Stage 1: Literature review

The extensive desk-based research provides a comprehensive overview of the types of NPS observed on the European market, along with the current criminological landscape for NPS, including their prevalence, detection-

resistance concealment methods, presence online, risks and potential health impacts. A variety of sources were reviewed, including academic articles, reports and official web sources, as the literature review also informed the development of the data collection instrument used for the written expert consultations.

Stage 2: Expert consultations

Supplementary to the literature review, written consultations were conducted with subject-matter experts. The selected occupational groups of experts were European law enforcement agencies (LEAs) and postal services. Both groups are essential for the tackling of NPS trafficking, with postal services being central to the efficient monitoring and interception of NPS trafficked via mail – a modus operandi frequently reported in the literature relating to NPS.

First-hand data from LEAs and postal services was collected through a structured set of questions, aiming to enhance the understanding of European LEA practices, NPS prevalence, technological capabilities and overall challenges. The consultation questions, information sheets and consent forms were approved by Sheffield Hallam University's ethics committee (ER62292219) and disseminated to the LEAs and postal services partnering in the Horizon Europe project ARIEN, which aims to combat the illicit drug trafficking chain. The documentation was sent by email, and the respondents were asked to return the completed documents to the researchers in a similar manner. The completed consultations were pseudonymised upon collection and kept separately from participants' consent forms. A total of 11 participants from five countries – Albania, Kosovo, the Republic of Moldova, Slovenia and the United Kingdom – took part in the written expert consultations, with LEA representatives from all five countries and postal service representatives only from Slovenia. The data was analysed in NVivo.

Literature review

NPS groups and prevalence

The literature consistently showed that the global NPS landscape is diverse and dynamic, with around 1 200 unique NPS identified by 139 countries globally between 2008 and 2023, and the emergence of over 960 of them reported in Europe between 1997 and 2023 (EMCDDA and Europol, 2024a). NPS affect countries and regions in different ways, leading to countries facing differing challenges when addressing an NPS issue and increasing the complexity of tackling NPS at the global and regional levels. The vastly unknown health impacts of NPS further increase the public threats they pose. Generally, the psychological and physiological effects of NPS can be sorted into stimulant-type (e.g. traditional cocaine, amphetamine and ecstasy), sedative-hypnotic-type (e.g. benzodiazepines), dissociative-type (e.g. ketamine) and hallucinogenic-type (e.g. LSD (lysergic acid diethylamide)) (EMCDDA, 2022). The biggest group of NPS reported for the first time on the global UNODC Early Warning Advisory (EWA) in 2023 were synthetic opioids (36 %), followed by stimulants (24 %) and synthetic cannabinoids (24 %), hallucinogens (12 %), and new benzodiazepines (4 %) (UNODC, 2024). Over 26 000 seizures of NPS were reported in 2022 in the EU, which amounted to more than 30 tonnes. Cathinones accounted for the greatest number of seizures (36.6 %), followed by cannabinoids (17.7 %), miscellaneous NPS (16.8 %), arylcyclohecylamines (14.9 %), phenethylamines (5 %), benzodiazepines (2.8 %), opioids (2.8 %), arylalkylamines (1.6 %), and tryptamines, piperidines and pyrrolidines, piperazine derivatives, and aminoindanes (each reported in less than 1 % of the seizures) (EMCDDA and Europol, 2024a). Below, some of these NPS groups are described in detail, based on the available data and on the potential level of risk they pose to the public.

Benzodiazepines are an important group of medicines first introduced in the 1950s that produce sedation and promote sleep, and are the most widely prescribed medicine group globally. However, they can cause rapid tolerance and dependence, potentially resulting in life-threatening withdrawal symptoms; thus, their prescription is subject to very strict restrictions. The combination of benzodiazepines with alcohol, opioids or other psychoactive substances increases the risks of fatal and non-fatal poisonings. The demand for benzodiazepines is strong and motivates criminals to divert legitimate medicines from the pharmaceutical market to the illicit one, sell unlicensed products or produce falsified benzodiazepines. The illicit pharmaceutical market has been found to contain both legitimate benzodiazepines and new benzodiazepines. The most frequently observed new benzodiazepines on the drug market are diazepam ('street Valium') and alprazolam ('fake Xanax'). New benzodiazepines are also sold as separate substances promoted to enhance the effects of other drugs, and for self-medication. Most of the new benzodiazepines are imported from China as powders, which are then made into tablets in Europe, allowing them to mimic the legitimate medicines; however, new benzodiazepines are reportedly also concealed and smuggled into prisons by infusing them into paper and clothing (EMCDDA and Europol, 2024a). Reports to the EU EWS for 2022 show that over 750 seizures of new benzodiazepines were conducted in the EU, accounting for around 3 % of all NPS seizures for that year. In terms of benzodiazepines, the European market in 2022 was dominated by etizolam (42.5 % of the total quantity seized) and flualprazolam (8.9 % of the total quantity seized), which were seized in powder, liquid and tablet forms, predominantly in northern Europe (EMCDDA and Europol, 2024a). Although the quantity of seized etizolam in 2022 was consistent with that seized in 2020, the quantity of seized flualprazolam decreased by more than half in the same period (21 % for 2020 (EMCDDA, 2022)), indicating that distributors and producers are shifting towards other new benzodiazepines (e.g. flubromazolam, clonazolam and bromazolam) to avoid the international controls on etizolam and flualprazolam implemented in late 2020 (EMCDDA and Europol, 2024a). New benzodiazepines can often be more potent than legitimate benzodiazepines, posing threats to public health (EMCDDA, 2022).

New opioids account for only a fraction of all NPS reported and seized in Europe, but are the most prominent NPS group (36 %) in terms of new substances that emerged and were reported to UNODC's EWA in 2023 (UNODC, 2024). Furthermore, they are of particular concern to public health due to their lethally high potency, leading to a high risk of life-threatening overdose due to respiratory depression (EMCDDA and Europol, 2024a). The majority of reported NPS opioids are fentanyl derivatives – specifically carfentanil (EMCDDA, 2020; EMCDDA and Europol, 2024a). Fentanyl and fentanyl analogues are highly potent substances, as the 'parent' substance – fentanyl – is between 50 and 100 times stronger than morphine. For instance, acetylfentanyl is approximately 15 times stronger than morphine, and carfentanil is approximately 10 000 times stronger than morphine. There is no known dose of carfentanil and other fentanyl analogues that is not lethal to humans. Criminals exploit the potency of fentanyl and fentanyl analogues by replacing a significant portion of their heroin with smaller amounts of the potent fentanyl analogues mixed with bulking agents, leading to uneven blends with high fentanyl concentrations and increasing the risks of fatal overdoses (National Crime Agency, 2019). New opioids are mostly sold as powders, but can also be found as tablets, capsules and liquids. The majority of the new opioids available in Europe originate from China, predominantly nitazene opioids, with Russia being the main source for carfentanil and India for tramadol. European sites linked to new opioids are rarely reported, and are mainly concerned with the mixing and packaging of the imported material. The first discovery of a potential European site where the production of new opioids – more specifically, fentanyl – took place was made in 2023 in Latvia, where 2 kg of fentanyl and various precursors and chemicals for its production were seized (EMCDDA and Europol, 2024a). New opioids are the fourth-largest NPS group monitored by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), now the European Union Drugs Agency (EUDA). Almost 750 seizures of new opioids were reported to the EU EWS in 2022, accounting for 3 % of the total

number of NPS seizures that year. Meanwhile, carfentanil has remained active, accounting for 40 % of the total new opioid seizures for 2022 and 49 % of the seized new opioids, with the majority of seizures reported in the Baltic region. The lethally high potency of new opioids and their exploitation by criminals pose a particular public health threat (EMCDDA and Europol, 2024a).

Synthetic cathinones are closely related to the phenethylamine family, which includes amphetamine and methamphetamine. Cathinone, the principal active ingredient found in the leaves of khat plants, is considered to be the prototype from which a range of synthetic cathinones have been developed. They act as central nervous system stimulants that mediate the activity of dopamine, norepinephrine and serotonin, mimicking the effects of cocaine, ecstasy, amphetamine and methamphetamine (UNODC, n.d.). By 2019, the majority of the synthetic cathinones seized at the EU's external borders originated in China; however, reports evidence that there has been a sharp rise in synthetic cathinones originating in India and targeted at European markets in recent years. Almost 70 illicit laboratories producing synthetic cathinones have been dismantled in Europe since 2013, with most of the sites being in Poland (77 %), the Netherlands (17 %), Spain, France and Slovakia (2 % each), with most of them producing 4-MMC and 4-CMC (EMCDDA and Europol, 2024a). Cathinone is structurally related to amphetamine, ephedrone to methamphetamine, and methylone to MDMA (3,4-methylenedioxymethamphetamine). The only cathinone derivatives under international drug control are amfepramone and pyrovalerone (UN 1971 Schedule IV), and methcathinone (UN 1971 Schedule I). Synthetic cathinones are often found in products sold as 'research chemicals', 'plant food', 'bath salts' or 'glass cleaner', usually in powder or tablet form. Mephedrone and methylone are typically sold as white or brown powders or as pills, often marketed as 'ecstasy'. Mephedrone is classified as Class B in the United Kingdom, is controlled at the national level in 12 EU Member States and is subject to control measures in Member States under a Council Decision adopted in 2010 (EUDA, n.d.a). Sometimes, the derivatives can be injected, although they are most often ingested or snorted. Almost 10 000 seizures of synthetic cathinones were reported for 2022, with only 78 seizures of three cathinones (3-CMC, 3-MMC and alpha-PHiP) accounting for 84 % of the total quantity of synthetic cathinones seized, which accounted for 73 % of the total quantity of NPS seized for that year (EMCDDA and Europol, 2024a). Currently, the short- and long-term effects and health risks of synthetic cathinones are largely unknown, with only a few reports on their toxicity to date and the majority of current knowledge derived from consumer reports and clinical observations. The most common observed symptoms include mild agitation and psychosis, as some of the adverse effects occur at the cardiac, psychiatric and neurological levels (EMCDDA and Europol, 2024a).

Since the introduction of national controls on mephedrone, **synthetic aminoindanes** have increased in popularity (Pinterova et al., 2017). Back in the 1970s, aminoindanes were reported to have bronchodilating and analgesic properties. Recent research evidences their potent effects on serotonin uptake and release, leading to effects similar to those of MDMA, and their trading as NPS. No aminoindanes are currently under international control. The 2-aminoindane is an amphetamine analogue, and its chemical structure can be modified to produce other substances, such as 5-IAI (5-Iodo-2-aminoindane) and MDAI (5,6-methylenedioxy-2-aminoindane). These three analogues are reported to be the most common NPS in the aminoindanes group. Aminoindanes are commonly found in powder and crystal form and are mainly ingested, but can sometimes be snorted (UNODC, 2013).

'Herbal highs' are not a recent market phenomenon and refer to the use of plant mixtures with minimal psychoactive effects. However, the composition of these herbal mixtures has changed substantially since the mid 2000s with the

introduction of **synthetic cannabinoids**. Since then, the number of new synthetic cannabinoids has greatly expanded, especially in recent years, although this expansion somewhat halted in 2023 for reasons that are still not entirely clear (EMCDDA and Europol, 2024a). The synthetic analogue of the principal psychoactive substance found in the cannabis plant – THC (tetrahydrocannabinol) – was first synthesised in 1988 under the name HU-210 and reportedly has at least 100 times more strength than THC. Due to the great similarities between the chemical structures of HU-210 and THC, the synthetic cannabinoid is categorised as a 'classical cannabinoid' and is accessible in the US market, while 'non-classical' synthetic cannabinoids have been reported by multiple countries globally. A variety of other synthetic cannabinoids that are structurally dissimilar to THC have emerged on global markets – JWH-018 consistently being the best-known, with potencies at least three times stronger than THC. THC and cannabis are controlled under several international drug control treaties; however, none of the synthetic cannabinoids are under international control, with only some countries controlling some of them at the national level. Synthetic cannabinoids usually act similar to THC and are available mostly in powder or tablet form, which is usually smoked, but can sometimes be ingested. Another consumption method is spraying liquid synthetic cannabinoids onto herbal materials or tobacco and smoking them (EMCDDA and Europol, 2024a). Most of the synthetic cannabinoids are imported as bulk powders from China, as their processing takes place in Europe. Up until 2023, reports of synthetic cannabinoid facilities in Europe were only concerned with the processing and packaging of the bulk powder; however, two sites, one in Spain and one in Greece, were identified in 2023, where evidence of synthetic cannabinoid synthesis was found, increasing the threats linked to synthetic cannabinoids for Europe even further (EMCDDA and Europol, 2024a). Synthetic cannabinoids are the largest NPS group, accounting for 25 % of all NPS in Europe, with over 4 500 seizures reported to the EU EWS in 2022 (EMCDDA and Europol, 2024a). Currently, there is limited data on the toxicity levels of synthetic cannabinoids and on their effects on the human body. Synthetic cannabinoids often contain several chemicals in different concentrations – a trait typical for NPS – thus challenging the differentiation of the effects of the various constituents. Synthetic cannabinoids have also reportedly been used to adulterate low-THC cannabis, following reports of unusual effects after consumption, which is a phenomenon observed in at least 11 Member States in 2020 and 2021. They have also been found in sweets in the EU, causing several severe poisoning cases (EMCDDA and Europol, 2024a), and in e-liquids and vaping products (EMCDDA and Europol, 2023). Due to their recent introduction to the market, some drug tests fail to detect synthetic cannabinoids, making them an attractive drug of choice for those subject to frequent testing procedures, including people in prisons and individuals undergoing drug treatments. Thus, the smuggling of synthetic cannabinoids in prisons is increasing, as the concealment methods have evolved to include paper impregnation (e.g. in letters, photographs, drawings) and vaping devices (EMCDDA, 2020).

Arylcyclohexylamines are a chemical class of drugs that were originally introduced as intravenous anaesthetics. A type of arycyclohexylamine is phencyclidine (PCP), which was first introduced in the medical industry in the 1950s, but was withdrawn due to its hallucinogenic and delirium effects and became internationally controlled. Ketamine is closely related to PCP, is a dissociative drug and is one of the oldest NPS. Ketamine abuse was first reported in the United States in the 1980s, with its emergence in Europe in the 1990s. It was originally synthesised as an anaesthetic in the 1960s and marketed as the medical alternative to phencyclidine. Ketamine underwent multiple risk assessments and was reviewed by the World Health Organization, which concluded in 2006 that the gathered information was insufficient to warrant the scheduling of ketamine (UNODC, 2013). Reports indicate that the majority of the ketamine on European markets is sourced from India, with some indications of imports from China and Pakistan. It usually reaches Europe through Belgium or the Netherlands and is often concealed using shell pharmaceutical companies, which are able to import up to 50 kg of ketamine for legitimate purposes; however,

illegitimate shipments often exceed 100 kg. Since it is rarely reported, there is limited evidence on domestic ketamine production, with a small number of seizures involving ketamine precursors and a few dismantled production sites in Belgium and the Netherlands. The dismantled sites indicated that extraction of medicinal products and ketamine crystallisation had been taking place in the facilities. Ketamine reports to the EU EWS have remained high in recent years, suggesting its established consistency on the markets. Almost 3 000 seizures of ketamine were reported in Europe in 2022, accounting for over 11 % of the total number of NPS seizures for that year, and amounting to almost 2.8 tonnes of the substance – more than double the quantity seized in 2020 (1.1 tonnes) (EMCDDA and Europol, 2024a). Ketamine is mainly snorted, but can also be injected. It has also been found in other drugs, such as MDMA and amphetamines, in combinations referred to as 'pink cocaine' or 'tucibi' (EMCDDA, 2023b).

NPS risks

The ease of purchasing NPS online increases their potential spread. The reasons why an individual might decide to use NPS vary and include self-medication, convenience, perceived safety, curiosity, self-exploration and recreation. The use of non-prescribed medication and illicit substances and the misuse of prescribed substances have shown to be more likely for individuals with unmet mental healthcare needs. A content analysis of Reddit posts investigated the occurrence and motivation of self-medication with NPS. The frequency of substances mentioned showed that etizolam and clonazolam (both benzodiazepines) were the most commonly mentioned substances between October 2022 and February 2023, followed by kratom (a plant-derived substance), 2-FMA (stimulant), ketamine (dissociative), diclazepam (benzodiazepine), 3-MeO-PCP (dissociative), flualprazolam (benzodiazepine) and 4F-MPH and 3-FPM (stimulants) (Holborn et al., 2023). Reddit users also commented that they resorted to self-medication with new benzodiazepines for the treatment of anxiety-related disorders and were drawn to using NPS after a life event, when substance substitution was needed, after being refused the prescription of higher doses of medical benzodiazepines and to manage pain and substance withdrawal. The research by Holborn et al. (2023) presents global issues with medical systems in terms of prescription of appropriate doses of medications and promoting openness, as indicated by multiple Reddit users. Stimulant-type NPS are predominantly reported for the self-medication of attention-deficit/hyperactivity disorder, as financial issues and the unlikely diagnosis of the disorder in adulthood are among the leading reasons for users to resort to NPS. Reddit users reported that their choice of utilising new stimulants is motivated by traumatic events and is a more favourable option than selective serotonin reuptake inhibitors (a group of prescription drugs mainly used to treat depression) due to the perceived reduced side effects of NPS. Overall, the motivations for NPS use for self-medication include dissatisfaction with the medical healthcare system, financial issues and the inability to receive a diagnosis.

NPS health impacts

NPS pose a growing global public health threat, designed to replace controlled and banned substances and consistently avoid controls. Their continuously changing chemical structures pose forensic, legal and law enforcement challenges, making them hard to trace and control. NPS require extensive laboratory and non-laboratory analyses and further medicolegal investigations to aid their identification, scheduling and control (Sajwani, 2023).

Illicit drugs pose a significant risk to public health, and NPS, by definition, are no exception. The use of NPS is often linked to health problems, with effects ranging from seizures to agitation, aggression, acute psychosis and dependence. NPS users have frequently been hospitalised with severe intoxications; however, the toxicity,

carcinogenic potential and long-term adverse effects of many NPS are currently unknown. The purity and composition of substances containing NPS are also usually unknown, often resulting in unintentional polysubstance use and leading to increased health emergencies and fatalities (UNODC, n.d.). The popularity and availability of NPS is influenced by the general perception that they are 'low risk' legally and in terms of their adverse health effects. NPS are available online, both on the Surface Web and on the Dark Web, expanding the reach of their harmful effects. Reportedly, the low cost of NPS, paired with their high accessibility, makes them the substance of choice for some consumers, while their effects are vastly unknown. A global study on NPS found that products containing MDMB-FUBINACA (a type of synthetic cannabinoid) were linked to over 600 poisonings over two weeks, 15 of which were fatal (Sajwani, 2023).

NPS detection and monitoring

The first global NPS monitoring system – the EWA – was introduced in 2013 by UNODC and serves as a tool for effective and evidence-based policy responses based on monitoring, analysing and reporting global and regional NPS trends (UNODC, 2024). In the EU, the EMCDDA (now EUDA) and the European Union Agency for Law Enforcement Cooperation (Europol) first introduced the EU EWS in 1997, which plays a central role in supporting preparedness and responding to NPS at the national and EU levels. The EU EWS is the first step out of the three-step legal framework ((i) information exchange; (ii) risk assessment; (iii) decision-making), intended to enable the EU to rapidly detect, assess and respond to the health and social threats posed by NPS. The EWA and the EWS are interdisciplinary and multi-agency networks that act as information-exchange facilitators, and their effectiveness directly depends on close monitoring, good communication between stakeholders, timely responses to emerging drug threats and early detection. When an NPS is formally notified, it is closely monitored through the EWS for signals of harm, in which the EUDA uses event-based data, toxicovigilance, signal management and open-source information. NPS can be put under intense monitoring, during which risk communication is issued, including public health alerts and initial reports that may lead to a risk assessment being produced (EUDA, n.d.b). The information input on the EU EWS and EWA is paramount for the identification of the most prevalent and harmful NPS, which pose the greatest health risks, therefore supporting the prioritisation of substances for placement under international control and national legislative responses (UNODC, 2024).

Between 2017 and 2021, 110 NPS production sites in 9 European countries were reported to the EMCDDA, which is a significant increase from the 46 NPS production sites in 12 countries reported between 2013 and 2016. The biggest increase was observed in the Netherlands with 16 production sites reported between 2013 and 2016 increasing to 55 sites between 2017 and 2021, followed by Poland with an increase from 9 to 40 sites for the same period. Synthetic cathinone production sites accounted for the greatest number of reported production sites (total $n = 110$), with 47 sites reported. The second biggest group was GHB/GBL ($n = 34$), followed by miscellaneous drugs ($n = 15$), synthetic cannabinoids and phenethylamines ($n = 5$ each), ketamine and opioids ($n = 4$ each), indolalkylamines ($n = 2$) and arylalkylamines ($n = 1$) (EMCDDA and Europol, 2024a).

Producers of NPS continually change their chemical structures to hinder law enforcement's ability to track them. The illegal passing or smuggling of NPS through borders is among the core challenges faced by law enforcement, as traditional detection methods are unlikely to detect NPS due to the modifications to their structure. Due to their ever-changing structures and the time required to study and understand their metabolic pathways, NPS detection using traditional drug-detection methods at the workplace or in institutions (e.g. prisons) is further challenged (Al-

Asmari, 2024). Another obstacle for the control and detection of NPS is the unavailability of toxicological and analytical screening tests (Sajwani, 2023).

NPS online presence and distribution

The initial interest in the interaction between sites on the Surface Web and illicit drugs was predominantly focused on how online communities can share information on manufacturing and extracting substances and not so much on how the Surface Web could facilitate drug trading. The interest has shifted considerably in recent years due to the increased availability of NPS in web shops and lifestyle pharmaceuticals. NPS are largely perceived to be part of a legal grey area and often include products that are legally produced and sold in one jurisdiction but remain illegal in others (Childs et al., 2022).

Surface and Dark Web marketplaces (the latter also known as crypto markets) play a crucial role in NPS distribution. As mentioned above, producers constantly change the chemical structures of NPS to avoid detection, leading to the introduction of new, slightly modified substances, with the former ones vanishing from the markets. Wadsworth et al. (2018) studied the lifespan of individual NPS sold on Dark Web marketplaces and the lifespan of their vendors over a period of 12 months. The results of the study indicated that the total number of individual NPS and vendors on the analysed crypto markets increased by over 70 % for the individual NPS and over 90 % for the vendors during the research period. One fifth of the NPS were reportedly available for the full duration of the study, and around one quarter of the individual NPS were available for a few months. Almost half of the vendors were active for around two months, and only 4 % of them appeared during the full duration of the study (Wadsworth et al., 2018). These results support the idea that, although the individual substances change, NPS numbers increase and indicate growth in the public's interest in NPS, leading to further public health concerns. What remains unclear is how their presence online affects the drug chain and linkages to the organisation of criminal networks that may be tied to more traditional offline illicit drug activity. Data on wider offline activities, individuals and groups has not yet been clearly linked to the facilitation and ease of NPS distribution online, leaving a blind spot for LEAs, as the online presence and legality of NPS could indicate the involvement of entirely different groups of offenders or individual offenders, organisational and hierarchical structures, and consumers.

Nevertheless, NPS wholesalers, retailers and dealers often use logistics companies and postal services to ship the substances, leading to individuals unknowingly trafficking NPS. Smaller amounts of NPS are likely to be shipped by courier services and express mail, whereas larger shipments are likely to be delivered by sea and air. NPS may be concealed using similar methods to those used for the trafficking of controlled drugs (e.g. camouflage trafficking), mislabelling and declaring the NPS as common goods or chemical products, or routing NPS to European ports where the substances are not controlled to minimise the risks of interception. Spain and the Netherlands are currently reported to be the key European import entry points for NPS from China and India (EMCDDA and Europol, 2024a).

Legal landscape

The ambiguous legal status of NPS and the adoption of disparate legal instruments at the national and regional levels as a response to NPS are among the key challenges in controlling and detecting these substances. Generally, jurisdictions employ generic controls on groups of substances, individual substance listings or hybrid model controls in response to NPS. The generic model allows the control of entire groups of substances based on their core chemical

structures, and is implemented within both NPS-specific regulations and general drug regulations. This model is often employed by countries with highly dynamic NPS markets to enable the control of large numbers of related NPS without specifically naming them individually, and is characterised by frequent updates due to the chemical diversification of the substances and by continuous landscape monitoring. Member States that employ the generic model include Belgium, Germany and Poland. The individual listings model is characterised by classifying individual substances and placing them under national controls based on their psychoactive effects, considering the potential harm-to-therapeutic-value ratio caused by controlling the NPS. Examples of Member States employing the individual listings model include Czechia, the Netherlands and Portugal. The hybrid model combines individual listings and generic controls, enabling the control of both individual substances and entire NPS groups. The hybrid model is employed by Ireland and France (Neicun et al., 2022).

All three NPS control models have their respective benefits and limitations, and careful assessment is required when a national control model is selected. Generic controls allow the control of large quantities of NPS and facilitate the anticipation of future substances. However, the development of generic controls can be time-consuming due to the complexity of some NPS groups and the requirement to specify substitution patterns, necessitating the implementation of individual NPS listings while the generic controls are in development (United Nations, n.d.a). In terms of individual listings, each substance is assessed on a case-by-case basis, and individual substances can be added to national controls through either regular processes or rapid procedures, enabling their temporary or permanent control. This is the preferred approach for countries that are affected by a limited number of NPS and is characterised by lengthy procedures for listing NPS individually, leading to a lack of synchronisation between the emergence of NPS and their control. Furthermore, minor variations in the chemical structure of a listed substance are also not covered by legislation within the individual listings model. Overall, disparities between control models at the national level can further challenge the international tackling of NPS, with certain substances shifting in legality depending on the jurisdiction's controls. Further efforts are required to unify NPS controls at the European level to address the international dimensions of the issue (United Nations, n.d.b).

Current operational practices

First-hand insights into the operational practices of five European LEAs and one postal service were gained through written expert consultations, focusing on NPS prevalence, the criminal modus operandi of individuals in the NPS trafficking chain and detection capabilities.

Prevalence

The consulted practitioners unanimously agreed that the prevalence of crimes involving NPS has increased in the past five years. The NPS most frequently observed by the experts in the past five years were synthetic cathinones (50 % of responses; substances mentioned include 2-MMC, 3-MMC and 3-CMC), synthetic cannabinoids (37.5 %) and synthetic opioids (12.5 %), which corroborates the reports and statistics detailed above, especially considering the number of new opioids that were officially identified in 2023.

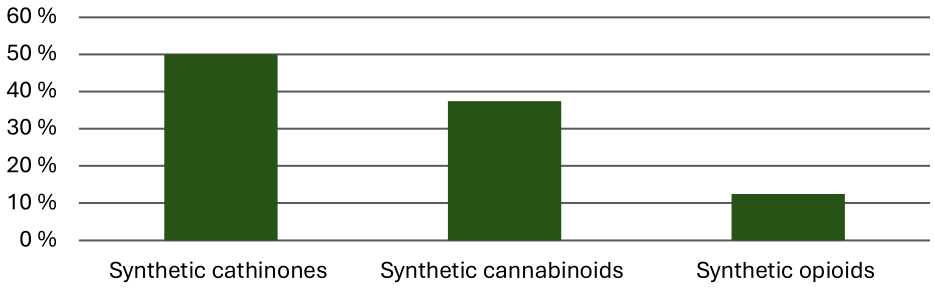


Figure 2.1. Most frequently observed NPS groups in the past five years

According to the practitioners, the Surface Web was reportedly the location where the most NPS were observed, followed by the Dark Web, international borders and other offline locations, while the Deep Web was the least frequently mentioned location for NPS. By contrast, none of the consulted experts indicated the Deep or Dark Webs as locations where they had observed the most illicit drug precursors. Instead, there was a higher response rate indicating offline locations. Furthermore, the experts specified that NPS were also observed on encrypted messaging applications and in local, national or international post offices. All consulted experts stated they had observed NPS being trafficked using postal or courier services.

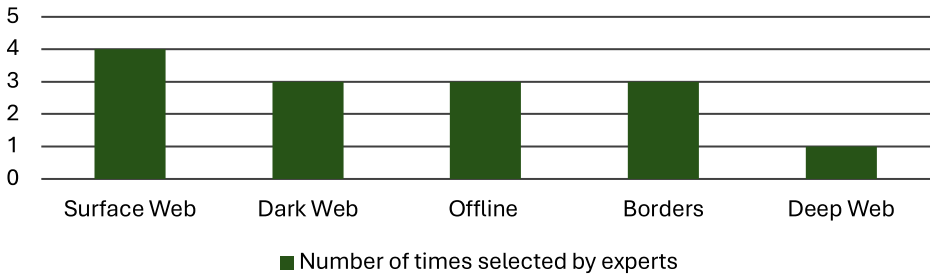


Figure 2.2. Online and offline locations where experts observed the most NPS

Modus operandi

The practitioners indicated that, from their experience, the groups of criminals dealing with NPS are different from the groups of criminals dealing with listed illegal drugs. They also stated that the strategies and modus operandi used by criminals dealing with NPS and criminals dealing with listed drugs vary. For instance, experts mentioned that criminals dealing with NPS avoid physical contact with consumers and other members of the criminal group by locating themselves online and often using cryptocurrencies to minimise the risks of detection and identification.

An example of an NPS modus operandi was given by one of the consulted LEAs in the context of synthetic cannabinoids ('spice') smuggled into prisons. It was stated that offenders were impregnating paper with spice and selling the sheets either as blank paper or as printed letters. According to the evidence gathered, the wholesale prices of the raw materials were relatively low (varying from EUR 850 for 250 g to EUR 1 900 for 1 kg), allowing the offenders to be efficient and consistent with the quality of the produced sheets. To impregnate the paper, the criminals were using between 5 g and 15 g of powder spice, diluted into a 250 ml bottle of acetone, yielding between 10 and 15 sheets. The offenders would sell the acetone with spice for approximately EUR 125 if 8 g of spice was used and for EUR 85 if 5 g of spice was used. The wholesale price of the impregnated paper was reported to be approximately EUR 425 for 25 sheets. The end-user price would vary, depending on the available supply in each

prison wing at a given time. Similarly, there were reports of paper impregnated with synthetic cannabinoids smuggled into Brazilian prisons, indicating the global dimensions of the issue (EMCDDA and Europol, 2024a).

NPS detection

The experts unanimously stated that NPS trafficking using postal or courier services is a frequent occurrence. This aligns with previous statements that NPS criminals avoid physical contact with consumers and other group members, thus dealing online and using postal or courier services to deliver substances. Some of the NPS detection methods for parcels the experts reported using within their organisations included X-rays, trace detectors and physical detection methods. However, the experts also reported that the current online methods of investigation for NPS appeared to be quite limited. They stated that they had no way to obtain information from encrypted platforms (e.g. WhatsApp, Telegram, Signal) and that their methods were not automated, requiring extensive and lengthy manual searches to detect NPS-related information online and on messaging platforms.

When asked which organisations and agencies are involved in the detection and investigation of NPS, the experts expanded that LEAs, customs authorities, national forensic institutes and laboratories, national crime agencies, regional organised crime units, and national technical-criminal and forensic expertise centres were among the key entities involved in NPS detection and investigation. However, the experts noted several issues that hindered their approaches to EU and international cooperation. They mentioned that differences in regulations can complicate data sharing between countries, as can ever-emerging technologies that, while useful, may not be adopted across the board. A challenge to EU and international cooperation mentioned repeatedly was the emergence and awareness of new substances, not yet under international control, across countries. One of the experts described a case where they first discovered the substance BMKGA by following a package intercepted in Germany that originated from China and was bound for their country. If the substance was not controlled in Germany, it would likely have reached its destination country and consumers. Additionally, some of the consulted LEAs were not part of the EU and indicated that their connection to the EU EWS would benefit the detection, monitoring and tackling of NPS at both the national and the international level.

To address these needs, the experts suggested starting with legislative harmonisation and adapting legislation to enable tighter cooperation between LEAs and postal services.

Conclusion

NPS pose a significant threat to Europe. The ever-changing chemical structures of these substances and the multitude of methods used to conceal them, along with their grey legal status and online availability, complicate their detection and thus their control. These factors also limit the acquisition of data on the health risks they might pose. The public health concerns are further elevated by the frequent unknown polysubstance consumption that occurs due to the combination of multiple NPS substances, leading to potential health crises. Corroboration between the reviewed literature and documentation and expert consultations is observed, as all sources report that synthetic cathinones are the most prevalent type of NPS in terms of seizures in Europe (EMCDDA and Europol, 2024a), with synthetic cannabinoids being a close second.

A multitude of areas should be improved to aid the detection and tackling of NPS, and to reduce their negative effects on public health. As stated above, many tests currently do not detect NPS, making them an attractive choice for people in prisons and individuals undergoing drug treatments. Further research is required on developing techniques and methods that can reliably detect a variety of NPS. Furthermore, the consulted practitioners reported less-than-optimal current capabilities for online investigation of NPS, which likely feeds into the present uncertainty over their facilitation and ease of distribution online. The current study therefore recommends more research into this area, both from an academic and from a law enforcement perspective. In addition, there is a need for synchronised efforts in the NPS legal landscape at the European level to ensure international continuity, timely and coordinated responses, and comprehensiveness of the established controls. This can be facilitated by shared intelligence on precursors and NPS, and by efforts to align national drug strategies and priorities holistically across Europe based on the flow of drugs across the continent, as opposed to keeping national perspectives isolated.

The trust between individuals and the healthcare system should be rebuilt, and healthcare professionals should be aware of the risks of individuals resorting to self-medication with more dangerous NPS when denied access to prescription drugs (Holborn et al., 2023), especially considering signs that the use of NPS among vulnerable populations may have increased (EMCDDA, 2022).

Additionally, the current research found that European countries not part of the EU face challenges in inputting and accessing data from the EU EWS, and the majority of their data is not fed into the system. This siloes intelligence gathering and further complicates tackling NPS at both the national and the European levels. Thus, considerations for involving more European countries should be made, and continuous improvement of international cooperation should be implemented to tackle the global dimensions of the NPS issue.

Acknowledgements

We are grateful to the experts who provided their valuable time for this work. This research was conducted as part of the ARIEN project, co-funded by the European Union. It is also funded by UK Research and Innovation under the UK government's Horizon Europe funding guarantee (grant number 10078198). For the purpose of open access, the authors have applied a Creative Commons Attribution (CC BY) licence to any author-accepted manuscript version of this paper arising from this submission.

References

Al-Asmari, A. I. (2024), 'A critical review of workplace drug testing methods for old and new psychoactive substances: Gaps, advances, and perspectives', *Saudi Pharmaceutical Journal*, Vol. 32, Issue 5, https://doi.org/10.1016/j.jsps.2024.102065.

Childs, A., Bull, M. and Coomber, R. (2022), 'Beyond the dark web: Navigating the risks of cannabis supply over the surface web', *Drugs: Education, Prevention and Policy*, Vol. 29, Issue 4, pp. 403–414, https://doi.org/10.1080/09687637.2021.1916439.

EMCDDA (2020), *New Psychoactive Substances: Global markets, glocal threats and the COVID-19 pandemic – An update from the EU early warning system*, Publications Office of the European Union, Luxembourg, https://doi.org/10.2810/845598.

EMCDDA (2022), *New Psychoactive Substances: 25 years of early warning and response in Europe – An update from the EU early warning system*, Publications Office of the European Union, Luxembourg, https://doi.org/10.2810/396103.

EMCDDA (2023), *European Drug Report 2023: Trends and Developments*, EMCDDA, https://www.euda.europa.eu/publications/european-drug-report/2023_en.

EMCDDA and Europol (2023), 'EU drug market: Cannabis – Retail markets', *EU Drug Market: Cannabis – In-depth analysis,* https://www.euda.europa.eu/publications/eu-drug-markets/cannabis/retail-markets_en.

EMCDDA and Europol (2024a), *EU Drug Market: New psychoactive substances – In-depth analysis*, https://www.euda.europa.eu/publications/eu-drug-markets/new-psychoactive-substances_en.

EMCDDA and Europol (2024b), *EU Drug Markets Analysis 2024: Key insights for policy and practice*, Publications Office of the European Union, Luxembourg, https://doi.org/10.2810/137611.

EUDA (n.d.a), 'Synthetic cathinones drug profile', EUDA website, https://www.euda.europa.eu/publications/drug-profiles/synthetic-cathinones_en#:~:text=top %20of %20page,Control %20status,are %20not %20under %20international %20control.

EUDA (n.d.b), 'The EU early warning system on new psychoactive substances (NPS)', EUDA website, https://www.euda.europa.eu/activities/eu-early-warning-system-on-nps_en.

Holborn, T., Schifano, F. and Deluca, P. (2023), 'No prescription? No problem: A qualitative study investigating self-medication with novel psychoactive substances (NPS)', *International Journal of Drug Policy*, Vol. 118, https://doi.org/10.1016/j.drugpo.2023.104109.

Lin, O. A., Chuang, P.-J. and Tseng, Y. J. (2023), 'Comparison of controlled drugs and new psychoactive substances (NPS) regulations in East and Southeast Asia', *Regulatory Toxicology and Pharmacology*, Vol. 138, https://doi.org/10.1016/j.yrtph.2023.105338.

National Crime Agency (2019), 'The use of clearnet and social media for the advertising and sale of fentanyl analogues', *Amber Alert*, National Crime Agency, https://nationalcrimeagency.gov.uk/who-we-are/publications/334-nca-amber-alert-online-sale-of-fentanyl-analogues/file#:~:text=Fentanyl %20analogues %20are %20synthetic %20opioids,pain %20conditions %20or %20palliative %20care.

Neicun, J., Roman-Urrestarazu, A. and Czabanowska, K. (2022), 'Legal responses to novel psychoactive substances implemented by ten European countries: An analysis from legal epidemiology', *Emerging Trends in Drugs, Addictions, and Health*, Vol. 2, https://doi.org/10.1016/j.etdah.2022.100044.

European Parliament and Council of the European Union (2004), Regulation (EC) No 273/2004 of the European Parliament and of the Council of 11 February 2004 on drug precursors (OJ L 47, 18.2.2004, p. 1, ELI: http://data.europa.eu/eli/reg/2004/273/oj).

Pinterova, N., Horsley, R. R. and Palenicek, T. (2017), 'Synthetic aminoindanes: A summary of existing knowledge', *Frontiers in Psychiatry*, Vol. 8, https://doi.org/10.3389/fpsyt.2017.00236.

Sajwani, H. S. (2023), 'The dilemma of new psychoactive substances: A growing threat', *Saudi Pharmaceutical Journal*, Vol. 31, Issue 3, pp. 348–350, https://doi.org/10.1016/j.jsps.2023.01.002.

United Nations (n.d.a), 'UN toolkit on synthetic drugs – Generic legislation', United Nations website, https://syntheticdrugs.unodc.org/syntheticdrugs/en/legal/national/genericcontrols.html.

United Nations (n.d.b), 'UN toolkit on synthetic drugs – Individual listing of substances', United Nations website, https://syntheticdrugs.unodc.org/syntheticdrugs/en/legal/national/individual.html.

UNODC (2013), *The Challenge of New Psychoactive Substances*, UNODC, Vienna, https://www.unodc.org/documents/scientific/NPS_2013_SMART.pdf.

UNODC (2020), 'Drug trafficking', *E4J University Module Series: Organized Crime; Module 3: Organized Crime Markets*, UNODC, https://www.unodc.org/e4j/zh/organized-crime/module-3/key-issues/drug-trafficking.html.

UNODC (2024), *Current NPS Threats*, Vol. 7, UNODC Laboratory and Scientific Service, Vienna, https://www.unodc.org/documents/scientific/Current_NPS_threats_VII.pdf.

UNODC (n.d.), 'UNODC early warning advisory on new psychoactive substances', UNODC website, https://www.unodc.org/LSS/Page/NPS.

Wadsworth, E., Drummond, C. and Deluca, P. (2018), 'The dynamic environment of crypto markets: The lifespan of new psychoactive substances (NPS) and vendors selling NPS', *Brain Sciences*, Vol. 8, Issue 3, https://doi.org/10.3390/brainsci8030046.

Modi operandi and trends of high-risk criminal networks for illegal immigration operating in Bulgaria

Aleksandar Atanasov

https://doi.org/10.3013/g30q0d61

Abstract

This article aims to explore and represent the currently exploited trends and strategies of organised crime groups active in Bulgaria and involved in the smuggling of illegal migrants across Europe as part of a larger high-risk criminal network. It details the prevailing trends and specific mechanisms employed in these criminal activities over the past three years, relying on a methodology of data analysis of different text sources and the professional experience of the author. The topic of the paper is researched from the perspectives of criminology, law enforcement and intelligence. The study identifies five primary factors – the geosocial factor, the local factor, the foreign factor, the factor of criminal and non-criminal actors and the geopolitical factor – that influence the characteristics of criminal groups engaged in illegal immigration, as observed in Bulgaria. These factors offer insights for enhancing operational and strategic responses to counter emerging threats posed by high-risk criminal networks of illegal immigration. The research emphasises the different organisational levels and operational functions of these criminal groups and their networks. It examines specific patterns of criminal activity over the past three years, including the roles of illegal migrants, their drivers, guides, field captains and middlemen and the leaders of the criminal organisations.

Keywords: illegal immigration, terrorism, modus operandi, trends, Bulgaria, organised crime groups, high-risk criminal networks, migrant smuggling.

Introduction

Illegal immigration has become one of the most prevalent and profitable criminal activities in recent years (Eurostat, 2023). The progression and escalation of this crime type are influenced by various factors, including international relations and geopolitical conflicts, the rising demand for this criminal service and the broader effects of globalisation.

Illegal immigration operates as an organised structure. This form of crime is typically carried out by highly structured networks comprising international and national channels, with individuals at various levels occupying specialised roles. For instance, certain individuals may facilitate connections with illegal immigrants and their groups, while others serve as drivers, navigators or boat operators or provide hidden accommodations. Often, a single person may assume multiple roles within the scheme. At the top of the pyramid are the organisers, who command and control the other levels. A crucial requirement for each organised crime group (OCG) involved in illegal immigration networks, as relevant to the current study, is bilingual capability. Each operating channel requires individuals who speak both the language of the host country or another international language and the language of those attempting to transit through.

Those at the top of the pyramid provide essential connections, funding, logistical support and human resources to various branches within the network. They coordinate the operations among different branches and establish links with partner countries where other OCGs are involved. These groups may operate in a decentralised manner, functioning independently within the country or across its different regions, or they may be part of a larger, centralised criminal network operating across multiple countries. OCGs work similarly to independent service providers within a free market, responding to demand from different groups of illegal migrants. The services offered depend on the capacity of the specific OCG within the broader network and on the financial resources of the migrants who engage them.

The combination of multiple OCGs forms extensive criminal networks. These networks sometimes develop through accidental or random associations, while in other cases they are intentionally orchestrated by key actors across various branches and countries.

This high risk factor directly impacts national security, as the demand among illegal migrants attempting to cross borders increases, and funds flow rapidly. These funds have the potential to corrupt government officials, finance additional criminal activities and support foreign fighters or radicalised individuals with violent or terrorist intentions. These individuals can exploit the opportunity of the illegal network to travel and integrate into mainland European societies, potentially operating as sleeper cells or engaging in disruptive activities.

Some OCGs and criminal networks channel their funds into private companies or even government institutions with the express purpose of fostering corruption or gaining unethical advantages over legally established companies. Numerous cases have shown that legal business infrastructures, such as car rental firms, are often created specifically to facilitate illegal activities, including migrant smuggling. Compromising government officials, law enforcement and other personnel undermines the state's national security. Cases of such involvement are frequently driven by economic incentives (Mediapool, 2023).

A recent report by the European Border and Coast Guard Agency (Frontex) identifies the Western Balkan route as the second most active migratory pathway into the European Union (Frontex, 2024), followed closely by the Eastern Mediterranean route. Bulgaria's geographical location places it at the intersection of these routes, positioning the country as a central player on the Balkan peninsula. This strategic factor emphasises the significance of Bulgaria's experience in combating illegal immigration. These circumstances underscore the relevance of this research and the urgent nature of the issues to be addressed.

Methodology and key terms

The methodology behind this research relies on qualitative data analysis of a diverse array of open-source information, including books, online articles, academic articles, news articles and other textual materials, along with the personal professional experience of the author.

The author's professional background in law enforcement provides contextual familiarity with the operational environment of migrant-smuggling networks. However, all analytical conclusions presented in this paper are derived exclusively from the open, verifiable sources cited in the references. Professional experience informs the interpretive framework but does not substitute for, or supplement, the cited evidence base.

This mixed-methods approach, combining open-source information and professional law enforcement expertise, allows for a more comprehensive understanding of the topic. The use of publicly available sources ensures transparency, while the specifics of the author's professional involvement provide insights otherwise inaccessible in open domains. The covered period of the research focuses on the last three years and represents the current trends in this type of criminal activity and the schemes involved in carrying it out.

Analytical scope and evidentiary basis

All analytical conclusions presented in this paper are derived exclusively from open, publicly verifiable sources cited in the references, including reports from the European Union Agency for Law Enforcement Cooperation (Europol) (2023, 2024), Frontex (2024), the Financial Action Task Force (FATF) (2022) and the United Nations Office on Drugs and Crime (UNODC) (2004). The author's professional experience in law enforcement provides contextual familiarity with the operational environment but serves solely as interpretive background – not as evidentiary support for any specific claims. Where professional context informs analytical framing, this is explicitly noted. No classified, confidential or otherwise non-citable material has been used as the basis for conclusions presented herein.

This approach combines the benefits of open access with the depth of analytical operational experience, allowing for a robust analysis. On the positive side, it expands the informational foundation of the research, enhancing reliability where open-source data alone may be insufficient. However, this methodology also introduces limitations inherent to experience-informed analysis, where certain contextual interpretations reflect the author's professional judgement as an expert analyst with an operational background.

For the purposes of this paper, we will use the United Nations definition of an OCG: 'a group of three or more individuals that is not spontaneous, accidentally formed, exists for a period of time and acts to perform at least one punishable by law crime for a period of more than four years, with the purpose of obtaining, directly or indirectly, financial or other material advantage' (UNODC, 2024).

As for 'high-risk criminal network', we will use the definition provided by Europol: 'A high-risk criminal network is an organised group engaged in serious and often transnational criminal activities that pose a significant threat to public safety and security. These networks are characterised by their agility, borderless operations, controlling structures, and destructive methods. High-risk criminal networks typically have a hierarchical structure with strong leadership that can coordinate activities across multiple jurisdictions' (Europol, 2024).

For logical simplification, we can conclude that two or more OCGs can form a criminal network, as they boost their criminal impact on society and multiply their unlawful force projection. Modus operandi is a distinctive method or pattern of behaviour that a criminal or group of criminals employs when committing crimes. The term translates from Latin as 'method of operating' (Britannica Editors, 2024).

The geosocial factor

As previously noted, the geographical significance of Bulgaria is essential within the Balkan peninsula. The country's location underscores its importance as a gateway to mainland Europe, which remains the primary destination for illegal migrants. These processes are not new and are historically recognised, tracing back to the old Silk Road and Bulgaria's role as the 'gateway to Asia' through the Bosphorus Strait.

This context highlights the Bulgarian–Turkish border as a critical hotspot for both law enforcement and illegal migrants. Known as the Strandzha–Sakar region, this area comprises the Strandzha and Sakar mountains, which span the entire Turkish border. While the region has some flat areas, it is predominantly rugged with highlands and mountainous terrain. Such geography presents a formidable challenge for the enforcement forces tasked with detaining and arresting those who attempt to cross undetected. The principles here mirror those of military operations in mountainous terrain, where conventional forces counteract guerrilla tactics.

OCGs exploit several modi operandi to maximise the terrain's advantages when attempting to bypass the country's first line of defence. This defence primarily comprises border police, the gendarmerie and various army units acting in a policing capacity.

1. **Exploiting various land-navigation tactics through specialised software or open-source mobile applications.** In this modus operandi, illegal migrants enter the country independently until they connect with a designated driver who transports them further inland. Numerous well-established routes are shared among groups, with one group often passing information on to the next. The model represents a typical mountain pass shared between one group that has already passed through and another. In almost all cases, migrants use their mobile phones offline or with VPN (virtual private network) data.

In this scenario, criminal networks employ terrain-exploitation guidance methods to facilitate covert border crossings. These methods, consistent with patterns identified in Frontex operational reports (Frontex, 2024), involve instructing migrants on movement timing, terrain selection and counter-detection practices that can maximise the geographical advantages described above.

As migrant groups move through the border region alone, one or more members often stay in contact with a non-Bulgarian national (typically another migrant, a Turkish citizen or someone from outside Europe) who coordinates the next steps with the local contacts – either Bulgarian nationals or others already within the country. These contacts arrange transport and shelter until the group can move towards other borders, usually Romania or Serbia. Crossings sometimes occur without a prior arrangement with an established network, as migrants can often secure transportation on arrival in Bulgaria. However, last-minute logistical failures sometimes force a change in drivers. This part of the journey typically lasts several days.

This modus operandi is highly risky, and there are frequent cases of migrants losing their lives at this stage. Often, this method is chosen by those without significant financial resources, while groups with more substantial funding opt for the next, safer and faster modus operandi.

2. **When the group is not alone, they employ similar tactics but with the assistance of a guide, or 'coyote'.** The guide is familiar with the terrain, including both secure and vulnerable areas, and can provide additional cover or handle emergencies if pursued by border forces. Guides may be Bulgarian nationals, Turkish citizens or migrants from non-EU countries. The guide's role includes connecting the group with the next unit in the chain – the drivers. It is not uncommon for the houses of locals in the Strandzha–Sakar region, or abandoned buildings, to be used as temporary shelters, which makes border crossing more secure and manageable, especially for groups with women and children.

In some cases, specialised groups of guides enter the country illegally to familiarise themselves with the terrain under the guidance of experienced instructors. Once trained, they can serve as coyotes for future migrant groups. On both sides of the border, specialised individuals (Bulgarian or non-Bulgarian nationals) are skilled at navigating the challenging Strandzha–Sakar terrain.

Breaching border defences is not technically difficult in terms of overcoming the static border fence wall and can be done using military-style tactics with conventional user-grade tools that can be acquired from a standard commercial shop. The rest of the country is divided by a significant mountain range. Most OCGs use the south route, but there are instances of the north route being used as well, with various route combinations possible. To fully address these border-crossing methods, a third modus operandi must also be mentioned.

3. **Crossing through official border checkpoints.** The methods employed here are varied and numerous. Migrants may be hidden in trucks, cars, buses or any other conceivable vehicle to pass undetected. Although some truck drivers claim ignorance of their passengers, a significant number are aware. In one case, migrants used the driver's password-protected Wi-Fi network while hiding between the truck's wheels, despite the driver's claim that he was unaware of their presence. Such situations are difficult to prosecute, as proving the driver's criminal intent is challenging when the migrants are concealed outside the truck's cabin. Analysing this aspect in detail merits an entirely separate study – and, by extension, a different article – and the same can be said for the other modi operandi.

When examining the country's geographical features and how its terrain is exploited, nearly all 'inner courses' – routes that transport illegal migrants from one location to another after the initial border crossing – follow a similar model.

- A **lead vehicle**, typically with a driver, takes the first position and commands the other vehicles involved in the transport. Sometimes, this lead vehicle includes a driver and a 'field captain'. In either case, the lead vehicle's role is to scout for law enforcement and alert the main vehicle to any potential police presence or hazards along the route. The lead vehicle also maintains contact with higher-ranking members of the criminal organisation and navigates the route to the final offloading destination.

- A **main vehicle** carries the migrants and a driver who communicates with the lead vehicle and follows a predetermined route coordinated between them.
- Occasionally, a **rear or support vehicle** is deployed, serving a similar role to the lead vehicle as a rear reconnaissance unit, protecting against police interception. The field captain may also be positioned in this rear vehicle, as it offers the safest position for escape in the event of a police intervention or arrest.

Figure 3.1. Modus operandi of vehicle deployment in migrant smuggling
NB: This figure shows a comprehensive model illustrating the tactical deployment of vehicles in smuggling operations. While the model presents a complex arrangement, it can be adapted or simplified according to the available resources and specific operational requirements of the crime group. The spatial distribution between vehicles may vary from several meters to temporal intervals of 5 to 15 minutes.

It is important to note that 2022 was a tragic year for law enforcement in Bulgaria, marking the darkest record since data collection began in 1942. Over five Bulgarian police officers lost their lives, most while conducting operations to counter illegal immigration. Police pursuits have surged as many drivers transporting illegal migrants within the country and in border regions attempt to evade police checks, often driving dangerously in hopes of escaping arrest if they can abandon the vehicle with the migrants inside.

In summary, OCGs operating in Bulgaria have developed significant expertise in traversing mountainous terrain and providing in-depth logistical support, such as coordinated vehicle convoys. These groups exploit the mountainous border regions, either by using guides or, at times, by leaving migrants to navigate the area on their own, directing them to points where designated vehicles await to transport them to hiding spots or across other borders.

Sometimes, routes are planned directly from point A to point B along main roads and highways. Other times, they are routed along secondary roads, away from major transport arteries where police presence and checkpoints are more concentrated.

This expertise has expanded to support other inter-country networks for migrant smuggling across the Western Balkans, where Bulgarian OCGs operate primarily to provide aggressive driving and logistical transport services.

Social dynamics also align with the country's geographical realities, drivers being the most sought-after asset for leaders of organised crime networks. The most skilled drivers often become field captains, and those who excel may advance to roles as recruiters or coordinators, acting as middlemen with minimal contact with the migrants. This distance provides greater security, as it follows the principle that 'the farther you are from the migrants, the safer you are from the authorities'.

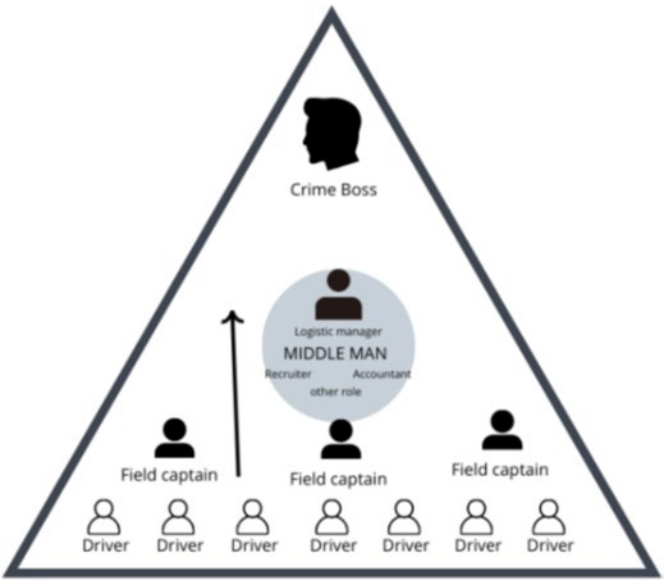


Figure 3.2. Potential career development pyramid of an illegal immigrant driver in an OCG

Bulgaria remains the poorest country in the European Union (BNT, 2023). The financial incentives in these criminal schemes are substantial, often yielding 'easy money' for just a few hours of work. A typical route, transporting migrants from the Turkish border to the capital or from the capital to the Romanian or Serbian border, takes about five to seven hours.

Factors such as ethnicity, nationality, age, gender or possession of a driver's licence are irrelevant – anyone who can drive and is willing to participate is recruited by criminal networks. While there are varied examples, the typical driver profile is that of a middle-aged man with a low socioeconomic status or a gambling addiction, often a Bulgarian national or a national of a country in the former Soviet sphere of influence.

A notable proportion of apprehended drivers have been associated with drug-user communities, as reported in Bulgarian enforcement operations and media coverage (Mediapool, 2023). These drivers are often among the most aggressive in evading police. Documented cases include drivers operating under the influence of methamphetamines, ecstasy or other stimulants, which may contribute to risk-taking behaviour during transport.

Europol's analysis of high-risk criminal networks documents instances where poly-criminal actors operate across multiple crime types, including drug trafficking and migrant smuggling (Europol, 2024). This pattern suggests potential overlap between drug-related criminal circles and migrant-smuggling operations, though the extent of such convergence varies by region and network structure.

When a person from a community with social vulnerabilities – such as gambling or drug addiction – is recruited and completes one or more profitable trips as a migrant driver, they can quickly become a 'local star'. The easy money earned acts as a social magnet, attracting others within these communities who wish to achieve rapid financial gain. This creates a form of local 'infection', turning neighbourhoods, small villages, drug-user communities or gambling groups into valuable recruitment pools for OCGs and criminal networks.

In conclusion, from a social perspective, the high-risk segments of criminalisation of society remain the primary recruitment targets for OCGs due to the low skill requirements for the easily replaceable role of drivers. On the other hand, more specialised roles – such as coyotes/guides, those who offer hiding places, and boatmen – demand specific skills and thus receive considerable investment and protection from criminal networks. However, for the common driver role, almost anyone can be considered suitable.

This article does not aim to examine every role and specific function within OCGs and migrant-smuggling networks, as a comprehensive analysis would require a much larger-scale study, which is beyond the scope of this work.

The local factor

For the purposes of this research, the term 'local factor' refers to the criminal infrastructure established and exploited within the host country of illegal immigrants. Although this infrastructure may be initiated or influenced by foreign entities, it is nonetheless developed, maintained and utilised in the host country. By 'criminal infrastructure', we refer to all the various roles and positions necessary to successfully coordinate border crossings, provide temporary shelter and manage domestic transport, moving migrants from one border or safe house to another.

The local factor in the host country oversees every stage of the transit process within its borders: (1) receiving migrants and either aiding their passage through border control or bypassing it illegally upon entry; (2) transporting migrants undetected along domestic routes from one key location to another; (3) providing temporary shelter between transport stages while preparing for the next border crossing; and (4) ensuring migrants' delivery to the exit border of the host country.

The local factor operates independently of the foreign network that maintains direct contact and coordination with the migrants themselves. It is important to distinguish that the local factor primarily provides a service to the criminal network. In this context, the local factor comprises nationals of the host country, such as Bulgarians, Romanians or other Europeans. Meanwhile, the foreigners are the non-Europeans who handle the migrants, manage finances and oversee the broader organisational structure and who directly communicate with the migrants, often speaking their language and understanding their needs. In this study, these foreigners will be referred to as the foreign factor. The foreign factor supplies funding, ensures service quality and depends on the local factor's assistance in return for a financial reward.

Figure 3.3. Schematic representation of the local factor model

NB: This figure shows the hierarchical structure wherein a single crime boss may oversee multiple generals while simultaneously managing various criminal branches beyond migrant smuggling, such as a drug trafficking operation.

If we consider an example, the local factor in Bulgaria is primarily operated by Bulgarian OCGs, which are often part of broader international criminal networks. However, in some cases, there are OCGs composed entirely of Moldovan, Romanian or other nationals, which operate as entirely local entities, managing the entire cycle of illegal border crossings – from entry at the Turkish or Greek borders, to hosting migrants within the country and ultimately delivering them to the Romanian or Serbian borders. This approach has a straightforward rationale: the fewer people involved in the operation, the fewer individuals among whom profits must be divided. Bulgarian OCGs use similar strategies abroad, including in countries like Austria, where they aim to operate independently to maximise financial gain and reduce the risk of external exposure. Similarly, there are cases of Bulgarian OCGs operating independently in Greece.

In other cases, the local factor is a hybrid structure involving both Bulgarian and international participants. For example, drivers may be nationals of Albania, Georgia, Kosovo, Moldova, Romania, Ukraine or other post-Soviet countries with lower economic status. Meanwhile, those issuing commands and providing locations for illegal migrants are typically Bulgarians. Similarly, hosts offering shelter or boatmen facilitating border crossings may also be Bulgarian or Romanian nationals. These individuals maintain direct communication with the segment of the network responsible for managing contact with the migrants and their families.

The modus operandi of the local factor within the host country's criminal infrastructure can be categorised into the following three primary operational models.

1. **Entirely domestic local factor.** The local factor consists exclusively of citizens from the host country. In this scenario, the OCG is established, developed and operated entirely within the host country.

2. **Mixed local factor.** The local factor is a collaboration between citizens of the host country and international partners from other countries. In this case, the OCG is international, incorporating diverse origins and spheres of influence.

3. **Foreign-only local factor.** The local factor is composed entirely of foreign nationals, with no direct ties to the host country. This model represents an external force imported specifically to execute particular orders or instructions issued by the foreign factor.

In the context of Bulgaria and its unique geographical features, we can identify the primary roles required within the local factor to support both the illegal immigrants and the foreign factor representing them. It is important to note that this is a generalised representation of the framework: roles may overlap, and one individual may fulfil multiple responsibilities. Nevertheless, each role carries distinct responsibilities that are critical to ensuring the successful transit of illegal immigrants through the host country.

1. **Leader / crime boss.** This individual serves as the mastermind and decision-maker of the OCG. They oversee all roles and branches within the organisation and act as the primary representative in the broader criminal network. The leader maintains contact with other OCGs for collaboration and coordinates with illegal immigration channels at a higher level, often interacting with other chiefs or bosses. To minimise risk, they stay far removed from lower-level operatives and avoid direct contact with the illegal immigrants. The leader / crime boss may also oversee multiple criminal sectors, such as migrant smuggling and drug trafficking.

2. **Chief executive officer (CEO) / general.** Operating as a key intermediary, the CEO or general directly manages the operatives working in the field. They liaise with the foreign representatives connected to the illegal immigrants, often requiring bilingual skills to communicate effectively. Their responsibilities include sharing the precise locations of illegal immigrants with drivers or guides (coyotes), ensuring the local factor can efficiently begin the transport process. Additionally, they monitor the actions of OCG members working directly with the immigrants to ensure that operations run smoothly.

3. **Manager, accountant and recruiter.** This trusted individual often rises through the ranks, starting as a driver or guide (coyote). They are responsible for recruiting new operatives, managing funds and providing logistical support such as vehicles, radios and communication devices. Their role is essential for maintaining operational efficiency and addressing logistical challenges.

4. **Logistics manager.** This individual oversees the vehicles and safe houses used during the illegal operations. They may own legal businesses, such as a rent-a-car company or properties, and may claim plausible deniability about their involvement in illegal activities. By leveraging legitimate assets, they support the smuggling network while reducing personal risk.

5. **Sole recruiter.** Often a field captain or driver, the recruiter focuses on enlisting low-profile members for the OCG. If specialised roles are required, such as hosts, logistics managers or boatmen, recruitment is handled at a higher level within the organisation.

6. **Field captain.** Acting as the on-ground leader, the field captain ensures orders from the CEO/general are executed during transport operations. They oversee the OCG's activities, address issues as they arise and uphold professional conduct during interactions with illegal immigrants.

7. **Drivers.** This category includes the following.

    - **7.1. Main vehicle driver.** Responsible for directly transporting the illegal immigrants. This is the most undesirable role due to its high likelihood of legal repercussions.
    - **7.2. Pilot/lead vehicle driver.** Operates ahead of the main vehicle, scouting for police checkpoints and ensuring a clear path.
    - **7.3. Rear vehicle driver.** Provides rear support to the convoy, maintaining surveillance and intervening if police attempt to disrupt the operation.

8. **Boatman.** This highly specialised role involves transporting illegal immigrants across water borders, such as the Danube River in Bulgaria. Boatmen are valuable assets due to their skill set and are challenging to replace.

9. **Guide/coyote.** These individuals facilitate land navigation for illegal immigrants, particularly across heavily guarded and difficult terrains like the Bulgarian–Turkish border. Their expertise in navigating mountainous and forested areas, often under the cover of night, is critical for successful border crossings.

In conclusion, the models of the local factor presented here are broad generalisations. In practice, OCGs often collaborate, collectively forming the complete local factor. Roles within these groups are fluid and may shift depending on the situation, the availability of resources, the movement of criminals and the specific demands of the foreign factor. The significance of this discussion lies in understanding that every host country is subject to the criminal infrastructure and influence of multiple OCGs. These groups collectively shape the larger criminal network. Furthermore, a single OCG may extend its operations across multiple host countries, establishing and maintaining local criminal infrastructure in each. This interconnected structure highlights the transnational nature of these networks and their ability to adapt and operate effectively across borders.

The foreign factor

As previously mentioned, the foreign factor represents the organisational aspect of criminal networks that functions entirely within the context of illegal immigrants and their supportive communities – mainly comprising citizens from countries outside the European Union. This factor includes individuals who are culturally, ethnically and familiarly connected to the illegal immigrants. These individuals may range from legal citizens with dual citizenship in host countries to second- or third-generation immigrants, refugees with humanitarian status or people undergoing legal status procedures.

The foreign factor forms a distinct microclimate of relationships. This microclimate embodies the continuous search and demand for logistical and transport services. It also reflects the dynamic interactions between illegal immigrants and legal refugees, along with a series of events that unfold both within and outside the host countries.

In most cases involving illegal immigrants transiting through Bulgaria, these individuals already have an established diaspora, friends or family waiting for them in central and western Europe. On the other end of the channel, they maintain connections with family members or relatives still residing in their home countries. These individuals often come from countries such as Egypt, Iran, Iraq, Lebanon, Pakistan, Palestine ([8]) and Syria (European Council on Refugees and Exiles, 2024), along with Libya, Morocco, Sri Lanka and some countries in central Asia.

In the model of the foreign factor, a two-component system ensures the safe passage of illegal immigrants through migrant-smuggling channels. The primary element that guarantees their safety is money. Typically, the funds are supplied by family members in the immigrants' home countries, while friends and relatives in the host or destination countries provide the necessary criminal contacts and connections.

It is important to note that, for illegal immigrants, this type of criminal activity is often not seen as morally reprehensible. Many individuals within their networks provide help – such as information or connections – without expecting financial compensation. The monetary factor becomes critical when services are required, especially when the foreign factor interacts with the local factor in various host countries.

This activity has given rise to specialised networks involving individuals – often foreign citizens in host countries – who have established strong, trustworthy connections with OCGs from high-risk criminal environments. These individuals act as facilitators, linking the demands of the foreign factor with the logistical capabilities of the local factor. They are capable of arranging services such as transportation, temporary accommodations and *ad hoc* solutions for illegal immigrants either attempting to cross borders or already present in the host countries.

The financial transactions supporting this system often rely on the well-documented Hawala method (FATF, 2022). In this model, third-party guarantors hold the funds until the agreed-upon service is completed. Once the service is verified, the money is released to the criminal actor facilitating the operation.

In Bulgaria, recent cases reveal that criminals representing the local factor frequently use video verification to confirm the safe delivery of illegal immigrants. Typically, low-level operatives or field captains record a video at the final destination, showing that all of the immigrants are alive and well. This footage serves as evidence for the guarantor, who then authorises the release of the funds. Once released, the money is transferred to the criminals involved in the local factor's operations, completing the transactional cycle.

If we are to describe the roles within the foreign factor, the following model emerges.

1. **Head connection.** This individual is typically a refugee – documented or not – or a professional criminal native to countries in the Middle East, North Africa or central Asia. They operate within the current host country where the illegal immigrants are in transit. The head connection maintains reliable relationships with various OCGs, their representatives and leaders. Additionally, they maintain contact with groups of illegal immigrants or foreign-factor agents in countries where immigrants are being hosted. Their primary

([8]) This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of the Member States on this issue.

responsibility is to secure clients for the local factor by leveraging their network of trust. An essential skill for this role is the ability to communicate in at least one language spoken by the local factor's representatives.

2. **Middle connections.** Subordinates of the head connection, these individuals act as intermediaries between the head connection and either OCG representatives within the local factor or groups of illegal immigrants. Their responsibilities include ensuring that OCGs in need of clients (illegal immigrants) connect with immigrants seeking their services. They play a crucial role in maintaining the flow and support at each stage of the criminal network. For instance, in Bulgaria, head connections with strong ties to high-risk local OCGs often rely on middle connections in Türkiye that consistently supply them with clients for their criminal 'tour operations'.

3. **Accountant.** This role involves managing the financial aspects of the operation. The accountant oversees the transfer of funds from illegal immigrants, which can originate from their personal bank accounts, cryptocurrency wallets or third-party representatives linked to family members in their home countries or relatives in central and western Europe.

4. **Driver or host.** In certain cases, the foreign factor may attempt to function as the local factor. There have been instances where illegal immigrants or citizens from non-EU countries take on responsibilities independently, managing the entire process themselves. These roles are similar to those of the local factor, involving tasks like providing accommodation to hide illegal immigrants or transporting them between locations.

As mentioned earlier, the roles within these models are often interchangeable, with individuals performing multiple functions depending on the situation. The foreign factor primarily represents service seekers, while the local factor constitutes service providers within the overall criminal network.

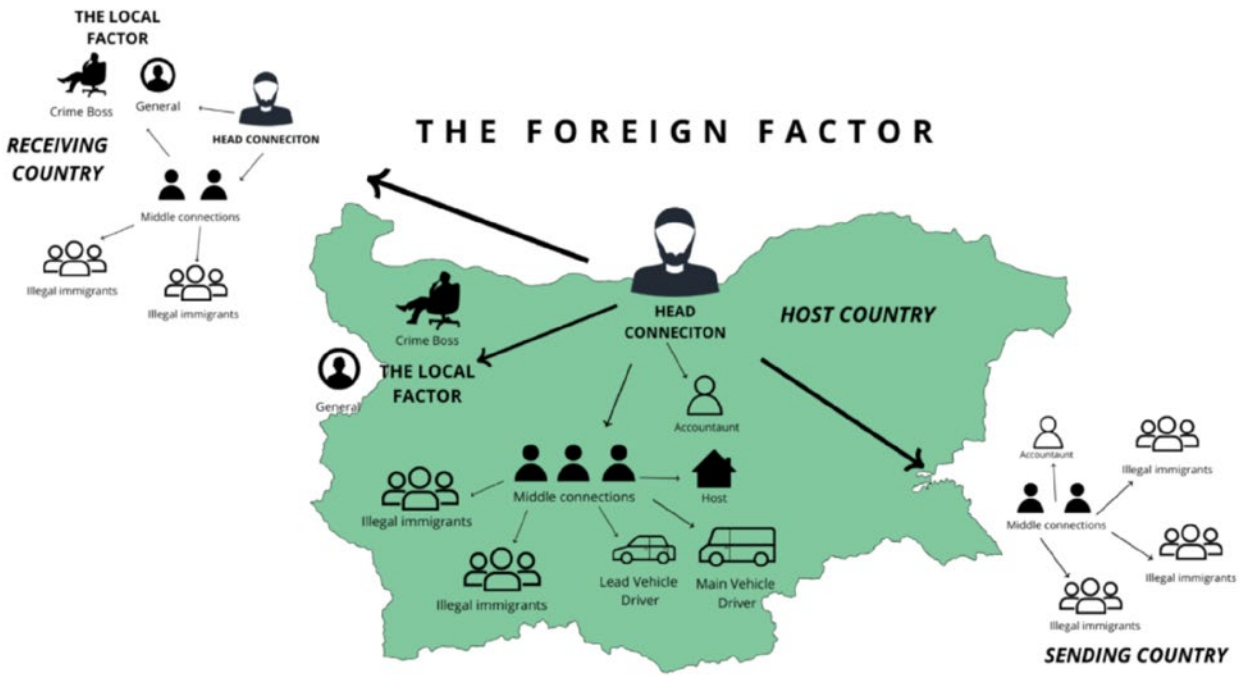


Figure 3.4. Schematic representation of the foreign factor model

NB: The provision of transport and hosting services is optional and not typically the responsibility of the foreign factor. These tasks are generally undertaken by the local factor, while the foreign factor primarily ensures a consistent supply of illegal immigrants to sustain the criminal network chain.

In conclusion, the foreign factor often comprises individuals who are well established within the host country. Some of these individuals operate legal businesses that directly or indirectly support the roles within the criminal networks. Their involvement can vary, but they frequently facilitate the gathering and movement of illegal immigrants or refugees.

In non-EU countries, such as Türkiye, similar hubs exist. However, in these locations, the gatherings typically attract individuals with well-established connections to criminal groups operating in Bulgaria. These hubs act as critical nodes in the network, bridging the foreign factor with local factors in host countries.

The internet also plays a significant role in facilitating these operations. Online platforms provide a continuous and accessible avenue for establishing contact with head connections or middlemen based in Bulgaria. These intermediaries can easily connect potential clients with OCGs specialising in migrant smuggling, effectively extending the reach and efficiency of these illicit networks.

The factor of criminal and non-criminal actors

Throughout this paper, we have referred to legal activities and entities – such as rent-a-car companies, non-European foreign nationals with legitimate businesses, government institutions and law enforcement personnel – that become directly or indirectly involved in the crime of migrant smuggling. In this section, we analyse the roles of these non-criminal actors and their cooperation with the criminal factors described earlier.

It is essential to recognise that illegal immigration is a multifactorial phenomenon. Even the smallest aspect of this crime on a larger scale requires some form of collaboration between two or more individuals. Unlike crimes such as burglary, assault or drug dealing, migrant smuggling inherently connects various spheres of society with the criminal underworld. This interconnectedness highlights the significant threat that illegal immigration poses to national security.

Below are examples and an analysis of different modi operandi and their actors within Bulgaria. The list remains dynamic and adaptable, reflecting the evolving tactics of high-risk criminal networks involved in migrant smuggling.

Rent-a-car companies

Rent-a-car companies play a pivotal logistical role in migrant-smuggling operations, particularly at the national level. When private vehicles or buses are used, they are easier to trace, prompting OCGs to adapt by frequently using rental cars and buses. Over time, this has fostered a growing collaboration between the private sector and law enforcement agencies.

However, not all rent-a-car companies comply with law enforcement efforts. Many continue to support criminal activities by neglecting to scrutinise their clients or their travel records. In some cases, rent-a-car companies are purposefully established as legal entities to serve criminal networks, providing a steady supply of untraceable vehicles for smugglers.

This tactic is critical to OCGs' operations because, when drivers transporting illegal immigrants are apprehended, the vehicles – and their connections to the companies – often remain undetected. Frequently, even the drivers themselves are unaware that they are using vehicles tied to front companies established by OCGs.

Fictional owners and proxy users

Another tactic involves individuals of low socioeconomic status who are used as proxy owners of multiple cars, phone numbers, private companies or even properties. These individuals are offered small financial incentives to register assets in their names, which are then exploited for criminal activities.

- **Vehicles.** Cars may be purchased or transferred under the proxy owners' names to avoid direct connections to the OCGs. These vehicles are then used in smuggling operations.
- **Phone numbers.** Mobile numbers linked to key figures in the criminal network are often registered under proxy owners, creating a layer of anonymity and breaking the chain of traceability to the actual operators.
- **Companies.** Shell companies established under the names of proxy owners serve as legal facades to launder money or provide logistical support, such as renting properties or vehicles for smuggling activities.

By leveraging these fictional or proxy owners, criminal networks effectively obscure their operations and shield themselves from direct accountability.

Food and drink establishments

Certain food and drink establishments, particularly those owned by non-Europeans (the foreign factor), often become hotspots for meetings where connections are established. Illegal immigrants or their intermediaries can easily find criminal contacts in well-known venues run by individuals from Türkiye or other non-EU countries.

It is crucial to note that this observation is not a generalised judgement against all non-European foreigners in Bulgaria. However, as previously discussed, many refugees or individuals fleeing war or poverty do not feel a moral obligation to adhere to Bulgarian laws. Often, the services provided at such establishments are perceived as favours to help someone in need. In some cases, intermediaries at these locations accept financial incentives for facilitating these connections.

TIR and truck parking lots

Truck parking lots, where Transports Internationaux Routiers (international road transport or TIR) vehicles (i.e. large cargo trucks) are hosted, sometimes serve as hubs for the exchange of illegal immigrants between different truck drivers. This can occur with or without the knowledge of the parking lot owners.

Within the trucking community, such parking lots are also centres for exchanging information about corrupted firms or drivers willing to participate in smuggling operations. This phenomenon is particularly notable in parking lots owned by Turkish nationals or individuals from other non-European backgrounds, where connections between drivers and OCGs may be established.

Non-Europeans with high social status

Non-Europeans with prominent social or economic standing in their communities often play complex roles in these activities. As respected leaders, they may feel a moral or social obligation to support migrant smuggling, seeing it as a form of altruism or as a way to bolster their reputation within their communities.

In some cases, these individuals face significant pressure from their minority groups to assist refugees in need. However, others exploit this situation for personal financial gain, leveraging their status to facilitate smuggling operations while enhancing their social or economic position.

Political party representatives, government employees and law enforcement personnel

These groups are categorised together due to their ability to exploit state power and influence to support or participate in migrant-smuggling activities. Corruption among state officials is typically driven by financial incentives, although other factors such as social or political pressures may also play a role.

An illustrative example involves representatives from a foreign embassy who were caught transporting illegal immigrants. Notably, this embassy was not from an Arab state, emphasising that corruption and involvement in smuggling activities are not confined to any specific region or culture.

Places of worship

Places of worship often serve as natural gathering points for refugees and illegal immigrants. These locations provide an environment where individuals in similar or related circumstances can connect. Frequently, they also facilitate interactions between various actors of the local or foreign factors.

Such places are sometimes used as camouflage, allowing illegal immigrants to blend in with legal residents and avoid detection. Due to the sensitive nature of law enforcement operations near religious sites, these areas are often perceived as safe zones from police checks or interventions. This complicates the efforts of law enforcement to disrupt the criminal networks exploiting these spaces.

Volunteer and paramilitary groups

Volunteer and paramilitary groups also play a significant role in the dynamics of migrant smuggling in Bulgaria. On one end of the spectrum, organisations like the Mission Wings Foundation (FAR, 2024) operate independently in the Bulgarian–Turkish border region to provide humanitarian assistance to illegal immigrants. While their intentions may be altruistic, their activities can inadvertently support illegal migration, creating challenges for law enforcement and border control. On the other end are paramilitary groups and self-organised volunteers that pose a direct threat to national security, as illustrated by the following examples.

- Paramilitary organisations have been observed operating in the region, often with the stated aim of protecting national borders. However, their unregulated activities have been associated with the mistreatment of illegal immigrants and the undermining of the authority of government forces (Ignatov, 2022).

- Volunteer groups led by convicted criminals, who use their public ambitions to gain influence, have also been reported (Shikerova, 2021). These groups have been accused of taking matters into their own hands, including through committing crimes against migrants in irregular situations, further complicating border security and enforcement efforts.

The dual pressures faced by the government are substantial. On one side, law enforcement must contain and manage paramilitary groups attempting to assert their authority in the region. On the other, they must address the continuous influx of illegal immigrants who seek to exploit the border region's vulnerabilities and establish connections with local criminal actors.

In conclusion, these sections highlight the symbiosis between strategically significant resources, locations and non-criminal spheres of business and social life, which are often exploited by criminal networks. OCGs capitalise on these naturally available opportunities or deliberately create them to gain an advantage in their high-risk criminal activities. This relationship between the legal and illegal spheres illustrates the complexity and adaptability of criminal networks involved in migrant smuggling.

The geopolitical factor

When we look beyond the hotspot zones in Bulgaria or the high-risk criminal networks operating across the Balkan peninsula to profit from criminal activities such as smuggling people from the Middle East, North Africa or central Asia, a distinct pattern begins to emerge. This pattern is evident in recent terrorist attacks in Europe connected to illegal immigrants (McGuinness and Gozzi, 2024) (Sinha, 2022), and in various professional and academic risk-assessment methodologies that reflect observations obtained through the author's professional experience in countering high-risk migrant-smuggling networks in Bulgaria.

The same patterns and conclusions are echoed in Europol's 2023 report on terrorism, which documents specific cases illustrating connections between illegal immigration and the national security of states. In some documented instances, terrorist organisations and lone-wolf radicals have sought to exploit the resources of OCGs to enter European nations, as illustrated by the case cited below. The strategic importance of Bulgaria as a geopolitical factor and a primary entry point to Europe is emphasised in the report, which notes that: 'In August 2022, a Moroccan foreign terrorist fighter (FTF) was arrested in Spain and another Moroccan FTF was arrested in Austria before being extradited to Spain. They had travelled together, entering the EU irregularly from Türkiye, passing through Bulgaria and the Western Balkan route (Europol, 2023).

The conventional criminal networks that facilitate international crime are exploited by foreign actors with malicious intentions. Through the pathways these criminal sectors create, there exists documented potential for exploitation by actors with such intentions (Europol, 2023). Illegal immigration – defined in criminal terms as migrant smuggling – extends beyond a criminal activity with significant financial and social repercussions. Security analysts have identified migrant-smuggling channels as a potential vulnerability that may be exploited by actors seeking to undermine regional stability and the national security of the state, highlighting the broader security dimensions of this phenomenon.

To underscore the significance of this factor with objectivity rather than prejudice, it is essential to highlight the documented associations between criminal involvement and radicalisation, particularly in the form of terrorist activities (Colomina et al., 2017), and especially within the younger immigrant populations (Bergen, 2017; Todorov, 2015). The psychology underlying individual cases of radicalisation and criminalisation is not novel. Some fall into the cycle of violence and lawlessness simply due to an inability to adapt effectively to the values and lifestyles of the modern Western world. Rather than becoming constructive members of society who could reap the benefits of peace, prosperity and stability, they remain alienated and marginalised, creating fertile ground for both terror and criminality (Madzharov, 2017). For others, personal histories or connections – such as the loss of family members, ties to individuals within terrorist organisations or lifelong exposure to criminal or extremist environments – ultimately shape their paths (Madzharov and Andonova-Tsvetanova, 2020).

The psychological factors that influence criminal and terrorist behaviours are strikingly similar, as are the methods of operation employed by OCGs and terrorist networks in their development, establishment and recruitment processes (Atanasov, 2022). A number of illegal immigrants entering Bulgaria carry their past experiences and histories, deeply ingrained in their identities. It can be reasonably assumed that among the illegal immigrant groups there are individuals who were actively engaged in combat, including ex-soldiers and veterans from foreign armies or militias. The reintegration of combat veterans from developed countries into society already poses a significant challenge. Adapting combatants from different cultural backgrounds presents an even greater difficulty, even in the absence of malicious or terrorist intentions.

The geopolitical implications of this phenomenon are highly significant, even for the illegal immigrants themselves. This importance is reflected in the symbolic terms and names used in their online communities or anonymous profiles, such as 'The road of the martyrs' or 'The village of the martyrs' (referring to Edirne, Türkiye).

The convergence of all these factors illustrates the challenge posed by the geopolitical dimension to Europe. Over time, the accumulation of various criminal elements and terrorist threats evolves into a substantial risk to the national security of the European Union and each individual Member State, ultimately influencing Europe's strategic and geopolitical standing on the world stage and shaping its perception among global rivals.

Conclusion

The findings of this study provide a comprehensive examination of the complex mechanisms, trends and structures underpinning organised criminal networks involved in migrant smuggling in Bulgaria – a key transit country in Europe.

This research underscores five critical factors shaping these criminal operations: geosocial, local, foreign, criminal/non-criminal actors and geopolitical influences. Each of these factors contributes to the adaptability and effectiveness of these networks in exploiting geographical, economic and social vulnerabilities. The analysis of their modi operandi reveals sophisticated strategies, including the use of the terrain, coordinated vehicle convoys and clandestine logistical hubs, which enable the seamless movement of illegal migrants. Furthermore, the networks display a dynamic integration of local and foreign actors, with a hierarchy that efficiently balances leadership, operational roles and financial systems.

Key conclusions include the following.

1. **Geosocial factor.** Bulgaria's strategic geographical location places it at the nexus of major migratory routes, such as the Western Balkan and Eastern Mediterranean pathways, making it a critical gateway for illegal migration into Europe. This factor, combined with its sociopolitical dynamics – including economic vulnerabilities and proximity to conflict regions – provides fertile ground for organised criminal networks to thrive.

2. **Local and foreign factors.** A seamless collaboration between domestic criminal infrastructures and foreign agents ensures the continuity of smuggling routes. The local factor facilitates transit and shelter, while the foreign factor coordinates funding and migrant flow.

3. **Criminal and non-criminal actors.** Criminal groups exploit legitimate enterprises, such as car-rental services and local businesses, and sometimes rely on corrupt officials. This nexus between legality and illegality complicates law enforcement efforts.

4. **Geopolitical implications.** Documented cases illustrate potential security-related interconnections, including specific instances where migrant-smuggling routes have been utilised by radicalised individuals, further emphasising the strategic importance of Bulgaria in European border security.

This study highlights the need for multifaceted strategies to combat these high-risk criminal networks. Enhanced international cooperation, intelligence sharing and targeted operational measures are essential. Furthermore, addressing socioeconomic disparities that fuel recruitment into these networks, along with stricter regulatory oversight of vulnerable sectors, is critical.

In conclusion, the integration of criminological, policing and intelligence frameworks offers a robust foundation to counter the evolving tactics of organised criminal networks. As Bulgaria continues to be a critical point of illegal migration, its experiences and strategies can inform broader European policies aimed at dismantling these illicit structures and safeguarding the pathways to Europe.

References

Atanasov, A. (2022), 'Local, homegrown terrorism and organized crime in the Western societies', *De Re Militari Journal*, Issue 7, pp. 2–9, https://drmjournal.org/wp-content/uploads/2022/06/de-re-militari-eng-issue-7.pdf.

Bergen, P. (2017), 'Bergen: A pattern in terror – second generation, homegrown', CNN website, https://edition.cnn.com/2017/05/24/opinions/homegrown-terrorism-opinion-bergen/index.html.

Britannica Editors (2024), 'Modus operandi', Encyclopedia Britannica website, https://www.britannica.com/topic/modus-operandi.

Bulgarian National Television (BNT) (2023), 'National statistics: Bulgaria remains the poorest country in the EU in terms of GDP distribution', BNT website, https://bnt.bg/news/national-statistics-bulgaria-remains-the-poorest-country-in-the-eu-in-terms-of-gdp-distribution-316332news.html.

Colomina, P., de France, O. and Saverot, D. (2017), From Criminals to Terrorists and Back? Quarterly report: France Globsec, Bratislava, https://www.iris-france.org/wp-content/uploads/2019/01/From-Criminals-To-Terrorists-And-Back-Quarterly-Report-France-Vol-2.pdf.

European Council on Refugees and Exiles (2024), 'Bulgaria: Statistics', Asylum Information Database, https://asylumineurope.org/reports/country/bulgaria/statistics/.

Europol (2023), *European Union Terrorism Situation and Trend Report 2023*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2813/302117.

Europol (2024), *Decoding the EU's Most Threatening Criminal Networks*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2813/811566.

Eurostat (2023), 'Immigration law enforcement in the EU: 2022 figures', Eurostat website, https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20230505-2.

FATF (2022), *Money laundering and terrorist financing risks arising from migrant smuggling*, FATF, https://www.fatf-gafi.org/content/dam/fatf-gafi/brochures/Migrant-smuggling-handout.pdf.

Foundation for Access to Rights (FAR) (2024), 'Foundation Mission Wings', FAR website, https://refugeelight.bg/en/service-providers/missionwings.

Frontex (2024), 'Significant rise in irregular border crossings in 2023, highest since 2016', Frontex website, https://www.frontex.europa.eu/media-centre/news/news-release/significant-rise-in-irregular-border-crossings-in-2023-highest-since-2016-C0gGpm.

Ignatov, T. (2022), 'A paramilitary organisation in Bulgaria is being investigated for a crime against the state', BNT website, https://bntnews.bg/news/razsledvat-paravoenna-organizaciya-u-nas-za-prestaplenie-sreshtu-darzhavata-obzor-1217405news.html.

Madzharov, E. (2017), 'Personality and psychological characteristics of the participants in organized criminal groups', Academy of the Ministry of the Interior, Sofia [unpublished manuscript].

Madzharov, E. and Andonova-Tsvetanova, Y. (2020), 'Research on individuals, members of organized crime groups with the Dark Triad Questionnaire', *Psychological Research*, Vol. 23, No 2, pp. 203–214.

McGuinness, D. and Gozzi, L. (2024), 'Scholz vows to speed up deportations after Solingen stabbings', BBC website, https://www.bbc.com/news/articles/cj081mrlm7eo.

Mediapool (2023), 'A 23-year-old policeman caught transporting migrants had to pay off a loan', Mediapool.bg website, https://www.mediapool.bg/23-godishen-politsai-hvanat-da-prevozva-migranti-imal-da-izplashta-kredit-news343498.html.

Shikerova, G. (2021), '"They started running on the road." Does the Ministry of Interior work with people like Dinko, the "refugee hunter"?', Radio Free Europe / Radio Liberty website, https://www.svobodnaevropa.bg/a/31585692.html.

Sinha, S. (2022), 'Migration and terrorism in Europe: A nexus of two crises', *International Journal on Responsibility*, Vol. 5, Issue 1, Article 7, https://commons.lib.jmu.edu/ijr/vol5/iss1/7/.

Todorov, V. (2015), 'Modern trends in the psychology of terrorism', Academy of the Ministry of the Interior, Sofia [unpublished manuscript].

UNODC (2004), *United Nations Convention against Transnational Organized Crime and the protocols thereto*, UNODC, Vienna, https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

Using survey data from offenders on the Dark Web to combat online child sexual abuse and exploitation

Hanna-Mari Lahtinen, Kirsi Honkalampi, Tegan Insoll, Juha Nurmi, Anna Ovaska, Nina Vaaranen-Valkonen

https://doi.org/10.3013/jja40744

Abstract ([9])

A 2024 report by the Childlight Global Child Safety Institute reveals that over 300 million children are victims of online sexual abuse and exploitation annually, indicating a hidden global pandemic. As a form of cybercrime, child sexual exploitation is one of the EU's priorities in the fight against serious and organised crime, and the European Union Agency for Law Enforcement Cooperation has recognised Dark Web networks as one of the key threats in child sexual exploitation. Most child sexual abuse material (CSAM) offenders remain undetected, limiting our knowledge of their motivations and behaviours. Existing research has largely relied on samples of convicted offenders, potentially overlooking important nuances within the broader offending population. This paper presents a model to collect data from CSAM offenders on the Dark Web and summarises results from a study on the data, focusing on differences between charged and uncharged CSAM users. Data includes responses from 3 782 anonymous offenders actively searching for CSAM or seeking help for their use of CSAM on the Dark Web. We compare three groups of CSAM searchers: (1) those admitting charges of sexual crimes against children; (2) those admitting charges of sexual crimes against adults; and (3) those admitting no charges. Additionally, we discuss the implications of the research for practitioners and how to use this information to target prevention strategies more effectively.

Keywords: CSAM offenders, Dark Web, sexual offending against children, data collection, hidden crimes.

([9]) This article is based on work from COST Action CA22128 (ImpleMéndez), supported by European Cooperation in Science and Technology (COST).

Introduction

The recently published European Union Agency for Law Enforcement Cooperation (Europol) report titled *EU Serious Organised Crime Threat Assessment* (Europol, 2025) identified child sexual exploitation as one of the key threats to the EU's internal security and a priority for the EU in combating serious and organised cybercrime under the 2022–2025 European multidisciplinary platform against criminal threats (Empact). Europol (n.d.) has identified Dark Web networks as a major threat contributing to this form of exploitation. Worryingly, evidence of child sexual abuse material (CSAM) linked to human trafficking is also emerging (National Center for Missing and Exploited Children, 2024).

One of the key challenges in combating sexual crimes against children is that they frequently go undetected by authorities (Lahtinen, 2022; Priebe and Svedin, 2008), and this is particularly true for victims of online child sexual exploitation and abuse (OCSEA). These victims seldom report their experiences to authorities (Colburn et al., 2023; Gemara et al., 2023), even when they have evidence such as photos, videos and messages. In OCSEA cases, reluctance to disclose and even denial of the events, despite evidence, pose significant challenges in criminal investigations, especially when human trafficking is involved (e.g. Lavoie et al., 2019). Consequently, few CSAM offenders are detected by law enforcement.

Most of the research on CSAM offenders has focused on forensic, clinical or community samples. The problem with these samples is that they are unrepresentative of child sex offenders (Salter et al., 2023a). Recently, research using online forums to collect data has increased. However, as Roche et al. (2025) showed, samples in these studies consist mostly of white men, between the ages of 18 and 35, living in North America or Europe. Thus, generalising findings from these studies to all CSAM offenders is problematic and more diversified recruitment methods are needed. Also, as recent research indicates, the types of CSAM crimes reported to police may differ from the types of crimes reported by victims in victim surveys (Finkelhor et al., 2023; Quayle et al., 2018). Therefore, research involving offenders undetected by law enforcement, based on more diverse samples, is needed to develop more effective measures to reveal, investigate and prevent these crimes.

A recent nationally representative study by Salter *et al.* (2023b) examined the prevalence of child sexual offending behaviours and attitudes among men in Australia, the United Kingdom and the United States. The study found that men who self-report online sexual offences are more likely to seek sexual contact with children if they are certain that no one would find out. In line with this finding, Insoll et al. (2022) indicated that 42 % of CSAM searchers on the Dark Web had tried to directly contact children online after viewing CSAM, and even more (58 %) reported feeling afraid that viewing CSAM might lead to sexual acts with a child or an adult. The study was based on a large sample of CSAM searchers on the Dark Web. These findings contrast with several previous studies, mainly based on forensic and clinical samples (see, for example, Babchishin et al., 2018, for a review), which estimate a relatively low risk for contact sexual abuse among CSAM users. Research (Napier et al., 2024; von Franqué et al., 2023) also indicates that CSAM use often persists after initial exposure, significantly increasing the risk of escalating to direct contact and endangering more children. These findings again underline the urgent need for studies that include larger samples of CSAM users outside of the criminal justice system and anonymous clinical services.

Multiple factors have been associated with sexual offending based on previous studies with samples of convicted offenders (e.g. Ward and Beech, 2006), yet a comprehensive understanding of what differentiates child sexual

abusers from non-abusing individuals remains elusive (Seto, 2019). While sexual interest in children is a known risk factor, not all individuals with paedophilia engage in offending behaviour (Finkelhor, 1984; Seto, 2019), highlighting the complexity of the issue. To account for these nuances, Seto (2019) proposed the motivation–facilitation model, which identifies paraphilic interests, high sex drive and intense mating effort as core motivations. Facilitators include trait factors (e.g. antisocial personality) and state factors (e.g. alcohol use), while situational elements – such as victim accessibility and lack of guardianship – interact with personal traits to influence offending risk.

The volume of reported CSAM has increased tremendously during the last decade. For example, a recent report by the Childlight Global Child Safety Institute (2024) revealed that over 300 million children are victims of online sexual abuse and exploitation annually. Furthermore, according to the *Global Threat Assessment 2023* (WeProtect Global Alliance, 2023), the US National Center for Missing and Exploited Children has reported analysing 32 million reports in 2022 (an 87 % increase compared with 2019), and the Internet Watch Foundation (2024) has observed that material is more extreme and violent compared with its earlier findings. Along with social media and the Surface Web, the Dark Web is one of the key forums where CSAM is shared. Nurmi et al. (2024) recently showed that the availability of CSAM on the Dark Web is alarming: one fifth of the onion domains on the Tor network share CSAM, it is easily available by using 21 out of 26 most-used Tor search engines, and 11.1 % of the search sessions using one of the Dark Web search engines – Ahmia.fi – were seeking CSAM despite the removal of CSAM websites from its search results and the blocking of CSAM queries. These findings collectively highlight the alarming extent of CSAM and justify prioritising child sexual exploitation in the fight against serious and organised crime, as part of the 2022–2025 Empact programme (Empact, n.d.).

To develop effective interventions to stop the sharing and using of CSAM, we need more knowledge from the offenders, including those undetected by law enforcement and those operating on the Dark Web. In this paper, we first present a model to collect data from CSAM offenders on the Dark Web. We aimed to develop a sustainable and replicable data collection model on OCSEA for national and international data collection. Through the model we aimed to gain a broader understanding of common patterns and trends of OCSEA. We specifically highlight the potential that the model has in collecting data from anonymous perpetrators on the Dark Web. Second, we illustrate the kind of information it can provide and how it can be used in the fight against CSAM crimes by presenting some of the key findings from a scientific study on the data (Lahtinen et al., 2025). We were interested in analysing the number of both legally charged and uncharged CSAM searchers and whether they differed in their individual, motivational and behavioural characteristics. To investigate this, we compared three groups of anonymous CSAM searchers on the Dark Web based on their self-reports: (1) those admitting charges of sexual crimes against children; (2) those admitting charges of sexual crimes against adults; and (3) those admitting no charges. This paper builds on a study previously published in the *Child Abuse and Neglect* journal. While the original paper presented the full research findings, the current paper focuses on the data collection model used in the study and highlights key results with direct relevance to law enforcement professionals. The aim is to support practitioners in identifying and responding to cases more effectively by translating research insights into actionable knowledge.

Methodology

The data collection model

We created an anonymous online 'Help us to know' survey that is shared via a Dark Web search engine – Ahmia.fi. According to Winter et al. (2018, p. 420), one of the most popular ways in which almost half of Tor users discover onion sites was through search engines such as Ahmia.fi. Ahmia.fi not only filters these websites, but also blocks the searches indicating sexual violence against children. Individuals who search for CSAM with the search engine get an invitation to participate in the survey instead of the search results they were looking for. They can choose to respond to the survey or not. They are also offered links to relevant online and offline help resources, including the ReDirection Self-Help Program (n.d.), for example. The programme is designed to support behavioural change and reduce the consumption of CSAM with the help of techniques based on cognitive behavioural therapy.

The survey includes 37 mandatory questions (available in 15 languages), with an option to select 'Prefer not to say' for any question. We collected both quantitative and qualitative data, including basic demographic information such as age (categorised) and gender. The survey combines validated measures (the Sexual Child Molestation Risk Assessment A and B to measure the self-reported frequency of sexually abusive behaviour in the past week (Landgren et al., 2020)) and custom-developed questions tailored to the study's purposes. The questions encourage respondents to reflect on their use of CSAM to understand the pathways and motivations behind their behaviour. Topics include known risk factors from previous research, such as child sexual abuse and CSAM perpetration, sexual interest in children, offender preferences for victim age and gender, CSAM use behaviour, adult pornography use and criminal behaviour. Situational factors and facilitators are also explored.

The survey also examines contact-seeking behaviour, specifics of contact with children and acts of sexual violence, whether physical or remote. Prior criminal behaviour is explored by asking respondents whether they have ever been legally charged with a violent offence or sexual offence (separate questions), with options for 'Yes, against an adult', 'Yes, against a child', 'No' and 'Prefer not to say'. An honesty check question at the end assesses how truthful participants were and their perception of others' honesty in the survey. For a more detailed description of the data collection model and the survey, see Insoll et al. (2024) and Lahtinen et al. (2025).

Ethical considerations

One of the key principles of research ethics is to avoid causing harm to participants. When collecting sensitive data on potential offences against children, the risk of psychological distress – including self-harm or suicidal thoughts – must be considered. Therefore, participants should be provided with information on accessing mental health support (Finnish National Board on Research Integrity, 2023). This model enabled us to provide the links to support resources both before the respondent even decided to respond to the survey and after they had finished answering questions.

To ensure respect for participants' rights, it is crucial that they voluntarily consent to participating and are clearly informed about the study's purpose and risks (informed consent). For sensitive data, maintaining strict confidentiality and preserving participants' anonymity is essential. Any personally identifiable information must be collected in accordance with relevant data protection laws (Finnish National Board on Research Integrity, 2023). For this reason,

the survey contained only a few questions on demographic information, and conducting the survey on the Dark Web virtually guarantees the anonymity of respondents.

When conducting online surveys, it is important to ensure that data is collected only from adults, as different ethical standards apply to children. Age can be verified through screening questions or consent forms. We decided to use a screening question asking respondents to confirm that they were at least 18 years old. The ethical aspects of this data collection model and research done based on it were evaluated and approved by the University of Eastern Finland Committee on Research Ethics.

Research methodology

In the first study we conducted based on the data (Lahtinen et al., 2025), we analysed the responses from the 3 782 anonymous offenders who were actively searching for CSAM or seeking help for their use of CSAM on the Dark Web and chose to respond to the English-language version of the 'Help us to know' survey between 1 July 2023 and 1 March 2024. Participants who indicated in the honesty check that they had not been honest in answering the questions (n = 627) were excluded from the analyses, along with those who did not to respond to the question on charges for sexual offences (n = 771). The final sample consisted of 2 384 respondents (63.0 % of the total sample).

To investigate the individual, motivational and behavioural characteristics predicting charges for sexual crimes against children or adults, we formed three groups based on responses to the question: 'Have you ever been charged with a sexual offence (e.g. indecent exposure, sexual coercion, rape, sexual abuse, child sexual abuse material offences, sexual harassment, grooming)?' Participants who answered 'Yes, against a child' (n = 474; 19.9 %) were assigned to the child sexual abuse offenders (CS) group. Those who answered 'Yes, against an adult' (n = 620; 26.0 %) were assigned to the adult sexual abuse offenders (AS) group. Respondents who selected 'No' (n = 1 290; 54.1 %) were placed in the no charges (NC) group. Additionally, 87 participants who reported charges for offences against both children and adults were included in the CS group.

Results

Characteristics of the sample

Among the final sample of participants, which totalled 2 384 individuals, 77.5 % identified as men. Meanwhile, 10.4 % identified as women, 4.6 % identified as non-binary and 7.6 % preferred not to disclose their gender. Most respondents (76 %) were young adults (18–34 years old) (see details in Figure 4.1 and Lahtinen et al., 2025). A little over half (54.1 %) reported having no charges for sexual offences. Additionally, 17.3 % of all respondents reported charges for other violent crimes against children, and 25.8 % reported charges for other violent crimes against adults.

Age group	n	Percent
18-24 years old	1210	51
25-34 years old	600	25
35-44 years old	249	10
45-54 years old	125	5
Over 55 years old	65	3
Prefer not to say	135	6

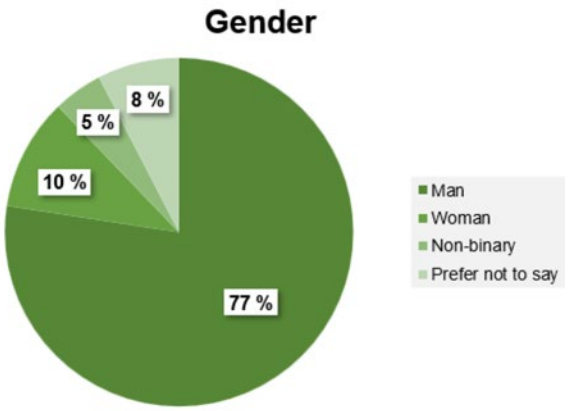


Figure 4.1. Age and gender of the participants

Recent analyses of the data by Insoll et al. (2024), based on a larger sample of 4 549 respondents, showed that 35 % of them found the survey when looking for help to stop using CSAM, and 41 % of respondents believe that it is possible to stop using CSAM. Many participants responded to the question about their feelings after answering the survey that simply completing the survey made them stop and reflect upon their own behaviour.

Summary of findings from the bivariate and multivariate analyses

First, we tested which variables in the data were associated with being charged for a sexual crime against a child (CS group) or an adult (AS group) with chi-square tests. Some of the key differences observed are described in Figures 4.2 and 4.3. All groups were most interested in the material depicting girls. However, we found significant differences in age preferences between the groups. The AS offender group reported most often that they were interested in the youngest category (infants and toddlers) (see details in Figure 4.2).

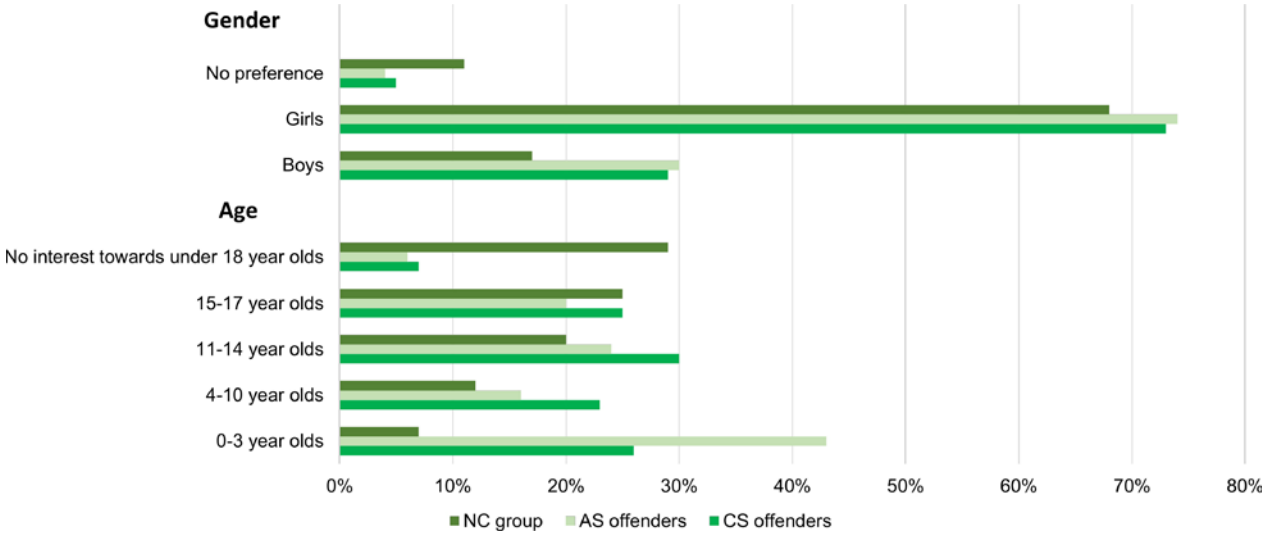


Figure 4.2. Victim preferences related to gender and age

From the motivational factors tested, sexual interest in children and desensitisation to adult pornography were associated with belonging to either the AS or the CS group. The AS group reported the highest percentage of sexual interest in children (78.9 %, with corresponding proportions of 52.5 % in the CS group and 34.1 % in the NC group). Desensitisation to adult pornography was most common in the NC group (20.2 %, with corresponding proportions

of 8.4 % in the CS group and 12.6 % in the AS group). Several behavioural factors – such as habitual viewing of adult pornography, watching CSAM for sexual arousal, grooming children and seeking physical contact or direct remote contact with a child – were associated with belonging to groups of sexual abuse offenders (AS or CS groups). Figure 4.3 describes that most respondents had neither groomed nor contacted children for sexual pleasure recently. CS offenders groomed and contacted children most often (see Figure 4.3).

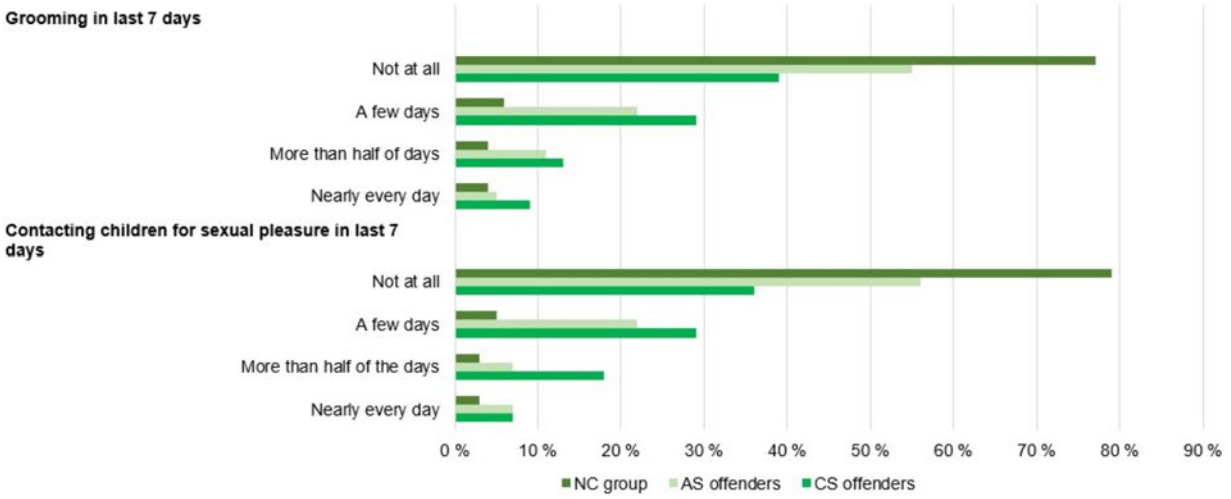


Figure 4.3. Frequency of grooming and contacting children

Second, we performed logistic regression on the variables significantly associated with belonging to either the AS or the CS group in bivariate analyses, to examine whether each variable indicated a greater likelihood of belonging to AS or CS offender groups than the NC group when the influence of other variables was controlled. These final analyses showed that four key factors predicted most of the differences between the groups: being charged with a violent offence against a child or an adult, searching for material depicting the sexual abuse of infants and toddlers, grooming children and having physical contact with children significantly increased the risk of belonging to the AS or CS group compared with the group that reported no charges (see more details in Lahtinen et al., 2025).

Conclusion

This paper emphasises the importance of using multiple data sources, including the Dark Web, for CSAM user research. Due to the hidden nature and volume of these crimes, innovative methods like using anonymous surveys of CSAM users outside of the criminal justice system are essential to complementing clinical and forensic data (see also Roche et al., 2025). The study demonstrates that engaging participants via a Dark Web search engine to reflect on their behaviour is an effective method for collecting large datasets from hard-to-reach populations. The resulting data can inform the development of both preventive strategies targeting CSAM use and tailored interventions for individuals at risk of offending. However, ethical considerations such as confidentiality and participant safety are crucial. Such studies also have their limitations. For example, participants often portray themselves positively in self-report surveys. Some respondents may have lied or exaggerated despite an honesty check at the end of the survey. It is also important to recognise that individuals accessing CSAM via the Dark Web may differ significantly from other user populations, which should be considered when interpreting the findings.

Initial findings from the anonymous Dark Web survey reveal significant differences in individual, behavioural and motivational characteristics between CSAM offenders who admitted being charged for a crime of sexual violence against a child or an adult and those who asserted no such charges. Factors like facing charges for other violent offences, searching for material depicting infant abuse, and grooming and initiating physical contact with children increased the risk of sexual crime charges. Notably, a group of adult offenders with antisocial backgrounds showed a sexual interest in children, often seeking CSAM depicting infants and toddlers and engaging in grooming or contact with children. Many of them had violent offence charges in addition to charges for sexual crimes, highlighting the need to investigate CSAM-related offences also during adult sexual crime investigations. Given that other police investigations often identify these high-risk individuals, the findings support Seto and Eke's (2024) recommendation to search for CSAM during such investigations. This approach may contribute to deterring high-risk individuals and enhancing the likelihood of detection.

Our findings also have significant implications for assessing, treating and managing the risk of individuals committing sexual offences. Adult sexual offenders with antisocial backgrounds likely require different interventions compared with those who commit sexual violence against children or use CSAM without criminal charges (see also Soldino et al., 2024). Additionally, it is crucial to assess their recidivism risk, sexual interests and potential for committing sexual crimes against children. However, it is important to remember that, although we found a population of CSAM users on the Dark Web with antisocial tendencies who might be resistant to preventive measures, a larger population lacked such tendencies and was thus likely to be more receptive to prevention. Finally, the finding that 41 % of respondents believed that it is possible to stop using CSAM is encouraging. Preventive efforts should be strategically directed towards this population. Based on our findings, it appears that Dark Web search engines – and potentially Surface Web search engines as well – could play a role in prevention by redirecting users to support services rather than providing access to harmful content. Notably, some respondents reported that completing the survey prompted reflection on their behaviour. This finding supports the continued use of the data collection model described in this article, particularly as a tool that may contribute to the early disruption of offending trajectories.

References

Babchishin, K. M., Merdian, H. L., Bartels, R. M. and Perkins, D. (2018), 'Child sexual exploitation materials offenders: A review', *European Psychologist*, Vol. 23, No 2, pp. 130–143, https://doi.org/10.1027/1016-9040/a000326.

Childlight Global Child Safety Institute (2024), *Into the Light – Childlight global index of child sexual exploitation and abuse prevalence*, Childlight, Edinburgh, https://www.childlight.org/uploads/publications/into-the-light.pdf.

Colburn, D. A., Finkelhor, D. and Turner, H. A. (2023), 'Help-seeking from websites and police in the aftermath of technology-facilitated victimization', *Journal of Interpersonal Violence*, Vol. 38, Issue 21–22, pp. 11642–11665, https://doi.org/10.1177/08862605231186156.

Empact (n.d.), 'EU policy cycle – Empact', Empact website, https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact.

Europol (2025), *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2813/0758057.

Europol (n.d.), 'Crime areas – Child sexual exploitation', Europol website, https://www.europol.europa.eu/crime-areas/child-sexual-exploitation.

Finkelhor, D. (1984), *Child Sexual Abuse: New theory and research*, The Free Press, New York.

Finkelhor, D., Turner, H., Colburn, D., Mitchell, K. and Mathews, B. (2023), 'Child sexual abuse images and youth produced images: The varieties of image-based sexual exploitation and abuse of children', *Child Abuse and Neglect*, Vol. 143, 106269, https://doi.org/10.1016/j.chiabu.2023.106269.

Finnish National Board on Research Integrity (2023), *The Finnish code of conduct for research integrity and procedures for handling alleged violations of research integrity in Finland – Guideline of the Finnish National Board on Research Integrity TENK 2023, Helsinki*, https://tenk.fi/en/advice-and-materials.

Gannon, C., Blokland, A. A. J., Huikuri, S., Babchishin, K. M. and Lehmann, R. J. B. (2023), 'Child sexual abuse material on the darknet', *Forensische Psychiatrie, Psychologie, Kriminologie*, Vol. 17, pp. 353–365, https://doi.org/10.1007/s11757-023-00790-8.

Gemara, N., Mishna, F. and Katz, C. (2023), '"If my parents find out, I will not see my phone anymore": Who do children choose to disclose online sexual solicitation to?', *Child and Family Social Work*, Vol. 30, Issue 1, pp. 4–14, https://doi.org/10.1111/cfs.13069.

Insoll, T., Ovaska, A. K., Nurmi, J., Aaltonen, M. and Vaaranen-Valkonen, N. (2022), 'Risk factors for child sexual abuse material users contacting children online: Results of an anonymous multilingual survey on the Dark Web', *Journal of Online Trust and Safety*, Vol. 1, No 2, https://doi.org/10.54501/jots.v1i2.29.

Insoll, T., Ovaska, A. K., Lahtinen, H., Honkalampi, K. and Vaaranen-Valkonen, N. (2024), *2KNOW: Collecting Data on Hidden Online Crimes – A case study on surveying online child sexual abuse offenders*, Project 2KNOW, https://4d226c6f-2fb2-4166-936f-bae8f2513b5a.usrfiles.com/ugd/4d226c_198e2b6b1ab04086b3f21e62aa3c2f86.pdf.

Insoll, T., Soloveva, V., Díaz Bethencourt, E., Nieminen, N., Leivo, K. et al. (2024), *What Drives Online Child Sexual Abuse Offending? Understanding motivations, facilitators, situational factors, and barriers*, Project 2KNOW, https://d506e357-3e96-4c5e-9946-08adb9467f94.filesusr.com/ugd/bd9606_46894722843345d2b7c2ac675b357bf1.pdf.

Internet Watch Foundation (2024), *IWF Annual Report 2023*, https://www.iwf.org.uk/annual-report-2023/.

Lavoie, J., Dickerson, K. L., Redlich, A. D. and Quas, J. A. (2019), 'Overcoming disclosure reluctance in youth victims of sex trafficking: New directions for research, policy, and practice', *Psychology, Public Policy, and Law*, Vol. 25, No 4, pp. 225–238, https://doi.org/10.1037/law0000205.

Lahtinen, H.-M. (2022), 'Child abuse disclosure: From the perspectives of children to influencing attitudes and beliefs held by interviewers', *Dissertations in Humanities and Theology*, Vol. 181, University of Eastern Finland, http://urn.fi/URN:ISBN:978-952-61-4459-7.

Lahtinen, H.-M., Honkalampi, K., Insoll, T., Nurmi, J., Quayle, E., Ovaska, A. K. and Vaaranen-Valkonen, N. (2025), 'Investigating the disparities among child sexual abuse material users: Anonymous self-reports from both charged and uncharged individuals', *Child Abuse and Neglect*, Vol. 161, 107299, https://doi.org/10.1016/j.chiabu.2025.107299.

Landgren, V., Malki, K., Bottai, M., Arver, S. and Rahm, C. (2020), 'Effect of gonadotropin-releasing hormone antagonist on risk of committing child sexual abuse in men with pedophilic disorder: A randomized clinical trial', *JAMA Psychiatry*, Vol. 77, No 9, pp. 897–905, https://doi.org/10.1001/jamapsychiatry.2020.0440.

Napier, S. S., Seto, M. C., Cashmore, J. and Shackel, R. (2024), 'Characteristics that predict exposure to and subsequent intentional viewing of child sexual abuse material among a community sample of internet users', *Child Abuse and Neglect*, Vol. 156, 106977, https://doi.org/10.1016/j.chiabu.2024.106977.

National Center for Missing and Exploited Children (2024), *CyberTipline Report*, https://www.missingkids.org/content/dam/missingkids/pdfs/cybertiplinedata2024/2024-CyberTipline-Report.pdf.

Nurmi, J., Paju, A., Brumley, B. B., Insoll, T., Ovaska, A. K. et al. (2024), 'Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy', *Scientific Reports*, Vol. 14, 7849, https://doi.org/10.1038/s41598-024-58346-7.

Priebe, G. and Svedin, C. G. (2008), 'Child sexual abuse is largely hidden from the adult society: An epidemiological study of adolescents' disclosures', *Child Abuse and Neglect*, Vol. 32, Issue 12, pp. 1095–1108, https://doi.org/10.1016/j.chiabu.2008.04.001.

Quayle, E., Jonsson, L. S., Cooper, K., Traynor, J. and Svedin, C. G. (2018), 'Children in identified sexual images – Who are they? Self- and non-self-taken images in the International Child Sexual Exploitation Image Database 2006–2015', *Child Abuse Review*, Vol. 27, Issue 3, pp. 223–238, https://doi.org/10.1002/car.2507.

ReDirection Self-Help Program (n.d.), https://www.redirectionprogram.com.

Roche, K., Pagacz, J., Lalumière, M. L. and Seto, M. C. (2025), 'Recruitment issues in research with people who are attracted to children: A systematic review', *The Journal of Sex Research*, Vol. 63, Issue 1, pp. 1–13, https://doi.org/10.1080/00224499.2025.2484197.

Salter, M., Woodlock, D., Whitten, T., Tyler, M., Naldrett, G. et al. (2023a), *Identifying and understanding child sexual offending behaviours and attitudes among Australian men*, University of New South Wales: Australian Human Rights Institute, https://www.humanrights.unsw.edu.au/news/worlds-largest-child-sexual-abuse-perpetration-prevalence-study-recommends-significant-investment-early-intervention-measures.

Salter, M., Whitten, T. and Woodlock, D. (2023b), 'The nature of online offending against children: Representative data from Australia, UK and the USA', *Searchlight 2023 – Childlight annual flagship report*, Childlight, Edinburgh, pp. 4–7, https://www.childlight.org/searchlight/the-nature-of-online-offending-against-children-population-based-data-from-australia-uk-and-the-usa.

Seto, M. C. (2019), 'The motivation-facilitation model of sexual offending', *Sexual Abuse*, Vol. 31, Issue 1, pp. 3–24, https://doi.org/10.1177/1079063217720919.

Seto, M. C. and Eke, A. W. (2024), 'Child sexual exploitation material offenses: Differences in individual and case characteristics based on how they came to attention of police', *Police Practice and Research*, Vol. 25, Issue 6, pp. 1–19, https://doi.org/10.1080/15614263.2024.2342782.

Soldino, V., López-Pinar, C. and Carbonell-Vayá, E. J. (2024), 'Contact sex offenders with adult and minor victims: Psychopathological and criminological differences', *Child Abuse and Neglect*, Vol. 154, 106896, https://doi.org/10.1016/j.chiabu.2024.106896.

Ward, T. and Beech, A. (2006), 'An integrated theory of sexual offending', *Aggression and Violent Behavior*, Vol. 11, Issue 1, pp. 44–63, https://doi.org/10.1016/j.avb.2005.05.002.

WeProtect Global Alliance (2023), *Global Threat Assessment 2023 – Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response*, https://www.weprotect.org/global-threat-assessment-23/.

Winter, P., Edmundson, A., Roberts, L. M., Dutkowska-Żuk, A., Chetty, M. et al. (2018), 'How do Tor users interact with onion services?', in: Enck, W. and Felt, A. P. (eds), *27th USENIX Security Symposium*, USENIX Association, pp. 411–428, https://www.usenix.org/conference/usenixsecurity18/presentation/winter.

von Franqué, F., Bergner-Koether, R., Schmidt, S., Pellowski, J. S., Peters, J. H. et al. (2023), 'Individuals under voluntary treatment with sexual interest in minors: What risk do they pose?', *Frontiers in Psychiatry*, Vol. 14, https://doi.org/10.3389/fpsyt.2023.1277225.

Breaking the vicious cycle: Confiscation, whistleblowing and technological innovations in the battle against criminal networks

Victoria Koutsoupia

https://doi.org/10.3013/f22wmd70

Abstract

High-risk criminal networks operate across all EU Member States, with significant disruptive consequences for both the economy and society. The landscape of organised crime is characterised by a networked environment where collaboration among criminals is seamless, systematic and profit-oriented. The most effective approach to severely weaken these networks is by targeting their illicit gains. The most significant – and perhaps the only effective – way to disrupt the criminal chain is through the confiscation of their profits. Additionally, whistleblowing and recent developments of similar practices are explored as effective methods for dismantling criminal networks. Confiscation targets the economic lifeblood of organised crime; whistleblowing improves detection and evidentiary leads; and technology (e.g. blockchain analytics, interoperable EU systems) scales both detection and recovery. The development of new technological tools offers more opportunities than ever to detect illegal profits and, consequently, seize them. Emerging technologies, such as artificial intelligence, blockchain and big data analytics, can play an important role in combating organised crime and enhancing law enforcement efforts. This paper explores confiscation as a strategy to combat organised crime and dismantle criminal networks, utilising new technologies to efficiently and effectively extract criminal profits. Furthermore, it delves into the efficiency of whistleblowing in disbanding and punishing criminal networks and ensuring justice. The paper examines these aspects not only by scrutinising recent legal developments but also by analysing case-law and providing examples of best practices from Member States. The analysis is structured accordingly: the second section defines the phenomenon; the third section examines confiscation; the fourth section analyses whistleblowing; the fifth section discusses technology-enabled crime and enforcement responses; and the last section concludes with policy priorities and future research.

Keywords: criminal networks, confiscation, whistleblowing, emerging technologies.

Methodology

This study employs a qualitative, multi-method design combining: (1) doctrinal legal analysis of EU and Member State instruments on asset recovery and whistleblower protection; (2) structured desk research of authoritative policy sources (e.g. serious and organised threat assessment reports by the European Union Agency for Law Enforcement Cooperation (Europol), European Commission communications and the new Directive (EU) 2024/1260 on asset recovery and confiscation); and (3) illustrative case studies to examine how confiscation, whistleblowing and technology interact in practice. Case studies were purposively selected based on three criteria: relevance to high-risk criminal networks; availability of triangulable public documentation (judgments, official reports, peer-reviewed literature); and variation in the underlying mechanism (confiscation-led disruption, whistleblower-led detection and technology-enabled investigation). Data was coded thematically across three pillars – confiscation, whistleblowing and technology – using an analytical framework that maps each pillar to its intended objective, mechanism of action, enabling legal tools and observable outputs. This framework supports within-case and cross-case comparisons and links findings back to the research problem. Limitations include reliance on secondary sources for some cases, uneven data granularity across Member States and absence of original interviews. Ethical considerations focus on the use of public sources and the protection of any named individuals through reliance on official documents and anonymised case descriptions, where appropriate.

1. Introduction

High-risk criminal networks generate revenues exceeding EUR 139 billion annually (European Commission, 2021), equivalent to approximately 1 % of the EU's gross domestic product (European Commission, 2020). These networks operate internationally, leveraging innovations in technology to enhance their activities. Such revenues could otherwise be utilised to improve public education and healthcare. High-risk criminal networks pose a significant threat to EU security, their operations spreading across the globe.

The enormity of the damage induced by such organised crime has been emphasised by the European Parliament and the Council (European Parliament, 2016, 2020). But what does 'high-risk criminal network' mean, and what strategies are employed to combat these malicious activities? This paper aims to dissect the role of confiscation in destabilising these networks, exposing their vulnerabilities and sabotaging their foundations.

To monitor these unlawful activities involving high-value targets, whistleblowing remains a critical tool. Our reliance on technology cannot be disregarded as these criminal networks also utilise it in their operations. The focus here is on the effective implementation of confiscation and whistleblowing to dismantle high-risk criminal networks in the digital age.

2. Defining serious and organised criminal activities in the EU

Organised crime refers to a consistent alliance of individuals engaged in illegal activities, adhering to an intricate system (Rider, 2023). Interestingly, the code of conduct and demeanour can hint at unity or shared mutual objectives within these groups (Gambetta, 2011). Crime is their regular occupation, usually involving affiliations with other criminal networks (Sergi, 2021). Organised crime is a sophisticated international operation (European Commission, 2021), involving members of multiple nationalities (Europol, 2021).

These networks thrive on cooperation, with operations orchestrated around profitability. Violence is unfortunately becoming more frequent and extreme (Europol, 2021). Some networks are mono-criminal, focusing on specific activities like drug trafficking or organised property crime, while others are poly-criminal, engaging in multiple types of criminal activity. The ominous potential of these high-risk criminal networks arises from their invasion of legitimate businesses, use of money-laundering tactics, resilience and adaptability, countermeasures to evade law enforcers, recruitment of minors and frequent reliance on corruption or violence. Therefore, understanding such high-risk networks paves the way to shattering their foundations, with the ultimate aim of bringing about trusted societal reform (European Commission: Directorate-General for Migration and Home Affairs and Kantar, 2020).

3. Confiscation of criminal assets

To impair the operations of high-risk criminal collectives, it is essential to target their financial underpinning, as illicit earnings are the lifeblood of their ventures (Hryniewicz-Lach, 2023). Enforced asset confiscation aims to be a powerful tool against these crime syndicates. Through judicial or authorised authority decisions, properties procured through unlawful pursuits are permanently confiscated. Thus, networks' prosperity and power are dramatically impeded. International collaboration is of paramount importance for the dynamic enforcement of asset seizures (Laghidze, 2023). Building close legal relations facilitates the forfeiture of properties derived from transnational criminal enterprises. Despite efforts to seize unlawfully acquired assets, which would have otherwise been laundered into the legitimate economy, the effectiveness of asset confiscation in the EU has been limited, with criminals retaining control over 98 % of their ill-gotten gains (Europol, 2016).

Asset recovery operates in five phases: identification, freezing, management, confiscation and disposal. Effective execution of these phases necessitates the collaborative efforts of diverse agencies – law enforcement, judiciary and asset management offices, to name a few. Within the EU, asset recovery offices, responsible for asset forfeiture and international cooperation, play a central role in this multi-agency network (Europol, 2021, p. 30).

The recently enforced Directive (EU) 2024/1260 on combating intensified criminal networks, with a focus on asset recovery and confiscation (European Parliament and Council of the European Union, 2024), exemplifies this crucial collective effort. Resolving discrepancies among national laws following the implementation of the previous asset recovery directive is essential to fostering effective inter-EU cooperation that adheres to the new confiscation rules. A strategic step towards disrupting high-risk criminal networks is the incorporation of unequivocal provisions on non-conviction-based confiscation (European Parliament and Council of the European Union, 2024a) and the introduction of an unexplained wealth confiscation regime (European Parliament and Council of the European Union, 2024b) as part of Directive (EU) 2024/1260. This innovative model targets organised crime by enabling the confiscation of assets without the requirement of a criminal conviction (Boeri et al., 2024). The United Kingdom's civil confiscation measures have proven to be particularly effective against organised crime (Hendry and King, 2016).

However, such revolutionary harmonisation of laws compels the provision of extensive security for fundamental rights at the EU level (Hryniewicz-Lach, 2023, pp. 243–267). Chapter V of Directive (EU) 2024/1260 outlines the mandatory protection at the national level for the right to a fair trial, effective remedy and defence for impacted individuals (European Union Agency for Fundamental Rights, 2012). This progress illuminates the potential for developing increasingly potent tools to streamline every stage of asset recovery (Sakellaraki, 2022). Demands to create a secure environment that substantially mitigates risks posed by high-risk criminal networks (European

Commission, 2020) are murmurings of a society impatient for change. The primary goal of the legislation is to pre-empt and combat organised crime and high-risk criminal networks.

Investing in efforts to prevent and combat these high-risk criminal networks addresses one of the most significant threats to the EU's security (European Union, 2024). Directive (EU) 2024/1260 targets crimes committed within criminal organisations. Profits from these illicit operations often pave the way for more serious cross-border crimes, as noted in recital 10 (Sakellaraki, 2022). Reallocating and investing confiscated assets into local communities can play a pivotal role in curbing the activities of high-risk criminal networks (Maugeri, 2024). While confiscation strikes at illicit gains, whistleblowing accelerates detection and case-building by providing insider information that is otherwise costly or impossible to obtain.

4. The power of whistleblowing

Unveiling criminal activities is like solving a complex puzzle, and the integral pieces that lead to its resolution are often supplied by whistleblowers. These individuals form the backbone of the investigative process, triggering 95 % of police investigations through their diligent reporting (Miethe and Rothschild, 1994). In the heart of flourishing organisations and societies lies the ability to recognise and address deviant behaviour (Bergemann, 2024). Here, the whistleblower plays the role of an internal watchdog, catching and reporting instances of misconduct or criminality as they occur (Gottschalk and Asting, 2022). As the world advances, so does the art of whistleblowing, evolving into an essential tool for detection, investigation and prosecution of economic crimes (European Parliament and Council of the EuropeanUnion, 2019a). European Union policymakers are harnessing the power of whistleblowing, aiming to uncover illicit activities on a broader scale (Karpacheva and Hock, 2024). The role of technology in whistleblowing is also becoming increasingly prominent. It can ensure stronger protections for the whistleblowers, increasing the volume of leaked information and facilitating its analysis and global distribution (Munro and Kenny, 2023).

In essence, whistleblowing serves as an efficient means to penetrate formidable criminal networks. Leaders who have so far managed to elude justice can now be targeted with accuracy. Acquiring specific information disrupts the foundations of these networks and leads to effective arrests. Although pivotal in unveiling high-risk criminal networks, whistleblowers inevitably expose themselves to potential dangers. They may face job loss, legal suits, threats or even physical harm. Therefore, creating a safe ecosystem for these individuals is indispensable, as it encourages reporting and aids in crime prevention, detection and penalisation (Terracol, 2023).

Countries worldwide are recognising this need and establishing robust whistleblower protection legislation (Vandekerckhove, 2010). Key among these is Directive (EU) 2019/1937 (Kaçiku Baljija and Min, 2023), which aims to harmonise whistleblower legislation among Member States, ensure confidentiality and protect against retaliation (Council of Europe, 2019). By contrast, the United States looks to monetary rewards as an incentive for whistleblowing, raising ethical dilemmas as this approach may be perceived as commercialising a public service. Nevertheless, the power of incentives in encouraging whistleblowing cannot be overlooked (European Commission, 2018).

Thus, a modified model that provides whistleblowers of high-risk criminal networks with protections, possible amnesty and leniency for their role in the network is proposed. Furthermore, significant rewards sourced from seized

criminal assets could be offered. Involving legal intermediaries in these processes can heighten efficiency and inspire confidence. They could serve as private attorney generals, earnestly joining the fight against high-risk criminal networks (Nyreröd and Andreadakis, 2023). Whistleblowing is not just a tool; it is a revolution that empowers societies to cleanse themselves of corruption. With the right environment, legislation and motivation, more individuals could be encouraged to come forward, holding a mirror to wrongdoing and ensuring that justice prevails. Both confiscation and whistleblowing now unfold in a technology-saturated environment, which criminals exploit – and which authorities can leverage. The following section considers these dual effects.

5. The rising challenge of tech-savvy criminal networks

Currently, criminal networks are adapting to contemporary advancements, employing technology-facilitated means such as encrypted interactions, social media and instant messaging services for illicit transactions and criminal endeavours. A considerable portion of their activities now occurs online, exploiting the secretive and pervasive nature of the Dark Web and various digital platforms (European Commission: Directorate-General for Migration and Home Affairs et al., 2021) that offer encrypted communication and transaction systems. These outlets give such criminal syndicates vast operational latitude – subterranean yet ubiquitous. Moreover, they exploit less regulated financial channels like virtual currencies, which exacerbates the problem's magnitude. The crypto-asset ecosystem exemplifies this, having grown rapidly to over 22 476 assets in circulation by early 2023 (Kapsis, 2023). Encryption's promise of anonymity serves as a veil, shielding criminals from law enforcement agencies' detection of unlawful profits, posing a complex regulatory challenge. A notable instance is the Silk Road (Adler, 2018), an online drug bazaar that used Bitcoin for transactions until halted by the US Federal Bureau of Investigation in 2013 ([10]). This example illustrates the dual nature of technology: it empowers criminal networks but also creates opportunities for law enforcement to innovate. These sophisticated technologies embolden high-risk criminal networks to undertake complex criminal activities (Demetis, 2023). For instance, a human trafficking ring used unique radio frequency identification microchips to catalogue its victims digitally (Barton and Laffan, 2016), intertwining exploitative practices with cutting-edge technology (Voas and Kshetri, 2017). Consequently, bridging technological risks with actionable strategies becomes essential for effective disruption. Thus, the pressing question becomes how law enforcement agencies can harness blockchain technology to detect, prevent and dismantle these organised criminal networks, and how blockchain can facilitate international collaboration in curbing high-risk criminal activities.

On a brighter note, digital tools have proven vital in enhancing whistleblower safety and protecting their identities, especially when using encrypted platforms like GlobaLeaks (Di Salvo, 2020). These tools highlight the practical implications of technology – not only as a threat vector but also as a safeguard for whistleblowers – underscoring the need for integrated policy responses. Still, a nuanced approach to digital tools is a requisite for better comprehending their impact on whistleblowing in the persistent fight against corruption (Fubini and Lo Piccolo, 2024).

([10]) Ross Ulbricht, the founder of the Silk Road, was convicted and sentenced to a double life sentence plus 40 years.

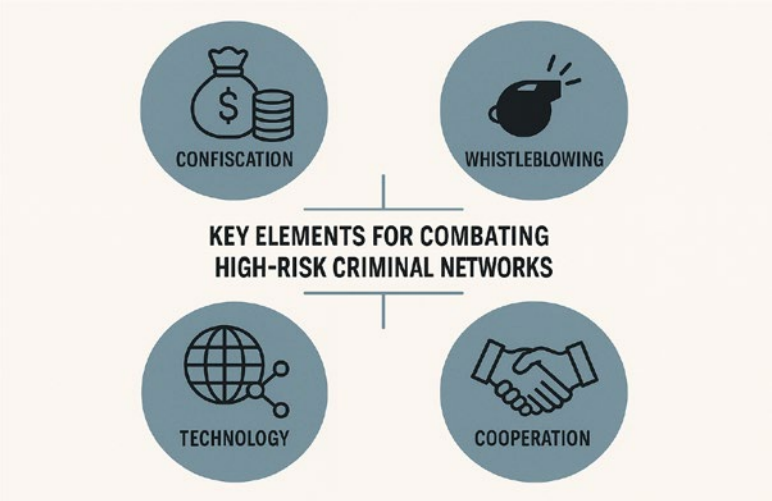


Figure 5.1. Key elements for combating high-risk criminal networks

Source: Conceptual diagram created by the author with AI support (Microsoft Copilot).

6. Conclusions

The European Union is actively grappling with the challenge of curbing the activities of high-risk criminal networks. Despite considerable steps having been made, a continuous and amplified effort remains essential to disbanding these complex criminal infrastructures. In enhancing these efforts, the EU has relied heavily on the Schengen information system (SIS) (European Commission, 2021, p. 3) and the European multidisciplinary platform against criminal threats (Empact). SIS is a consolidated database that empowers competent authorities in identifying offenders and their illicit wealth derived from organised crime (European Union, 2019ba, 2019b). Empact, on the other hand, functions as a multidimensional collaboration platform ([11]) among diverse authorities (European Commission, 2021). This includes law enforcement, taxation departments, magistrates, European institutions and agencies, non-EU countries, international organisations and the private sector ([12]).

The prospect of these platforms is set to be enhanced by a forthcoming framework for the interaction of EU information systems, the purpose of which is an integrated data check across these systems. The primary objective of this framework is to address identity fraud efficiently (Council of Europe, n.d.). Furthermore, a marked improvement in the disruption of criminal networks can be brought about by enhancing cooperation among law enforcement authorities. This involves an exchange of information and collaborative investigations with non-EU country authorities. Intelligence-driven strategies are of crucial importance for combating the multifaceted structure of these networks. In order to ensure the efficacy of such investigations, it is essential to strengthen the jurisdiction of the competent authorities, while cognisant of the transborder aspect of these criminal activities. Member States need to establish clear objectives, dedicate resources, facilitate investigators' work through training and creatively employ the existing legal apparatus in a holistic, coherent and committed manner (Council of Europe, 2022).

([11]) Between 2018 and 2021, EU crime priorities included cybercrime, drugs trafficking, facilitation of illegal immigration, organised property crime, trafficking in human beings (for all forms of exploitation), excise and missing trader intra-community fraud, illicit firearms trafficking, environmental crime, criminal finances and money laundering and document fraud.

([12]) The EU policy cycle for organised and serious international crime is utilised to define the cooperation framework for setting common priorities. Empact serves as the operational platform that facilitates cooperation between practitioners. It is the only programme that utilises intelligence-led policing and a multidisciplinary and integrated approach to combating organised crime.

Innovative solutions like developing an open-source platform could greatly augment criminal investigations and furnish crucial leads about assets held by criminals, their associates and instated businesses (Europol, 2021). A sound understanding of burgeoning technologies can also aid law enforcement authorities. Furthermore, technologies such as regtech (regulatory technology), can foster regulatory compliance and enable oversight of financial markets (Anagnostopoulos, 2018), including the crypto-asset ecosystem.

In essence, high-risk criminal networks pose a direct threat to the EU's security fabric by generating illicit profits and leveraging advanced technologies for evasion. Despite illicit assets being seized as a deterrent, only a fraction of the criminal proceeds is successfully recovered, due to a lack of seamless transborder cooperation and enforcement. Given such predicaments, proactive measures like whistleblower protections, leniency agreements or rewards might encourage insiders to report illicit activities. Additionally, criminal activities involving digital platforms, cryptocurrencies and encrypted technologies complicate investigations. This necessitates a coordinated EU effort, with advanced data sharing and specialised tools being critical for dismantling criminal networks and safeguarding society against such threats. Equally important is the role of whistleblowing, which provides early intelligence and actionable leads that complement technological and legal measures. Priority actions may include: (1) harmonising confiscation frameworks across Member States; (2) strengthening whistleblower protection and incentives; (3) using advanced analytics and blockchain tools for asset tracing; and (4) enhancing cross-border intelligence sharing. Future research should focus on the effectiveness of integrated strategies combining confiscation, whistleblowing and technology, and explore the ethical implications of AI-driven enforcement tools.

References

Adler, D. (2018), 'Silk Road: The dark side of cryptocurrency', *Fordham Journal of Corporate and Financial Law*, 21 February.

Anagnostopoulos, I. (2018), 'Fintech and regtech: Impact on regulators and banks', *Journal of Economics and Business*, Vol. 100, pp. 7–25, https://doi.org/10.1016/j.jeconbus.2018.07.003.

Barton, H. and Laffan, D. A. (2016), 'The dark side of the internet', in: Connoly, I., Palmer, M., Barton, H. and Kirwan, G. (eds), *An Introduction to Cyberpsychology*, Taylor and Francis, London, pp. 58–70, https://doi.org/10.4324/9781003092513.

Bergemann, P. (2024), 'How social influence affects reporting: Toward an integration of crime reporting, whistleblowing, and denunciation', *Annual Review of Sociology*, Vol. 50, pp. 209–228, https://doi.org/10.1146/annurev-soc-030222-013736.

Boeri, F., Di Cataldo, M. and Pietrostefani, E. (2024), 'Localized effects of confiscated and re-allocated real estate mafia assets', *Journal of Economic Geography*, Vol. 24, Issue 2, pp. 219–240, https://doi.org/10.1093/jeg/lbad035.

Chin, K. (1996), *Chinatown Gangs: Extortion, enterprise and ethnicity*, Oxford University Press, New York, https://archive.org/details/chinatowngangsex0000chin_e0o5/mode/2up.

Council of Europe (2019), 'The protection of whistleblowers: Challenges and opportunities for local and regional government', CG36(2019)14 final of 3 April, https://rm.coe.int/the-protection-of-whistleblowers-challenges-and-opportunities-for-loca/16809312bd.

Council of Europe (2022), 'Regional study on legislation with focus on search, seizure and confiscation of cybercrime proceeds and prevention of money laundering on the Internet – Eastern Partnership region – CyberEast project report', https://rm.coe.int/regional-study-on-legislation-with-focus-on-search-seizure-and-confisc/1680a956e2.

Council of Europe (n.d.), 'Financial investigations', Council of Europe website, https://www.coe.int/en/web/moneyval/implementation/financial-investigations.

Demetis, D. (2023), 'Organised crime – The cyber dimension', in: Rider, B. (ed.), *A Research Agenda for Organized Crime*, Edward Elgar Publishing, Cheltenham, pp. 177–194, https://econpapers.repec.org/RePEc:elg:eechap:20952_8.

Di Salvo, R. P. (2020), *Digital Whistleblowing Platforms in Journalism – Encrypting leaks*, Palgrave Macmillan, Cham, https://doi.org/10.1007/978-3-030-38505-7.

European Commission (2018), Commission staff working document – Impact assessment – Accompanying the document 'Proposal for a directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law', SWD(2018) 116 final of 23 April, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52018SC0116.

European Commission (2020), Communication on the EU security union strategy, COM(2020) 605 final of 24 July, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0605.

European Commission (2021), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU strategy to tackle organised crime 2021–2025, COM(2021) 170 final of 14 April, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0170.

European Commission: Directorate-General for Migration and Home Affairs and Kantar (2020), *Special Eurobarometer 502 – Report – Corruption*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2837/91891.

European Commission: Directorate-General for Migration and Home Affairs, Ernst & Young, Government Transparency Institute, Optimity Advisors, RAND Europe and Centre for the Study of Democracy (2021), *Mapping the risk of serious and organised crime infiltration in legitimate businesses – Final report*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2837/64101.

European Parliament (2016), 'Report on the fight against corruption', A8-0284/2016, https://www.europarl.europa.eu/doceo/document/A-8-2016-0284_EN.pdf.

European Parliament (2020), 'European Parliament resolution of 17 December 2020 on the EU security union strategy', P9_TA(2020)0378, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0378_EN.pdf.

European Parliament and Council of the European Union (2019a), Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, p. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj), Recital 2.

European Parliament and Council of the European Union (2019b), Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27, ELI: http://data.europa.eu/eli/reg/2019/817/oj).

European Parliament and Council of the European Union (2019c), Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj).

European Parliament and Council of the European Union (2024a), Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation (OJ L, 2024/1260, 2.5.2024, ELI: http://data.europa.eu/eli/dir/2024/1260/oj), Recital 2.

European Parliament and Council of the European Union (2024b), Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation (OJ L, 2024/1260, 2.5.2024, ELI: http://data.europa.eu/eli/dir/2024/1260/oj), Article 15.

European Parliament and Council of the European Union (2024c), Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation (OJ L, 2024/1260, 2.5.2024, ELI: http://data.europa.eu/eli/dir/2024/1260/oj), Article 16.

European Union Agency for Fundamental Rights (2012), 'Opinion of the European Union Agency for Fundamental Rights on the confiscation of proceeds of crime', 3/2012, 4 December, p. 6, paragraph 6, https://fra.europa.eu/sites/default/files/fra-opinion-3-2012_confiscation-of-proceeds-of-crime.pdf.

Europol (2016), *Does Crime Still Pay? Criminal asset recovery in the EU – Survey of statistical information 2010–2014*, European Police Office (Europol), The Hague, https://www.europol.europa.eu/publications-documents/does-crime-still-pay.

Europol (2021), *European Union Serious and Organised Crime Threat Assessment – A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2813/346806.

Fubini, A. and Lo Piccolo, A. (2024), 'Anti-corruption initiatives and the digital challenge: The role of civil society organizations and whistleblowing infrastructures in the Italian context', *American Behavioral Scientist*, l. 70, Issue 8, https://doi.org/10.1177/00027642241268590.

Gambetta, D. (2011), *Codes of the Underworld – How criminals communicate*, Princeton University Press, https://jlupub.ub.uni-giessen.de/server/api/core/bitstreams/fcba5645-1e22-4eaf-8c46-d7a94e2c36ca/content.

Gottschalk, P. and Asting, C. (2022), 'Crime signal detection theory: Two case studies of the five-stage model from observer to whistleblower', *Deviant Behavior*, Vol. 43, Issue 4, pp. 461–471, https://doi.org/10.1080/01639625.2020.1816147.

Hendry, J. and King, C. (2016), 'Expediency, legitimacy, and the rule of law: A systems perspective on civil/criminal procedural hybrids', *Criminal Law and Philosophy*, Vol. 11, pp. 733–757, https://doi.org/10.1007/s11572-016-9405-6.

Hryniewicz-Lach, E. (2023), 'Expanding confiscation and its dimensions in EU criminal law', *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 31, Issue 3–4, pp. 243–267, https://doi.org/10.1163/15718174-bja10046.

Kapsis, I. (2023), 'Crypto-assets and criminality: A critical review focusing on money laundering and terrorism financing', in: Jasinski, D., Phillips, A. and Johnston, E. (eds), *Organised Crime, Financial Crime, and Criminal Justice – Theoretical concepts and challenges*, 1st edition, Routledge,, London, pp. 122–141, https://doi.org/10.4324/9781003020813-8.

Karpacheva, E. and Hock, B. (2024), 'Foreign whistleblowing: The impact of US extraterritorial enforcement on anti-corruption laws in Europe', *Journal of Financial Crime*, Vol. 31, Issue 1, pp. 1–13, https://doi.org/10.1108/JFC-11-2022-0283.

Kaçiku Baljija, S. and Min, K. (2023), 'Evaluating the effectiveness of whistleblower protection: A new index', *Data and Policy*, Vol. 5, e28, https://doi.org/10.1017/dap.2023.20.

Laghidze, E. (2023), 'Seizure and confiscation as an effective means of combating transnational organized crime', *Law and World*, Vol. 9, No 25, pp. 146–155 , https://doi.org/10.36475/9.1.15.

Maugeri, A. M. (2024), 'Regulation (EU) 2018/1805: Mutual recognition of freezing and confiscation orders between efficiency and safeguards – "Proceedings in criminal matters" and non-conviction based confiscation', *New Journal of European Criminal Law*, Vol. 15, Issue 2, pp. 164–208, https://doi.org/10.1177/20322844241239781.

Miethe, T. D. and Rothschild, J. (1994), 'Whistleblowing and the control of organizational misconduct', *Sociological Inquiry*, Vol. 64, Issue 3, pp. 322–347, https://doi.org/10.1111/j.1475-682X.1994.tb00395.x.

Munro, I. and Kenny, K. (2023), 'Networked whistleblowing, counter-hegemony and the challenge to systemic corruption', in: Gabbioneta, C., Clemente, M. and Greenwood, R. (eds), *Organizational Wrongdoing as the 'Foundational' Grand Challenge – Consequences and impact*, Vol. 85, Emerald Publishing, https://doi.org/10.1108/S0733-558X20230000085007.

Nyreröd, T., Andreadakis, S. and Spagnolo, G. (2023), 'Money laundering and sanctions enforcement: Large rewards, leniency and witness protection for whistleblowers', *Journal of Money Laundering Control*, Vol. 26, No 5, pp. 912–925, https://doi.org/10.1108/JMLC-05-2022-0068.

Rider, B. (ed.) (2023), *A Research Agenda for Organized Crime*, Edward Elgar Publishing, Cheltenham, https://econpapers.repec.org/RePEc:elg:eebook:20952.

Sakellaraki, A. (2022), 'EU asset recovery and confiscation regime – *Quo vadis*? A first assessment of the Commission's proposal to further harmonise the EU asset recovery and confiscation laws – A step in the right direction?', *New Journal of European Criminal Law*, Vol. 13, Issue 4, pp. 478–501, https://doi.org/10.1177/20322844221139577.

Terracol, M. (2023), *How Well Do EU Countries Protect Whistleblowers? Assessing the transposition of the EU whistleblower Protection Directive*, Transparency International, https://images.transparencycdn.org/images/2023_How-well-do-EU-countries-protect-whistleblowers_EN.pdf.

Vandekerckhove, W. (2010), 'European whistleblower protection: Tiers or tears?', in: Lewis, D. (ed.), *A Global Approach to Public Interest Disclosure*, Edward Elgar Publishing, Cheltenham, pp. 15–35, https://gala.gre.ac.uk/id/eprint/4360.

Voas, J. and Kshetri, N. (2017), 'Human tagging', *Computer*, Vol. 50, Issue 10, pp. 78–85, https://doi.org/10.1109/MC.2017.3641646.

Transfer of avatar training effects to mock investigative interviews with adult witnesses

Mari-Liis Tohvelmann, Kristjan Kask, Shumpei Haginoya, Pekka Santtila

https://doi.org/10.3013/vpag3r71

Abstract

Interviewing witnesses is a delicate and complex process that must follow certain principles. Previous studies have noted that investigative interviews with adult victims and witnesses are often of low quality. Research also suggests that interviewing skills improve when the interviewers are given feedback on their performance. We have created a web-based adult witness avatars (AWA) software to simulate investigative interviews with adult victims and witnesses that would help interviewers train question types that will allow the witnesses to recall more accurate accounts. We examined whether avatar interviews coupled with feedback (versus no feedback) would result in improvements in interviews with human mock witnesses. Half of the 58 participants received process feedback after each of four simulated interviews. The avatars revealed predefined memories and made errors as a function of algorithms formulated based on previous empirical research on the response behaviour of adult witnesses in experimental studies. We found that feedback was linked to a high proportion of recommended questions within the AWA training itself. Receiving feedback after the simulated interviews increased the proportion of recommended questions (i.e. free recall and open questions) in mock interviews with human interviewees compared with not receiving feedback (67 % versus 49 %, respectively). However, there were no significant differences between feedback and control groups in terms of correct or incorrect details elicited from the mock witnesses. Future steps and implications for this type of software in training investigative interviewing skills will be discussed.

Keywords: interviewer training, adult witnesses, avatars, serious gaming, feedback, transfer effect.

1. Introduction

Interviews with victims and witnesses are an important source of evidence, especially in tackling organised crime such as high-risk criminal networks. Unfortunately, these statements can be influenced by inappropriate interviewing methods, potentially resulting in hampered investigations or even miscarriages of justice (Milne and Bull, 1999). Therefore, it is important that witnesses are interviewed appropriately.

Asking questions that elicit accurate answers is an important element of recent best practice guidelines (Principles on effective interviewing for investigations and information gathering, 2021; United Nations, 2024; Halley et al., 2023; UK Ministry of Justice, 2022; Bjerknes and Fahsing, 2018; Griffiths and Rachlew, 2018; Fisher and Geiselman, 1992). These guidelines all stress asking questions that facilitate good communication with the witness and will help them recall as much information as possible. Unfortunately, interviewers have difficulties in applying these principles in practice (Walsh et al., 2025).

Questions can be categorised in different ways (Nunan et al., 2020) as productive and unproductive (Griffiths and Milne, 2006), appropriate and inappropriate (Phillips et al., 2011), or recommended and not recommended (Pompedda et al., 2017). It is preferable to enhance witnesses' recall by letting them freely recollect what they have experienced or direct their recall using open questions (Oxburgh et al., 2010). On the contrary, option-posing, repeated, suggestive or misleading questions are not recommended as they increase the proportion of inaccurate information (Otgaar et al., 2023). Therefore, the wording of questions posed to witnesses is central to ensuring the detail and accuracy of witness statements.

Theory-based training is the most common way of training interviewers (Pompedda, 2018). It increases the interviewers' knowledge of the topic but may not actually improve their interviewing skills (Lamb, 2016). Immediate personalised continuous feedback is needed to change interviewer behaviour (Casey and Powell, 2021). As technology adds new possibilities, serious gaming solutions in virtual environments have been found to be effective in improving learners' performance (Graafland et al., 2012; van der Zee et al., 2012). Such solutions are particularly attractive as they make the provision of immediate feedback quick and cost-effective (see Kask et al., 2024). However, research has focused on child interviewing; therefore, there is a lack of methods for training in adult witness interviewing (Tohvelmann and Kask, 2022).

Tohvelmann and Kask (2022) therefore proposed a serious gaming solution targeted at improving the quality of interviews with adult witnesses. Tohvelmann et al. (2025) created a web-based solution called adult witness avatars (AWA) to simulate investigative interviews with adult victims and witnesses. They examined whether simulated interviews with avatars, coupled with feedback (versus no feedback), would improve interview quality. Interviews with repeated feedback included a higher proportion of recommended questions (i.e. free recall and open questions) than those without feedback (90.3 % versus 72.6 %, respectively). However, despite these promising results, it is not known whether the effect of this training in avatar interviews would transfer to subsequent interviews with real witnesses.

1.1. Current study

Given that Tohvelmann et al. (2025) showed that repeated feedback after a series of simulated investigative interviews increased the proportion of recommended questions in avatar interviews, we examined whether this training effect would transfer to interviews with human mock witnesses. More precisely, we examined whether AWA training sessions coupled with feedback (versus no feedback) would be effective in changing (novice) interviewer behaviour both during training and in subsequent interviews with a human mock witness. First, we hypothesised that receiving feedback (versus not receiving feedback) regarding questions asked during the avatar interviews would result in (a) an increased number of recommended questions, (b) a decreased number of non-recommended questions, and (c) a higher proportion of recommended questions overall. Second, we hypothesised that having received feedback (versus not having received feedback) during the avatar interviews would result in (a) an increased number of recommended questions, (b) a decreased number of non-recommended questions, and (c) a higher proportion of recommended questions in subsequent interviews with human mock witnesses. Third, we hypothesised that the participants who had received feedback (versus those who had not received feedback) during the avatar training session would elicit (a) more correct details, (b) fewer incorrect details, and (c) a higher proportion of correct details overall. Fourth, we also hypothesised that participants asking a higher proportion of recommended questions during avatar interviews would (a) ask a higher proportion of recommended questions in interviews with human mock witnesses; and (b) elicit a higher proportion of correct details in these interviews.

2. Method

We preregistered the desired sample size, including variables, hypotheses and planned analyses on AsPredicted ([13]). The dataset containing all primary study variables can be obtained from the authors.

2.1. Participants

We recruited 60 interviewer participants but two of them were excluded as their interviewees could not be reached for the online interview. Therefore, the final number of interviewer participants was 58 (see 'Characteristics' in Table 6.1). The experiment was conducted in Estonian. The participants were neither law students nor third-year psychology students (since legal psychology is an optional course for the third-year students at the university) and had conducted no prior investigative interviews. The feedback and control groups did not differ significantly in terms of gender, $\chi2(2) = 1.47$, $p = 0.48$, age, $t(56) = -1.355$, $p = 0.18$, or education level, $\chi2(3) = 2.83$, $p = 0.24$. We also recruited 58 interviewee participants (see 'Characteristics' in Table 6.1). The feedback and control groups did not differ significantly in terms of gender, $\chi2(1) = 0.17$, $p = 0.681$, age, $t(53) = 0.066$, $p = 0.947$, or education level, $\chi2(3) = 2.96$, $p = 0.40$. The participants did not receive any form of recompense for their participation.

([13]) https://aspredicted.org/blind.php?x=JQN_DX3.

Table 6.1. Demographics of interviewers and interviewees

Characteristics	Interviewers	Interviewees
Mean age	23 years (SD ([14]) = 2.8, range 19–29)	32.8 years (SD = 10.4, range 18–56)
Gender	30 males, 27 females, 1 non-binary	26 males, 31 females, 1 did not disclose gender
Native language	55 Estonian, 3 Russian	57 Estonian, 1 did not disclose native language
Highest education level	45 secondary education, 11 vocational education, 2 higher education	2 basic education, 14 secondary education, 6 vocational education, 35 higher education

2.2. Study design

We used a between-subjects design with two groups: (a) a feedback group (n = 29), where participants received process feedback after interviewing each avatar; and (b) a control group (n = 29), where participants did not receive any feedback. Each participant performed four interviews with avatars and one with the human mock witness. The four avatars were the same for each participant, but their order was randomised. The mock witness was interviewed through Google Meet.

2.3. Materials

Four AWAs (two males and two females, comprising three victims and one bystander) were created based on real-life crime scenarios (for more details, see Tohvelmann et al., 2025). Response algorithms were created based on a systematic review of experimental studies examining how actual adult witnesses behave during interviews (see Tohvelmann et al., 2025), thereby allowing us to simulate how a real adult would respond to different types of questions. Responses consisted of answers containing correct details (the details mentioned by the victims and witnesses based on the information from actual court verdicts) and incorrect details (created by the manuscript authors and known to be false).

2.4. Procedure

Participants were tested individually in Tallinn University's experimental psychology laboratory. The Board of Research Ethics at Tallinn University approved the study, with all the participants signing a fully informed consent form stipulating the possibility to withdraw from the study at any time during the experiment.

Participants were seated in front of a laptop computer where the videos of the AWAs were displayed. First, each participant had to read a description of best practices in investigative interviewing of adults and answer two questions about what they read. If they answered incorrectly, the same questions were asked again until both questions were answered correctly. Before the interviewing process started, each participant was also presented with 10 pairs of questions (randomised between the versions) and had to choose the correctly formed one (four different versions, see Appendix 6.1) and mark their selection. No feedback was given on these decisions.

([14]) SD refers to standard deviation.

Each participant interviewed four avatars (for more detail, see Tohvelmann et al., 2025). Before each interview, participants read a short description of the criminal case of the AWA to be interviewed (e.g. 'a security guard reported that two men left a store without paying for a teddy bear, then one of them punched the security guard in the face'). Participants then had 10 minutes to find out what happened, a time frame previously shown to be sufficient for producing a training effect in increasing the proportion of recommended questions (see Pompedda et al., 2022). If they were satisfied that they had found out what had happened, they could finish the interview earlier. The participants' questions were audio-recorded. To ask a question, the participants had to press a red button that initiated the recording. After asking a question, they had to press a black square that ended the recording. The operator then manually coded the question type (free or cued recall, open, closed, forced-choice, suggestive or misleading questions) and the detail type that the question addressed. The latter included general information (yes, no, don't know, etc.), avatar personal information (name, etc.), location, time, action (who did what), objects (e.g. knife), offender characteristics, victim/witness characteristics and the manner in which the crime was committed (e.g. 'he attacked with a knife'). The software then launched a video clip with the avatar's response, which included either correct or incorrect details, depending probabilistically on the type of question asked. If there were two possible incorrect answers available, the operator chose manually which answer to play depending on the storyline (but not accuracy) of previous AWA answers. At the end of the interview, the participants reported what they believed the AWA had witnessed/experienced. After interviewing four avatars, participants repeated the task of choosing the correctly formed question from among the different question pairs. Again, no feedback was given on their decisions.

After each interview, the control group (n = 29) proceeded to learn the story of the next avatar and started the next interview. The feedback group (n = 29) received feedback on four of the questions (two recommended and two non-recommended questions) they had used during the preceding interview. Over the four interviews, as many different question types as possible were covered. Specifically, if the interviewer used several different new question types during the interview, these were prioritised during the feedback session. Regardless, feedback was always provided for at least two recommended and two non-recommended questions. However, if the interviewer did not ask any questions of a particular type at all (either recommended or non-recommended), feedback was given on only two questions. As a result, the number of questions the participant received feedback on could vary. Example feedback to recommended questions would be: 'You asked the avatar, "Where were you?", which is an open question; carry on with these types of questions'. For non-recommended questions, feedback might be 'You asked "Was there one or two persons?", which is an option-posing question; try to phrase this question in a more open manner next time'.

After the avatar training session, the interviewers conducted an interview with a human interviewee using Google Meet. The interviewees first signed an informed consent form and were shown one of the two half-minute-long video clips, selected at random (one video clip was of a mock theft where two women interacted with a man, and one of the women stole the man's mobile phone; the other was of two women interacting with a man, and by the end of video clip the man thought that something was missing from his backpack). Roughly a week later, they were interviewed with a mean (M) delay of 6.7 days (SD = 0.8, range from 6 to 10 days). There were no differences between the feedback and control groups, $t(56) = -0.82$, $p = 0.419$ (feedback M = 6.6, SD = 0.6 versus control M = 6.8, SD = 1.0). Finally, the interviewers gave the AWA a realism rating on a 10-point Likert scale with anchors 1 = not at all realistic and 10 = very realistic. The experiment lasted about 120 minutes. Finally, participants were briefed about the aim of the study.

2.4.1. Coding of interviews

During the interviews with the AWAs, the operator (Mari-Liis Tohvelmann) coded all the questions asked by the participants into one of seven categories (see Table 6.2; see also Tohvelmann et al., 2025). Free and cued recall and open questions were later grouped as recommended questions, and closed, forced-choice, suggestive and misleading questions as non-recommended questions. The coded question types were saved by the programme together with the correct and incorrect details that the AWAs provided in response to the questions.

Table 6.2. Question categories with definitions and examples

Free recall	These utterances help the interviewee to recall a response with minimal influence from the interviewer.	'Tell me everything.'
Cued recall	These utterances are similar to free recall, but related to a previous statement elicited from the interviewee.	'You mentioned a bag. Tell me everything about the bag.'
Open questions	These questions focus the interviewee's attention on a particular detail and ask for an explanation (usually using words such as 'who', 'where', 'what' and 'how').	'Where did you go with him?'
Closed questions	These questions focus on the details the interviewee may have mentioned and do not require a particular type of response, although they can be answered 'yes' or 'no'.	'Did it happen in the living room?'
Forced-choice questions	These questions provide response options from which the interviewee must choose.	'Did it happen once, twice or three times?'
Suggestive questions	These questions imply what kind of response is expected, using details that the interviewee may have mentioned before.	'He touched you, didn't he?'
Misleading questions	These questions strongly indicate the kind of response expected from the interviewee but mention a detail that was not included in the interviewee's previous responses.	'So I understand that the hat was red' (if the colour of the hat was not mentioned before and is not known).

After the avatar interviews, an independent research assistant re-coded the question type classifications (recommended or not recommended) for a random sample of 48 interview transcripts. The interrater reliability was Cohen's $\kappa = 0.84$ (95 % confidence intervals (CI) 0.82 to 0.90), $p < 0.001$. Similarly, after the mock interviews, an independent research assistant re-coded the question type classifications (recommended or not recommended) for a random sample of 12 interview transcripts with an interrater reliability of Cohen's $\kappa = 0.87$ (95 % CI 0.79 to 0.95), $p < 0.001$.

Mock witness reports of what they had witnessed in the video clip were coded as accurate (the details reported by the participant matched the details in the video) or inaccurate (participant reported something not present in the video). The interrater reliability for the coding using 12 randomly selected reports using Kendall tau analysis was $\tau\_b = 0.985$, $p < 0.01$ for accurate details, and $\tau\_b = 0.977$, $p < 0.01$ for inaccurate details.

Besides the number of correct and incorrect responses produced by the avatars, we calculated the proportion of correct avatar responses relative to all potential correct avatar responses in the system.

2.5. Data analyses

The dependent measures for testing hypothesis 1 were the number of recommended and non-recommended questions, and the proportion of recommended questions. Free recall, cued recall and open questions were grouped as recommended questions; closed, forced-choice, suggestive and misleading questions were grouped as non-recommended questions. The proportion of recommended questions was calculated by dividing the number of recommended questions by the sum of recommended and non-recommended questions in each interview.

To evaluate how receiving feedback affected the questions asked, we conducted three separate 2 (group: feedback × control; between-subjects) × 4 (time: interviews 1–4; within-subjects) repeated measures analyses of covariances (ANCOVAs), controlling for participants' age, gender and education, with the number of recommended questions, the number of non-recommended questions and the proportion of recommended questions as dependents. When Mauchly's test of sphericity was significant, we used a Greenhouse-Geisser correction. We used SPSS (Statistical Package for the Social Sciences) version 27 with p level < 0.05. To test hypothesis 1, we were interested in both the group (feedback versus control) main effect and the group × time interaction.

When the interaction effect was statistically significant, we conducted pairwise comparisons with a Bonferroni correction.

To test hypotheses 2 and 3 we used t-tests for independent samples. To test hypothesis 4 we used correlation analyses (Pearson) and z-tests. The hypotheses were preregistered on AsPredicted ([15]).

3. Results

3.1. Descriptive analyses

The average length of the avatar interviews from the first to the last question was 548 seconds (SD = 80, range 89 to 612 seconds), with no differences between the feedback and control groups, $t(230) = -1.41$, $p = 0.161$ (feedback M = 540, SD = 80 versus control M = 555, SD = 79).

The average length of mock witness interviews from the first to the last question asked was 345 seconds (SD = 158, range 106 to 745 seconds), with no differences between the feedback and control groups, $t(56) = -1.41$, $p = 0.163$ (feedback M = 316, SD = 157 versus control $M = 374$, SD = 156).

([15]) https://aspredicted.org/blind.php?x=JQN_DX3.

The average realism rating of the AWAs was M = 5.41 (SD = 1.41, range 2–8) with a difference between feedback and control groups, $t(56) = 4.11$, $p = 0.001$, Cohen's $d = 1.245$ (95 % CI 0.524 to 1.628), with the former rating the AWAs to be more realistic than the latter (feedback M = 6.09, SD = 1.26 versus control M = 4.74, SD = 1.23).

The question categorisation task results did not differ between the control and feedback groups either before (feedback M = 9.79 (SD = 0.49) versus control M = 9.69 (SD = 0.71), $t(56) = 0.644$, $p = 0.261$) or after the avatar training session (feedback M = 9.83 (SD = 0.47) versus control M = 9.59 (SD = 0.63), $t(56) = 1.66$, $p = 0.051$). As four different versions were used, randomised to the participants, we tested whether there were differences between the versions. No significant differences were found ($p > 0.08$ in all versions).

3.2. Effect of feedback on question type while controlling for covariates

The descriptive statistics for the number of recommended and non-recommended questions and the proportion of recommended questions in both the feedback and control groups and for each interview are presented in Table 6.3.

Table 6.3. Differences in interview quality between feedback and control groups

Number of interviews		Recommended		Not recommended		Proportion of recommended	
		M	SD	M	SD	M	SD
1	Feedback	14.66	6.10	4.55	3.62	74.41	21.42
	Control	14.03	6.72	6.07	4.66	69.21	23.36
2	Feedback	17.24	5.24	3.48	3.52	83.07	17.72
	Control	16.03	6.01	6.00	4.30	72.34	18.67
3	Feedback	19.72	5.08	1.66	2.07	91.55	11.97
	Control	17.48	6.12	5.38	3.90	75.62	16.22
4	Feedback	21.48	5.65	1.72	2.42	92.28	11.98
	Control	19.72	6.93	5.45	4.20	77.24	18.00
Overall	Feedback	18.10	6.22	3.07	3.34	84.20	18.36
	Control	16.99	6.58	5.51	4.25	74.73	19.19

First, we analysed the results concerning the number of recommended questions. Mauchly's test of sphericity was not significant, so sphericity was assumed. The analysis showed that there was no main effect of group, $F(1, 53) = 1.06$, $p = 0.31$, $\eta p^2 = 0.02$, $1 - \beta$ ([16]) $= 0.17$, or of time, $F(3,159) = 0.47$, $p = 0.70$, $\eta p^2 = 0.01$, $1 - \beta = 0.14$. As shown in Figure 6.1,

([16]) $1 - \beta$ indicates statistical power.

participants in the feedback group did not use more recommended questions than participants in the control group. There was also no interaction between group and time, $F(3, 159) = 0.44$, $p = 0.73$, $\eta p^2 = 0.01$, $1 - \beta = 0.14$, and pairwise comparisons indicated no differences within interviews.

Next, we analysed the results concerning the number of non-recommended questions. As Mauchly's test of sphericity was significant, we used a Greenhouse-Geisser correction. The analysis showed that there was a significant main effect of group, $F(1, 53) = 11.72$, $p = 0.001$, $\eta p^2 = 0.18$, $1 - \beta = 0.92$, but not of time $F(2\ 543\ 134.781) = 0.25$, $p = 0.86$, $\eta p^2 = 0.01$, $1 - \beta = 0.10$. Figure 6.2 shows that the number of non-recommended questions was higher for the control group than for the feedback group. Lastly, there was no interaction between group and time, $F(2{,}543{,}134.781) = 2.70$, $p = 0.057$, $\eta p^2 = 0.048$, $1 - \beta = 0.596$. However, pairwise comparisons indicated differences between feedback and control groups within interviews 2, 3 and 4 ($p = 0.001$).

Finally, we analysed the results concerning the proportion of recommended questions. As Mauchly's test of sphericity was significant, we used a Greenhouse-Geisser correction. ANCOVA indicated a significant main effect of group, $F(1, 53) = 8.39$, $p = 0.005$, $\eta p^2 = 0.137$, $1 - \beta = 0.812$. There was no significant main effect of time, $F(1.969{,}104.352) = 0.43$, $p = 0.65$, $\eta p^2 = 0.01$, $1 - \beta = 0.12$, and no interaction between group and time, $F(1\ 969\ 104.352) = 2.52$, $p = 0.086$, $\eta p^2 = 0.045$, $1 - \beta = 0.491$. However, pairwise comparisons indicated differences between feedback and control groups within interviews 3 and 4 ($p = 0.001$). Figure 6.3 illustrates that the proportion of recommended questions increased in the feedback group with each subsequent interview, while in the control group it did not.

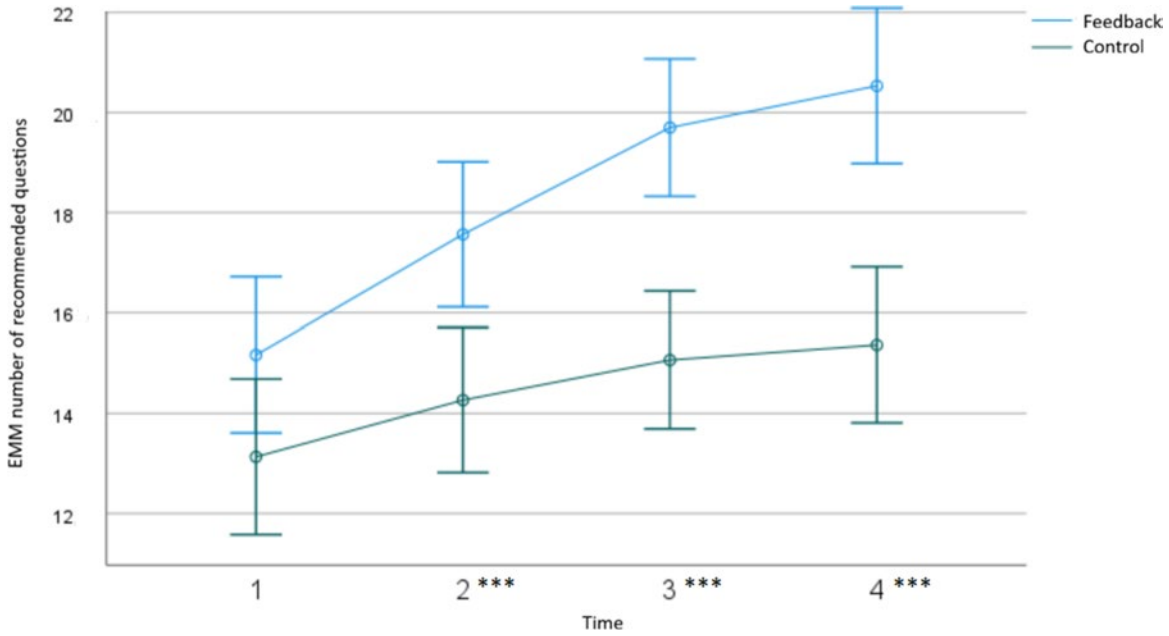


Figure 6.1. Estimated marginal means (EMM) of the difference between feedback and control groups in the number of recommended questions across four AWA interviews

NB: Error bars show 95 % confidence intervals. ***, $p < 0.001$.

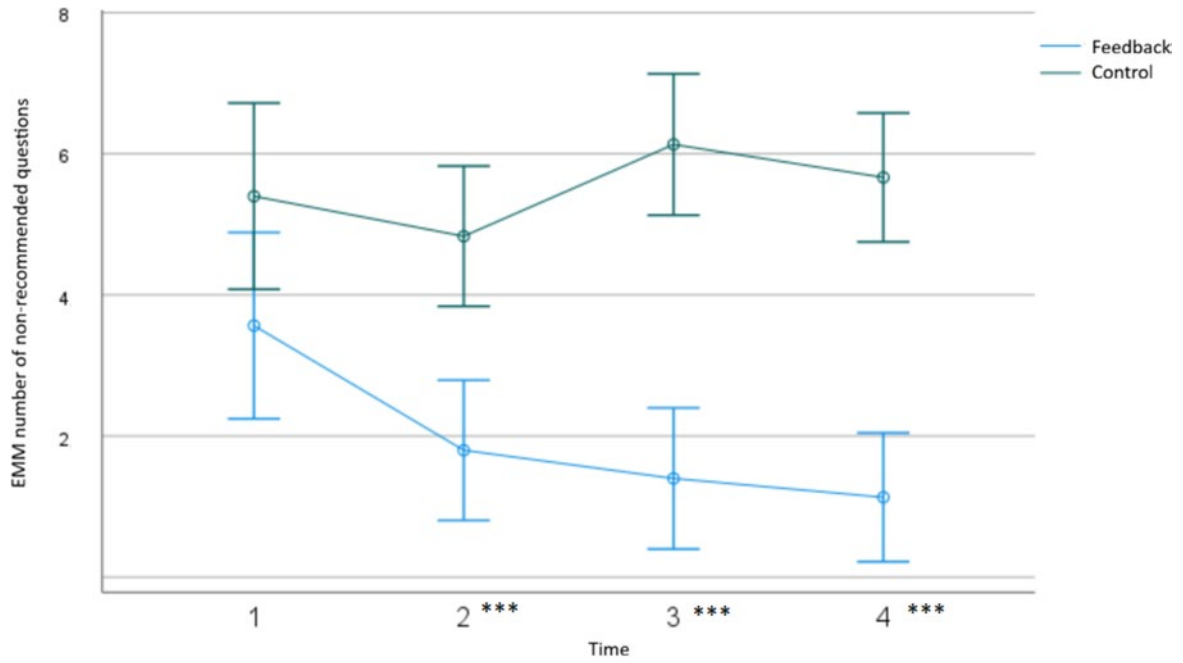


Figure 6.2. EMM of the difference between feedback and control groups in the number of non-recommended questions across four AWA interviews

NB: Error bars show 95 % confidence intervals. *** = $p < 0.001$.

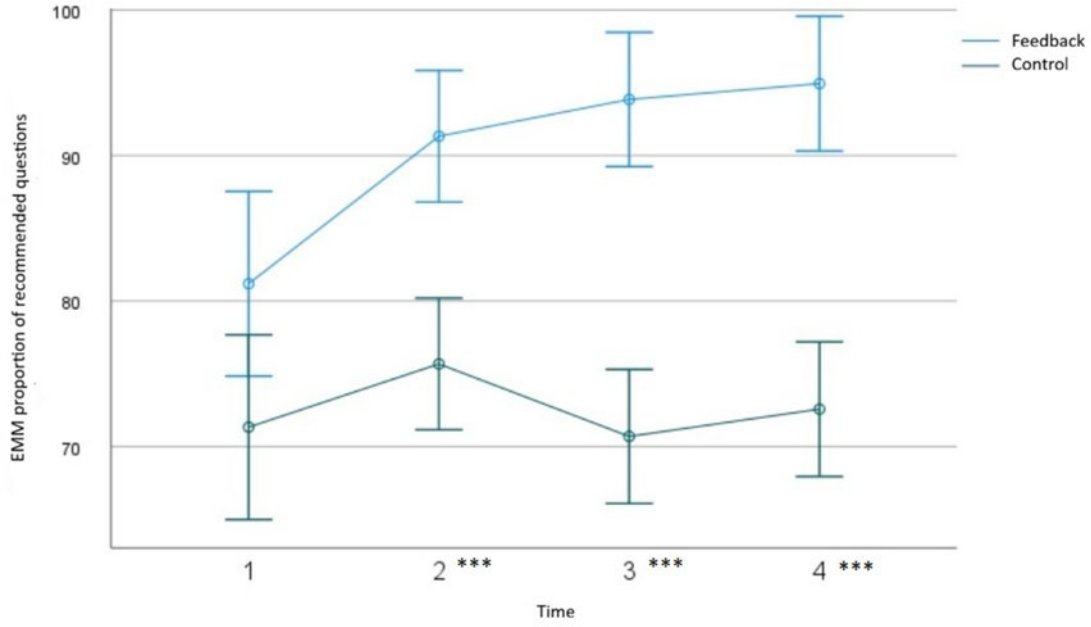


Figure 6.3. EMM of the difference between feedback and control groups in the proportion of recommended questions across four AWA interviews

NB: Error bars show 95 % confidence intervals. *** = $p < 0.001$.

Next, hypothesis 2 was tested. The feedback and control groups did not differ in the number of recommended questions in the interviews with human mock witnesses (see Table 6.4), $t(56) = -0.05$, $p = 0.96$, while the feedback group asked significantly fewer non-recommended questions than the control group, $t(56) = -3.32$, $p = 0.002$, $d = 0.872$. Also, the feedback group asked a higher proportion of recommended questions than the control group, $t(56) = -3.43$, $p = 0.001$, Hedge's $g = 0.89$.

Table 6.4. Differences between feedback and control groups in the number and proportion of question types in mock interviews with human mock witnesses

Category	Group	*n*	M	SD
Number of recommended questions in mock interview	Feedback	29	9.14	5.40
	Control	29	9.21	5.42
Number of non-recommended questions in mock interview	Feedback	29	5.14	5.48
	Control	29	10.38	6.50
Proportion of recommended questions in mock interview	Feedback	29	0.67	0.23
	Control	29	0.49	0.16

Next, hypothesis 3 was tested. The feedback and control groups did not differ in the number of correct details (see Table 6.5), $t(56) = -0.445$, $p = 0.658$, or the number of incorrect details, $t(56) = 0.049$, $p = 0.961$, or the proportion of correct details, $t(56) = -0.883$, $p = 0.381$, elicited from the human mock witnesses.

Table 6.5. Differences between feedback and control groups in the number and proportion of details elicited from human mock witnesses

Category	Group	*n*	M	SD
Number of correct details in mock interview	Feedback	29	80.62	43.04
	Control	29	85.90	47.09
Number of incorrect details in mock interview	Feedback	29	23.41	20.54
	Control	29	23.10	27.22
Proportion of correct details in mock interview	Feedback	29	0.78	0.16
	Control	29	0.80	0.12

Finally, hypothesis 4 was tested. The proportion of recommended questions in avatar interviews predicted the proportion of recommended questions in the mock witness interviews, $r(58) = 0.655$, $p = 0.001$. However, the proportion of correct details elicited from the human mock witnesses was not correlated with either the proportion of recommended questions in the interviews with the human mock witnesses, $r(58) = -0.091$, $p = 0.499$, or the proportion of recommended questions in the avatar interviews, $r(58) = -0.105$, $p = 0.434$. When feedback and control groups were analysed separately, only the proportion of recommended questions in avatar interviews was significantly and positively correlated with the proportion of recommended questions in interviews with human mock witnesses in the feedback group, $r(58) = 0.606$, $p = 0.001$, and in the control group, $r(58) = 0.620$, $p = 0.001$. The difference between the correlations was not significant using *z*-tests, $z = -0.081$, $p = 0.468$.

4. Discussion

We examined whether training with AWAs coupled with feedback would be effective in changing interviewer behaviour within the AWA training sessions and in subsequent interviews with human mock witnesses. We found that feedback was linked to a high proportion of recommended questions within the AWA training session itself. Importantly, we also demonstrated that interviewers who had received feedback during AWA training sessions asked a higher proportion of recommended questions in mock witness interviews. However, there were no significant differences between the feedback and control groups in terms of correct or incorrect details elicited from mock witnesses.

4.1. AWA training effects

In testing hypothesis 1, groups did not differ in the number of recommended questions. However, the feedback group asked fewer non-recommended questions and had a higher proportion of recommended questions than the control group, especially in interviews 2 to 4, immediately following feedback.

These results are largely in line with the previous experiment where AWA was used (Tohvelmann et al., 2025); however, the only major difference in present results is that there was no significant group or group × time interaction effect for the number of recommended questions. Overall, we can state that process feedback given to novice interviewers improved the overall proportion of recommended questions, as shown in previous similar studies where immediate and personalised feedback was given during avatar-based training sessions (Pompedda, 2018). These results confirm that serious gaming solutions contribute to improving the quality of interviews. The current study indicated that the overall proportion of recommended questions increased, though this was caused more by a decrease in the number of non-recommended questions than by an increase in the number of recommended questions.

4.2. Transfer effects

In hypothesis 2 testing, the feedback and control groups asked a similar number of recommended questions, but the feedback group asked fewer non-recommended and thus a higher proportion of recommended questions. These findings support previous notions that continuous feedback is crucial in creating a change in interviewer behaviour (Casey and Powell, 2021).

The third hypothesis was not supported – the feedback group did not elicit more correct, fewer incorrect or a higher proportion of correct details than the control group. The explanation for this finding could be that our sample was young and inexperienced in investigative interviewing; therefore, it may have been difficult for them to ask questions that are important in collecting evidence in real-life cases. Participants may have been concentrating more on the storyline and trying to find the potential offender rather than helping the avatars recall details otherwise necessary for police investigation. Therefore, more action-related questions (e.g. 'What happened after the conversation?'; 'Uh-uh, what happened next?') were asked even when the operator instructed the participants to ask for more details. Also, participants may have been pressured by the 10-minute time limit, which may have led them to concentrate on the storyline in order to get a complete report of the incident. On the other hand, they were interviewing mock witnesses from a distance (using Google Meet) and asked the mock witnesses about a short (one

minute long) video clip they had seen on average a week ago. As the video clip was short, there were not many details to elicit, resulting in a possible floor effect.

Another possible reason for the lack of significant differences between groups could be the relatively short delay period used with adult participants. Adults tend to show higher accuracy in testimony than children or older adults (Fitzgerald and Price, 2015) and are less affected by the delay period (Flin et al., 1992; Memon et al., 2003). The proportion of accurate details elicited from adult witnesses in the control group with a one-week delay period after viewing a mock event is generally around 80 % to 90 % (e.g. Gabbert et al., 2009; Hope et al., 2014). Therefore, when a short delay period like the one used in this study is implemented, it is likely that the control group who did not receive any intervention will demonstrate a ceiling effect in terms of the accuracy of the details they provide. Considering this, future research might benefit from using a longer delay period.

The proportion of recommended questions in avatar and human mock-witness interviews were positively correlated, but correct details were unrelated to question type. This correlation appeared in both feedback and control groups, with no significant difference between them. These results suggest that there were consistent individual differences between the participants. It may have been that the training sessions with avatars with the feedback group and the non-feedback group improved the use of recommended questions but did not train the participant to follow a traditional interviewing structure as the participants did not have any prior knowledge of that topic.

Participants in the feedback group rated AWAs as more realistic than those in the control group. AWAs use algorithms to generate responses based on the types of questions asked. Participants who received feedback may have learned that asking recommended questions would lead to a more logical storyline, whereas participants who did not receive any feedback may have been confused during the process due to the incorrect details the avatars recalled. Therefore, these participants may have considered that the AWA did not understand them properly and the programme needs to be improved.

There were no differences between the groups in question categorisation tasks before and after AWA training. As this task was given right after the participants read the description of the best practices of investigative interviewing of adults, which included answering two control questions correctly, their knowledge about the topic was tested using surface cues (i.e. recognition memory). However, for a deeper and more conscious learning process to emerge, a task where they must formulate the questions themselves (as they did in interviewing different avatars) could have resulted in different findings.

4.3. Limitations

The AWA training session was conducted by a single experimenter. To reduce the risk of categorising the question types in a similar manner, post-experiment interrater reliability analyses were conducted, indicating good reliability. Also, the number of correct pieces of information did not increase in mock interviews with human adult witnesses. This finding may be explained by the fact that our interviewers were not police investigators or police cadets, so they had very limited knowledge about the components of evidence in interviews (such as the time, place and manner of conducting the crime). As this study was conducted with student participants, the results cannot directly be generalised to practitioner samples.

4.4. Future research

Future research can focus on adding a modelling component to AWA training sessions, in addition to feedback, as previous studies have shown that the combination of feedback and modelling lead to greater improvement in interviewers' questioning style than feedback alone (Haginoya et al., 2021). In future, the human operator who currently codes question types and styles could be replaced by an artificial intelligence system that can be trained (machine learning) to code these question types and styles automatically (see Haginoya et al., 2023).

5. Conclusion

In the present study, we confirmed that training with AWAs paired with feedback had an effect on interviewer behaviour both within the AWA training sessions (replicating Tohvelmann et al., 2025) and now also in subsequent interviews with human mock witnesses. Our results demonstrate the potential to help interviewers use more recommended questions. Traditional training sessions are often time-consuming, costly and difficult to arrange (Pompedda, 2018), especially when they involve immediate and personalised feedback. The proposed solution offers a cost-effective means of helping practitioners train their question formulation skills, as this can currently be conducted remotely via the web in investigators' workplaces. However, before AWA can be fully implemented by law enforcement agencies, it should be tested with real police investigators to determine whether training effects transfer to their real interviews with victims and witnesses, who are an important source of information in criminal proceedings, especially in cases concerning high-risk criminal networks. These findings and tools could then be incorporated into initial academy training to set strong interviewing habits from the start. Agencies can then provide brief booster sessions at regular intervals throughout an officer's career to refresh skills and prevent drift. This approach has the potential to keep practice aligned with evidence.

References

Bjerknes, O. T. and Fahsing, I. A. (2018), *Etterforskning – Prinsipper, metoder og praksis* [*Investigation – Principles, methods and practice*], Fagbokforlaget, Bergen, https://hdl.handle.net/11250/4325149.

Casey, S. and Powell, M. B. (2021), 'Usefulness of an e-simulation in improving social work student knowledge of best-practice questions', *Social Work Education*, Vol. 41, No 6, pp. 1253–1271, https://doi.org/10.1080/02615479.2021.1948002.

Fisher, R. P. and Geiselman, R. E. (1992), *Memory Enhancing Techniques for Investigative Interviewing: The cognitive interview*, Charles C. Thomas, Springfield, Illinois, https://psycnet.apa.org/record/1992-98595-000.

Fitzgerald, R. J. and Price, H. L. (2015), 'Eyewitness identification across the life span: A meta-analysis of age differences', *Psychological Bulletin*, Vol. 141, No 6, pp. 1228–1265, https://doi.org/10.1037/bul0000013.

Flin, R., Boon, J., Knox, A. and Bull, R. (1992), 'The effect of a five-month delay on children's and adults' eyewitness memory', *British Journal of Psychology*, Vol. 83, Issue 3, pp. 323–336, https://doi.org/10.1111/j.2044-8295.1992.tb02444.x.

Graafland, M., Schraagen, J. M. and Schijven, M. P. (2012), 'Systematic review of serious games for medical education and surgical skills training', *British Journal of Surgery*, Vol. 99, Issue 10, pp. 1322–1330, https://doi.org/10.1002/bjs.8819.

Gabbert, F., Hope, L. and Fisher, R. P. (2009), 'Protecting eyewitness evidence: Examining the efficacy of a self-administered interview tool', *Law and Human Behavior*, Vol. 33, No 4, pp. 298–307, https://doi.org/10.1007/s10979-008-9146-8.

Griffiths, A. and Milne, R. (2006), 'Will it all end in tiers? Police interviews with suspects in Britain', in: Williamson, T. (ed.), *Investigative Interviewing – Rights, research, regulation*, Willan, London, pp. 167–189, https://doi.org/10.4324/9781843926337.

Griffiths, A. and Rachlew, A. (2018), 'From interrogation to investigative interviewing', in: Griffiths, A. and Milne, R. (eds), *The Psychology of Criminal Investigation: From theory to practice*, Routledge, London, pp. 154–178, https://doi.org/10.4324/9781315637211-9.

Halley, J., Walsh, D., Myklebust, T. and Bjerknes, O. T. (2023), 'Structured models of interviewing', in: Oxburgh, G. E., Myklebust, T., Fallon, M. and Hartwig, M. (eds), *Interviewing and Interrogation: A review of research and practice since World War II*, Torkel Opsahl Academic EPublisher, Brussels, pp. 257–281, https://www.legal-tools.org/doc/ln43ta/.

Haginoya, S., Yamamoto, S. and Santtila, P. (2021), 'The combination of feedback and modeling in online simulation training of child sexual abuse interviews improves interview quality in clinical psychologists', *Child Abuse and Neglect*, Vol. 115, https://doi.org/10.1016/j.chiabu.2021.105013.

Haginoya, S., Ibe, T., Yamamoto, S., Yoshimoto, N., Mizushi, H. et al. (2023), 'AI avatar tells you what happened: The first test of using AI-operated children in simulated interviews to train investigative interviewers', *Frontiers in Psychology*, Vol. 14, https://doi.org/10.3389/fpsyg.2023.1133621.

Hope, L., Gabbert, F., Fisher, R. P. and Jamieson, K. (2014), 'Protecting and enhancing eyewitness memory: The impact of an initial recall attempt on performance in an investigative interview', *Applied Cognitive Psychology*, Vol. 28, Issue 3, pp. 304–313, https://doi.org/10.1002/acp.2984.

Kask, K., Baugerud, G. A. and Volbert, R. (2024), 'Editorial: Technological solutions helping to train specialists' interviewing skills of possible victims and witnesses', *Frontiers in Psychology,* Vol. 15, https://doi.org/10.3389/fpsyg.2024.1406867.

Lamb, M. E. (2016), 'Difficulties translating research on forensic interview practices to practitioners: Finding water, leading horses, but can we get them to drink?', *American Psychologist*, Vol. 71, No 8, pp. 710–718, https://doi.org/10.1037/amp0000039.

Memon, A., Bartlett, J., Rose, R. and Gray, C. (2003), 'The aging eyewitness: Effects of age on face, delay, and source-memory ability', *Journals of Gerontology – Series B*, Vol. 58, Issue 6, pp. 338–345, https://doi.org/10.1093/geronb/58.6.P338.

Milne, R. and Bull, R. (1999), *Investigative Interviewing: Psychology and practice*, Wiley, Chichester.

Nunan, J., Stanier, I., Milne, R., Shawyer, A. and Walsh, D. (2020), 'Source handler telephone interactions with covert human intelligence sources: An exploration of question types and intelligence yield', *Applied Cognitive Psychology*, Vol. 34, Issue 6, pp. 1473–1484, https://doi.org/10.1002/acp.3726.

Otgaar, H., Houben, S. T. L., Muris, P. and Howe, M. L. (2023), 'Does interviewing affect suggestibility and false memory formation?', in: Oxburgh, G. E., Myklebust, T., Fallon, M. and Hartwig, M. (eds), *Interviewing and Interrogation: A review of research and practice since World War II*, Torkel Opsahl Academic EPublisher, Brussels, pp. 193–209, https://www.legal-tools.org/doc/v3wphg/.

Oxburgh, G. E., Myklebust, T. and Grant, T. (2010), 'The question of question types in police interviews: A review of the literature from a psychological and linguistic perspective', *International Journal of Speech, Language and the Law*, Vol. 17, Issue 1, pp. 45–66, https://doi.org/10.1558/ijsll.v17i1.45.

Phillips, E., Oxburgh, G. E., Gavin, A. and Myklebust, T. (2011), 'Investigative interviews with victims of child sexual abuse: The relationship between question type and investigation relevant information', *Journal of Police and Criminal Psychology*, Vol. 27, pp. 45–54, https://doi.org/10.1007/s11896-011-9093-z.

Pompedda, F. (2018), *Training in Investigative Interviews of Children: Serious gaming paired with feedback improves interview quality*, Åbo Akademi University, Turku, https://doi.org/10.13140/RG.2.2.29825.07526.

Pompedda, F., Antfolk, J., Zappalà, A. and Santtila, P. (2017), 'A combination of outcome and process feedback enhances performance in simulations of child sexual abuse interviews using avatars', *Frontiers in Psychology*, Vol. 8, https://doi.org/10.3389/fpsyg.2017.01474.

Pompedda, F., Zhang, Y., Haginoya, S. and Santtila, P. (2022), 'A mega-analysis of the effects of feedback on the quality of simulated child sexual abuse interviews with avatars', *Journal of Police and Criminal Psychology*, Vol. 37, pp. 485–498, https://doi.org/10.1007/s11896-022-09509-7.

'Principles on effective interviewing for investigations and information gathering' (2021), interviewingprinciples.com website, https://interviewingprinciples.com/.

Sternberg, K. J., Lamb, M. E., Esplin, P. W., Orbach Y. and Hershkowitz I. (2002), 'Using a structured protocol to improve the quality of investigative interviews', in: Eisen, M., Quas, J. A. and Goodman, G. S. (eds), *Memory and Suggestibility in the Forensic Interview*, Lawrence Erlbaum Associates Publishers, Mahwah, pp. 409–436, https://psycnet.apa.org/record/2001-05106-017.

Tohvelmann, M.-L. and Kask, K. (2022), 'From child to adult victims and witnesses: Ways of improving the quality of investigative interviews', *Juridica International*, Vol. 31, pp. 136–146, https://doi.org/10.12697/JI.2022.31.10.

Tohvelmann, M.-L., Kask, K., Palu, A., Haginoya, S. and Santtila, P. (2025), 'Providing feedback in simulated investigative interviews with adult witness avatars increases the use of free recall and open questions', *International Journal of Police Science and Management*, Vol. 27, Issue 2, pp. 182–198, https://doi.org/10.1177/14613557241310014.

UK Ministry of Justice (2022), *Achieving Best Evidence in Criminal Proceedings: Guidance on interviewing victims and witnesses, and guidance on using special measures*, https://assets.publishing.service.gov.uk/media/6492e26c103ca6001303a331/achieving-best-evidence-criminal-proceedings-2023.pdf.

United Nations Department of Peace Operations, United Nations Office of the High Commissioner for Human Rights and United Nations Office on Drugs and Crime (2024), *Manual on Investigative Interviewing for Criminal Investigation*, https://resourcehub01.blob.core.windows.net/$web/Policy %20and %20Guidance/corepeacekeepingguidance/Thematic %20Operational %20Activities/Police %20and %20Law %20Enforcement/2024.01 %20Manual %20on %20Investigative %20Interviewing %20for %20Criminal %20Investigation %20(2024).pdf.

Van der Zee, D.-J., Holkenborg, B. and Robinson, S. (2012), 'Conceptual modeling for simulation-based serious gaming', *Decision Support Systems*, Vol. 54, Issue 1, pp. 33–45, https://doi.org/10.1016/j.dss.2012.03.006.

Walsh, D., Areh, I., Barela, S., Boukalova, H., Bull, R. et al. (2025), 'A co-ordinated global initiative to enhance interview practice', *Investigative Interviewing: Research and practice*, Vol. 15, Issue 1, pp. 7–27, https://iiirg.org/wp-content/uploads/2025/09/II-RP-15-Special-Bilingual-Issue-2025-WEB.pdf.

Appendix 6.1. Examples of question categorisation pairs

1	Tell me what happened in the house.	Were there a lot of people?
2	Tell me what he/she was wearing.	Was he/she wearing a sweater or a hoodie?
3	What else do you remember?	Can you remember anything else?
4	You don't remember anything else, do you?	Tell me what else you remember about the incident.
5	Tell me more about this car.	Was the car red?
6	What colour was the car?	Was the car blue or green?
7	Tell me what happened in the house.	Did something happen?
8	Tell me who did what.	Was there a fight?
9	Were you afraid?	What did you feel?
10	Tell me what you were thinking when you saw this.	Were you afraid or not while all this happened?

Interviewing cooperating witnesses in organised crime cases in Poland: Lessons to learn from the principles on effective interviewing for investigations and information gathering

Denis Solodov

https://doi.org/10.3013/e2d5n738

Abstract

Interviewing cooperating witnesses in organised crime cases presents unique challenges and opportunities for law enforcement. The paper examines, within this context, the application of the principles on effective interviewing for investigations and information gathering (the Méndez principles), adopted under the auspices of the United Nations, to enhance the efficacy and integrity of information gathering during criminal investigations. The Méndez principles, which emphasise non-coercive, ethical and scientifically grounded interviewing techniques, provide a framework for improving the accuracy and reliability of cooperating witnesses' testimonies, mitigating biases and reducing associated risks. The author outlines the significance of integrating the Méndez principles into the national criminal justice system to foster trustworthy investigative outcomes with these in mind. This approach addresses the complexities of organised crime cases, ensuring that cooperating witnesses provide valuable and reliable information to support the pursuit of justice.

Keywords: Méndez principles, effective interviewing, organised crime, witness testimonies, non-coercive interviewing techniques, ethical interviewing, Poland.

Introduction

The fight against organised crime presents unique challenges for law enforcement agencies worldwide, requiring sophisticated investigative techniques and strategies to ensure the collection of accurate and reliable evidence.

One such challenge is interviewing cooperating witnesses, whose testimonies often serve as a cornerstone for building strong cases against organised criminal enterprises. Cooperating witnesses, by virtue of their proximity to criminal networks, can provide crucial insights into the structure, operations and key actors involved in illicit activities. Nonetheless, eliciting truthful, comprehensive and verifiable information from these individuals is a nuanced process that demands effective methodologies.

The Méndez principles, officially known as the 'principles on effective interviewing for investigations and information gathering' ([17]), represent a progressive framework designed to enhance the integrity and efficacy of information gathering in criminal investigations. Rooted in the valuing of non-coercion, ethical conduct and scientific rigour, the principles prioritise building trust and rapport with interviewees while minimising the risk of false and misleading statements. Overall, by providing a transparent, rights-focused framework, these international guidelines seek to:

1. enhance the fairness and integrity of judicial processes;
2. improve the reliability of information gathered during interviews;
3. protect vulnerable individuals from mistreatment and abuse;
4. promote international standards of justice, transparency and institutional accountability.

Their application within the context of organised crime investigations is particularly significant, given the high stakes and well-known complexities associated with these cases. Techniques from investigative interviewing, including developing trust and understanding the motivations of witnesses, are critical in managing cooperating witnesses, who often have vested interests (Fisher, 2010; Vallano et al., 2011).

The paper explores the possible application of the Méndez principles in interviewing cooperating witnesses in the example of the Polish criminal justice system. The author aims to identify key best practices promoted by the Méndez principles that can enhance the credibility and effectiveness of interviewing and investigation processes in general. The findings emphasise the importance of adopting non-coercive and ethical interviewing techniques to foster trust, ensure accurate testimony and support the overarching goals of criminal justice. This approach not only enhances the reliability of cooperating witness testimonies but also strengthens the overall legitimacy and fairness of the justice system. The author seeks to underline the critical role that ethical and scientifically grounded interviewing techniques play in achieving these outcomes, offering some insights for practitioners and policymakers.

Relevant scientific studies and selected case-law were examined using a narrative review approach to provide an overview of existing practices and challenges. Sources were drawn from legal databases with preference given to recent publications on investigative interviewing. The purpose of this review was to identify patterns and shortcomings in the Polish handling of cooperating witness interviews and to place them in the wider context of international recommendations (Tartaro, 2021).

([17]) 'Principles on effective interviewing for investigations and information gathering' (2021), interviewingprinciples.com website, https://interviewingprinciples.com/.

Cooperating witnesses in Poland

There are four types of protected witnesses in Polish criminal proceedings. The first is the police informant, who provides information on criminal activity but is not themselves under investigation. Such interviews are conducted during police intelligence-gathering activities (Sprengel, 2019; Horosiewicz, 2015; Taracha, 2006). The police officers who dealt with the informants are legally obliged to protect the identity of confidential informants (Article 22 of the Law on Police of 6 April 1990). Organisational aspects of the interview are defined by internal regulations. Later, such an informant could be a witness in criminal proceedings and receive a protected status. The second, the anonymous witness, is the one whose identity is kept secret by the decision of the court or prosecutor if there is a justified fear of danger to their life, health, freedom or property. Only the court, the prosecutor and, if necessary, a police officer handling the case have access to the witness's personal information. The defence party may access testimony in a way that does not reveal the identity of the witness. The testimony of an anonymous witness may be taken remotely using dedicated technical means (Article 184 of the Polish Code of Criminal Procedure). Secrecy applies to the information about the anonymous witnesses' identity, not the content of their testimony (Wiliński, 2019). The third type is the quasi-crown witness, or 'small crown witness' (Articles 60 and 61 of the Polish Penal Code), a cooperating suspect who provides law enforcement with significant information on the circumstances of the crime committed together with others. The law does not require the disclosure of all information related to the crime, but only the information that enables law enforcement to establish all the circumstances necessary to successfully conclude the proceedings. This condition is also satisfied when the authorities already possessed certain information, unbeknownst to the suspect, who nevertheless disclosed it to them to the best of their knowledge (Mistygacz, 2020). As a reward for the quasi-crown witness, there is obligatory mitigation of the criminal penalty. The court may also suspend the execution of the penalty, apply probation, waive related sanctions (e.g. fines, compensations, forfeitures) or even abstain from imposing a penalty if the cooperating suspect played a minor role in the crime and provided information that helped to prevent another crime. The institution of quasi-crown witnesses in Poland is used not only in organised crime cases but in other types of criminal cases as well.

The fourth type is the crown witness *sui generis*, whose status is regulated by dedicated legal provisions of the Polish Act on Crown Witnesses of 25 June 1997. A crown witness is a legal institution allowing individuals suspected of committing a crime to provide testimony in exchange for reduced penalties or immunity from punishment. The primary goal of this institution is to uncover crimes committed by organised criminal groups, providing evidence necessary for effective prosecution. Not every suspect could be a crown witness and not in every type of criminal case. The status of a crown witness applies solely to individuals involved in organised crime who have cooperated with others in the commission of certain types of criminal offences listed in the law (Potulski, 2024). The provisions of the Act on Crown Witnesses do not apply to a suspect who committed, attempted to commit or cooperated in the commission of murder; persuaded another person to commit such a crime to initiate criminal proceedings against them; or led an organised criminal gang aimed at committing a crime or fiscal criminal offence (Article 4). However, the mere fact of committing a murder, if unrelated to the ongoing case, does not prevent the suspect from becoming a crown witness. According to the Supreme Court of Poland ruling of 2004, the Act on Crown Witnesses only excludes individuals who cooperated in the commission of murder from obtaining crown witness status in that specific case, not in all crimes they may have committed (Supreme Court of Poland, 2004).

There is a two-stage procedure in which the decision to grant crown witness status is made by the court after an appropriate motion is filed by the prosecutor (procurator). It starts with the candidate for crown witness status

providing statements to the prosecutor, the content of which should fulfil the conditions set by the Act on Crown Witnesses. Based on the prosecutor's request, the court interrogates the candidate before issuing its decision on granting the protected status. Following the court's decision to grant such a status, the prosecutor separates the materials related to the crown witness and discontinues the proceedings. It is important that statements made by a candidate seeking to become a crown witness to the prosecutor cannot be used as testimonial evidence later if the court rejects the prosecutor's motion. Their content is also classified until the court's decision on granting protected status comes into force (Article 23 of the Act on Crown Witnesses).

Only the third type (the quasi-crown witness) and the fourth type (the crown witness *sui generis*) fit the general concept of a cooperating witness as one who collaborates with justice (Council of Europe, 2022). The first and second types, police informants and anonymous witnesses, do not meet the criteria for cooperation in the same way as they are, by definition, not directly involved in the crimes about which they provide information.

For the aim of this article, it is necessary to refer to the legal nature of the crown witness testimony and its evidentiary value in Polish criminal proceedings. The testimony of quasi-crown witnesses constitutes a legitimate source of evidence, just like any other kind of evidence, as there are no special legal provisions requiring that such statements be treated differently from other testimonial evidence. As a legitimate piece of evidence, the crown witness testimony is subject to free evaluation, just like any other evidence during criminal proceedings, regardless of whether it is the only direct evidence in the case or circumstantial evidence that logically completes a chain of circumstantial evidence in a way that clearly points to the main fact (Supreme Court of Poland, 2001).

A quasi-crown witness, being a criminal suspect, provides testimony during an interrogation. The subject of the testimony is the circumstances of criminal activities conducted by the suspect and other participants. The situation is more complicated in the case of a crown witness *sui generis*, who should first be interrogated as a suspect and then, after obtaining a protected status, interviewed as a crown witness, thus combining two different procedural roles and legal statuses.

Practical challenges

There are known practical challenges regarding the use of the crown witness testimony for investigative and evidentiary purposes. First, regardless of the type, a crown witness is not an impartial person since such a witness is highly motivated to testify. There is a risk that the crown witness is driven by the desire to avoid criminal responsibility and present testimony that is as favourable as possible to the authorities (Kowalewska-Borys, 2004). According to the Court of Justice of the European Union, the use of such testimonies might question the fairness of the proceedings and raise some issues, as such testimonies are not prone to manipulation and 'may be made purely to obtain the advantages offered in exchange, or for personal revenge' (*Arnold G. Cornelis* v *the Netherlands*, 2004). 'The sometimes ambiguous nature of such statements and the risk that a person might be accused and tried on the basis of unverified allegations that are not necessarily disinterested must not, therefore, be underestimated' (*Erdem* v *Germany*, 1999; *Lorsé* v *the Netherlands*, 2004; *Verhoek* v *the Netherlands*, 2004). As an additional guarantee against unreliable, untruthful testimonies, in the case of crown witness *sui generis*, Polish law allows, under predefined conditions, criminal proceedings against the witness to be resumed within five years of the case being discontinued. These conditions include the commission of a new crime, failure to fulfil legal obligations (of a crown witness) or the emergence of new facts that affect the legal basis of the decision to grant a protected legal status. When applied,

these provisions effectively reverse all privileges associated with this status, thus providing a strong incentive for crown witnesses to provide reliable information.

Second, by definition, the crown witness testimony is intended to be the main incriminating evidence in the case (Lach, 2019). This interpretation derives from legal provisions and prevailing judicial practices. It happens that the crown witness is the only source of detailed information about the criminal event and the actions of its participants (Court of Appeals in Warsaw, 2018; Court of Appeals in Warsaw, 2016; Supreme Court of Poland, 2013). Insufficient corroborating evidence may increase the risk of wrongful conviction. In practice, the reliability of the crown witness testimony as the main source of incriminating evidence is sometimes assessed during a procedural experiment (Article 211 of the Polish Code of Criminal Procedure). The experiment takes the form of recreating the course of the event, constituting the subject of the court examination and verifying the witness's ability to recognise and navigate the location of the event.

Third, there are limited possibilities for the defence party to participate in the crown witness interviews. In principle, the active participation of the defence in the examination of the testimonial evidence helps to ensure that the information is properly scrutinised and that potential biases or inconsistencies in the testimony are identified. According to the UN's 2024 Manual on Investigative Interviewing for Criminal Investigation, 'professional interviewers welcome the presence of defence lawyers as a legal resource, an eyewitness to the fairness of the interview, and a safeguard against misunderstandings' (United Nations, 2024). In practice, quasi-crown witnesses who provided accusatory testimonies during the preliminary proceedings tend to exercise their right to remain silent later at the trial stage, which essentially prevents the defence from verifying the statements and confronting them (Mrowicki, 2020). In the case of a crown witness *sui generis*, the situation might be different since such a witness is legally required to deliver testimony before the court.

Fourth, there is a question regarding the effectiveness of some interviewing techniques, given the relatively greater awareness of knowledgeable interviewees in this area. Criminals with prior experience in criminal matters or, for example, special training in counteracting commonly used (known) interviewing techniques might be more adept at manipulating interview dynamics. In this situation, it may be more challenging for the interviewers to obtain reliable and comprehensive information (Kwasiński, 2019). It can be assumed that in the case of crown witnesses, their prior knowledge of the matters under investigation, combined with the awareness that the investigators' success depends on their testimonies, creates an incentive to manipulate the disclosure of relevant information to increase this dependency. Some crown witnesses hold high-ranking positions within criminal organisations, which can influence their behaviour during interviews. Studies show that high-status suspects may attempt to assert control and manipulate the process of interviewing due to their previous authoritative roles (Hoekstra, 2024). Thus, the interviewing techniques used in other types of cases may not be effective in eliciting full and reliable testimonies. Polish investigators often prioritise obtaining confessions or confirmations, whereas investigative interviewing emphasises free recall to elicit unprompted, detailed narratives. Applying this model could help overcome the manipulation risks identified above.

Having outlined the Polish legal framework governing cooperating witnesses, the next section considers how the Méndez principles may be applied within that framework. The intention is to show where these international standards could strengthen the fairness and evidentiary reliability of current investigative practices.

Application of the Méndez principles

The Méndez principles were developed to replace coercive and abusive interviewing practices (Principles on effective interviewing for investigations and information gathering, 2021; United Nations, 2022a; Gudjonsson, 2023). They focus on promoting methods that are non-coercive, humane and effective, emphasising the importance of respecting the dignity and rights of individuals while improving the quality and reliability of information obtained during interviews. Interviewers are encouraged to use psychological research and proven techniques to build rapport, foster cooperation and elicit accurate information. Empirical research from several jurisdictions demonstrates that rapport-based models produce more accurate statements and fewer false admissions than traditional interviewing techniques (Powell et al., 2005; Walsh et al., 2010; Bull, 2018; Gudjonsson et al., 2011).

In Polish investigations, interviews often rely on structured, closed questions designed to confirm facts that are already known to investigators. Investigative interviewing, as promoted by the Méndez principles, instead favours open-ended questions, such as 'Can you describe what happened?' (instead of 'Did you see X commit the act?') or 'Were you instructed by Y?' (Lach, 2019), that allow witnesses to give fuller and more spontaneous accounts. This change of focus can increase the amount and quality of information obtained. In addition, interviews are usually summarised in written protocols, with the interviewer paraphrasing statements rather than recording them verbatim, which can lead to the loss of contextual detail and affect the evidentiary reliability of the testimony (Mrowicki, 2020).

In the case of cooperating witnesses, the investigative interviewing model, which is widely advertised by the Méndez principles, can be more effective for several reasons.

1. **Building rapport and trust.** Investigative interviewing techniques, such as the PEACE model (planning and preparation, engage and explain, account, closure, evaluation), emphasise building rapport and trust with the interviewee. Crown witnesses, who often come from high-ranking positions within organised criminal networks, may be more willing to cooperate if they feel respected and understood.

2. **Ethical and scientifically based approach.** Investigative interviewing avoids coercive and manipulative tactics, which, as numerous studies show (Halley et al., 2023; Gudjonsson, 2023; Walsh et al., 2010), can lead to false confessions or unreliable information. This ethical approach is crucial when dealing with crown witnesses, as their testimony may significantly impact the outcome of a case.

3. **Comprehensive information gathering.** Investigative interviewing focuses on obtaining complete, accurate and reliable information. This model ensures that all relevant details are revealed and thoroughly examined, which is essential when interviewing crown witnesses with extensive knowledge of illicit activities.

4. **Reducing biases and risk of memory contamination.** Investigative interviewing techniques are designed to minimise an interviewer's psychological biases and prevent contamination of the witness's memory. This is particularly relevant to the situation of the crown witnesses, as their statements need to be credible and exempt from damaging external influences.

5. **Adaptability.** Investigative interviewing can be tailored to the specific needs and characteristics of the interviewee. This flexibility allows interviewers to correctly address psychological and tactical issues that arise during the interview. It also refers to the understanding of the crown witness's motivation for cooperation, such as leniency or a desire for redemption, that may influence the content of their testimonies.

6. **Validation and clarification.** The investigative interviewing emphasises the importance of proper validation of the interviewee's account by probing for details that align with known evidence or can be verified later during further inquiry.

In addition, the Méndez principles recommend that all interviews be documented comprehensively, preferably through audio or video recording. In the case of crown witnesses, the later analysis of the recordings may help to reveal patterns of withholding or apparent inconsistencies that need further scrutiny. Proper documentation of the interview enhances the credibility of the witness's statements in legal proceedings. The defence team is more likely to challenge the reliability of testimony from crown witnesses, given their motivations for cooperation. A recorded and thoroughly documented interview process serves as an objective basis to counter such challenges. It allows for subsequent inquiries to verify that the witness was not coerced, misled or improperly influenced – important concerns given the unique, sensitive position of crown witnesses. It is worth noting that the mandatory recording of quasi-crown witness interviews is among the recommendations issued by the Polish Ombudsman in his recent appeal to the Minister of Justice to expedite appropriate legislative changes. The Ombudsman supports his position by highlighting the risks of such witnesses refusing to cooperate during court proceedings, as along with the challenges faced by the defence when unable to attend pretrial interviews. The recordings may also provide a reliable account of the conditions under which the testimony was given, addressing any concerns about potential coercion or unlawful influence by law enforcement. The Ombudsman underscores that reliance on written protocols alone is insufficient to meet the standards of a fair trial, particularly in cases where the prosecution's evidence depends heavily on such testimonies. This procedural reform is deemed essential to uphold the principles of adversarial proceedings, equality of arms and the right to a robust defence (Starzewski, 2025).

In the case of a crown witness *sui generis*, their testimonies during the first stage of the status-awarding procedure – namely, when being interrogated by the prosecutor and then by the court – are documented using written protocols. The law does not mandate audio or video recordings, which is often explained by security concerns. Nonetheless, this limitation raises questions about the transparency and reliability of the documentation process. The absence of audiovisual recording can lead to disputes over the accuracy of the testimony, as written protocols may fail to capture all the nuances of the interrogation. While security concerns are valid, these can be addressed by implementing robust data protection measures and restricting access to the recordings.

The following table provides a comparative overview of the main procedural and methodological distinctions between current Polish interviewing practices and those recommended by the Méndez principles.

Table 7.1. Comparison of Polish interviewing practices and the Méndez principles

Aspect	Current practices	Méndez/investigative interviewing
Question style	Predominantly closed, confirmatory, often confrontational	Open-ended, exploratory, rapport-based
Documentation	Written protocols	Audiovisual recording
Focus	Confirmation, confession	Rapport, recall, accuracy
Defence participation	Limited	Encouraged to ensure fairness
Oversight	Internal controls	Independent review, accountability

The comparison above demonstrates that adopting the Méndez principles could strengthen both the procedural transparency and the evidentiary credibility of cooperating witness interviews in the Polish criminal justice system.

Conclusions

1. The application of the Méndez principles offers significant potential for enhancing the reliability of crown witness testimonies by offering scientifically grounded tools to enhance the effectiveness of interviews. By adopting non-coercive and ethical interviewing techniques, law enforcement can improve the accuracy and reliability of information gathered from both crown and quasi-crown witnesses.

2. The Méndez principles prioritise the protection of witness rights, ensuring interviews are conducted ethically and following international human rights standards, which is essential for maintaining the overall legitimacy of the criminal justice system.

3. One key element of the Méndez principles is the emphasis on building rapport, which can be particularly useful when dealing with high-ranking interviewees who can be familiar with investigative processes and common interviewing techniques. By fostering trust, interviewers can ensure cooperation without resorting to pressure or intimidation, facilitating reliable and comprehensive testimonies. Implementing these recommendations can strengthen the evidentiary value of the crown witness's testimony by addressing potential legal challenges based on the assumption that the witness's statements are coerced and unreliable.

4. The comprehensive documentation of the interview, including audio and video recordings, serves as a safeguard, enhancing the credibility of the investigative processes and protecting against potential disputes over the reliability of the crown witness's statements.

5. Recommendations for implementation in Poland: introduce mandatory audiovisual recording of cooperating witness interviews; provide training in investigative interviewing for prosecutors and investigators; clarify defence participation rules to enhance transparency; establish independent oversight to ensure compliance with ethical and methodological standards.

References

Bull, R. (2013), 'What is "believed" or actually "known" about characteristics that may contribute to being a good/effective interviewer?', *Investigative Interviewing: Research and Practice*, Vol. 5, Issue 2, pp. 128–143, https://iiirg.org/wp-content/uploads/2021/02/II-RP-Volume-5-Issue-2-Bull.pdf.

Bull, R. (2014), 'When in interviews to disclose information to suspects and to challenge them?', in: Bull, R. (ed.), *Investigative Interviewing*, Springer Science, New York, pp. 167–182, https://psycnet.apa.org/doi/10.1007/978-1-4614-9642-7_9.

Bull, R. (2018), 'PEACE-ful interviewing/interrogation: What research can tell us', in: Shigemasu, K., Kuwano, S., Sato, T. and Matsuzawa, T. (eds), *Diversity in Harmony – Insights from psychology: Proceedings of the 31st International Congress of Psychology,* John Wiley and Sons, New York, pp. 189–210, https://doi.org/10.1002/9781119362081.ch10.

Bull, R. (2023), 'Improving the interviewing of suspects using the PEACE model: A comprehensive overview', *Canadian Journal of Criminology and Criminal Justice*, Vol. 65, Issue 1, pp. 80–91, https://psycnet.apa.org/doi/10.3138/cjccj.2023-0003.

Clarke, C. and Milne, R. (2017), 'Interviewing suspects in England and Wales', in: Walsh, D., Oxburgh, G., Redlich, A. and Myklebust, T. (eds), *International developments and practices in investigative interviewing and interrogation – Volume 2: Suspects*. Routledge, London, pp. 133–152, https://doi.org/10.4324/9781315769677.

College of Policing (2022), 'Investigative interviewing', College of Policing website, first published 23 October 2013, https://www.college.police.uk/app/investigation/investigative-interviewing/investigative-interviewing.

European Cooperation in Science and Technology (2023), 'Memorandum of Understanding for the implementation of the COST Action "Establishing networks to implement the principles on effective interviewing for investigations" (ImpleMéndez) CA22128', COST 038/23, https://e-services.cost.eu/files/domain_files/CA/Action_CA22128/mou/CA22128-e.pdf.

Judgment of the Court of Appeal in Warsaw of 16 November 2016, II AKa 148/16, LEX nr 2174843.

Judgment of the Court of Appeal in Warsaw of 29 October 2018, II AKa 324/18, LEX nr 2592965.

Fisher, R. P. (2010), 'Interviewing cooperative witnesses', *Legal and Criminological Psychology*, Vol. 15, Issue 1, pp. 25–38, https://doi.org/10.1348/135532509X441891.

Gudjonsson, G. H. (2023), 'Background to interviewing vulnerable persons', in: Oxburgh, G. E., Myklebust, T., Fallon, M. and Hartwig, M. (eds), *Interviewing and Interrogation: A review of research and practice since World War II*, Torkel Opsahl Academic EPublisher, Brussels, pp. 71–101, https://www.cilrap.org/interviewing.

Gudjonsson, G. H. and Pearse, J. (2011), 'Suspect interviews and false confessions', *Current Directions in Psychological Science*, Vol. 20, Issue 1, pp. 33–37, https://psycnet.apa.org/doi/10.1177/0963721410396824.

Halley, J., Walsh, D., Myklebust, T. and Bjerknes, O. T. (2023), 'Structured models of interviewing', in: Oxburgh, G. E., Myklebust, T., Fallon, M. and Hartwig, M. (eds), *Interviewing and Interrogation: A Review of Research and Practice Since World War II*, Torkel Opsahl Academic EPublisher, Brussels, pp. 271–281.

Hoekstra, M. R. (2024), 'Dynamic aspects of investigative interviewing high-status fraud suspects', *Investigative Psychology and Offender Profiling*, Vol. 22, Issue 1, e1641, https://doi.org/10.1002/jip.1641.

Horosiewicz, K. (2015), *Współpraca z osobowymi źródłami informacji*, Wolters Kluwer, Warsaw.

Kowalewska-Borys, E. (2004), 'Instytucja świadka koronnego w świetle zasady prawdy materialnej', in: Marek, A. (ed.), *Współczesne problemy procesu karnego i jego efektywność*, TNOiK, Toruń, pp. 179–189.

Kowalewska-Borys, E. (2004), *Świadek koronny w ujęciu dogmatycznym*, Zakamycze, Kraków.

Lach, A. (2019), 'Świadek koronny jako źródło dowodów', in: P. Hofmański (ed.), *System Prawa Karnego Procesowego,* Wolters Kluwer, Warsaw, pp. 4853–4871.

Mistygacz, M. (2020), '„Mały świadek koronny" w świetle zasad procesu karnego', in: Hara, G. and Mrowicki, M. (eds), *Instytucja „małego świadka koronnego" – praktyka, kontrowersje, wyzwania*, Biuro Rzecznika Praw Obywatelskich, Warsaw, pp. 29–51, https://bip.brpo.gov.pl/pl/content/instytucja-malego-swiadka-koronnego-praktyka-kontrowersje-wyzwania.

Mrowicki, M. (2020), 'Instytucja małego świadka koronnego w praktyce sądów powszechnych', in: Hara, M. and Mrowicki, M. (eds), *Instytucja „małego świadka koronnego" – praktyka, kontrowersje, wyzwania*, Biuro Rzecznika Praw Obywatelskich, Warsaw, pp. 13–28, https://bip.brpo.gov.pl/pl/content/instytucja-malego-swiadka-koronnego-praktyka-kontrowersje-wyzwania.

Potulski, S. (2024), *Świadek koronny w polskim procesie karnym: Ocena instytucji z perspektywy sędziego i adwokata*, Wolters Kluwer, Warsaw.

Powell, M. B., Fisher, R. P. and Wright, R., 'Investigative interviewing', in: Brewer, N., Kipling, D. and Williams, D. (eds), *Psychology and Law: An empirical perspective,* Guilford Press, New York, 2005, pp. 11–42, https://psycnet.apa.org/record/2005-07316-002.

'Principles on effective interviewing for investigations and information gathering' (2021), interviewingprinciples.com website, https://interviewingprinciples.com/#comp-179e548ce41.

Council of Europe (2022), 'Recommendation of the Committee of Ministers to member States on the protection of witnesses and collaborators of justice', CM/Rec(2022)9, https://search.coe.int/cm?i=0900001680a5fe33.

Judgment of the Supreme Court of Poland of 7 March 2001, IV KKN 617/00, *OSNKW*, 2001(7–8), p. 60.

Judgment of the Supreme Court of Poland of 4 April 2013, II KK 67/13, LEX nr 1317923.

Starzewski, Ł. (2025), 'Problemy z instytucją tzw. "małego świadka koronnego". Kolejne pismo Rzecznika do MS' ['Problems with the institution of the so-called "minor crown witness". Another letter from the Commissioner to the Ministry of Justice'], Rzecznik Praw Obywatelskich website, https://bip.brpo.gov.pl/pl/content/rpo-maly-swiadek-koronny-problemy-ms-kolejne.

Taracha, A. (2006), *Czynności operacyjno-rozpoznawcze: Aspekty kryminalistyczne i prawnodowodowe*, Wydawnictwo UMSC, Lublin.

Tartaro, C. (2021), *Research Methods for Criminal Justice and Criminology: A text and reader*, Routledge, London, https://doi.org/10.4324/9781003051763.

United Nations (2022a), Resolution adopted by the General Assembly on 15 December 2022, 'Torture and other cruel, inhuman or degrading treatment or punishment', 77/209, 5 January 2023, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/762/02/PDF/N2276202.pdf?OpenElement.

United Nations (2022b), Resolution adopted by the general assembly on 15 December 2022, 'Human Rights in the Administration of Justice', 77/219, 6 January 2023, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/762/62/PDF/N2276262.pdf?OpenElement.

United Nations (2024), *Manual on Investigative Interviewing for Criminal Investigation*, https://resourcehub01.blob.core.windows.net/$web/Policy %20and %20Guidance/corepeacekeepingguidance/Thematic %20Operational %20Activities/Police %20and %20Law %20Enforcement/2024.01 %20Manual %20on %20Investigative %20Interviewing %20for %20Criminal %20Investigation %20(2024).pdf.

Vallano, J. P. and Schreiber Compo, N. (2011), 'A comfortable witness is a good witness: Rapport-building and susceptibility to misinformation in an investigative mock-crime interview', *Applied Cognitive Psychology*, Vol. 25, Issue 6, pp. 960–970, https://psycnet.apa.org/record/2011-27489-015.

Walsh, D. and Bull, R. (2010), 'What really is effective in interviews with suspects? A study comparing interviewing skills against interviewing outcomes', *Legal and Criminological Psychology*, Vol. 15, Issue 2, pp. 305–321, https://doi.org/10.1348/135532509X463356.

Wiliński, P., 'Przesłuchanie świadka anonimowego (świadka incognito)', in: Skorupka, J. (ed.), *System Prawa Karnego Procesowego. Tom VIII Dowody. Część 4*, Wolters Kluwer, Warsaw, pp. 4781–4798.

Disinformation as a service: The emerging high-risk criminal networks of 'influence' operators

Zaur Gouliev

https://doi.org/10.3013/ysdm1y14

Abstract

Disinformation is no longer confined to state propaganda or isolated online actors; it has become a commodified criminal service. Networks of influence operators now offer disinformation as a service, executing campaigns for paying clients, including state actors and private entities, in the same manner as cybercrime-for-hire schemes. This convergence of disinformation, cybercrime and organised criminal structures constitutes a major internal security threat. These hybrid operations blur the distinction between state-backed activity and criminal enterprise, complicating attribution, disruption and prosecution. In effect, disinformation has become an underworld commodity, one that exploits the reach of global digital infrastructure to manipulate public opinion at scale. This study examines disinformation as a service through a multilayered methodology combining three lines of evidence. First, a case study of the 'Doppelganger' campaign shows how state-linked operators assembled and maintained a large-scale disinformation network using cloned media sites, ad-tracking software and bulletproof hosting. Second, a market-based supply analysis of over 25 Surface Web and 15 Dark Web marketplaces identifies the retail ecosystem behind influence for hire, documenting the sale of engagement, narrative amplification and targeting services. Third, a macro-level analysis shows the wider landscape of foreign information manipulation and interference within the context of elections. We map actor trends, attack patterns and evolving tactics. The findings reveal a mature criminal ecosystem in which influence operations are traded as modular services, supported by technical infrastructure borrowed from cybercrime markets. The article concludes by assessing the implications for European law enforcement.

Keywords: Disinformation as a service, organised cybercrime, high-risk cybercriminal networks, election interference, foreign information manipulation and interference.

Introduction

Organised cybercrime adapts quickly to advances in policing (National Crime Agency, 2024). Networks increasingly buy infrastructure and operational support from service providers that sell crime-as-a-service capabilities at scale, a pattern observed in markets for cybercrime services (Collier et al., 2021). These vendors supply tooling and tradecraft that frustrate forensic work while improving anonymity and operational security (National Cyber Security Centre, 2023). In parallel, disinformation as a service (DaaS) has started emerging, with state and non-state actors purchasing influence operations from motivated criminals. Documented cases have found these 'entrepreneurs of influence' turning disinformation and fake news into an instrument of hybrid warfare (Laruelle et al., 2021). Scholarship on DaaS is sparse; adjacent work examines profit incentives in advertising technology, cyber-enabled fraud and market infrastructures for crime as a service (e.g. Braun et al., 2019; Loukas et al., 2020; McGuire et al., 2013; Collier et al., 2021; Brangetto et al., 2016; Pijpers et al., 2020). Prior studies also show loose, hybrid online–offline structures rather than single hierarchies (Broadhurst et al., 2014), noting: 'a wide variety of organizational structures … enterprise or profit-oriented activities … require leadership, structure, and specialisation.'

These services range from hiring fake influencers to push hashtags to launching full-spectrum campaigns using stolen data and cloned news sites. DaaS lowers the barrier to entry and makes capabilities once reserved for states available at a lower cost. Vendors on encrypted channels openly market troll farms, bot networks and turnkey fake-news packages alongside malware and access. Automation and, increasingly, AI strengthen scale, speed and persistence across botting, phishing, account takeover and content production (United Nations Office on Drugs and Crime, 2025). Clients include authoritarian regimes and profit-seeking organisations that purchase bespoke influence services (Insikt Group, 2019; Thomas et al., 2023). These actors deploy computational propaganda to destabilise societies and erode trust in institutions, an issue now treated as a European security risk (Arceneaux et al., 2021; Shahbaz, 2018; Oxford Internet Institute, 2020; Bradshaw et al., 2020; Colomina et al., 2021). Convergence between influence operators and organised cybercrime is increasingly visible. The Russian-linked 'Doppelganger' campaign shows how ideology and criminal capability intersect (VIGINUM, 2023; EU DisinfoLab, 2025). Recent unrest illustrates the societal harm being inflicted. During the Dublin riots in November 2023 and the Southport riots in August 2024, influence networks exploited crime events and spread unverified claims about perpetrators' immigrant status, which fuelled anti-immigrant sentiment and violence. Telegram, X (formerly Twitter) and Gab were key dissemination platforms. In Dublin, anonymous Telegram channels coordinated rioting that escalated into looting, assaults on Gardaí and attacks on migrant camps. In Southport, narratives about a 'two-tier justice system' catalysed protests across the United Kingdom and Northern Ireland, with far-right groups coordinating real-time attacks on mosques and asylum centres (Gouliev et al., 2024; Dunne, 2024; Institute of Strategic Dialogue, 2024). Research indicates that many of the relevant channels were run by foreign actors and amplified awareness of the riots (Morley-Davies, 2024; O'Keeffe, 2024; McDermott, 2024). The pattern is platform agnostic across mainstream and alt-tech services, and actors rebuild quickly even after arrests and takedowns, aided by decentralised platforms and weak moderation.

Operationally, campaigns blend ideological aims with profit and draw on a commoditised market. We analysed over 25 Surface Web forums and about 15 Dark Web forums. For operational reasons we do not name venues, and we include only redacted snippets. Listings show marketplaces selling influence capability using illegal bots and tooling that seed, amplify and target content. Dedicated sections advertise hacking tools, and we observe clear expansion into social media manipulation services. Behavioural analysis of traders shows the same actors offering

crimeware and influence tooling in parallel, including bundles that pair stealer logs, remote-access tools, ransomware, rootkits and bulletproof hosting with social media marketing (SMM) panels, account farms, bulk SMS and engagement boosts.

We also examined bot artefacts linked to the 'Doppelganger' campaign, which indicate that cybercrime infrastructure is being reused in inside information operations. This article combines that supply-side evidence with a 'Doppelganger' case study and a quantitative analysis of foreign information manipulation and interference (FIMI) incidents from the Institute of Global Politics. We describe the tactics, techniques and procedures (TTPs), the actors and the infrastructure, and we set out implications for law enforcement ahead of CEPOL 2025.

The 'Doppelganger' campaign

The Doppelganger campaign operationalises the DaaS supply chain described above. EU and US reporting link the activity to Russian entities, and describe an architecture built from disposable front-end domains, a traffic-direction layer and high-fidelity clones of legitimate outlets. First reported in mid 2022, the operators copied recognised media brands and placed pro-Kremlin material into European information spaces; this was then widely copied. Lookalike sites of outlets such as *Bild*, *20 Minutes*, *ANSA*, *The Guardian* and *RBC* appeared. The network registered typosquatted domains, replicated design and typography and published locally targeted headlines. Distribution relied on seeded social accounts and cross-posting across channels. A commercial tracker sat at the centre. Keitaro, an advertising platform, was repurposed to enforce geofencing, ASN (autonomous system number) / IP (Internet Protocol) checks, referrer and user-agent rules and time-of-day scheduling so that users in different locations received different content. Posts were timed to match EU time zones and were automated to maximise the volume of posts. The infrastructure prioritised resilience, and bulletproof hosting shielded key nodes. Domains and nameservers rotated, while multistage redirection concealed origins and only served payload pages to in-scope visitors. The same link could return a clone in one country and benign content elsewhere. Known crawler ranges and common research VPN (virtual private network) end points were filtered or shown decoys. Cloned pages doubled as phishing lures for credential capture. Some delivery chains carried malware. Procurement and payments used cryptocurrency for domains, hosting, traffic purchases and cash-out. The workflow matches call-centre-style fraud operations that use the same proxy infrastructure and labour markets, placing these providers inside the broader cybercrime economy rather than outside it.

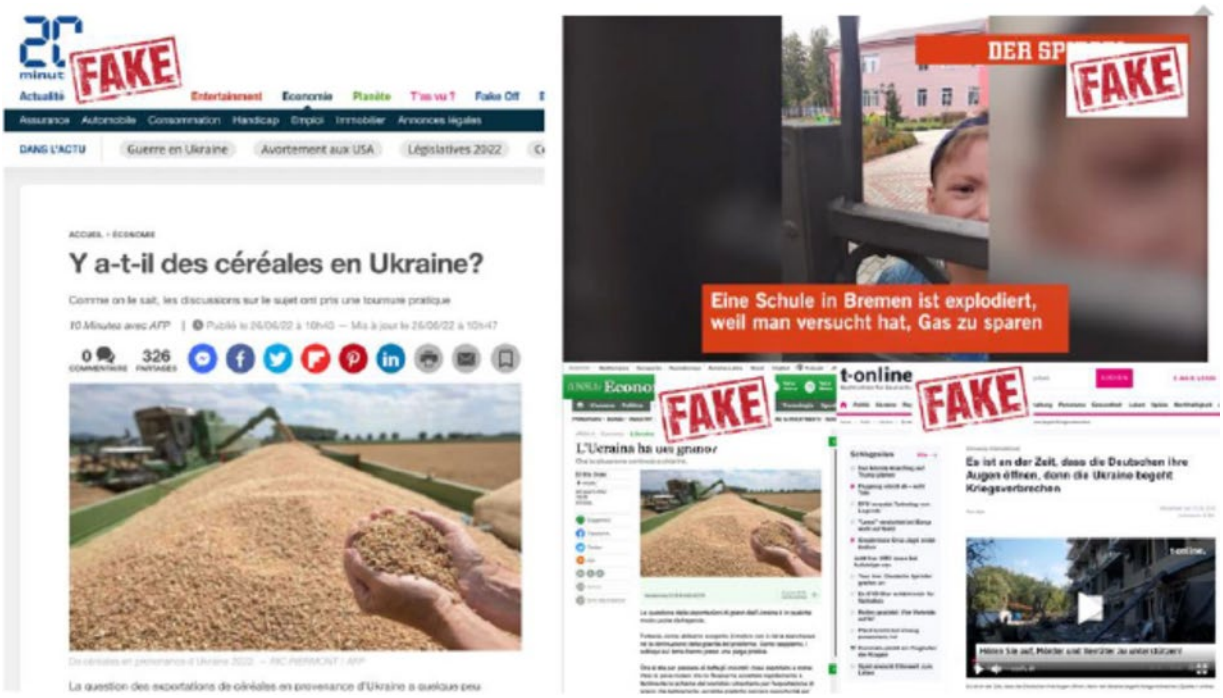


Figure 8.1. Cross-platform delivery in the 'Doppelganger' campaign

Source: EU DisinfoLab.

The core payload sits on cloned news web pages, and traffic is driven by seeded social accounts on mainstream platforms (e.g. Facebook, X (formerly Twitter)). The campaign mixes formats, articles, image overlays, subtitled video and sponsored ads to funnel users back to the clones for narrative uptake and further propagation ([18]). Operators registered many small permutations of media URLs, for example 'washingtonpost.pm'. Content moved between nodes, which reduced the value of simple hash matching and complicated historical crawling. Redirection logic changed frequently, sometimes within a day, which weakened static indicators. Figure 8.2 shows enforcement scaling month-on-month while operator output also grows, signalling takedown resilience and quick rebuild cycles. Open reporting associates' parts of the infrastructure with Russian advanced persist threat (APT) capabilities, notably APT28, indicated support from state units to contractor-style teams operating the influence stack.

([18]) EU DisinfoLab, 'Doppelganger – Media clones serving Russian propaganda', EU DisinfoLab website, https://www.disinfo.eu/doppelganger.

Infrastructure of the network

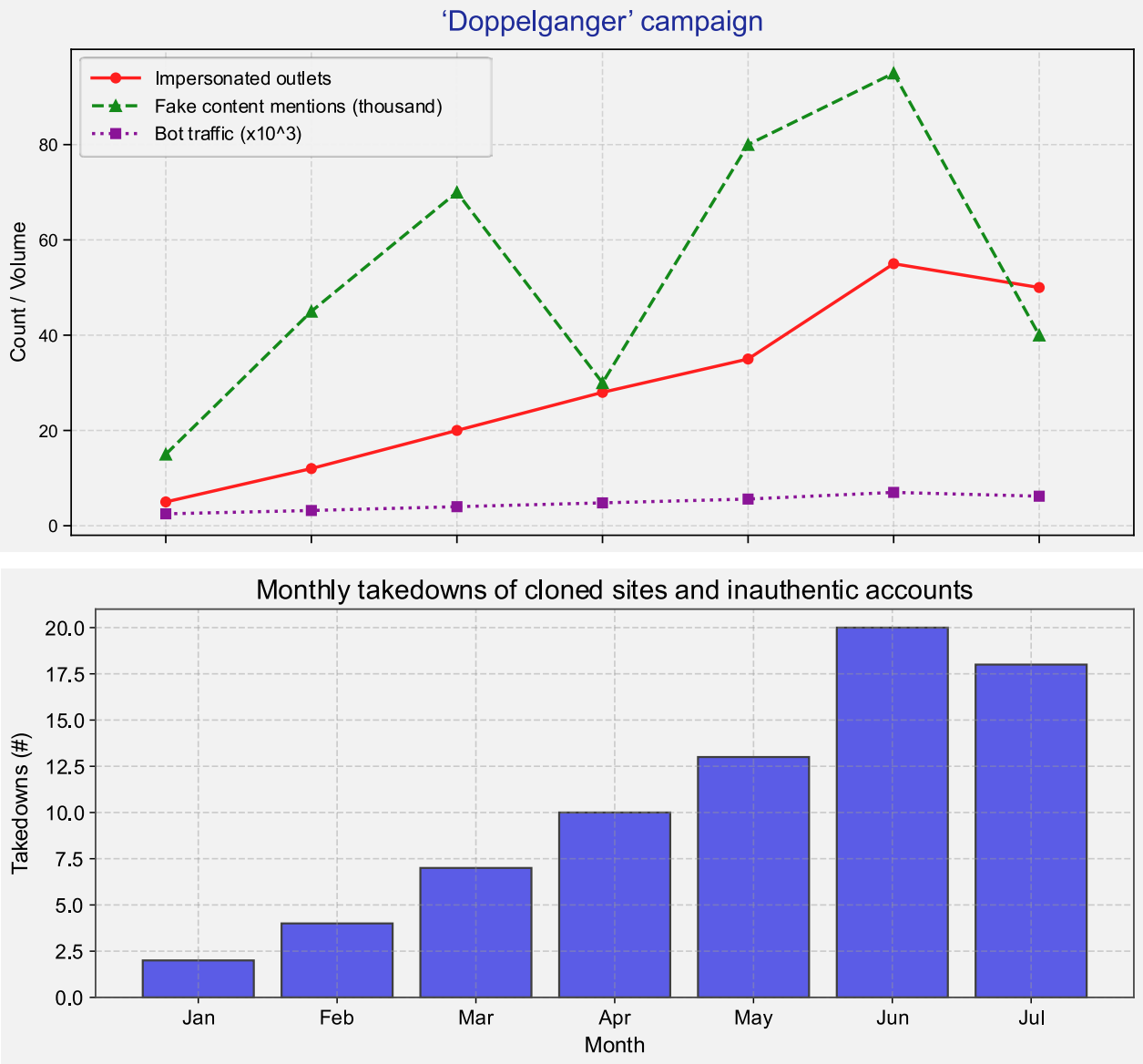


Figure 8.2. Campaign activity versus enforcement, January to July

Source: The author.

The top panel shows growth in impersonated outlets, fake-content mentions (thousands) and bot traffic. The bottom panel shows the monthly takedowns of cloned sites and inauthentic accounts. Outputs rose despite increasing takedowns, with only a modest dip after June, indicating rapid reconstitution and infrastructure churn.

- **Impersonation.** Typosquatted domains mimicking news outlets (e.g. bild.de versus bi1d.de), with cloned design and locally tailored headlines.
- **Distribution.** Seeded social media accounts and cross-posting on multiple platforms to drive traffic to the fake sites.

- **Traffic direction.** Commercial ad-tracking software such as Keitaro was used for geofencing and rule-based delivery that steered users by IP location and matched narratives to local contexts.
- **Automation and timing.** Posting activity aligned with target time zones (e.g. EU daytime) and largely automated to sustain volume.

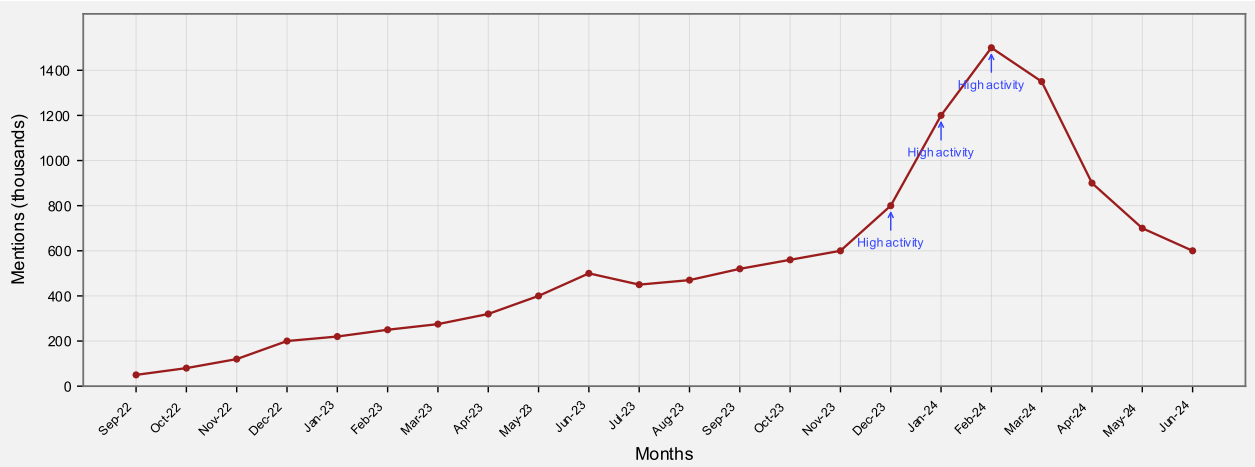


Figure 8.3. Timeline of 'Doppelganger' campaign mentions, September 2022 to June 2024

Mentions climb steadily from late 2022, then spike between December 2023 and March 2024, peaking in February. Activity remained elevated after exposure, suggesting that platform actions did not durably suppress reach and that operators bypassed or rebuilt around removals.

The content strategy tracked Russian geopolitical objectives. During energy price spikes and key political dates, localised stories framed support for Ukraine as costly or unfair and pushed themes aligned with Russian interests. Narrative laundering increased perceived legitimacy: items circulated across multiple clones and then moved through fabricated profiles and community groups, making distribution look organic rather than coordinated. Figure 8.3 highlights post-exposure spikes and sustained volume, consistent with the evasion of platform takedowns.

State reporting attributes the operation to organisations under the Russian presidential administration, including Structura and the Social Design Agency, with direction linked to Sergei Kiriyenko. Evidence cited included domain-registration patterns, technical overlaps across nodes, and internal materials indicating tasking and resourcing. The campaign used AI-assisted content, large-scale cloning and coordinated amplification with automated accounts and fabricated personas. Platform responses were inconsistent. Gaps in domain and hosting policy enabled rapid reconstitution after sanctions and seizures.

Forum-based supply analysis

As part of this research, we analysed over 25 Surface Web forums and 15 Dark Web marketplaces that trade in both cybercrime tools and influence-for-hire services. For operational reasons, we are not naming these platforms, forums and marketplaces. These platforms act as commercial hubs for cybercriminals where influence services have become a routine product category alongside malware, access brokers and credential-stealer logs. Forum sections such as Blackhat and Grayhat include established vendors offering SMMs that provide bulk engagement, content placement

or account management on major social media platforms. Figure 8.4 shows a typical forum hierarchy where influence services appear alongside listings for botnets, keyloggers and operational security support, confirming how manipulation and cybercrime intersect within shared infrastructure.

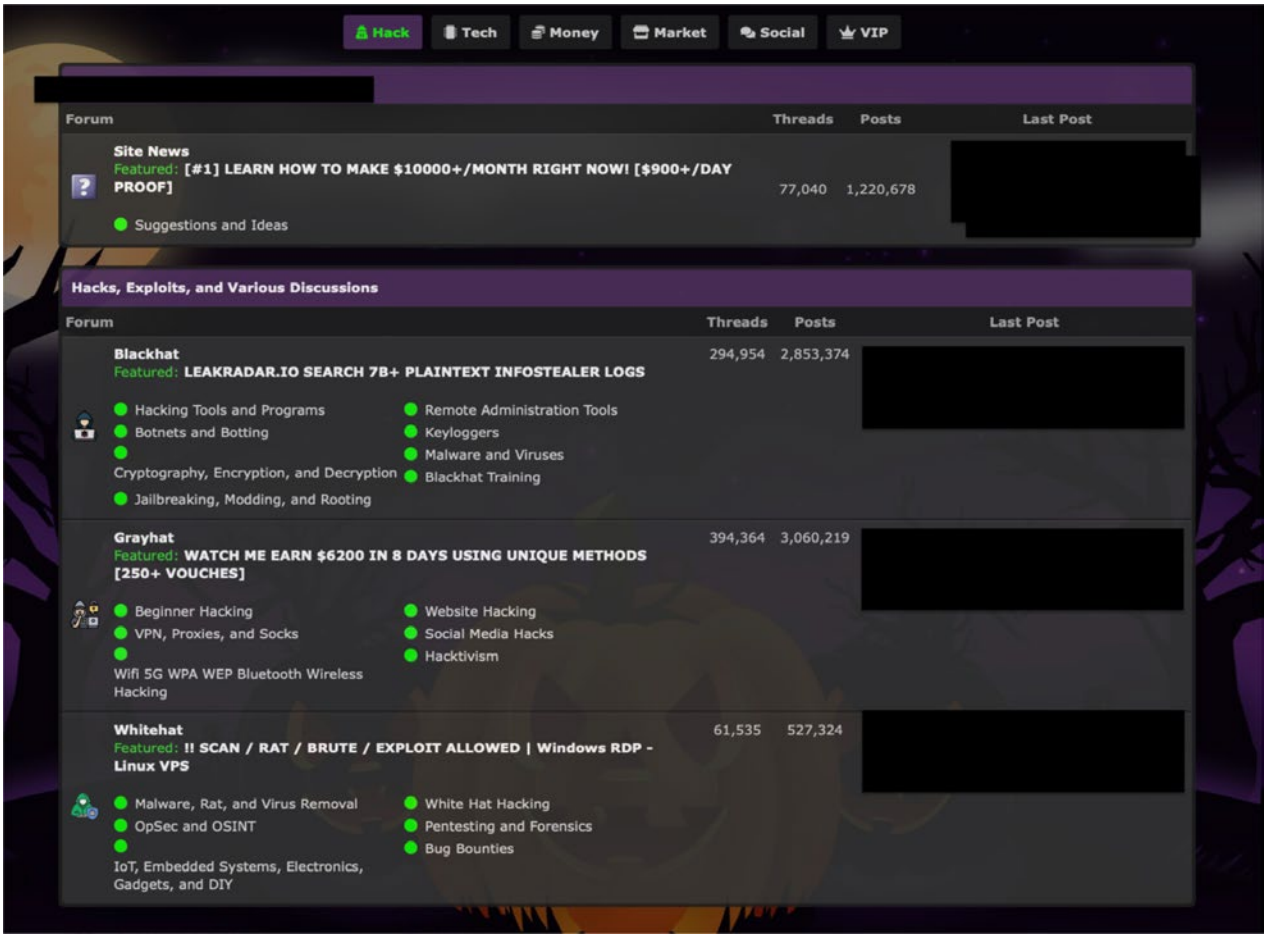


Figure 8.4. Forum index and category structure
Source: The author.

Figure 8.4 presents an index view of a Surface Web forum examined in the investigation. It illustrates how influence-related services are embedded within established cybercrime ecosystems. Sections such as Blackhat, Grayhat and Whitehat host overlapping discussions and vendor threads advertising tools, infrastructure and training. These categories mix traditional cybercrime activities (botnets, keyloggers and remote-access tools) with social media manipulation and 'hacktivism' subforums, showing the convergence of technical exploitation and influence operations under the same market architecture.

Listings across these markets demonstrate a standardised, menu-driven model. Vendors advertise 'verified' or 'aged' accounts, engagement packages and promotion bundles that cover every major platform: Facebook, Instagram, TikTok, Telegram and X (formerly Twitter) (Figures 8.5–8.7). These services include the sale of fake articles, comments, reactions, event promotion, group-member inflation and targeted astroturfing, with optional geographical or demographic filters. Buyers can choose the content type, country, delivery volume and referrer source from drop-down catalogues resembling conventional marketing dashboards. We also obtained access to one of these SMM

tools, confirming the scale of its inventory and its integration with APIs (application programming interfaces) that automate purchases across multiple platforms.

Figure 8.5. Vendor listings offering influence and engagement services
Source: The author.

Active vendor threads advertised SMM panels that automate inauthentic activity across multiple platforms. Each thread represents a commercial offer for engagement metrics such as likes, followers, comments, views or reposts on Facebook, Instagram, YouTube, TikTok, and X (formerly Twitter). Services are presented in a retail format with pricing, bulk discounts, customer reviews and free-trial options. The listings illustrate how this influence manipulation has become a commoditised service, accessible through the same mechanisms as other cybercrime tools.

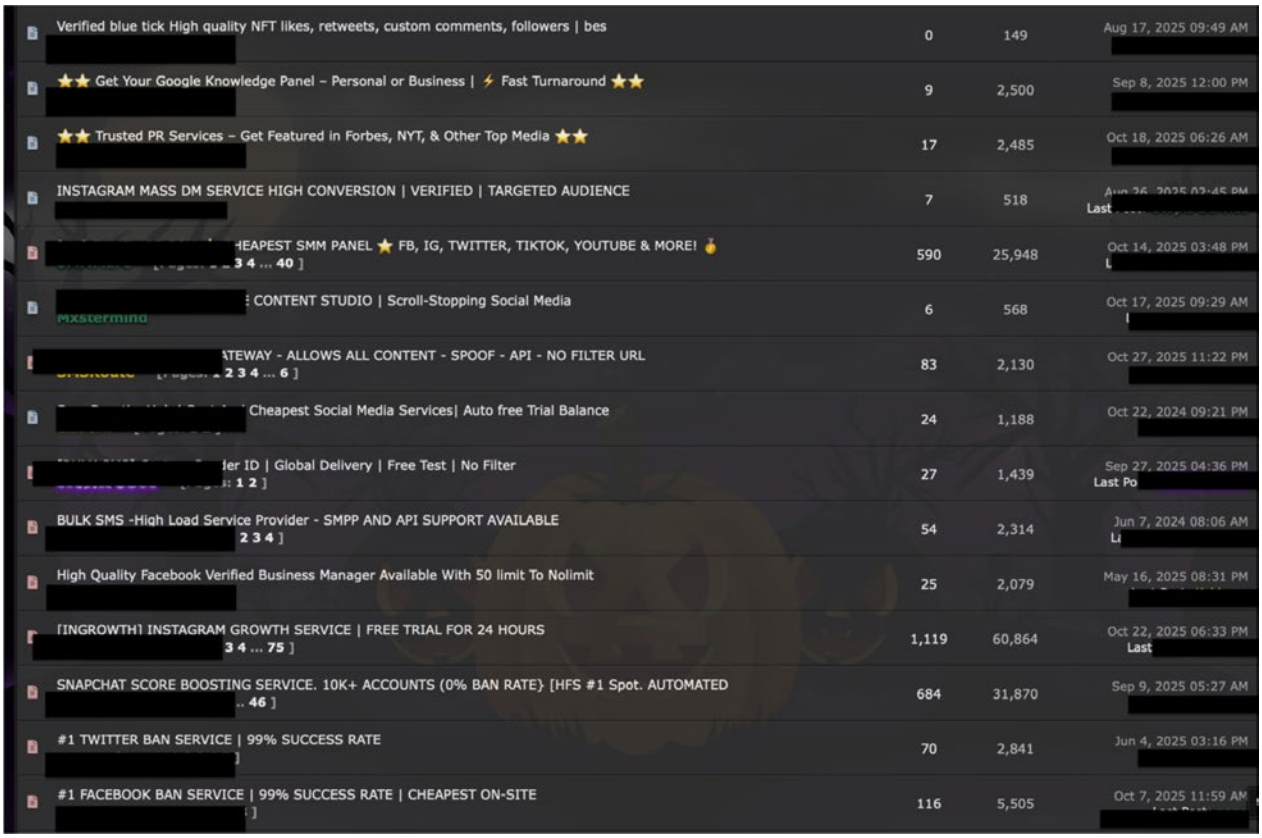


Figure 8.6. Extended marketplace offers supporting influence operations

Source: The author.

Figure 8.6 shows a continuation of the same forum environment where disinformation-related capabilities coexist with wider cybercrime tools. Alongside SMM and engagement services, vendors advertise bulk SMS gateways with API access, sender-ID spoofing and automated delivery systems. Other listings promote account-banning services, verified profile generation and traffic manipulation through API spoofing or 'no-filter' URL methods. Together, these offers illustrate the breadth of the disinformation ecosystem, where influence amplification, infrastructure abuse and account manipulation are available from the same supply base used for conventional cybercrime.

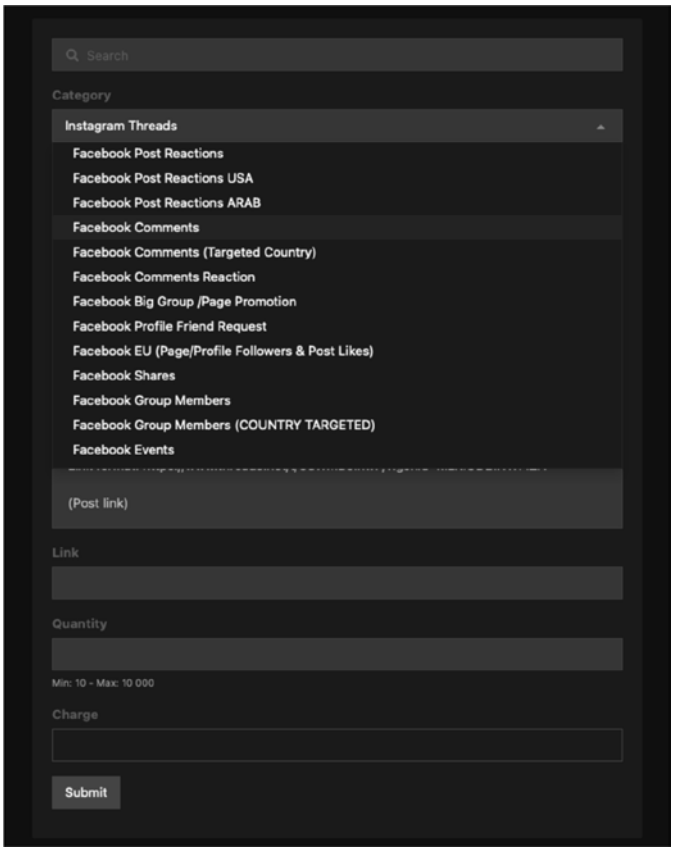


Figure 8.7. Interface of an influence-for-hire automation tool
Source: The author.

Figure 8.7 shows the interface of one of the tools analysed in this study. The platform is purpose-built for automating paid engagement, allowing users to select services, input links and order inauthentic activity at scale. Options include quantity controls, pricing and submission fields, confirming that manipulation services operate through standardised marketing-style dashboards.

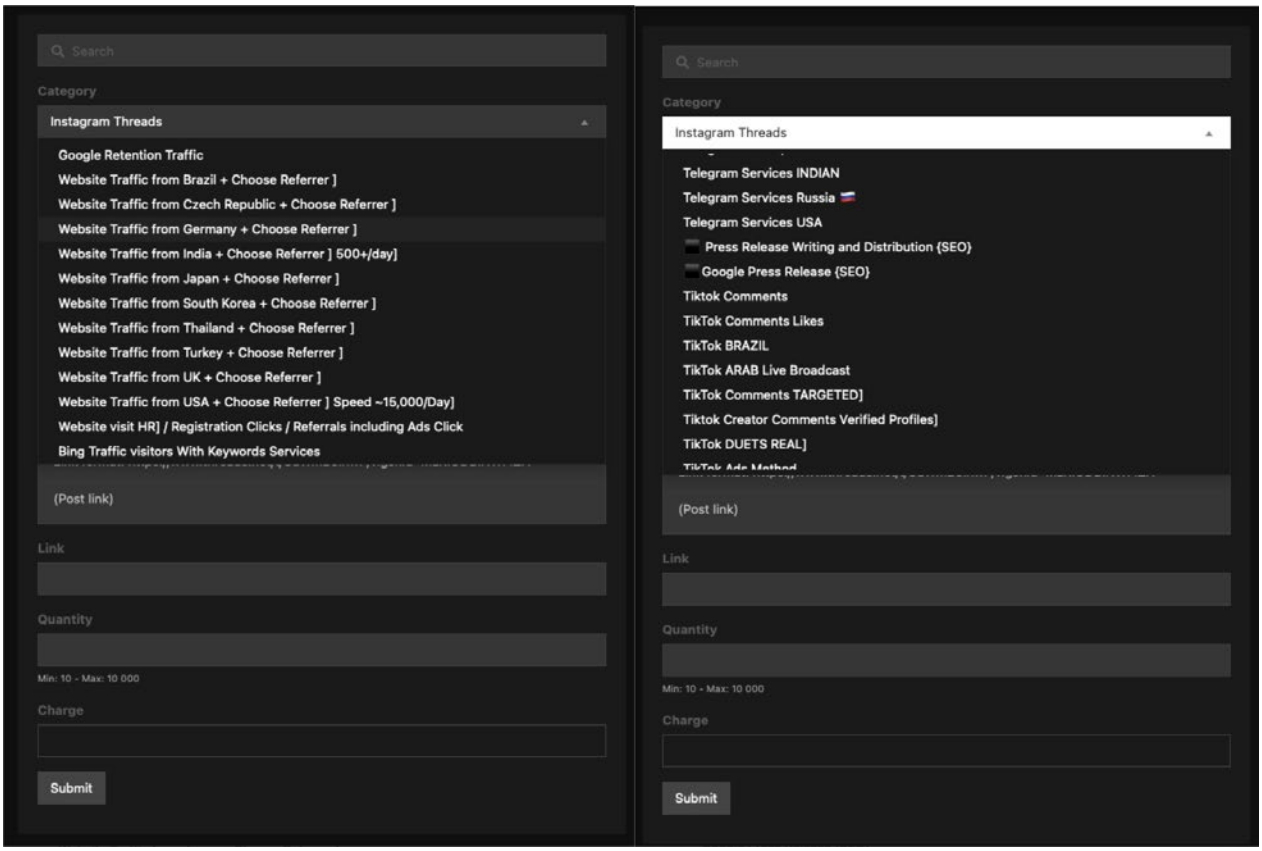


Figure 8.8. Cross-platform service catalogue – Facebook and Meta ecosystem
Source: The author.

NB: Left snippet: this view from the same tool displays Facebook-related categories, offering engagement actions such as post reactions, comments, shares, group-member additions and event promotion. Buyers can specify target countries, languages or audience types, showing how DaaS markets enable precise targeting within mainstream social platforms. Right snippet: this interface section lists traffic and promotion services across Telegram, TikTok, YouTube and regional web domains. It includes press-release distribution, website visits, SEO-based placements and regional targeting options.

The visibility of these services across both Surface Web and Dark Web spaces demonstrates the breadth and normalisation of DaaS. Influence, amplification and visibility can now be purchased through the same retail logic as spam campaigns or credential sales. This commoditised ecosystem forms the operational backbone supporting larger information operations such as the 'Doppelganger' campaign. Having established the micro-level market architecture, the next section moves to a macro-level examination of FIMI incidents.

State-crime convergence in foreign information manipulation and interference

'Doppelganger' showed how a campaign is assembled; the forum review showed where the parts come from. We will now look at the macro level and examine how those market components scale into election-focused FIMI using the Institute of Global Politics election-incident dataset (Fulde-Hardy et al., 2024). Interference concentrates where the payoff is highest, and the calendar is predictable. Presidential contests dominate, followed by general or federal elections; legislative, referendum and municipal contests remain in scope when margins are tight or policy

stakes are visible. This distribution matches a market logic in which clients buy reach and clarity of narrative, and vendors pre-package services for known electoral windows.

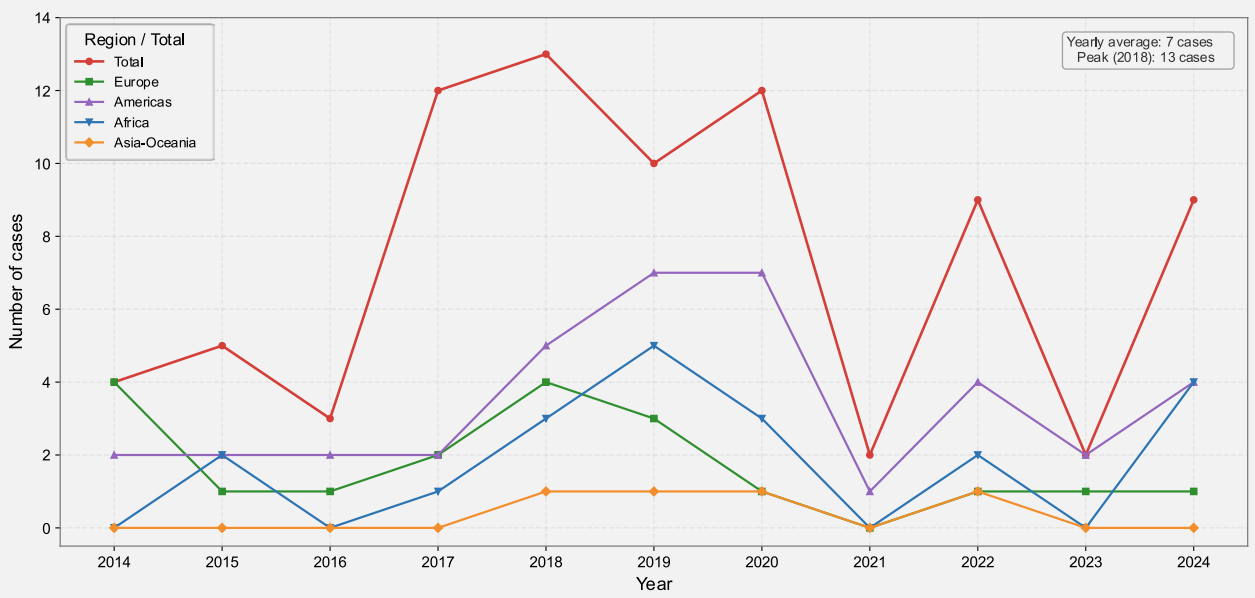


Figure 8.9. Confirmed FIMI election cases, 2014–2024

Source: The author, using the Institute of Global Politics FIMI dataset from Fulde-Hardy et al., 2024.

Figure 8.9 presents the number of confirmed election interference incidents over a 10-year period. The dataset records an average of eight cases per year, with a peak of 13 in 2018. Activity intensifies around major global election cycles, notably in 2018–2020, followed by a brief decline and a renewed rise in 2024. Regional variation shows Europe and the Americas as the most frequent targets, with emerging incidents in Africa and Asia/Oceania. The pattern indicates a cyclical mobilisation of foreign information manipulation around key electoral events rather than a continuous upward trend, suggesting adaptation by both threat actors and platform defenders.

Interference concentrates where the payoff is highest and the calendar is predictable. Presidential contests dominate, followed by general or federal elections; legislative, referendum, and municipal contests remain in scope when margins are tight or policy stakes are visible. This distribution matches a market logic in which clients can buy reach and clarity of narrative, and vendors pre-package services for known electoral windows. Activity comes in waves, and peaks cluster around electoral super-cycles and high-salience crises, followed by adaptation on both attacker and platform sides. The post-2020 dip is better read as a change in tradecraft and reporting than a decline in risk.

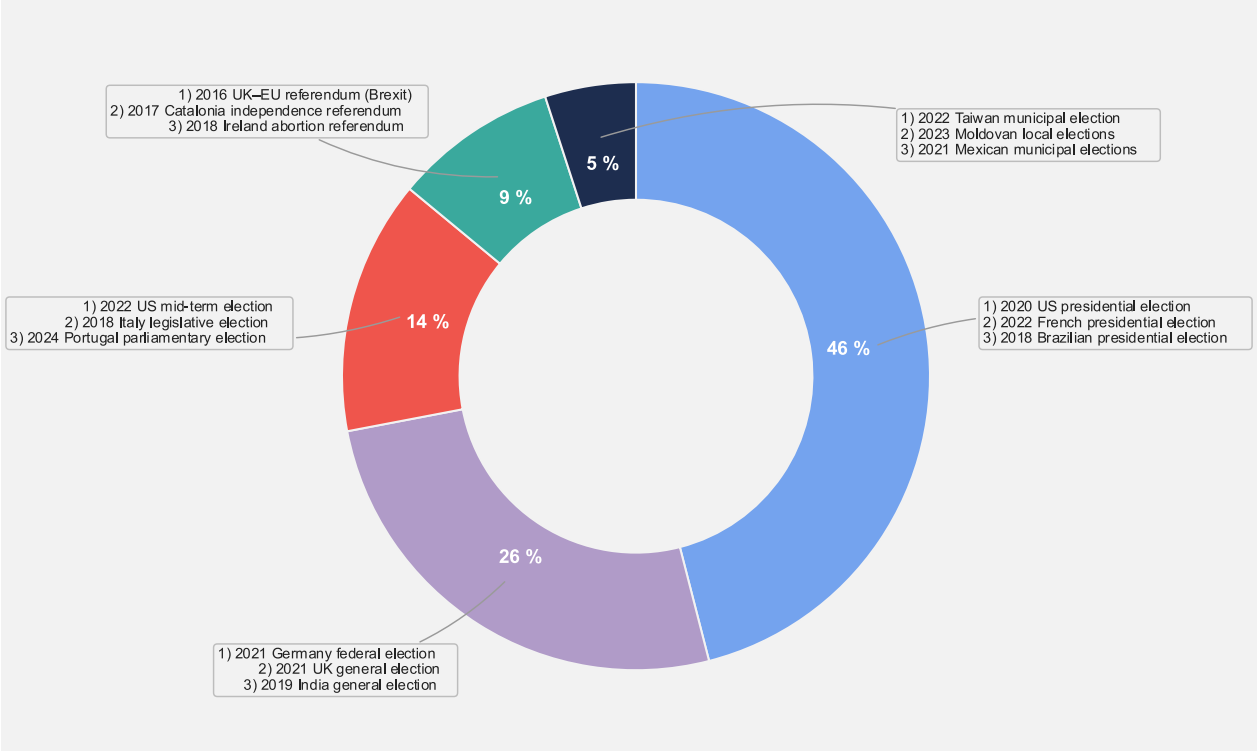


Figure 8.10. Foreign election interference by election type, 2024

Source: The author, using the Institute of Global Politics FIMI dataset from Fulde-Hardy et al., 2024.

Figure 8.10 illustrates the distribution of election types most frequently targeted by foreign interference. Presidential elections represent nearly half of all recorded cases (46 %), reflecting their visibility and strategic importance. General and federal elections account for 26 %, while mid-term and legislative elections make up 14 %. Referendums (9 %) and local or municipal elections (5 %) are also targeted, showing that interference extends beyond national contests to influence political outcomes at multiple levels of governance.

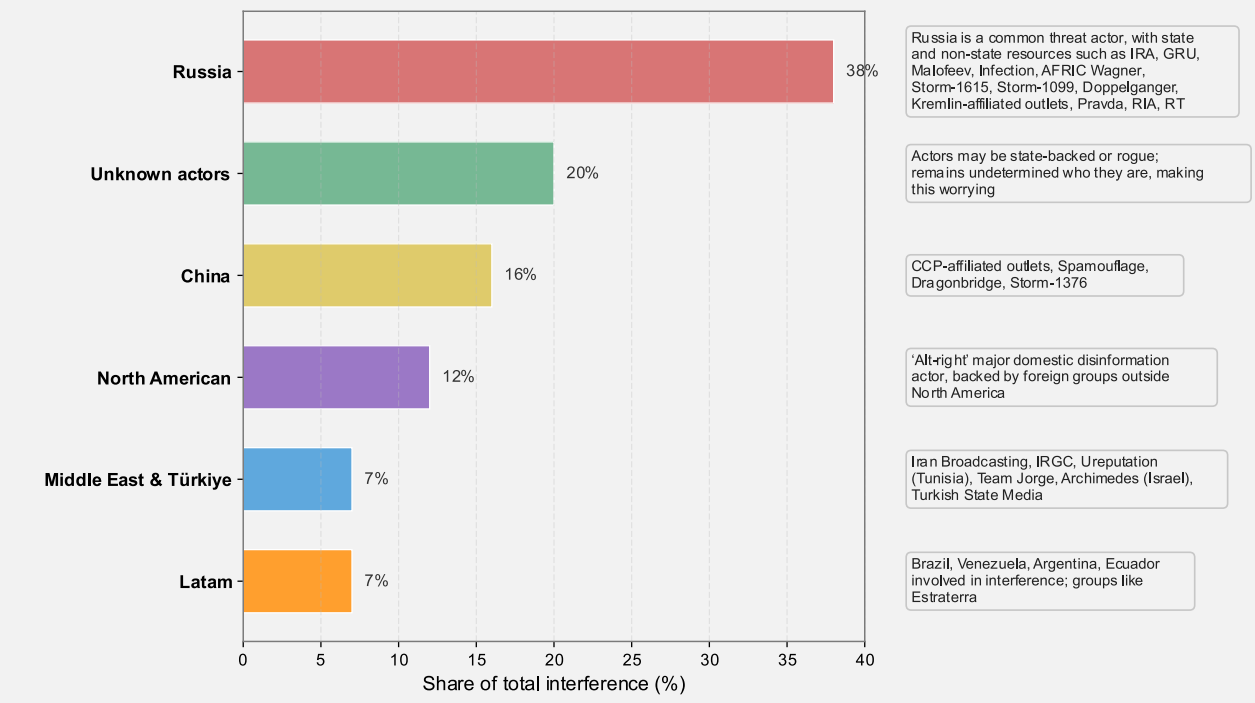


Figure 8.11. Threat actors in foreign election interference, 2024

Source: The author, using the Institute of Global Politics FIMI dataset from Fulde-Hardy et al., 2024.

Figure 8.11 presents the principal actor groups identified in documented cases of foreign election interference. Russia accounts for 38 % of attributed incidents, reflecting its established ecosystem of state and proxy entities such as the Internet Research Agency, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation and campaigns like 'Doppelganger'. China follows with 16 %, primarily linked to coordinated networks such as Spamouflage and Dragonbridge. North American and Middle Eastern actors each contribute smaller shares (12 % and 7 %), while Latin American entities account for another 7 %. Notably, 20 % of the cases remain unattributed, indicating a substantial number of operations that likely involve contractors or hybrid actors, further complicating attribution and enforcement. Attribution reflects the same contractor ecosystem seen on forums. Russia accounts for the largest attributed share, followed by China, and there remains a large unknown segment. That unattributed tranche is consistent with cut-outs, intermediaries and blended state–criminal tasking that frustrate clean linkage.

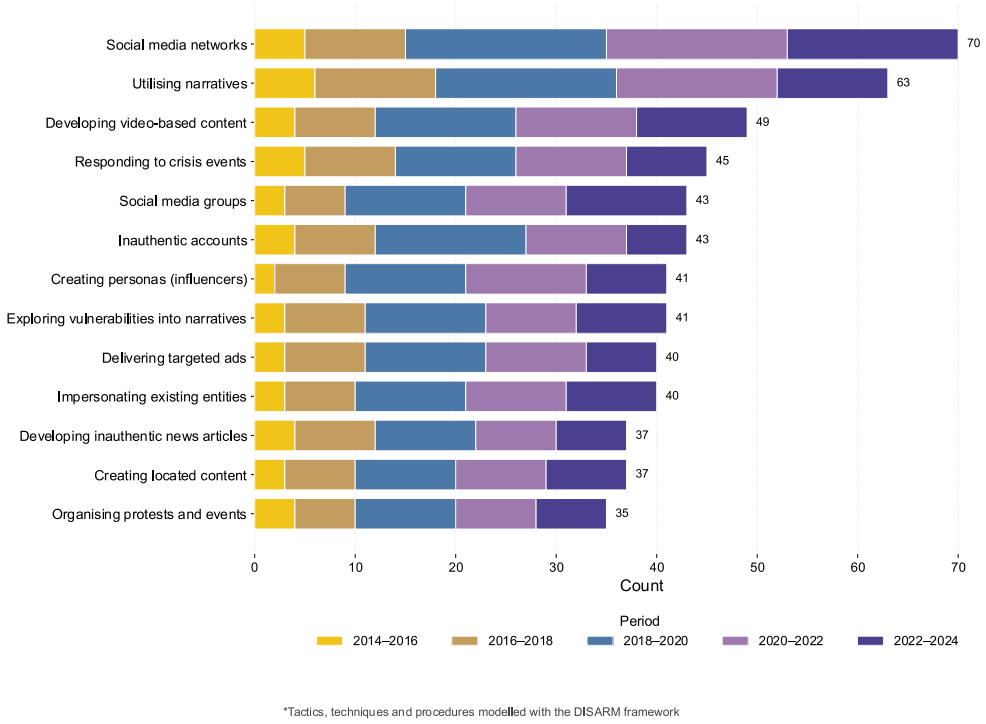


Figure 8.12. Common tactics, techniques and procedures used in foreign information manipulation and interference

Source: The author, using the Institute of Global Politics FIMI dataset from Fulde-Hardy et al., 2024.

Figure 8.12 shows the most frequently observed TTPs across documented FIMI incidents between 2014 and 2024, modelled using the DISARM (disinformation analysis and risk management) framework. The data highlights social media networks and the use of existing narratives as dominant techniques, followed by video-based content, crisis exploitation and the creation of inauthentic accounts. Growth across all categories in recent years (2020–2024) reflects the industrialisation of disinformation tradecraft and its increasing overlap with cybercrime tooling. These methods mirror the DaaS supply market, where services such as persona creation, targeted advertising and social media manipulation are available as packaged capabilities.

The methods line up with what the supply side sells. Social network operations, narrative exploitation, video-led content, inauthentic accounts and personas, targeted advertising and impersonation dominate, with steady growth over time. These behaviours are modular, purchasable and easily reassembled across platforms, which explains their persistence through takedowns and rapid rebuild cycles.

This macro view connects the mechanics of disinformation campaigns to election outcomes: marketised distribution and protection make interference scalable, resilient and timely in relation to democratic events. We next translate these findings into law enforcement tasking and disruption points.

Challenges and countermeasures for law enforcement

The decentralised and borderless nature of these operations present challenges to law enforcement, particularly in attribution and enforcement. Criminal actors exploit jurisdictional complexities, using servers and infrastructure spread across multiple countries, as exemplified by 'Doppelganger' operations. These activities thrive in legal grey zones, complicating prosecution efforts. Moreover, the rapid evolution of adversarial technologies, such as geofencing tools and adversary-in-the-middle (AiTM) kits (Microsoft Threat Intelligence, 2022), often outpaces the development and deployment of countermeasures, leaving law enforcement agencies perpetually on the back foot. International collaboration is critical in addressing these transnational threats, but differing legal frameworks and enforcement priorities among nations impede unified responses. The necessity for cross-border cooperation and knowledge sharing is increasingly recognised, with initiatives such as the VIGILANT (vital intelligence to investigate illegal disinformation) and ATHENA (an exposition on the foreign information manipulation and interference) projects emerging to bolster law enforcement capabilities.

VIGILANT is an EU-funded research project that equips European police authorities with cutting-edge tools to detect and analyse disinformation campaigns. It integrates over 30 forensic and analytical tools into a modular platform and enables law enforcement to identify coordinated networks, fabricated content and tampered multimedia (VIGILANT, 2024). In addition to providing advanced detection capabilities, VIGILANT offers extensive training to police authorities to help enhance their understanding of disinformation's social drivers and psychological impacts. A peer-to-peer network further facilitates the sharing of insights and strategies across jurisdictions, fostering a unified EU response to disinformation campaigns. This is complemented by the ATHENA project, which addresses the broader challenge of protecting democratic processes from FIMI. It combines technical innovation with behavioural and societal analysis to develop novel countermeasures against FIMI (ATHENA, 2024). There are tools such as a disinformation analysis dashboard and a dynamic knowledge graph, which provide actionable insights for governments and law enforcement. Similarly, it offers training and resources in recognising and countering FIMI threats.

Both these projects are promising and well timed by the European Union, as it recognises the need for multidisciplinary strategies, blending technological innovation with social and behavioural insights to address the growing nexus of disinformation and cybercrime.

References

Arceneaux, P. and Harman, M. (2021), 'Social cybersecurity: A policy framework for addressing computational propaganda', *Journal of Information Warfare*, Vol. 20, No 3, pp. 24–43, https://www.jstor.org/stable/27124997.

Brangetto, P. and Veenendaal, M. A. (2016), 'Influence cyber operations: The use of cyberattacks in support of influence operations', in: Pissanidis, N., Rõigas, H. and Veenendaal, M. (eds), *2016 8th International Conference on Cyber Conflict – Cyber power*, NATO CCD COE Publications, Tallinn, https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf.

Braun, J. A. and Eklund, J. L. (2019), 'Fake news, real money: Ad tech platforms, profit-driven hoaxes, and the business of journalism', *Digital Journalism*, Vol. 7, Issue 1, pp. 1–21, https://doi.org/10.1080/21670811.2018.1556314.

Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S. (2014), 'Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime', *International Journal of Cyber Criminology*, Vol. 8, Issue 1, pp. 1–20, https://research-management.mq.edu.au/ws/portalfiles/portal/62156293/Publisher%20version%20(open%20access).pdf.

Chavane, C., Amaury-Jacques, G. and Seznec, K. (2024), 'Master of puppets: Uncovering the DoppelGänger pro-Russian influence campaign', Sekoia, 21 May, https://blog.sekoia.io/master-of-puppets-uncovering-the-doppelganger-pro-russian-influence-campaign/#h-observables.

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A. and Chua, Y. T. (2021), 'Influence, infrastructure, and recentering cybercrime policing: Evaluating emerging approaches to online law enforcement through a market for cybercrime services', *Policing and Society*, Vol. 32, Issue 1, pp. 103–124, https://doi.org/10.1080/10439463.2021.1883608.

Colomina, C., Sánchez Margalef, H. and Youngs, R. (2021), 'The impact of disinformation on democratic processes and human rights in the world', PE 653.635, European Parliament: Directorate-General for External Policies of the Union: Policy Department for External Relations, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf.

Cybersecurity and Infrastructure Security Agency (2022), *Russian state-sponsored and criminal cyber threats to critical infrastructure*, https://www.cisa.gov/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf.

Dunne, S. A. (2024), 'Too far right? The role of alt-tech and mainstream social media platforms in far-right political violence', UCD Centre for Digital Policy, https://digitalpolicy.ie/too-far-right-the-role-of-alt-tech-and-mainstream-social-media-platforms-in-far-right-political-violence-dr-sarah-anne-dunne/.

European Network Against Crime and Terrorism (2024), 'State of play policy report 01 – Public version – September 2024', https://enact-eu.net/enact-state-of-play-policy-report-2024/.

Fulde-Hardy, M. and François, C. (2024), 'IGP releases new dataset of online foreign information operations targeting elections', Institute of Global Politics, 26 June, https://igp.sipa.columbia.edu/news/igp-releases-new-dataset-online-foreign-information-operations-targeting-elections.

Ganguli, P. (2024), 'The rise of cybercrime-as-a-service: Implications and countermeasures', *International Journal for Multidisciplinary Research*, Vol. 6, Issue 5, https://doi.org/10.36948/ijfmr.2024.v06i05.27724.

Gouliev, Z. and Dunne, S. A. (2024), 'Policing alt-tech for disinformation? VIGILANTly moving in the right direction', UCD Centre for Digital Policy, https://digitalpolicy.ie/policing-alt-tech-for-disinformation-vigilantly-moving-in-the-right-direction-zaur-gouliev-and-dr-sarah-anne-dunne/.

Insikt Group® (2019), 'The price of influence: Disinformation in the private sector', *Recorded Future*, 30 September, https://www.recordedfuture.com/research/disinformation-service-campaigns.

Institute of Strategic Dialogue (2024), 'ISD submission on the Irish state's response to disinformation and digital/media literacy', https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_committee_on_tourism_culture_arts_sport_and_media/submissions/2024/2024-11-06_submission-institute-for-strategic-dialogue_en.pdf.

Laruelle, M. and Limonier, K. (2021), 'Beyond "hybrid warfare": A digital exploration of Russia's entrepreneurs of influence, *Post-Soviet Affairs*, Vol. 37, Issue 4, pp. 318–335, https://doi.org/10.1080/1060586X.2021.1936409.

Loukas, G., Patrikakis, C. Z. and Wilbanks, L. R. (2020), 'Digital deception: Cyber fraud and online misinformation', *IT Professional*, Vol. 22, Issue 2, pp. 19–20, https://doi.org/10.1109/MITP.2020.2980090.

Marvi, A., Chew, S. and Boonyakarn, P. (2024), 'Chinese espionage group UNC3886 found exploiting CVE-2023-34048 since late 2021', Mandiant, https://cloud.google.com/blog/topics/threat-intelligence/chinese-vmware-exploitation-since-2021/.

McDermott, S. (2024), 'The disinfluencers: How over 150 anonymous "Irish" accounts are swamping X with extreme views', *The Journal*, https://www.factchecking.ie/articles/the-disinfluencers-how-over-150-anonymous-irish-accounts-are-swamping-x-with-extreme-views.

McGuire, M. and Dowling, S. (2013), 'Chapter 2: Cyber-enabled crimes – fraud and theft', *Cyber Crime: A review of the evidence – Research report 75*, Home Office, https://assets.publishing.service.gov.uk/media/5a755a94e5274a59fa7177f7/horr75-chap2.pdf.

Menlo Security (2024), 'Highly evasive and adaptive threats (HEAT)', Menlo Security website, https://www.menlosecurity.com/what-is/highly-evasive-adaptive-threats-heat.

Microsoft Threat Intelligence (2022), 'From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud', 12 July, https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/.

Microsoft Threat Intelligence (2023), 'Analysis of Storm-0558 techniques for unauthorized email access', 14 July, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/.

Milanovic, M. and Schmitt, M. N. (2020), 'Cyber attacks and cyber (mis)information operations during a pandemic', *Journal of National Security Law and Policy*, Vol. 11, No 1, pp. 247–284, https://centaur.reading.ac.uk/93850/.

Müller, M. (2024), *Looking Doppelganger: An analysis of evolving state-sponsored disinformation tactics*, University of Twente, https://purl.utwente.nl/essays/102708.

Morley-Davies, J. (2024), 'How did foreign actors exploit the recent riots in the UK?', Royal United Services Institute, 28 August 2024, https://www.rusi.org/explore-our-research/publications/commentary/how-did-foreign-actors-exploit-recent-riots-uk.

National Crime Agency (2024), *National Strategic Assessment 2024: Cross-cutting threat enablers*.

National Cyber Security Centre (2023), 'Experts reveal latest insights into world of cyber criminals', 11 September, https://www.ncsc.gov.uk/news/experts-reveal-insights-cyber-crime-ecosystem.

Newman, H. (2022), *Foreign Information Manipulation and Interference Defence Standards: Test for rapid adoption of the common language and framework 'Disarm'*, European Centre of Excellence for Countering Hybrid Threats and NATO Strategic Communications Centre of Excellence, https://www.hybridcoe.fi/wp-content/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf.

O'Keeffe, C. (2024), 'Foreign actors are influencing more extreme protests on the domestic scene', *Irish Examiner*, 6 May, https://www.irishexaminer.com/news/spotlight/arid-41387437.html.

Oxford Internet Institute (2020), 'Computational propaganda: Investigating the impact of algorithms and bots on political discourse in Europe', European Commission website, https://doi.org/10.3030/648311.

Oxford Internet Institute (2021), 'Social media manipulation by political actors an industrial scale problem', University of Oxford website, 13 January, https://www.ox.ac.uk/news/2021-01-13-social-media-manipulation-political-actors-industrial-scale-problem-oxford-report.

Pijpers, P. B. M. J. and Ducheine, P. A. L. (2020), 'Influence operations in cyberspace: How they really work', University of Amsterdam: Amsterdam Center for International Law, https://doi.org/10.2139/ssrn.3698642.

Athena (2024), 'An exposition on the foreign information manipulation and interference', European Commission website, https://doi.org/10.3030/101132686.

Reddick, J. (2024), 'Change Healthcare confirms BlackCat/ALPHV behind ransomware attack', *The Record from Recorded Future News*, 29 February, https://therecord.media/change-healthcare-ransomware-attack-blackcat-alphv.

Shahbaz, A. (2018), Freedom on the Net 2018 – The rise of digital authoritarianism, Freedom House Washington, DC, https://freedomhouse.org/sites/default/files/FOTN_2018_Final.pdf.

Thomas, E. and Reyes, K. D. (2023), 'Commercial disinformation', Institute of Strategic Dialogue, https://www.isdglobal.org/isd-explainer/commercial-disinformation/.

United Nations Office on Drugs and Crime (2025), 'Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia', Cybercrime Technical Brief Series, Regional Office for Southeast Asia and the Pacific, Bangkok https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf.

United States Department of Justice (2024), 'Justice department disrupts covert Russian government-sponsored foreign malign influence operation targeting audiences in the United States and elsewhere', Office of Public Affairs, 4 September, https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence.

Vigilant (2024), 'Vital intelligence to investigate illegal disinformation', Vigilant project website, https://www.vigilantproject.eu/.

Viginum (2023), 'RRN: A complex and persistent information manipulation campaign – Technical report', 19 July, https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf.

Wahlstrom, A., Mainor, D. and Kapellmann Zafra, D. (2024), 'Life after death? IO campaigns linked to notorious Russian businessman Prigozhin persist after his political downfall and death', Mandiant, 28 March, https://cloud.google.com/blog/topics/threat-intelligence/io-campaigns-russian-prigozhin-persist.

How forensic linguistics can help fight international crime ([19])

Luna Filipović

https://doi.org/10.3013/zqwncw42

Abstract

This research-based contribution has two goals: to illustrate some of the areas in which forensic linguistic expertise can help fight international crime and to shed light on the importance of applying knowledge from linguistic research on multilingual communication in forensic investigations. The overall focus is on the evidentiary contribution of forensic linguistic insights obtained through the analysis of communication between law enforcement and suspects or reluctant witnesses and of communication among suspects interacting on the Dark Web. We will provide an overview and examples from the author's peer-reviewed research on police questioning in both the United States and the United Kingdom that highlight multiple aspects relevant to the quantity and the quality of elicited evidence, including the questioning method, awareness about linguistic and cultural differences and quality of language service provisions. We will also take a closer look at some features of non-native English – the language of international crime – and illustrate how this knowledge can be applied in the analysis of communicative exchanges on the Dark Web, resulting in investigative benefits and empirically enriched training courses for police forces globally.

Keywords: forensic linguistics, policing, miscommunication, non-native English, Dark Web.

Introduction

Studying language and communication in the context of organised crime has to be one of the priorities in tackling criminal networks because organised crime starts with communication. Similarly, when perpetrators are apprehended

([19]) This paper is dedicated to the memory of Professor Ross Anderson (Computer Laboratory, University of Cambridge), with whom I was hoping to collaborate for the Dark Web study mentioned here and whose life ended suddenly and unexpectedly over a year ago. Professor Anderson was a pioneer, an innovator and a true giant in the field of cybersecurity, remarkable in every way, as a scholar, friend and fighter for what he believed was right for society. It is my hope that the pilot idea introduced here – of recruiting multilingual forensic linguistic analysis for the purpose of helping the fight against international organised criminal networks on the Dark Web – will inspire (much-needed) further research and practical applications of forensic linguistic analysis in this and related areas.
The author would also like to thank to two anonymous reviewers whose comments and suggestions inspired significant improvements in this paper. Any remaining errors remain exclusively with the author.

it is through communication with them that we stand the best chance of obtaining valuable information that can help prevent future crimes. Forensic linguistics is an empirical discipline that studies language use in the context of criminal law. It is known to have helped solve crime via authorship identification that led to the capture of many serious criminals, with one of the most well-known being the Unabomber in the United States in the 1990s, which is the case that marked the first instance of forensic linguistic evidence being deemed enough to issue a search warrant in the US justice system. Since then, forensic linguists have been used as expert witnesses or consultants more readily in criminal investigations and trials. However, forensic linguistics is still an underutilised tool, since its applications are much broader and wider with a potential to cover many more cases that those in which it is currently used (see Leonard et al., 2017 for further details and examples).

In this paper the focus is on something even more underutilised: a forensic linguistic analysis informed by knowledge about language differences and multilingualism that can, in turn, inform the elicitation of best evidence in the context of international criminal investigations. As a backdrop, this paper briefly describes two main suspect questioning methods (the United States versus the United Kingdom), which are most widely adopted worldwide (and sometimes combined) and which exemplify instances of both good and bad practices from both locales. In particular, the focus is on the cross-linguistic and cross-cultural conflicts arising in suspect questioning that may lead to elicitation of inadequate or misleading evidence. This paper argues that police training highlighting these conflicts with authentic examples from real-life datasets and including forensic linguistic analyses can improve the efficiency and quality of evidence-gathering in international policing. We will then discuss another investigative domain within which multilingual forensic linguistic expertise is very much underutilised, and that is the determination of the language of origin of perpetrators through analyses of chats on the Dark Web with non-native English as a lingua franca. Forensic linguists who are multilingual and understand how English (or any other language) is spoken non-natively by individuals with different first languages can point to features in non-native use that reveal the first languages of the speaker, which can assist in specialist training for discovering which groups are involved in collaborative criminal activities.

Eliciting better evidence through forensic linguistic insights

For the purpose of the discussion and argumentation in this paper, we will rely on a unique database of authentic, real-life exchanges between US and UK law enforcement and suspects in criminal investigation (a total of over 200 cases). So far, approximately half of the database (just over 100 cases) has been processed and studied by the TACIT lab (e.g. Filipović, 2021, 2022a, 2022b; Filipović et al., 2018; Hijazo-Gascón, 2019; Musolff, 2019; Pounds, 2019), and this is where the examples and findings reported in this paper come from. All the data were obtained through research collaborations with various police jurisdictions in California and England that our lab ([20]) engaged in during the last two decades (2006–2026). All the data and publications received ethical permissions from the universities where the author and her academic colleagues were employed. The publication of data excerpts was agreed upon with data providers and all non-anonymous data sections were anonymised prior to publication and used solely for that purpose. The offences included serious crime (armed robbery, homicide, sexual assault). The languages spoken by the victims, witnesses and suspects (other than English) include Spanish, Lithuanian, Polish, Portuguese and Russian. The methodology in the studies presented here included both qualitative and quantitative approaches to data analysis. The conversations in these files were coded by the present author using NVivo12 software (with 30 %

([20]) www.tacit.org.uk.

of the processed data also coded by another coder and tested for interrater reliability, which was 0.98, thus confirming the objectivity of the coding). The coding captures instances of miscommunication that were identified via either (a) clear communication breakdowns (e.g. one of the interlocutors says 'Pardon?', 'Excuse me?', 'What do you mean?') or (b) the clear indication that the response was ambiguous and potentially leading to the interlocutors drawing very different or even opposite conclusions from the same interaction (e.g. 'He dropped the bags by the bushes' – was this on purpose or accidental?). The reasons behind the miscommunications were divided into (a) those related to linguistic meaning and form (e.g. complex words or structures or culturally specific content) and (b) those pertaining to general language usage (e.g. relying on inferences rather than obtaining explicit confirmation). The comparative analyses reveal a statistically higher occurrence of miscommunication in bilingual police interviews and interrogations than in monolingual ones (see Filipović, 2021, 2022a, for further details, multiple examples and precise statistical information for the relevant comparisons), which signals the clear importance of these interactions for research and also for practice, as our societies and the criminal elements therein are increasingly multilingual. It is also relevant to highlight that the number of instances of miscommunication was higher in the United States policing context than the United Kingdom one. Another important point to make here is that cross-linguistic and cross-cultural contrasts require closer attention also because they can inform other spheres of interaction and criminal activity where this knowledge can come in handy (e.g. in the analysis of Dark Web communications, addressed further below). We now turn to the insights that multilingual forensic linguistic analyses have given us that can explain these findings.

Sources of miscommunication part 1: the questioning method and inferences

The United Kingdom and the United States differ considerably in their interviewing techniques and approaches to suspect interviews. The UK police employ non-adversarial interviewing strategies aimed at eliciting the best evidence possible (based on the PEACE approach, i.e. planning and preparation, engage and explain, account, closure, evaluation) and the United States applies the adversarial approach (based on the Reid technique) aimed at eliciting confession (although certain US states are slowly phasing out the Reid technique, e.g. California; see Filipović, forthcoming, for details). Miscommunication was found to be more frequent in the United States than the United Kingdom data overall, in part because of this striking difference in the questioning method. Similar findings were reported in the context of false confessions (i.e. when innocent people admit guilt due to personal reasons or mental health issues; Meissner et al., 2014) and inadvertent confessions (i.e. when people are not aware that miscommunication has occurred and that their answers were taken to be a confession or admission of guilt; Filipović, 2021; see also the next section for an example). Below we can see an example of the high-pressure, insistent questioning in the United States that leads to miscommunication and elicitation of compromised data that can easily be thrown out of court based on multilingual forensic linguistic analysis. In example (1) below, police officer 1 is the main investigator while police officer 2 acts as an interpreter (see Filipović, 2022a and forthcoming, for more examples and discussion).

(1)

Police officer 1: Did he push her? Did he push her onto the bed?

Police officer 2: *¿La empujaste?*

[Did you push her?]

Suspect: *Solo sus manos*.

[Only her hands]

Police officer 2: *¿La empujaste sobre la cama, si o no?*
[Did you push her on the bed, yes or no?]
Suspect: No, sobre la cama no la toqué.
[No, on the bed I did not touch her]
Police officer 2: No, he did not push her.

We can notice that the suspect was saying that he pushed the victim's hands, so he did not fully deny pushing but he specified the kind of pushing that occurred (i.e. the pushing of hands). The coercive insisting on a yes-or-no answer and the pressure put on the suspect here means that information is lost. Furthermore, the translation equivalent that police officer 2 is using is inadequate – '*sobre*' does not mean 'onto' it means 'on'. Spanish does not have a category of dynamic prepositions (i.e. those that indicate a change of location, such as into, onto, or out of) like English does. As result, we have the misinformation that the suspect did not push the victim at all, and while he may not have touched her when she was on the bed that still does not mean that he did not push her onto the bed (by pushing her hands). Precision in expression and translation is relevant for understanding the victim's injuries and the extent of suspect's admission, which saves time and resources, while at the same time achieving equality in access to justice and avoiding miscarriages of justice (see also the section 'Sources of miscommunication, part 2: language and culture contrasts').

Many instances of miscommunication in both the United Kingdom and the United States stem from the general reliance on inferences (which is common to any type of interaction in any language). Additionally, interlocutors can be uncooperative and exploit the possibility that a miscommunication was left unresolved, as was the case in the following:

(2)
Police officer: Did you threaten to kill her?
Suspect: Her brother threatened to kill me.
Police: When did he threaten you?

In this example we see that the police officer did not elicit an admission but rather inferred it (i.e. the suspect threatened because he had been threatened himself earlier) and moved on to the next line of questioning, but there was no valid admission given that would legally stand and an opportunity to secure it was lost. This happens quite often because police communication, like other types of communication, can be reliant on inferencing rather than explicitness – this is how humans interact, and too much insistence on explicitness can lead to communication breakdown. The devil lies in the detail or, rather, in finding the right balance between maintaining rapport and not allowing manipulation by the suspect (see Filipović, 2019, and Musolf, 2019, for some examples of success versus failure in this regard).

Another issue arising in the UK data is the observation that lengthy non-confrontational questioning can sometimes lead to extended police time, which could be avoiding through some specific adjustment in phrasing questions to ensure that the suspect is not able to avoid answering them while avoiding coercion at the same time (see Filipović, 2019; Pounds, 2019; Musolff, 2019). In other words, a balance may need to be struck in terms of when to insist on clarification and when to let the suspect elaborate, because it is through the suspect's elaboration that we find out

the crucial details that implicate involvement in crime (see Musolff, 2019, for detailed analyses and examples). One thing that we certainly do not want to do is lose our interlocutor, which happens when, for instance, a suspect start responding but then decides to shut down and evoke their right to silence due to coercion. This occurs in the US data but not in the UK data, so we can conclude that US questioning methods hinder evidence elicitation or leads to miscommunication more often than UK questioning methods, and reflected in the Méndez principles for non-coercive investigative interviewing developed and adopted by the United Nations ([21]).

Sources of miscommunication, part 2: language and culture contrasts

Forensic linguistic analyses performed on police transcript data reveals that, in addition to miscommunications due to the way humans rely on inference, as discussed in the previous section (and also in Filipović, 2019, in more detail), there are other types of miscommunication that stem from language-specific and culture-specific features that differentiate one language from another, as illustrated in examples (3) and (4).

(3)
Police: Did she fall, or did he drop her?
Interpreter: *¿Ella se cayó o la botaste?*
[She fell or you threw her?]
Suspect: *Si, se me cayó*.
[Yes, to me it happened that she fell]
Interpreter: He dropped her.

The key notion to focus on here is that of intentionality, namely the information about whether something was done on purpose or not, which can be crucial for certain legal outcomes, thus making this information detail very important in police questioning. Intentionality is a concept that is expressed differently in different languages (Filipović, 2007, 2019). For instance, while speakers of Spanish consistently use different words or constructions to specify whether causation was intentional or not, English leaves this important information ambiguous. In the example above, 'He dropped her' could refer to either intentional or accidental act of dropping but it seems to have been interpreted as referring to an intentional act, because on this occasion it connects back to the police officer's distinction between falling (accident) and dropping (strongly indicating intention, reinforced by the Spanish translation equivalent offered ('*botar*' = 'throw'), which is clearly intentional). English verbs and constructions do not specify intentionality, and consequently this ambiguity, which is resolved negatively for the suspect, impacts the overall negative judgement – the police officers think they got a confession for an intentional act of dropping, which indicates murder rather than manslaughter. You can see how this line of miscommunication can lead to potentially catastrophic outcomes, especially in the countries like the United States that still exercises the death penalty. Crucially, this distinction for intentionality exists in many other languages, such as Italian, Greek and Serbian, and findings like this have very wide applicability. Here we have only demonstrated one of the many important insights into language contrasts that forensic linguistic analysis gives us. It is important to raise awareness about this and similar cross-linguistic contrasts in the context of eliciting evidence.

([21]) interviewingprinciples.com.

The example below shows how cultural differences create miscommunication with potentially serious consequences:

(4)
Police: *¿Con quién, uh, usas el locker?*
Translation: With whom, uh, do you use the locker?
Suspect: *Con otro amigo pero no, su nombre sí no sé*.
Translation: With another friend but I don't, I don't know his name.
Police: *¿No sabes el nombre de él?*
Translation: You don't know his name?

We can observe in the excerpt (4) above that the suspect's reference '*amigo*' ('friend') to a person whose name he did not know was suspicious to the police officer and this reflected negatively on the suspect in this case. However, this is indeed a very common and appropriate usage of the word 'friend' in Latin American cultures, while it sounds awkward in the context of the American English-speaking culture: why would you call anyone your friend if you do not even know their name? In this case the police officer was noticeably annoyed and started viewing the suspect as uncooperative and treating him with suspicion, which ultimately led to a complete breakdown of rapport and refusal to be questioned further on the part of the suspect. Heightened sensitivity with regard to linguistic and cultural contrasts and also close collaborative work between law enforcement and language professionals can raise awareness about how to detect and resolve such conflicts in multilingual exchanges.

Language service provision

One of the most striking findings that the comparative forensic linguistic analysis of the police transcripts presented here is that transcripts of US police interviews are bilingual: they include exchanges both in the original language and in a translation that is the product of the interpreting during the interview, and a subsequent control translation by another translator that is different from the one present in the interview. All US interrogations are transcribed verbatim; that is, everything that the speakers said, including speech features such as hesitations and concurrence by uttering 'um', is provided. By contrast, UK transcripts are non-verbatim, which means that substantial portions of the dialogue can be missing, and they also do not include any lines in the original language of the interviewee – they are typically produced in English only, though in some very rare cases bilingual transcripts may be produced but only if requested by the police. In the United States, bilingual police transcripts are the norm in the state of California where our US data come from. In addition to the advantage of bilingual transcript production, US police interview data have a further beneficial feature – that of a control interpreter/translator presence. US police interview recordings are given to another language specialist post-interrogation, who (independently) provides a full translation of everything that was said during the interrogation in a column parallel to the transcript of the record of the original exchange (see Filipović, 2022b). Not only does this make it easier to study the evidence collected and verify what has been said without having to replay the tapes, which is time-consuming and expensive, it also makes it much faster to detect any translation and communication issues in the interview that may be of timely importance for the investigation, in addition to ensuring quality control in the judiciary process and full legal rights. This is particularly relevant in the United States and in jurisdictions that have similar practices (i.e. where bilingual police officers still act as interpreters) (see Filipović et al., 2018). We can see the importance of using a qualified interpreting service in the previously cited examples (1, 3 and 4) from our US portion of the dataset. Multilingual police officers acting as interpreters is highly problematic, as interpreting is a skill that needs to be taught explicitly through

professional training. However, multilingual police officers may be able to help with their knowledge about the languages they speak, such as what the linguistic and cultural stumbling blocks may be between two or more languages they speak and working together with the interpreter to prepare for the interview and avoid those stumbling blocks in the best possible way (Mayfield, 2017). Such relevant language and communication skills can be honed through forensic linguistic training ([22]).

Forensic linguistics on the Dark Web

Multilingual forensic linguistic analysis can be helpful in another domain, currently not widely utilised, namely detecting the language of origin in criminals by recognising L1 (first-language) patterns in L2 (second-language) English used on the Dark Web. English is the global international language nowadays for science, education, global entertainment and crime. It is the most frequent language used on the Dark Web ([23]), but not all the English there is used by natives. Many English users have another language as their L1 and, as is well known in psycholinguistic literature, the L1 influence is very strong and persists even at the highest levels of proficiency (see Hawkins et al., 2012, for exemplification and discussion). Crucially, bilinguals cannot 'switch off' their other language, as it were; it is something that is impossible to control perfectly and consistently.

We have ample evidence that this is the case. We have studied large electronic corpora (over 140 million words) containing data from speakers of 40 different L1s for an educational project (the 'English Profile' project; see Hawkins et al., 2012). It is there that we noticed that certain errors by learners of L2 English are systematically revealing of their L1. The key idea here is that error profiles can be created for languages or language groups so that we can identify, for example, Chinese L2 English as opposed to Russian L2 English. Most often the predictions can be made about a language family rather than specific languages, such as Romance (Spanish, Italian, Romanian, etc.) L2 English as opposed to Slavic (Polish, Russian, Ukrainian, etc.) L2 English. Below are some examples extracted from L2 learner data with different L1s:

(5)

a) I by bus go to train station (L1 Chinese) (*).
b) Yesterday came my friend (L1 Spanish) (*).
c) I like very much that car (L1 Italian) (*).

All of these sentences are marked with an asterisk because they are grammatically incorrect in English, but they reflect what would be the correct grammar in Chinese, Spanish and Italian, respectively. Word order is just one of the relevant features that can help us reveal non-native English. Others include gender marking (for example, speakers of Slavic languages use 'he' or 'she' in many cases where English speakers use 'it') and definite and indefinite articles (such as 'the' or 'a') – languages that do not have articles, such as Russian, Turkish and Korean, make it difficult for speakers to acquire and use articles in L2 English properly even at the highest levels of L2 English proficiency (see Filipović et al., 2013).

([22]) See www.tacit.org.uk for further information.
([23]) See https://slcyber.io.

We used this knowledge about typological language contrasts that cause difficulty in the acquisition of non-native English and checked for similar occurrences in exchanges among different cybercriminals on the Dark Web. For example, one very telling feature that we immediately noticed is the consistent lack of articles in the L2 English used in chats known to be involving Russian users (e.g. we find outputs like 'piece of cake' instead of 'a piece of cake'). English native speakers do not omit articles in this fashion even when using an efficient medium such as texting. Staying on the same theme of articles, if somebody wants to get help by using AI to translate, in this case, from a language without articles (such as Russian and most other Slavic languages) to languages with articles (such as English, German or Italian), translation choices will be made by AI that are based on statistics rather than the specifics of the current case or a particular context. A human analyst who knows both languages is necessary to establish whether a reference to 'gun' in Russian would be better rendered as 'a gun' or 'the gun': the former indicating a lack of prior awareness of there being a gun and the latter implying the speaker knew about the prior existence and presence of the gun, which can result in a different interpretation of the whole event (e.g. the suspect being part of a premeditated armed robbery versus being blindsided about the weapons involved) (see Coulthard, 2007, for details of a real case where such use of articles in English was crucial; see also Filipović, forthcoming, for other contrastive features in translation that AI cannot capture yet).

The central claim here is that a forensic linguistic analysis will benefit from being informed by applied language typology – that is, the field that studies multiple language contrasts at different levels of meaning and grammar that cause cross-linguistic conflicts in second or additional language learning and multilingual communication across different spheres of life, such as legal or medical (Filipović, 2017a, 2017b). Knowledge about the key typological differences between any two languages would enable us to determine, or at least narrow down, the possible linguistic and cultural background of individuals that are involved in and collaborating with criminal networks on the Dark Web, and also more generally members of international criminal networks who communicate via any kind of electronic media platform.

Furthermore, it is important to reiterate here that forensic linguists and multilingual specialists will still be needed in spite of the technological progress made in the domain of AI-assisted translation and analysis. In the context of international organised crime, the perpetrators are often bilingual or multilingual, able to switch from one language to another frequently and able to create and use novel codes, abbreviations or inferable omissions, which are hard for AI to master. For instance, Capuset al. (2005) cites an example of innovative phonetic spelling in an SMS in French used in this context: '*Ti vawar si ti don pah mon larsan*', which in proper French would have been written as: '*Tu vas voir si tu donnes pas mon argent*' ('You'll see if you don't give me my money'). A human analyst immediately understands what is going on here and deciphers the message instantly, and this matters a lot when time is of the essence.

The examples given here should be understood as a proof-of-concept proposal at present, which should build on findings within applied language typology and second-language-acquisition research, and include a systematic incorporation of multilingual forensic linguistic analysis in the crime investigations that take place on the Dark Web. Some automated models that can help us in this regard have already been developed and trialled on L2 learner data – the proposal here is to use the Dark Web as a corpus large enough to test and improve the current technology.

There are numerous AI tools that perform language detection in speech and text, but the field is still very underdeveloped for various reasons. For example, the various translation engines are primarily oriented towards

the target language (i.e. the language into which translation happens) rather than the source language. Furthermore, AI tools can mistakenly identify some outputs as coming from different speakers of English just because the AI model was trained on thematic information (e.g. references to Italian places such as Rome or Italian specialities such as *spaghetti al ragù*) (see Brooke et al., 2012, for a critical overview and discussion). AI tools would certainly be helpful in speeding up identification processes in the future and helping narrow down the potential pool of L1s detectable in the use of L2 English for criminality purposes. At the moment, training these tools require large datasets, which are not available, as indicated in previous research (Tetreault et al., 2012). AI is also unreliable when it comes to identifying outputs with high proficiency in the L2, and erroneously identifies texts produced by L2 English-speaking humans as fully AI-generated (see Liang et al., 2023). Thus, at present, multilingual AI cannot do the invaluable work of human multilingual forensic linguistic analysis, especially as criminals are constantly trying to be more creative in their use of language (as we saw earlier in the example of phonetic texting in French). Forensic linguists, with a typological, multilingual and multicultural knowledge base, may stand a better chance of figuring out the crucial, investigation-relevant information in this context.

Conclusions

In this paper we offered an original overview of the connections between findings from different studies, different types of data and different locales, which all point to the relevance of forensic linguistic analyses in multilingual and multicultural police investigations. We brought to light the neglected importance of applying insights from decades' worth of academic work on multilingualism and language typology to the contexts of forensic data analysis, evidence elicitation and evidence evaluation.

Forensic linguistic analysis and professional training based thereon helps to elicit better evidence. It provides empirical insight into what works and what does not with regard to many aspects of the investigative process, including different questioning methods, linguistic and cultural contrasts and language service provision, which are all relevant – if not crucial – in police communication across borders. We also exemplified the value of integrating multilingualism and a language typology knowledge base into the forensic analysis of any type of communication relevant to law enforcement.

The main practical conclusion to draw is that we need to integrate the findings and authentic, real-life examples like the ones presented in this paper into regular training provision for law enforcement and other crime investigators, such as the financial police. This can be done through the development of hands-on, situation-based training courses that teach police officers through first-hand exposure how to detect, prevent and resolve miscommunications and investigate their source in a way that maintains rapport and does not compromise the investigation and the quantity and quality of evidence, and all based on the latest scientific and empirical confirmations from both real-world fieldwork and lab work as done by our group. Visit our website for the latest research, professional training and a free sample toolkit ([24]), along with the policy-informing documents we contributed to (Korkman et al., 202; Mayfield, 2017).

([24]) See https://www.tacit.org.uk/toolkit/.

References

Brooke, J. and Hirst, G. (2012), 'Robust, lexicalized native language identification', in: Kay, M. and Boitet, C. (eds), *Proceedings of COLING 2012: Technical papers, COLING 2012 Organizing Committee, Mumbai,* pp. 391–408, https://aclanthology.org/C12-1025/.

Capus, N., Griebel, C. and Havelka, I. (2024), *Multilingual Communications Surveillance in Criminal Law: The role of intercept interpreters-translators*, Edward Elgar Publishing, Cheltenham, https://doi.org/10.4337/9781035331475.

Coulthard, M. (2007), An Introduction to Forensic Linguistics: Language in evidence, Routledge, London, https://doi.org/10.4324/9780203969717.

Filipović, L. (2019), 'Evidence-gathering in police interviews: Communication problems and possible solutions', *Pragmatics and Society*, Vol. 10, Issue 1, pp. 9–31, https://doi.org/10.1075/ps.00013.fil.

Filipović, L. (2021), 'Confession to make: Inadvertent confessions and admissions in United Kingdom and United States police contexts', *Frontiers in Psychology*, Vol. 12, https://doi.org/10.3389/fpsyg.2021.769659.

Filipović, L. (2022a), 'Language and culture as sources of inequality in US police interrogations', *Applied Linguistics*, Vol. 43, Issue 6, pp. 1073–1093, https://doi.org/10.1093/applin/amac022.

Filipović, L. (2022b), 'The tale of two countries: Police interpreting in the UK vs. in the US', *Interpreting*, Vol. 24, Issue 2, pp. 254–278, https://doi.org/10.1075/intp.00080.fil.

Filipović, L. and Hawkins, J. A. (2013), 'Multiple factors in second language acquisition: The CASP model', *Linguistics*, Vol. 51, Issue 1, pp. 145–176, https://doi.org/10.1515/ling-2013-0005.

Filipović, L. and Vergara, S. A. (2018), 'Juggling investigation and interpretation: The problematic dual role of police officer-interpreter', *International Journal of Speech Language and the Law*, Vol. 5, Issue 1, pp. 62–79, https://ojs.letras.up.pt/index.php/LLLD/article/download/4547/4262.

Hawkins, J. A. and Filipović, L. (2012), *Criterial Features in L2 English: Specifying the reference levels of the Common European Framework*, Cambridge University Press, Cambridge.

Korkman, J., Otgaar, H., Geven, L. M., Bull, R., Cyr, M. et al. (2025), 'White paper on forensic child interviewing: Research-based recommendations by the European Association of Psychology and Law', *Psychology, Crime & Law*, Vol. 31, Issue 8, pp. 987–1030, https://doi.org/10.1080/1068316X.2024.2324098.

Leonard, R., Ford, J. E. R. and Christensen, T. K. (2017), 'Forensic linguistics: Applying the science of linguistics to issues of the law', *Hofstra Law Review*, Vol. 45, Issue 3, pp. 881–897, https://scholarlycommons.law.hofstra.edu/hlr/vol45/iss3/11/.

Liang, W., Yuksekgonul, M., Mao, Y., Wu, E. and Zou, J. (2023), 'GPT detectors are biased against non-native English writers', *Patterns*, Vol. 4, Issue 7, 100779, https://doi.org/10.1016/j.patter.2023.100779.

Mayfield, K. (2017), 'Language services protocol for law enforcement bodies', https://www.hf.uio.no/multiling/english/projects/flagship-projects/forensic/open-access-repository/guidelines-and-protocols/language-services-protocol_katrina-mayfield-2017-vf.pdf.

Meissner, C. A., Redlich, A. D., Michael, S. W., Evans, J. R., Bhatt, S. et al. (2014), 'Accusatorial and information-gathering interrogation methods and their effects on true and false confessions: A meta-analytic review', *Journal of Experimental Criminology*, Vol. 10, pp. 459–486, https://doi.org/10.1007/s11292-014-9207-6.

Musolff, A. (2019), 'You keep telling us different things, what do we believe?' Meta-communication and meta-representation in police interviews', *Pragmatics and Society*, Vol. 10, Issue 1, pp. 32–48, https://doi.org/10.1075/ps.00014.mus.

Pounds, G. (2019), 'Rapport-building in suspects' police interviews: The role of empathy and face', *Pragmatics and Society*, Vol. 10, Issue 1, pp. 97–124, https://doi.org/10.1075/ps.00017.pou.

Tetreault, J., Blanchard, D., Chalill, A. and Chodorow, M. (2012), 'Native tongues, lost and found: Resources and empirical evaluations in native language identification', *in: Kay, M. and Boitet, C. (eds), Proceedings of COLING 2012: Technical papers, COLING 2012 Organizing Committee, Mumbai, pp. 2585–2602*, https://aclanthology.org/C12-1158.pdf.

Value added tax fraud, false invoicing and the evolution of associated money-laundering dynamics

Pasquale Danese

https://doi.org/10.3013/mpg60a72

Abstract

Value added tax fraud, false invoicing and money laundering reveal increasingly close connections with the activities of organised crime, presenting complex operational challenges in identifying the intersections between illicit economic–financial phenomena and criminal structures. Within this context, money laundering evolves through progressively sophisticated methodologies, giving rise to new paradigms that disrupt the 'classic' archetype of the three-stage model: placement–layering–integration. Can the traditional model still be considered valid, or does it require reformulation in light of the increasingly innovative practices adopted by criminal organisations?

This study, starting from a contextual analysis of the operations of criminal organisations in the globalised economy, aims to answer this question by developing, with the aid of artificial intelligence tools, a specific mathematical function capable of outlining the main trends in money laundering and exploring the challenges posed by a phenomenon as pervasive as it is protean.

The connection between false invoicing, money laundering and organised crime emerges as a pivotal issue in the fight against criminal organisations. These entities exploit such practices not only to finance their illicit activities but also to infiltrate the legal economy, undermining the foundations of legality and social equity.

Keywords: VAT fraud and false invoicing, placement–layering–integration phases, declining sigmoid curve of money laundering, dissociation phase, three-level analysis.

Introduction

Money laundering constitutes one of the fundamental mechanisms through which criminal organisations perpetuate and amplify their economic and social influence. Recent analyses, including the European Union Agency for Law Enforcement Cooperation (Europol) report *Decoding the EU's Most Threatening Criminal Networks* and the Italian Anti-Mafia Investigative Directorate (DIA) semi-annual report for the second half of 2023 (DIA, 2023), highlight the significant evolution of money-laundering dynamics. These developments reflect the increasing sophistication of criminal networks and their penetration into legal economic and financial circuits.

The traditional assumption that money laundering primarily involves introducing illicit cash into legal financial systems needs to be reconsidered. Modern criminal organisations, now highly structured, generate illicit capital within legal financial systems, making the tracking and the countering of these activities increasingly complex. Consequently, the illicit proceeds requiring laundering are no longer confined to cash but extend also to resources produced directly within legal economic systems and the rapidly expanding domain of crypto-assets.

Europol's analysis underscores the agility, transnational nature and significant control that criminal networks exert over legal economic sectors within the European Union. These networks employ professional facilitators and advanced technologies, such as crypto-assets, to establish illicit financial networks that are exceptionally difficult to decipher.

In particular, Europol's report examines the methods and strategies employed by the EU's most threatening criminal networks to launder illicit capital. The report identifies several key characteristics.

— Agility: 96 % of the criminal networks are capable of independently laundering their illicit proceeds, using legal business structures to conceal the origins of funds.

— Transnationality: 68 % of these organisations consist of members from diverse nationalities and operate on an international scale.

— Control: the networks infiltrate vulnerable sectors such as construction, logistics and hospitality, employing shell companies and other legal structures to disguise illicit activities.

The utilisation of legitimate corporate structures is a cornerstone of money-laundering strategies, consistently involving professional intermediaries. According to Europol, over 86 % of criminal networks rely on such structures to facilitate laundering, while 71 % employ corruption to obstruct investigations and influence judicial proceedings.

At the national level, Europol's findings are closely mirrored by the Italian context. The semi-annual report by the DIA for the second half of 2023 highlights how Italian criminal organisations have adopted an 'entrepreneurial' model. This model replaces overt violence with the silent control of territory through corruption and economic infiltration. This transformation has enabled these organisations to consolidate their presence across various legal sectors, using shell companies, trusts and complex corporate structures to obscure the illicit origins of their funds.

The DIA report, based on investigations conducted by Italian law enforcement, reveals the adoption of increasingly sophisticated strategies, including false invoicing, value added tax (VAT) fraud, trade-based money-laundering schemes and the frequent use of emerging technologies.

These methods allow criminal organisations to exploit seemingly legitimate economic systems, further embedding themselves within the legal economy and strengthening their foothold in key industries.

Methodology and objectives

The context outlined serves as the foundational premise of this study, which aims to propose a more updated and coherent criminological model for money laundering. This model seeks to guide preventive and repressive policy decisions while supporting investigative and criminological efforts more broadly.

The term 'money laundering' first appeared in the English language in the 1970s, gaining prominence in journalistic accounts related to financial and political scandals (Oxford English Dictionary, 2026; Madinger and Kinnison, 2011). However, the practice of reintegrating illicitly obtained proceeds into the legal economy predates this period, notably during the American Prohibition era (1920–1933). Criminal organisations, including the Italian American Cosa Nostra, actively sought methods to 'clean' cash derived from illegal activities such as the illicit alcohol trade, prostitution, gambling and extortion. These groups often utilised seemingly legitimate businesses, such as laundries, restaurants, bars and other commercial establishments, to justify otherwise inexplicable cash flows. It is plausible that the notion of 'washing' money contributed to the subsequent adoption of the term 'money laundering' (Madinger and Kinnison, 2011; Unger and van der Linde, 2013).

The criminological model describing illicit capital laundering, based on the paradigm of placement–layering–integration, raises a fundamental question: is it still current and fully descriptive of the phenomenon, or does it require reformulation to account for the more modern operations of criminal organisations?

Other scholars have questioned the continued relevance of this model, approaching the issue from various perspectives but converging on the conclusion that a broader approach is necessary. This is especially true in investigator training (Cassella, 2018) given the increasing prevalence of economic and cybercrime in money laundering dynamics (Sultan and Mohamed, 2024).

The foundational premise of this study asserts that advanced criminal organisations now operate with an entrepreneurial structure, facing no difficulty in laundering cash through the management of legitimate businesses.

Thanks to schemes involving VAT fraud and false invoicing, these organisations demonstrate an increasing capacity to generate illicit revenues directly within legal financial systems, including through the use of crypto-assets. This phenomenon represents a significant shift in the placement phase of illicit capital, traditionally associated with the introduction of criminal proceeds as cash into legal economic channels. Such changes mean that illicit resources are now generated directly within banking systems rather than as cash, rendering techniques like 'smurfing', the structuring of transactions to obscure the origins of funds, less relevant. This shift redefines the relationship between

criminal organisations and cash, which no longer necessarily marks the starting point of the 'paper trail' but can instead serve as its end point.

The conventional approach to combating money laundering can no longer be confined to the prevention and suppression of behaviours aimed at introducing illicit cash into legal financial circuits. Instead, it is crucial to identify models that better reflect the trends exhibited by the most insidious and dangerous criminal organisations. These groups have already infiltrated the economic fabric, generating illicit revenues directly within it, compromising the integrity of economic and financial systems, and undermining competition and economic equality.

Using artificial intelligence tools, a model has been developed to mathematically represent the inverse relationship between the level of 'sophistication' of a criminal organisation and the percentage of cash generated relative to total illicit proceeds. This model is essential for the considerations explored in the remainder of this study.

The declining sigmoid curve of money laundering

As previously highlighted, this study builds on empirical evidence outlined in Europol's report, *Decoding the EU's Most Threatening Criminal Networks*, at the European level, and the DIA's semi-annual report for the second half of 2023, which confirms these trends within a national context. An inverse proportionality can be observed between the complexity and sophistication of crimes committed by a criminal organisation and the percentage of cash generated relative to the total illicit proceeds accumulated. For instance, an organisation engaged in predatory crimes (such as theft, robbery and extortion) tends to produce proceeds exclusively in cash, relying on laundering schemes that adhere to the traditional three-stage model of placement–layering–integration. In contrast, more complex and sophisticated criminal organisations, particularly those involved in financial crimes, generate illicit proceeds that are already integrated into the legal financial system and adopt different laundering schemes and phases.

A further evolution is evident in organisations active in cybercrime, which accumulate proceeds exclusively in cryptocurrencies. These have become the preferred instruments for facilitating illicit transactions online and on the Dark Web.

Thus, there is a progressive reduction in the proportion of cash generated as the operational complexity and technological integration of criminal organisations increase.

To analyse this phenomenon, a mathematical function has been developed with the assistance of artificial intelligence tools. This function represents the relationship between the level of criminal sophistication and the percentage of cash generated:

— x = criminal sophistication index;

— y = percentage of cash (the share of illicit proceeds in cash relative to the total illicit revenues generated).

The criminal sophistication index increases incrementally on a scale from 0 to 100. A value of 0 represents an organisation solely engaged in predatory crimes. Progressing along the x-axis, the index rises through the following categories: organisations involved in illicit trafficking (15), basic economic crime (30), more complex economic crimes such as VAT fraud and false invoicing (50), corporate and financial crimes (80), and cybercrime networks (100).

It is important to note that there are criminal groups engaged in activities such as robberies or illicit trafficking that are highly complex, organised and disciplined. Therefore, the criminal sophistication index should be understood as an indicator of the complexity of crimes committed, relative to the organisation's ability to generate illicit proceeds through various systems and methods.

The percentage of cash generated by a criminal organisation relative to the total illicit proceeds is represented on the y-axis, ranging from 0 to 100.

A critical point on the x-axis is located at a value of 50, which corresponds to criminal organisations engaged in more complex economic and financial crimes, such as VAT fraud and false invoicing. Groups that reach this level of sophistication are potentially capable of generating illicit proceeds directly within legal financial circuits and in increasingly significant proportions.

Based on the parameters described above, which characterise the criminal phenomena under investigation, the following function can be implemented:

$$y(x) = \frac{C}{1 + e^{k(x-x_0)}}$$

Where:
y represents the percentage of cash relative to the total illicit proceeds;
x is the criminal sophistication index;
C denotes the maximum percentage of cash (in this case C = 100, i.e. 100 %);
e is known as the Euler's number (approximately 2.718);
k is the constant that determines the slope of the curve (approximated in this instance to k = 0.2);
$x0$ represents the critical point of the function ($x0$ = 50).

The function described above generates the graph in Figure 10.1.

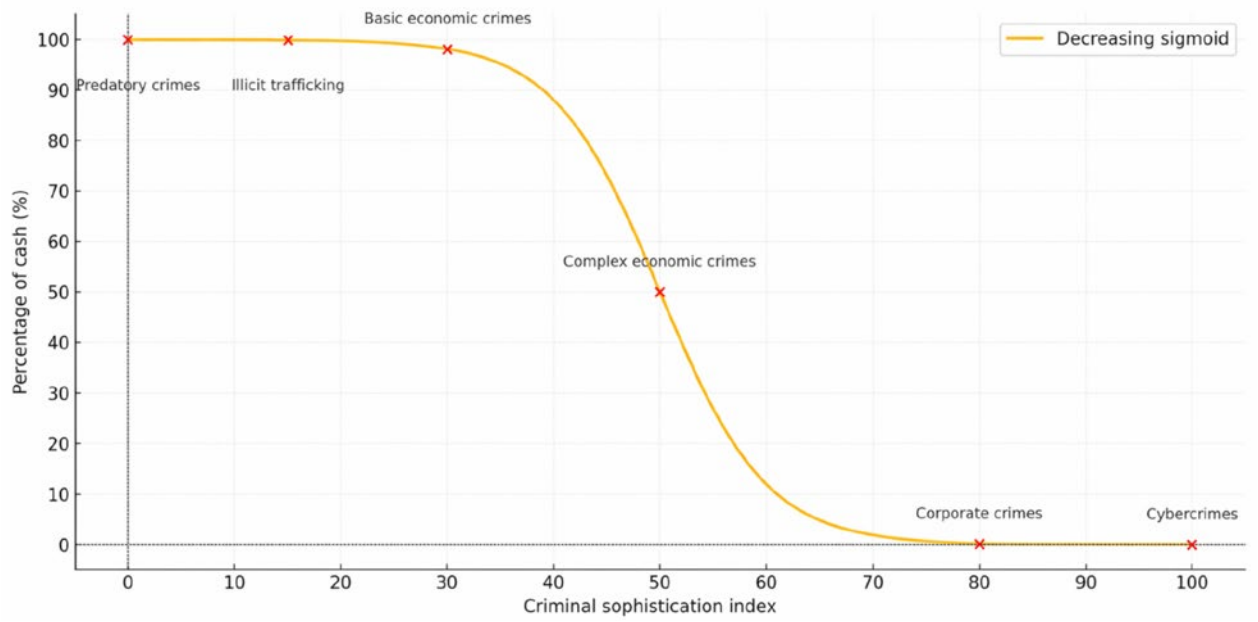


Figure 10.1. Criminal phenomena under investigation

Interpretation of the graph

The graph illustrates a declining sigmoid curve that depicts the relationship between the criminal sophistication index (x) and the percentage of cash generated as a proportion of total illicit proceeds (y).

At the initial values, ($x = 0$), which represents criminal groups engaged in predatory crimes (e.g. theft, robbery, extortion), and $y = 100$, as these groups generate the entirety of their illicit proceeds in cash. To launder these proceeds, such organisations must rely on third parties or adopt schemes rooted in the traditional three stages of placement–layering–integration.

As the sophistication index increases ($x > 0$), the cash percentage (y) remains dominant for groups involved in illicit trafficking (e.g. drug trafficking, smuggling, counterfeiting). However, the utilisation of logistical and legal structures enables these organisations to generate part of their illicit proceeds through other means, such as tax evasion or fraud, which are sometimes employed to facilitate laundering. Although laundering methods still depend on the placement–layering–integration model, the growing operational complexity alters their efficacy and potential.

Moving further along the x-axis, the criminal sophistication index increases to levels corresponding to basic economic crime. This includes groups operating in the informal economy, whose proceeds predominantly come from 'off-the-books' revenue. For example, this is observed in the informal economies within immigrant communities, particularly non-EU migrants. In this context, the cash percentage remains prevalent but begins to decrease further as the operation of businesses and other legal structures facilitates additional means of enrichment. These organisations, however, still face the challenge of managing large quantities of accumulated cash, particularly to ensure continuous remittances to their countries of origin.

The criminal sophistication index reaches a critical point ($x = 50$) associated with criminal groups specialising in complex economic and financial crimes, such as VAT fraud and false invoicing. These organisations are capable of generating illicit proceeds directly within legal financial systems. This phenomenon represents an evolution from the past, where fraudulent invoicing was primarily the domain of 'specialists' operating shell companies. Today, however, it has become a strategic sector for many criminal organisations, exploited to generate significant profits while minimising the economic and legal risks associated with other illicit activities.

At this level of sophistication ($x = 50$), a significant increase in synergies between organised crime and white-collar professionals can be observed. Professionals such as accountants, notaries and lawyers provide essential contributions to the planning and execution of complex frauds, expanding the 'grey area' of intersections between the legal sector and criminal activity. This level of complexity necessitates the adoption of laundering methods that go beyond traditional models.

Further along the x-axis ($x = 80$), highly sophisticated criminal organisations emerge, dedicated exclusively to complex economic and financial crimes, corporate offences, stock market manipulation and corruption in public administration. These groups generate illicit proceeds entirely within legal financial systems, which, in theory, are traceable and subject to seizure and confiscation measures. To mitigate this risk, such organisations adopt strategies to monetise their accumulated illicit funds in cash, transferring them outside the legal circuits through the systematic use of cash mules. This method involves withdrawing money from the accounts of companies used to commit illicit acts and delivering it directly to the perpetrators of the fraud, with intermediaries retaining a percentage as a fee for their services.

In cases such as those described, which are becoming increasingly widespread and significant, the traditional placement–layering–integration money-laundering model is no longer a suitable framework. Instead, money laundering occurs through inverse methods (Danese et al., 2022), whereby illicit funds initially accumulate in the bank accounts of shell companies, which play a central role in the criminal economy.

The next stage, required to complete the process, involves the monetisation of illicit proceeds through fractional withdrawals. While these operations resemble the concept of smurfing, they represent its algebraic inverse: rather than depositing small amounts of cash to integrate funds into legal financial circuits, funds are withdrawn from accounts to convert them into cash. This stage finalises the laundering process, making the funds available for further illicit activities, such as loansharking and bribing public officials.

However, even monetisation operations entail significant costs and various risks. This raises an important question: why not source cash from organisations with an excess supply? The demand for monetisation intersects with the supply of cash from less sophisticated criminal groups ($x < 50$), particularly those active in illicit trafficking and the informal economy ($15 < x < 50$). These groups, retaining a commission, supply cash to economic and financial criminals who, in exchange, conduct wire transfers abroad on their behalf. Such transfers often exploit non-cooperative jurisdictions in terms of criminal, tax or anti-money-laundering enforcement and are typically intended to finance drug trafficking, smuggling or cross-border remittances.

This phenomenon also explains the resurgence of underground banking systems in Europe, particularly among non-EU immigrant communities.

Finally, those engaged in cybercrime operate on an entirely different plane, characterised by the absence of cash and the bypassing of traditional financial systems. They generate illicit proceeds in crypto-assets, concealing their origin through unregulated platforms that ensure anonymity. Techniques employed include mixing and tumbling services, which fragment transactions to prevent tracking, and the use of non-custodial wallets for cryptocurrency storage.

In such cases, the traditional three-phase model (placement–layering–integration) proves obsolete and inadequate for describing these new operational methods.

Conclusions

The analysis conducted in this study highlights the radical evolution of money laundering, moving away from the traditional paradigm based on the three stages of placement–layering–integration. Modern criminal organisations have achieved levels of sophistication that render many of the investigative strategies employed to date obsolete. Given this increasingly complex landscape, it is imperative not only to update countermeasures but also to redefine the theoretical categories that guide criminological analyses of the phenomenon.

The classical money-laundering model remains valid in cases where criminal organisations need to launder illicit proceeds generated in cash. As indicated in the graph, this applies to organisations operating at values corresponding to $x < 50$. However, beyond this critical point, the model proves inadequate in describing the operational methods of contemporary criminal groups, particularly those involved in complex economic and financial sectors or in crypto-related activities. In such cases, illicit proceeds are often already integrated into the legal financial system or generated directly in digital environments, eliminating the need for an initial placement phase.

To describe the laundering processes of funds generated directly within legal financial systems or in crypto-assets, the introduction of a new operational phase is proposed: the dissociation phase. This phase addresses the primary need to distance illicit proceeds from the context in which they were generated, preventing them from being traced back to the original criminal activity or subjected to asset seizure.

To better understand the findings of this analysis, it is necessary to consider the methods of generating illicit proceeds within three distinct operational levels:

- cash, relating to physical money and tangible material wealth;
- traditional finance, encompassing centralised and regulated financial circuits, such as banks, credit institutions, payment institutions and electronic money operators;
- digital and decentralised finance (DeFi), relating to the realm of crypto-assets and blockchain-based tools, and characterised by the absence of centralised intermediaries, pseudo-anonymity and high operational autonomy.

The laundering of proceeds generated at the cash level can be analysed and described using the traditional model. The placement phase represents the critical moment when cash is introduced into legal financial circuits or converted into crypto-assets. Indeed, the model remains applicable even in cases where criminal organisations launder cash directly into crypto-assets, using, for instance, crypto ATMs or other channels within the crypto ecosystem.

Thus, it can be asserted that, starting from the cash level, money laundering proceeds according to the traditional model, involving an initial placement phase within both traditional finance and digital, decentralised finance (Gabbiadini et al., 2024).

Different considerations must be made when illicit proceeds are generated at the other two levels. In these contexts, money laundering does not require a placement phase but rather a dissociation phase, aimed at separating the funds from the context in which they were generated to obscure their illicit origin. Unlike the layering phase, which emphasises complexity and concealment through multiple transactions, the purpose of the dissociation phase is to clearly separate illicit proceeds from their original source. The idea is essentially to move to another 'level' to evade traceability.

This necessity is particularly pronounced in traditional finance and can be achieved through the following:

— transfers and transactions involving non-cooperative jurisdictions in terms of criminal, tax and anti-money-laundering compliance (such operations allow for the separation and distancing of illicit proceeds from the domestic jurisdiction where they were generated, obscuring their origin and hindering investigative efforts);

— monetisation, converting illicit proceeds to cash;

— transferring funds to the level of digital and decentralised finance, utilising laundering methods based on crypto-assets.

In DeFi, laundering processes follow specific methods tailored to the unique characteristics of the system. The dissociation phase can occur:

— within the same level, using tools such as mixers and tumblers or fragmenting transactions across different blockchains to disrupt traceability;

— by transferring crypto-assets to other levels, such as traditional financial circuits (e.g. conversion to fiat currency via regulated or unregulated exchanges) or cash (via cash-out and monetisation).

Particular attention must be paid to DeFi, an ecosystem based on blockchain and decentralised protocols such as smart contracts, decentralised exchanges, liquidity pools and non-custodial wallets. Unlike centralised finance, DeFi is characterised by the absence of centralised intermediaries. Criminal organisations with substantial crypto-assets in liquidity pools and non-custodial wallets could engage in transactions with other organisations that require cryptocurrencies, operating as an underground banking system within the crypto world.

The analysis of the three levels demonstrates that the traditional three-phase model remains effective at the cash level. However, the introduction of the dissociation phase is essential for understanding operational mechanisms within legal financial circuits and DeFi. These dynamics underscore the evolution of money laundering and the need to adapt criminological models and, consequently, counterstrategies to the specific characteristics of different contexts.

The proposed analytical model proves fundamental for policymaking and predictive purposes, offering tools to understand and combat the evolution of money laundering. It also provides a solid foundation for specialised investigator training. Simultaneously, it is crucial to strengthen international cooperation, particularly within the EU, and to promote the adoption of new technologies for investigative purposes to effectively address the challenges posed by modern criminal networks.

References

Cassella, S. (2018), 'Toward a new model of money laundering: Is the "placement, layering, integration" model obsolete?', *Journal of Money Laundering Control*, Vol. 21, Issue 4, pp. 494–497, https://doi.org/10.1108/JMLC-09-2017-0045.

Danese, P., Andriani, G., Chiappetta, M., Ranaudo, A. and Zuppetti, A. (2022), *Terrorismo e Riciclaggio – Evoluzione, disciplina e strumenti di contrasto*, 15 December, Aracne, Rome, https://www.aracneeditrice.eu/pubblicazioni/terrorismo-e-riciclaggio-massimo-chiappetta-antonio-ranaudo-pasquale-danese-giovanni-andriani-andrea-zuppetti-9791221803853.html.

Europol (2024), *Decoding the EU's Most Threatening Criminal Networks*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2813/811566.

Gabbiadini, R., Gobbi, L. and Rubera, E. (2024), 'Riciclaggio e blockchain: Si può seguire la traccia nel mondo cripto?', *Questioni di Economia e Finanza (Occasional Papers)*, No 893, Publishing and Printing Directorate of the Bank of Italy, https://data.europa.eu/doi/10.32057/0.QEF.2024.893.

Madinger, J. and Kinnison, N. (2011), *Money Laundering – A guide for criminal investigators – Third edition*, 14 December, Routledge, New York, https://doi.org/10.1201/b11845.

Oxford English Dictionary (2026), 'money laundering (n.)', Oxford English Dictionary website, https://doi.org/10.1093/OED/2976349490.

DIA (2023), *Relazione del Ministro dell'Interno al Parlamento sull'attività svolta e sui risultati conseguiti dalla Direzione Investigativa Antimafia – Luglio–Dicembre 2023 [Report of the Minister of the Interior to the Italian Parliament on the activities carried out and the results achieved by the Anti-Mafia Investigative Directorate – July–December 2023]*, https://direzioneinvestigativaantimafia.interno.gov.it/wp-content/uploads/2021/12/Rel.-Sem.-2-2023-WEB.pdf.

Sultan, N. and Mohamed, N. (2024), 'The money laundering typologies and the applicability of placement-layering-integration model in undocumented South Asian economies: A case of Pakistan', *Journal of Money Laundering Control*, Vol. 27, Issue 4, pp. 741–762, https://doi.org/10.1108/JMLC-08-2022-0116.

Unger, B. and van der Linde, D. (2013), *Research Handbook on Money Laundering*, Edward Elgar Publishing Cheltenham, https://doi.org/10.4337/9780857934000.

Navigating the symbiosis between organised crime and terrorism: Assessing the impact of foreign terrorist fighters on criminal networks ([25])

Murat Tınas

https://doi.org/10.3013/8gs0km03

Abstract

The modern global security landscape is increasingly challenged by organised crime, fuelled by economic globalisation and technological advancements that expand criminal networks and their illicit activities. European Union strategies emphasise disrupting high-risk criminal networks, acknowledging their impact on socioeconomic systems, legal economies and the rule of law. This paper highlights the growing threat of such networks in Europe, exacerbated by the involvement of foreign terrorist fighters and returnees over the past decade. The intersection of organised crime and terrorism has gained attention in academic and law enforcement circles. Moving beyond traditional views that treat them separately, recent studies explore their interconnectedness, focusing on conditions that foster cooperation and motivations for terrorist engagement in criminal activities. The Syrian conflict has amplified these dynamics, with foreign terrorist fighters intensifying illicit financial flows and collaborating with transnational criminal groups. Shared financial channels further blur distinctions between terrorism and organised crime, implicating fighters in diverse illicit activities. Using a desk-based approach, this research analyses literature and open-source data to trace the evolution of this nexus, examine the hybrid nature of these activities and assess the risks posed by foreign terrorist fighters. The findings reveal a dynamic relationship with global impacts, posing significant security threats and driving political, economic and social instability.

Keywords: organised crime, terrorism, criminal networks, foreign terrorist fighters, returnees, foreign terrorists.

([25]) This study incorporates and builds upon content from the author's previously published work, which has been significantly revised and expanded with new sources and original sections to address the current research scope: Tınas, M. (2023), 'Symbiotic relations between terrorism and organized crime in the Levant: Cases of PKK and DAESH', in: Ahmet Demirden (ed.), *Emerging Issues in Terrorism Studies*, Nobel.

1. Introduction

The relationship between organised crime and terrorism has long been a focal point in both academic research and law enforcement practices. Recent trends and incidents, particularly in the last decade, have underscored how individuals with criminal backgrounds have leveraged their connections to illicit networks to support terrorist operations. The collapse of governance and public order in the Levant has further exacerbated this issue. Terrorist organisations have significantly enhanced their capabilities in generating, transferring and laundering funds, as well as in transnational smuggling and trafficking activities. In the Middle East and North Africa (MENA) region, the interplay between terrorism and organised crime has moved beyond opportunistic cooperation, shedding light on the shared social environments and networks that facilitate their convergence. Among these organisations, the Kurdistan Workers' Party (PKK) and Islamic State in Iraq and Syria (ISIS) ([26]) stand out for their ability to exploit these hybrid networks to sustain and expand their operations.

This study aims to delve deeper into the intricate and evolving relationship between organised crime and terrorism, with a particular focus on foreign terrorist fighters who have recently become pivotal links within these networks. The paper begins with a theoretical exploration of the evolution of these relationships, followed by an in-depth analysis of the scale and characteristics of the nexus between crime and terrorism. This study is based on a qualitative, desk-based research design that combines descriptive and analytical approaches. The research primarily relied on secondary sources, including academic literature, official government reports, institutional publications and policy-oriented analyses. The analysis involved thematic categorisation of data, focusing on three interrelated research questions: (1) How does cooperation between organised crime and terrorism evolve from opportunistic to symbiotic forms? (2) In what ways do foreign terrorist fighters facilitate this transformation? (3) What implications do these interactions have for security policy and law enforcement cooperation?

In conclusion, this study highlights how the hybrid nature of these relationships exacerbates instability across the Levant, undermining political, economic and social structures in the region. While the connection between organised crime and terrorism is not a new phenomenon, the last decade has seen a significant transformation of these ties from temporary alliances to deeply interdependent, symbiotic relationships, further fuelled by the involvement of foreign terrorist fighters.

2. The symbiotic relationship between terrorism and organised crime

The intersection between terrorism and organised crime has long been a subject of academic debate and a focal point for law enforcement agencies (Schmid, 1996; Makarenko, 2004; Shelley et al., 2005; Reitano et al., 2017). This nexus challenges the traditional dichotomy that views terrorism and organised crime as distinct phenomena with diverging goals and operational methods. Alex Schmid's (1996) seminal study brought this discussion to the forefront by highlighting their interconnections, paving the way for broader discourse on the conditions under which these entities cooperate and why terrorist groups increasingly resort to criminal activities to sustain their operations. Then, there are even studies examining how organised criminal groups and terrorist organisations form alliances, adopt each other's tactics and occasionally integrate operations, especially in unstable regions (Makarenko and Mesquita, 2014).

([26]) Both the PKK and ISIS have been designated as terrorist organisations internationally by numerous states including the Member States of the European Union, the United States, Canada, Australia, Türkiye and many international organisations.

One of the key challenges in addressing this nexus lies in defining terrorism itself. While there is no universally accepted definition (Schmid, 2023), the political and ideological motivations behind terrorist acts set them apart from purely profit-driven criminal activities. However, over the past few decades, the financial aspects of terrorism have gained significant attention (Biersteker and Eckert, 2008; Schmid, 2018). This shift is primarily due to two reasons. First, in the past, counterterrorism efforts were predominantly understood as a direct military confrontation aimed at eliminating terrorists through armed force. However, contemporary perspectives have shifted, recognising that combating terrorism is intrinsically tied to disrupting its financial streams. This paradigm shift has not only expanded the scope of counterterrorism strategies but has also highlighted the intricate relationship between terrorism and organised crime. Understanding how terrorist groups generate, transfer and utilise funds, often through criminal activities such as smuggling, drug trafficking and money laundering, has become crucial. This evolution in counterterrorism practices underscores the necessity of addressing the crime–terrorism nexus to effectively dismantle the operational capabilities of terrorist organisations.

Second, a notable transformation has occurred within terrorist organisations in the last decades, particularly in their operational and financial strategies. Historically, ideologically driven groups were often reluctant to engage in direct organised criminal activities, as such actions were perceived to contradict their ideological narratives and undermine their legitimacy. However, the current trend reveals a growing involvement of terrorist organisations in profit-driven ventures, effectively blurring the lines between ideological and criminal motivations. This shift reflects both pragmatic and strategic adaptations, as these groups increasingly rely on illicit activities such as drug trafficking, smuggling and extortion to sustain and expand their operations. By integrating criminal enterprises into their frameworks, terrorist organisations not only secure funding but also exploit the vulnerabilities of global financial and governance systems, further entrenching their influence and resilience. These activities are carried out in two ways. The first group consists of legal activities that serve criminal purposes like charity fundraising, collecting donations or trading manufactured commodities. The second group of profit-making financial activities involves organised criminal activities like raising money through illegal migrations and smuggling (Shelley and Melzer, 2008; Shelley et al., 2005).

The interplay between ideological and financial objectives increasingly shapes the nature of cooperation between terrorist and criminal actors. While organised crime groups remain primarily motivated by profit, terrorist organisations often rationalise their participation in illicit markets through ideological narratives that frame criminal proceeds as legitimate means of sustaining a so-called higher cause. In this regard, foreign terrorist fighters play a pivotal bridging role, blending ideological justification with criminal expertise. Many of them possess practical experience in smuggling, trafficking and money laundering, yet remain ideologically aligned with extremist networks. This duality creates an operational and motivational overlap where profit-seeking and ideological commitment reinforce each other rather than contradict one another.

In the last decade, converging methods and shared networks have started to be a focal point in both academic research and law enforcement practices. Terrorist organisations and organised crime groups share many operational methods, including illicit fundraising, money laundering and smuggling. They also rely on similar networks and techniques to achieve their goals. For instance, both utilise alternative financial systems like hawala and cryptocurrencies, exploit false documentation and engage in cross-border illicit trade. These shared practices are particularly evident in conflict zones like Syria and Iraq, where the collapse of state authority has created a conducive

environment for criminal and terrorist activities to flourish (Kupatadze and Argomaniz, 2019, p. 269; Adal, 2021, p. 2). Studies have shown that during the Syrian conflict, the smuggling of oil, antiquities and other commodities surged, facilitated by the breakdown of governance and the proliferation of terrorist groups (Nellemann et al., 2018, p. 22; Napoleoni, 2004). Organisations like the PKK and ISIS capitalised on these opportunities to finance their operations.

The United Nations Security Council (UNSC) has similarly highlighted that certain terrorist organisations collaborate with transnational organised criminal groups in various capacities, such as money laundering, facilitating access to smuggling routes, forging documents and trafficking drugs to finance their operations (UNSC, 2015). The involvement of foreign terrorist fighters has further enhanced the ability of terrorist groups to generate, transfer and conceal illicit funds, and engage in transnational smuggling and trafficking. Reitano et al. (2017, p. 9) point out this connection by noting that many ISIS recruits relied on drug trafficking as a significant revenue source and operated within overlapping networks in Europe for recruitment. Moreover, both terrorist organisations and criminal groups utilise similar financial mechanisms, including cryptocurrencies and informal systems like hawala, to carry out their activities. It is also reported that, in certain instances, terrorists have obtained pyrotechnic substances, possibly sourced through networks involved in organised crime (Europol, 2023, p. 18). The recent *European Union Terrorism Situation and Trend Report* also indicates the fact that investigations revealed links between right-wing extremist groups and organised crime networks in a mix of online and offline channels for fundraising, including donations, merchandise sales and criminal activities like drug and weapons trafficking (Europol, 2024, p. 40). This overlap demonstrates that foreign terrorist fighters or returnees may participate not only in acts of terrorism but also in organised criminal activities, such as human smuggling and illicit financial transfers (Rekawek et al., 2019, p. 18). The UNSC (2020) similarly acknowledged the rising threat posed by the interconnectedness of terrorism and organised crime, emphasising that such alliances often emerge opportunistically based on shared interests, common operational territories or mutual adversaries. Additionally, it is important to note the role of prisons as environments that can foster radicalisation and recruitment, where personal relationships between criminals and extremists may strengthen these linkages (Basra and Neumann, 2016, pp. 30–32). Prisons thus serve as spaces where social connections are forged, facilitating collaboration between organised crime and terrorist networks (Europol, 2024, p. 25).

In summary, the relationship between terrorism and organised crime has evolved beyond a simple nexus into a genuinely symbiotic interaction (Reitano et al., 2017, p. 9), calling for a comprehensive re-evaluation of existing threat assessment frameworks. Traditional perspectives treat these two phenomena as separate categories of crime, largely due to their differing objectives, despite notable similarities in their methods and operations. However, this conventional approach falls short in capturing the evolving complexity of the threat. As Shelley et al. (2008, pp. 43–63) highlight, the interaction between terrorist organisations and criminal networks has become increasingly intricate and interconnected. Given the diminishing clarity of boundaries between the two phenomena, threat assessment methodologies must adapt by focusing on the shared methods and overlapping motivations that characterise these groups.

3. The role of foreign terrorist fighters in fostering the symbiosis between organised crime and terrorism

The issue of foreign fighters in general or foreign terrorist fighters in particular is not a new phenomenon in many respects as the involvement of foreigners in civil conflicts has been one of the fundamental features of many conflicts (Tınas, 2020, p. 132). However, the phenomenon of foreign fighters and foreign terrorist fighters has garnered increasing attention in the last decade from both academia and international institutions, particularly in the context of current transnational conflicts (Dawson, 2021). Despite their frequent interchangeable use in media and academic discourse, these terms represent distinct concepts with implications for policy, security and legal frameworks.

Malet (2013, p. 9) defines foreign fighters as 'non-citizens of conflict states who join insurgencies during civil conflict'. Similarly, Hegghammer (2010, pp. 57–58) refines the concept, emphasising four criteria: involvement in an insurgency, lack of citizenship or kinship links to the conflict state, absence of affiliation with official military organisations and absence of financial compensation. The UNSC (2014) defines the term as 'nationals who travel or attempt to travel to a State other than their States of residence or nationality, and other individuals who travel or attempt to travel from their territories to a State other than their States of residence or nationality, for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training, including in connection with armed conflict'. This definition emphasises the intent and purpose of the individual's actions, distinguishing foreign terrorist fighters from broader categories of foreign fighters. The distinction between foreign fighters and foreign terrorist fighters lies primarily in intent and association. Foreign fighters may engage in civil conflicts without necessarily adhering to a terrorist ideology or participating in terrorist activities. However, the boundaries between these categories are often blurred. Financial, ideological and political overlaps can lead foreign fighters to be categorised as foreign terrorist fighters, particularly when their actions align with recognised terrorist organisations.

Regarding the conceptualisation, an essential aspect of the debate revolves around what constitutes 'foreignness'. Conventional definitions emphasise citizenship and territorial boundaries, yet these criteria may oversimplify the complex identities of individuals involved. Jawaid (2017, p. 102) critiques this state-centric approach, arguing that shared ethnic, kinship or ideological ties can supersede formal citizenship in motivating participation in conflicts. This transnational dimension challenges traditional notions of state boundaries and citizenship, necessitating a more nuanced understanding of 'foreign' while using the concept. Another critical element in defining foreign terrorist fighters is their role within a conflict. The term 'fighter' often evokes images of individuals engaged in direct combat. However, many foreign terrorist fighters serve in non-combat roles, such as logisticians, propagandists, medics and recruiters. From this perspective, the use of the term 'fighter' in the concept of foreign terrorist fighters appears to fall short of adequately capturing the multifaceted nature of the phenomenon. This limitation becomes evident in its inability to precisely define the range of activities undertaken by such individuals, thereby creating conceptual ambiguities. Furthermore, the term 'fighter' inherently carries a normative bias, often connoting a positive struggle associated with noble or just causes. Such a connotation risks overshadowing the illicit and violent objectives of these actors. From this perspective, this study argues that the inclusion of 'fighter' is neither necessary nor appropriate, and that employing the term 'foreign terrorist' alone would offer a more precise and analytically robust representation of the issue.

The relationship between organised crime and terrorism is inherently complex and evolves over time, displaying distinct characteristics across different regions. Since 2010, this connection has manifested in various forms in the MENA region, with an increasing number of case studies highlighting its far-reaching and harmful consequences (Makarenko 2004; Shelley et al., 2005; Reitano et al., 2017). Regarding the connection and cooperation between these two groups, this study adopts a layered understanding of cooperation, ranging from opportunistic to symbiotic forms, emphasising that foreign terrorist fighters often act as key enablers in transforming temporary, transactional relationships into sustained symbiotic cooperation between terrorists and criminal entities. In this context, cooperation is not viewed as a static or uniform condition but as a continuum that evolves based on mutual needs, external pressures and shared operational environments (Kupatadze and Argomaniz, 2019; Makarenko, 2004). Opportunistic cooperation typically emerges in fragile or conflict-affected zones where both actors temporarily benefit from exchanges of resources such as weapons, routes or financial services. Transactional cooperation involves more systematic and profit-driven collaboration, often characterised by the provision of logistical or financial support in return for operational advantages. At the most advanced level, symbiotic cooperation reflects an enduring convergence in which criminal and terrorist organisations internalise each other's methods, adapt overlapping governance structures and co-opt similar recruitment and financing mechanisms. Foreign terrorist fighters, due to their mobility, transnational connections and hybrid skill sets, accelerate this transformation by bridging local criminal economies with global radical networks. As a result, cooperation in the crime–terrorism nexus increasingly transcends short-term pragmatism and evolves into a self-reinforcing system of mutual dependency that challenges conventional crime-fighting and counterterrorism frameworks.

The participation of foreign terrorists has introduced a complex layer to the crime–terrorism nexus. Foreign terrorists frequently serve as intermediaries between terrorist organisations and transnational criminal networks, facilitating collaboration through their expertise in areas such as smuggling routes, document falsification and illegal financial transactions (Reitano et al., 2017; Basra and Neumann, 2016; Gallagher, 2016). This specialised knowledge significantly bolsters the operational capabilities of terrorist entities. Moreover, upon returning to their countries of origin, many terrorists remain involved in criminal enterprises, thereby deepening the intertwined relationship between terrorism and organised crime. As Kupatadze and Argomaniz (2019, p. 262) have observed, this relationship has recently transitioned from a mere nexus to a symbiotic dynamic, wherein both entities adopt each other's methods to achieve their primary objectives. Empirical data reinforce the existence of this convergence, indicating that considerable numbers of perpetrators of ISIS-linked attacks in Europe possessed prior criminal experience. Such findings highlight the extent to which terrorism and organised crime increasingly draw from overlapping social and operational environments (Europol, 2016; Mullins, 2016, pp. 26–30; Vidino et al., 2017; Europol, 2023, p. 22).

One significant factor to consider is the rising number of foreign terrorists and returnees from Syria and Iraq, many of whom have established ties with criminal organisations and possess in-depth knowledge of transnational smuggling routes. The participation of foreign individuals in civil conflicts has been a recurring characteristic of numerous armed confrontations throughout history. However, the conflicts in Iraq and Syria, particularly since the early 2000s, have drawn an unprecedented influx of foreign terrorists. The surge of foreigners, particularly from Europe, the Middle East and North Africa, and the potential return of these individuals to their countries of origin, have raised significant security concerns regarding their involvement in terrorist activities.

Initially, attention from scholars and law enforcement agencies centred on the direct threat posed by returnees, such as their potential to carry out attacks, plan and coordinate operations, establish new terrorist cells or recruit additional members. However, a parallel concern has emerged, emphasising the risk that returnees may leverage the advanced skills gained during their engagement in terrorist activities to participate in organised crime. This criminalisation of returnees poses a distinct threat, as it may further entrench the intersection between terrorism and transnational crime (Gallagher, 2016, p. 51).

The past two decades of instability in the MENA region have profoundly disrupted not only the region itself but also its broader periphery. The collapse of governance structures in Levantine states since the early 2000s has created fertile ground for terrorist organisations to expand their capabilities in generating, transferring and laundering illicit funds, and engaging in transnational smuggling and trafficking activities. Notably, these illicit financial flows and the involvement of terrorist groups in such activities saw a significant escalation following the outbreak of the Syrian conflict in 2011. Addressing these threats necessitates robust, institutionalised collaboration among neighbouring states, encompassing intelligence and financial information exchange, harmonised legal instruments and multilateral operational mechanisms such as joint task forces or regional security frameworks designed to counter the hybrid dynamics of terrorism and organised crime. However, a significant barrier to such cooperation lies in the absence of effective public order within the Levant, particularly in Syria, Iraq and Lebanon. The near collapse of state structures in these nations not only creates a conducive environment for the proliferation of terrorism and organised crime but also hinders the execution of coordinated international efforts to combat these challenges effectively.

Within this period, ISIS, as a prime example, has become notorious for its engagement in organised criminal activities, including kidnapping, smuggling antiquities and weapons, human trafficking and other illicit operations. According to van der Veer (2019), involvement in ISIS often parallels participation in organised crime, blurring the distinctions between terrorist and criminal behaviour. Numerous reports highlight ISIS's extensive ties with criminal networks in Europe, facilitating activities such as human trafficking, the illicit trade of historical artefacts and the production of forged documents (Reitano et al., 2017). Additionally, ISIS and Al-Qaeda-affiliated groups have reportedly generated significant revenue by exploiting the movement of migrants from the MENA region to Europe (Reitano et al., 2017). Gallagher (2016, p. 54) further documented instances where ISIS operatives engaged in criminal enterprises, such as extorting forced donations, international drug trafficking and document forgery. His findings also emphasise a notable shift within such groups, where ideological commitment often gives way to personal financial motives over time. Numerous studies emphasise the significant overlap between individuals involved in terrorist attacks, particularly those who have returned from conflict zones in Iraq and Syria, and members of organised criminal groups (Bakker, 2006; Simcox, 2015; Mullins, 2016).

Second, one of the earliest and most prominent examples of the crime–terrorism nexus in practice is the PKK, which has been designated as a terrorist organisation by Türkiye, the United States and the EU for decades. Since the 1980s, the PKK has actively engaged in drug trafficking, facilitating the transport of narcotics from eastern Türkiye to Europe (Europol and European Monitoring Centre for Drugs and Drug Addiction, 2019, p. 36; Ministry of Foreign Affairs of the Republic of Türkiye, n.d.). According to Reitano et al. (2017, pp. 17–18), in an EU-funded study, the PKK 'has been known to toe the line between terrorism and organised crime, engaging in a number of illegal economic operations such as humans, drugs and cigarettes smuggling and other forms of organised crime, including extortion and money laundering, among its profit generating activities' and 'over the span of three decades, the PKK has funded its

operations through various means including state sponsorship, criminal activities and legal business enterprises'. Additionally, the PKK is known to be involved in the illegal transnational trade of fuel and tobacco products (Kupatadze and Argomaniz, 2019, p. 267). It has also been reported that the PKK not only profits from the illicit drug trade between Iraq, Iran and Türkiye but also receives financial support from heroin traffickers operating within Europe (United Nations Office on Drugs and Crime, 2010, p. 46; Basra, 2019, p. 46). Media and law enforcement reports suggest that the PKK's drug trafficking activities are particularly concentrated in Belgium and the Netherlands (Esen, 2017). The PKK's involvement in human smuggling further underscores its integration into transnational organised crime. The group has facilitated the movement of foreign terrorists into conflict zones (Tınas and Demirden, 2020, pp. 18–27) and returnees often possess detailed knowledge of illicit smuggling routes. During their recruitment and travel to and from conflict zones, particularly in European countries, PKK operatives acquire expertise in using safe houses, falsifying documents, navigating border crossings and liaising with traffickers. These skills and networks are subsequently leveraged to support broader transnational organised criminal activities, amplifying the PKK's influence within the crime–terrorism nexus.

In general, foreign terrorists play a multifaceted role in fostering organised crime in Europe and in its near neighbourhood, acting as catalysts and participants in transnational criminal networks. Their skills, experience and connections significantly enhance the operational capacity of organised crime groups, creating a dangerous synergy between terrorism and organised crime in the last decade. First, foreign terrorists often serve as intermediaries linking terrorist organisations and organised criminal groups, leveraging their expertise in smuggling, forgery and trafficking to facilitate the movement of goods, people and illicit funds. This collaboration blurs the lines between the two entities, resulting in a symbiotic relationship that undermines security efforts and poses significant challenges to law enforcement agencies. Second, foreign terrorists exploit transnational smuggling routes, trafficking arms, drugs and humans, with reports linking returnees from Syria and Iraq to the transport of contraband across European borders. Third, the ability of foreign terrorists to produce or acquire forged travel documents has been instrumental in facilitating the clandestine movement of individuals across borders. This expertise, honed during their involvement in terrorist networks, is often repurposed to support organised crime activities, including human trafficking and illegal migration. Forged documents also enable the evasion of law enforcement and enhance the operational security of both terrorist and criminal groups. Beyond logistical capabilities, another important role that foreign terrorists and returnees have is that they can serve as conduits for radicalisation and recruitment for terrorist organisations from their criminal networks. Last but not the least, financial crimes, including money laundering, further illustrate their role in hybrid threats, as they utilise knowledge from managing terrorist finances to obscure proceeds from drug trafficking and other illicit activities. Evidence from case studies, such as those concerning ISIS-linked networks and the Paris and Brussels attacks, underscores the seamless transition of foreign terrorists between criminal and terrorist roles, destabilising social and security systems. Addressing this convergence requires coordinated international efforts, enhanced border controls and comprehensive de-radicalisation programmes to mitigate long-term risks.

The modern global security landscape faces persistent challenges from organised crime, driven by economic globalisation and rapid technological progress, facilitating the proliferation of criminal networks and broadening their illicit activities. Recent EU strategies highlight the necessity to disrupt high-risk criminal networks, recognising their multifaceted criminal enterprises that disrupt socioeconomic systems, infiltrate legal economies and subvert the rule of law. In this regard, the evolving relationship between terrorism and organised crime demands a re-

evaluation of traditional threat assessment frameworks. Moreover, the threat posed by high-risk criminal networks in Europe has escalated in the past decade due to the inclusion of foreign terrorists and returnees in the subject. The longstanding assumption that these two phenomena are distinct fails to capture the hybrid and symbiotic nature of their relationship. Instead, future studies must focus on the operational and behavioural similarities between these groups and the shared environments that facilitate their convergence. By adopting a more integrated approach, policymakers and law enforcement agencies can better understand and counter the multifaceted threats posed by the crime–terrorism nexus.

4. Conclusion

The distinction between terrorism and organised crime has become increasingly ambiguous, posing significant challenges for policymakers and practitioners in security bureaucracies, particularly with the growing involvement of foreign terrorist fighters. Returnees not only invigorate criminal networks but also amplify the convergence between organised crime and terrorism. Prevailing scholarship often emphasises alliances between terrorists and criminal groups as tactical arrangements designed to achieve their distinct objectives. However, as this study highlights, such traditional perspectives may fall short, as they presume a clear separation of goals while overlooking the deeper relationship between these entities. Therefore, future research could build upon these findings through empirical case studies or comparative analyses that examine how foreign terrorists operationalise cooperation between terrorist and criminal organisations across different regions.

Foreign terrorists play a critical role in strengthening organised crime in Europe and its neighbouring regions by acting as intermediaries and participants in transnational criminal networks. They leverage their skills in smuggling, forgery and trafficking to facilitate the movement of goods, people and illicit funds, creating a dangerous synergy between terrorism and organised crime. Foreign terrorists and returnees also exploit smuggling routes, engage in arms and drug trafficking and produce forged documents, enabling clandestine operations and evasion of law enforcement. Furthermore, they contribute to radicalisation and recruitment for terrorist organisations while utilising financial crimes to obscure illicit proceeds, highlighting the urgent need for coordinated international efforts to address these hybrid threats.

From a law enforcement perspective, addressing the crime–terror symbiosis requires enhanced cross-border intelligence sharing, integration of financial and criminal databases, and preventive mechanisms targeting radicalisation within criminal milieus. Effective countermeasures demand multilevel coordination among national and international bodies alongside the establishment of specialised joint intelligence platforms for tracking foreign terrorists. Strengthening financial intelligence units is also critical to being able to detect, trace and disrupt illicit financial flows that sustain both criminal and terrorist networks. Beyond reactive operations, preventive strategies must include de-radicalisation programmes within correctional facilities, post-release monitoring mechanisms and community-based interventions designed to reduce recidivism among returnees. Furthermore, digital transformation and the use of advanced analytics, including artificial-intelligence-assisted threat mapping and cross-border data fusion centres, can enhance early detection capacities. Collectively, these measures highlight that an effective response to the hybrid threat posed by terrorism and organised crime must combine policing, intelligence and prevention-oriented approaches under a unified strategic framework.

To conclude, for more active counterstrategies, a more nuanced understanding is required, recognising that the relationship between terrorism and organised crime has evolved into a symbiotic and transformative dynamic, far beyond temporary or opportunistic collaborations. This relationship is marked by shared operational needs and overlapping structural characteristics, making their activities increasingly interdependent. Furthermore, counterterrorism strategies must account for the intersection between political agendas and profit-driven motives, which frequently reinforce one another within terrorist organisations. Addressing these complexities necessitates a paradigm shift in both the conceptualisation of the crime–terrorism nexus and the development of policies aimed at mitigating its multifaceted threats. In other words, addressing the crime–terrorism nexus as a transnational and evolving challenge remains essential. Given its dynamic and globalised nature, it requires sustained, adaptive and cooperative approaches at both regional and international levels, rather than one-time or isolated countermeasures. Long-term strategies should balance preventive, intelligence-based and institutional efforts, recognising that the boundaries between terrorism and organised crime will continue to shift as these networks evolve.

References

Adal, L. (2021), *Organized Crime in the Levant – Conflict, transactional relationships and identity dynamics*, Global Initiative Against Transnational Organized Crime, Geneva, https://globalinitiative.net/wp-content/uploads/2021/03/Organized-Crime-in-the-Levant-Conflict-transactional-relationships-and-identity-dynamics-GITOC.pdf.

Bakker, E. (2006), *Jihadi Terrorists in Europe – Their characteristics and the circumstances in which they joined the jihad: An exploratory study*, Netherlands Institute of International Relations Clingendael, The Hague, https://www.clingendael.org/sites/default/files/pdfs/20061200_cscp_csp_bakker.pdf.

Basra, R. (2019), *Drugs and Terrorism: The overlaps in Europe*, European Monitoring Centre for Drugs and Drug Addiction and International Centre for the Study of Radicalisation, London, https://icsr.info/wp-content/uploads/2019/11/ICSR-Report-Drugs-and-Terrorism-The-Overlaps-in-Europe.pdf.

Basra, R. and Neumann, P. R. (2016), 'Criminal pasts, terrorist futures: European jihadists and the new crime-terror nexus', *Perspectives on Terrorism*, Vol. 10, Issue 6, pp. 25–40, https://www.jstor.org/stable/26297703.

Biersteker, T. J. and Eckert, S. E. (2008), *Countering the Financing of Terrorism*, Routledge, London, 12 September, https://doi.org/10.4324/9780203944639.

Turkish National Police: Counter Narcotics Department (2021), *Turkish Drug Report: Trends and developments*, https://www.narkotik.pol.tr/kurumlar/narkotik.pol.tr/TUB %C4 %B0M/2021-TURKISH-DRUG-REPORT.pdf.

Dawson, L. L. (2021), 'A comparative analysis of the data on western foreign fighters in Syria and Iraq: Who went and why?', *ICCT Research Papers*, International Centre for Counter-Terrorism, The Hague, https://icct.nl/sites/default/files/2022-12/Dawson-Comparative-Analysis-FINAL-1.pdf.

Esen, H. (2017), 'PKK drug smuggling network busted in Belgium', *Anadolu Agency*, 2 September 2017 (updated 3 September 2017), https://www.aa.com.tr/en/europe/pkk-drug-smuggling-network-busted-in-belgium/899976.

European Union Agency for Law Enforcement Cooperation (Europol) (2016), 'Changes in modus operandi of Islamic State (IS) revisited', https://www.europol.europa.eu/cms/sites/default/files/documents/modus_operandi_is_revisited.pdf.

Europol and European Monitoring Centre for Drugs and Drug Addiction (2019), *EU Drug Markets Report*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2810/796253.

Europol (2023), *European Union Terrorism Situation and Trend Report 2023*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2813/302117.

Europol (2024), *European Union Terrorism Situation and Trend Report 2024*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2813/4435152.

Gallagher, M. (2016), '"Criminalised" Islamic State veterans – A future major threat in organised crime development?', *Perspectives on Terrorism*, Vol. 10, Issue 5, pp. 51–67, https://www.jstor.org/stable/26297654.

Hegghammer, T. (2010), 'The rise of Muslim foreign fighters: Islam and the globalization of jihad', *Quarterly Journal: International Security*, Vol. 35, Issue 3, Winter, pp. 53–94, https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/The_Rise_of_Muslim_Foreign_Fighters.pdf.

Hutchinson, A. (2002), 'International drug trafficking and terrorism: Testimony before the Senate Judiciary Committee Subcommittee on Technology, Terrorism, and Government Information', U.S. State Department website, https://2001-2009.state.gov/p/inl/rls/rm/9239.htm.

Jawaid, A. (2017), 'From foreign fighters to returnees: The challenges of rehabilitation and reintegration policies', *Journal of Peacebuilding & Development*, Vol. 12, Issue 2, pp. 102–107, https://www.jstor.org/stable/48603172.

Kupatadze, A. and Argomaniz, J. (2019), 'Introduction to special issue – Understanding and conceptualising European jihadists: Criminals, extremists or both?', *European Journal of Criminology*, Vol. 16, Issue 3, pp. 261–277, https://doi.org/10.1177/1477370819829971.

Makarenko, T. (2004), 'The crime–terror continuum: Tracing the interplay between transnational organised crime and terrorism', *Global Crime*, Vol. 6, Issue 1, pp. 129–145, https://doi.org/10.1080/1744057042000297025.

Makarenko, T. and Mesquita, M. (2014), 'Categorising the crime–terror nexus in the European Union', *Global Crime*, Vol. 15, Issue 3–4, pp. 259–274, https://doi.org/10.1080/17440572.2014.931227.

Malet, D. (2013), *Foreign Fighters: Transnational identity in civil conflicts*, Oxford University Press, New York.

Ministry of Foreign Affairs of the Republic of Türkiye (n.d.), 'Türkiye's contributions in the fight against drug trafficking', https://www.mfa.gov.tr/turkiye_s-contributions-in-the-fight-against–drug-trafficking.en.mfa.

Mullins, S. (2016), 'The road to Orlando: Jihadist-inspired violence in the West, 2012–2016', *CTC Sentinel*, Vol. 9, Issue 6, pp. 26–30, https://ctc.westpoint.edu/wp-content/uploads/2016/06/CTC-SENTINEL_Vol9Iss612.pdf.

Napoleoni, L. (2004), 'The new economy of terror: How terrorism is financed', *Forum on Crime and Society*, Vol. 4, No 1–2, pp. 31–48, https://www.unodc.org/documents/data-and-analysis/Forum/V05-81059_EBOOK.pdf.

Nellemann, C., Henriksen,R., Pravettoni, R., Stewart, D., Kotsovou, M. et al. (eds) (2018), *World Atlas of Illicit Flows*, Norwegian Centre for Global Analyses, Global Initiative Against Transnational Organized Crime and International Criminal Police Organization, https://globalinitiative.net/wp-content/uploads/2018/09/Atlas-Illicit-Flows-FINAL-WEB-VERSION-copia-compressed.pdf.

Reitano, T., Clarke, C. and Adal, L. (2017), *Examining the nexus between organised crime and terrorism and its implications for EU programming*, International Centre for Counter-Terrorism, The Hague, 13 April, https://icct.nl/sites/default/files/import/publication/OC-Terror-Nexus-Final.pdf.

Rekawek, K., Szucs, V., Babikova, M. and Lozka, K. (2019), *The Input: Pathways to jihad – A thematic analysis of 310 cases*, Globsec, Bratislava, 29 May, https://www.counterextremism.com/sites/default/files/The-Input-Pathways-to-Jihad.pdf.

Schmid, A. P. (1996), 'The links between transnational organized crime and terrorist crimes', *Transnational Organized Crime*, Vol. 2, No 4, 4 February, pp. 40–82.

Schmid, A. P. (2018), 'Revisiting the relationship between international terrorism and transnational organised crime 22 years later', *ICCT Research Papers,* International Centre for Counter-Terrorism, The Hague, 29 August, https://icct.nl/sites/default/files/import/publication/ICCT-Schmid-International-Terrorism-Organised-Crime-August2018.pdf.

Schmid, A. P. (2023), 'Defining terrorism', *ICCT Reports,* International Centre for Counter-Terrorism, The Hague, 13 March, https://icct.nl/sites/default/files/2023-03/Schmidt%20-%20Defining%20Terrorism_1.pdf.

Shelley, L. I. and Melzer, S. A. (2008), 'The nexus of organized crime and terrorism: Two case studies in cigarette smuggling', *International Journal of Comparative and Applied Criminal Justice*, Vol. 32, Issue 1, pp. 43–63, https://doi.org/10.1080/01924036.2008.9678777.

Shelley, L. I., Picarelli, J. T., Irby, A., Hart, D. M., Craig-Hart, P. A. et al. (2005), *Methods and Motives: Exploring links between transnational organized crime and international terrorism*, United States Department of Justice: National Institute of Justice, Washington, DC, 23 June, https://www.ojp.gov/pdffiles1/nij/grants/211207.pdf.

Simcox, R. (2015), *'We will conquer your Rome': A study of Islamic State terror plots in the West*, Henry Jackson Society: Centre for the Response to Radicalisation and Terrorism, London, 29 September, https://henryjacksonsociety.org/wp-content/uploads/2015/09/ISIS-brochure-Web.pdf.

Tınas, M. (2020), 'Broadened perspective on foreign (terrorist) fighters in Syrian civil war', *Liberal Düşünce Dergisi*, Vol. 25, No 97, 20 March, pp. 131–146, https://doi.org/10.36484/liberal.682637.

Tınas, M. and Demirden, A. (2020), *Foreign Terrorist Fighters in PKK/YPG in Syria: Violent extremism backfires*, Turkish National Police Academy, Ankara, https://cdn2.pa.edu.tr/Upload/Rapor/Dosya/foreign-terrorist-fighters-in-pkkypg-in-syria-violent-extremism-backfires.pdf.

Turkish National Police: Counter Narcotics Department (2021), Turkish Drug Report: Trends and developments, https://www.narkotik.pol.tr/kurumlar/narkotik.pol.tr/TUB %C4 %B0M/2021-TURKISH-DRUG-REPORT.pdf.

United Nations Office on Drugs and Crime (2010), *The Globalization of Crime: A transnational organized crime threat assessment*, Vienna, https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.

UNSC (2014), Resolution 2178, S/RES/2178, 24 September, https://docs.un.org/en/S/RES/2178%20(2014).

UNSC (2015), 'Report of the Secretary-General on the threat of terrorists benefiting from transnational organized crime', S/2015/366, 21 May, https://docs.un.org/en/S/2015/366.

UNSC (2020), 'Action taken by Member States and United Nations entities to address the issue of linkages between terrorism and organized crime – Report of the Secretary-General', S/2020/754, 29 July, https://docs.un.org/en/S/2020/754.

Van der Veer, R. (2019), 'The crime–terrorism nexus', in: Sweijs, T. and Pronk, D. (eds), *Strategic Monitor 2018–2019*, Netherlands Institute of International Relations Clingendael, The Hague, 7 February, https://www.clingendael.org/publication/crime-terrorism-nexus.

Vidino, L., Marone, F. and Entenmann, E. (2017), *Fear Thy Neighbor – Radicalization and jihadist attacks in the West*, Ledizioni LediPublishing, Milan.

The role of data-driven policing in tackling high-risk criminal networks in the Netherlands

Wendy Schreurs, Jessica Cozzi, Jurjen Jansen

https://doi.org/10.3013/m5f6q668

Abstract

Communication is central to organised crime, and offenders increasingly rely on encrypted phones to exchange sensitive information while avoiding detection. Although encryption is crucial for safeguarding fundamental rights and the digital safety of citizens, governments, businesses and society, it also restricts the ability of law enforcement and judicial authorities to exercise their legal powers, as criminals exploit secure communication services for illicit purposes. In the context of high-risk criminal networks (HRCNs), however, encrypted communication can become a valuable data source once law enforcement gains lawful access. Decrypted datasets have enabled the Dutch police, in collaboration with international partners, to make arrests, seize substantial quantities of drugs and gain insight into criminal processes. As HRCNs continue to adapt their communication methods, the police must also anticipate this evolving digital landscape. One approach is to combine multiple data sources – such as automatic number plate recognition, open-source intelligence, video footage and confiscated digital devices – to create a more comprehensive operational picture. In response, the Dutch police launched the national programme 'data-driven collaboration' to strengthen their ability to collect, store, analyse and operationalise diverse forms of data. This paper discusses the future of data-driven policing in tackling HRCNs, based on interviews with strategic key players within the Dutch police.

Keywords: data-driven policing, encryption, technology, organisation, human aspects, criminal networks.

Introduction

In the digital age, rapid technological advancement has transformed various aspects of society, including organised crime. Criminal networks depend heavily on communication, and offenders increasingly rely on encrypted phones to exchange sensitive information while avoiding detection by law enforcement. Although encryption is vital for

protecting fundamental rights and digital safety, it simultaneously limits the ability of law enforcement agencies (LEAs) to exercise their legal powers, as criminals exploit secure communication services for illicit activities.

High-risk criminal networks (HRCNs) pose significant social and economic threats, and the ability to access and analyse large volumes of criminal communication has proven crucial for law enforcement (European Union Agency for Law Enforcement Cooperation, 2024a). Recent investigations into encrypted platforms such as EncroChat, Sky ECC and ANOM have enabled the Dutch police, in collaboration with international partners, to make arrests, seize large quantities of drugs and gain insight into criminal processes. Yet HRCNs are adaptive and continuously modify their communication strategies to evade detection, resulting in an ongoing cycle of innovation and countermeasures.

At the same time, the increasing digitalisation of society provides new opportunities for law enforcement, leading to the growing adoption of data-driven policing (DDP). Building on intelligence-led policing, DDP seeks to use all available and relevant data to enhance preventive, investigative and operational outcomes (Barros et al., 2024; Barros, 2022). Implementing DDP, however, introduces a range of technological, organisational, human and ethical challenges. The use of algorithms and artificial intelligence (AI) raises questions about transparency, accountability and the conditions under which data analysis may guide decision-making.

This study aims to address the following central research question: to what extent do technological, human, organisational and ethical aspects influence the effectiveness of DDP in tackling HRCNs within the Dutch National Police?

Theoretical background

The use of data in tackling high-risk criminal networks

The global rise of digitalisation has increased the use of data and encrypted communication tools. The prevalence of data and encryption across crimes has grown for two reasons. Encryption is widely embedded in both software and hardware, making it easily available to criminals. Second, it enables criminals to conceal crucial information and communications, which significantly aids criminal activity. As a result, LEAs are increasingly facing data and encryption challenges in their investigations. Research on the role of encryption in the Dutch criminal justice chain showed that encryption is common in all types of crime, but to a fairly large extent more so in high impact crime and plays a significant role in all types of organised crime (Jansen et al., 2023). This prevalence underlines the relevance of focusing on HRCNs in this study.

Encryption can both obstruct and enhance criminal investigations. It limits direct access to evidence, making it harder to identify relevant individuals or activities. However, even when the encrypted code cannot be cracked, alternative methods, such as the use of metadata, can still provide valuable evidence. Decrypting data, when successful, can significantly accelerate investigations and reveal crucial insights, such as modus operandi and criminal collaborations.

Despite its challenges, encryption also offers practical benefits for LEAs, such as providing reliable and unaltered evidence, which is often considered more trustworthy than witness statements. The study by Jansen et al. (2023) suggests that while encryption complicates criminal investigations, law enforcement continues to adapt and

develop new methods to overcome these obstacles. As technology evolves, ongoing investment in skills and knowledge related to encryption and digital tools is crucial. Although the impact of encryption is difficult to quantify, it shapes both the opportunities and challenges LEAs face in modern investigations.

When data are decrypted, LEAs gain access to a potential goldmine of information and intelligence. Within the Dutch National Police, crypto analysis teams (CATs) were established to analyse these large datasets. This development has been a catalyst for the adoption of DDP within the Dutch police.

Data-driven policing

DDP is part of a broader big data revolution across sectors such as healthcare, finance, transportation and criminal justice (Davis et al., 2022). While definitions vary, most describe DDP with a focus on its use, purpose and impact on law enforcement. Afzal and Panagiotopoulos (2024) explain that DDP uses tools such as data analysis, surveillance, predictive algorithms and public information to make police work more efficient and accurate. It combines different types of data, such as neighbourhood history, criminal profiles and crime records. Examples include the Real-Time Analysis Critical Response Division in Los Angeles and the Domain Awareness System in New York (Afzal and Pangiotopoulos, 2024). Jansen (2018, p. 2) employs a more preventive definition, illustrating how policing has transitioned from reacting to crimes after they happen, to preventing them proactively, thanks to data and new technology.

The emphasis of DDP is on using the insights, clues, connections and patterns obtained from data to guide police work in the form of detection, enforcement and emergency aid (den Hengst and Wijsman, 2023). Within the Dutch police, initiatives such as the operational information yield teams have developed tools to automatically process and analyse large datasets (i.e. big data) (Roest, 2023). Big data systems are characterised as follows: 'they make use of vast quantities of data from a variety of data sources, and, using rapid computer processing and algorithms, identify correlations or patterns in the data, often patterns that humans would otherwise overlook, in order to classify new instances in the domain of interest' (Davis et al., 2022).

In 2023, the Dutch police launched a national programme called 'data-driven collaboration' (*Datagedreven Samen Werken*) aimed at facilitating data-driven operations across organisational levels. The police possess numerous internal and external data sources, such as automatic number plate recognition (ANPR), sound and motion sensors, video footage, and open-source intelligence (OSINT). It is anticipated that both the sources and the amount of data will continue to increase in the future (Dutch National Police, 2023).

Police (business) models in a digital police organisation

With the rise of intelligence-led policing, the intelligence cycle has been utilised by LEAs to systematically process intelligence analyses and criminal investigations.

Intelligence-led policing

The intelligence cycle (United States Department of Defense: Joint Chiefs of Staff, 2013) is an internationally accepted model used to describe intelligence work, which is also utilised by the Dutch police, as shown in Figure 12.1 (den Hengst and Wijsman, 2023). At the centre of the intelligence cycle is the joint operational mission. This outlines the

goal to which the intelligence should contribute, namely the decision-maker's intention. The model consists of six steps: (1) direction and planning, (2) collection, (3) data processing, (4) analysis, (5) dissemination and (6) continuous evaluation of both the process and the content. The impact that the decision-maker has by choosing an intervention based on intelligence is not reflected in this model. Additionally, the model lacks specific guidance for dealing with big data.

DDP is not seen as an entirely new approach, but rather as an enhancement of intelligence-led policing as data and their interpretation have become more widely accessible (Barros et al., 2024).

Figure 12.1. Intelligence cycle used by the Dutch police

The CSAE (collect, store, analyse, engage) model

To address the limitation of traditional intelligence cycles in a big data environment, particularly in the domain of cyber-facilitated crime, the CSAE model (Figure 12.2) was established (van de Sandt et al., 2021). This model provides a multilayered framework that integrates diverse investigative disciplines into a single coherent approach.

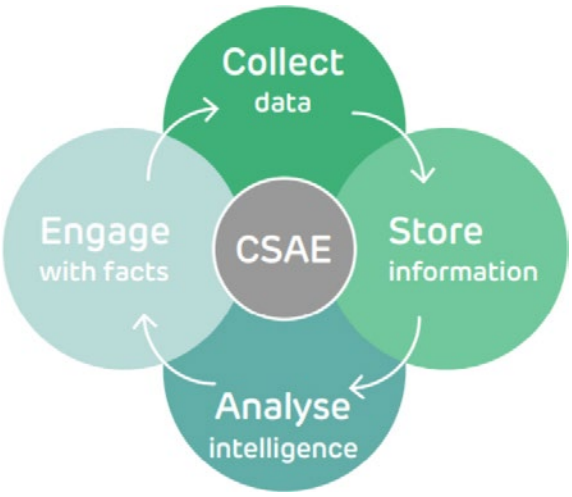


Figure 12.2. The stages of the CSAE model

The foundation of this model lies in the social and behavioural aspects of what we now refer to as traditional investigations, such as investigative interviews and physical surveillance. The second layer incorporates the technical perspective of digital investigations, which emerged in the 1980s. More recently, a numerical dimension incorporating advanced mathematical and statistical methods has been introduced into law enforcement practices. The synthesis of these three layers – social and behavioural, technical and numerical – constitutes data scientific investigations. This approach allows LEAs to identify complex patterns within HRCNs that would otherwise remain undetected by traditional methods alone (van de Sandt et al., 2021).

The primary objective of criminal investigations is to identify suspects and establish who did what to facilitate prosecution. LEAs hold a monopoly on this process of bringing suspects to justice. Before the digital age, all criminal investigations were what we now call traditional, offline investigations and forensics. These investigations primarily focused on the human aspects of crime, making them largely social and behavioural in nature. Investigators relied on techniques such as observations, investigative interviews and eavesdropping to uncover the truth, often supported by traditional forensic sciences like ballistics, DNA analysis, fingerprinting and pathology, which dealt with physical evidence from the offline world (van de Sandt et al., 2021).

As crimes became increasingly intertwined with and facilitated by information technologies, evidence began to shift to hardware and online environments, leading to the emergence of digital investigations. Digital forensics, involving computers, networks, mobile devices, etc., was developed to recover evidence from data storage devices. While digital investigations provided an additional layer to traditional investigative methods, their introduction marked a fundamental shift in the legal, organisational and technical dynamics of the justice system. The integration of traditional and digital investigations has been an ongoing process for many LEAs worldwide (van de Sandt et al., 2021). By integrating the CSAE model and the intelligence cycle, a new business model for data-driven policing was created (Figure 12.3) (den Hengst and Wijsman, 2023). In this model, the joint operational assignment is still central, but more attention is paid to the underlying business process and the need for multidisciplinary collaboration between, among others, AI experts, domain experts and intelligence analysts. Additionally, it includes the evaluation phase from the intelligence cycle. This business model acknowledges both the role of the decision-maker and the complexity of intelligence work when dealing with large amounts of data (den Hengst and Wijsman, 2023).

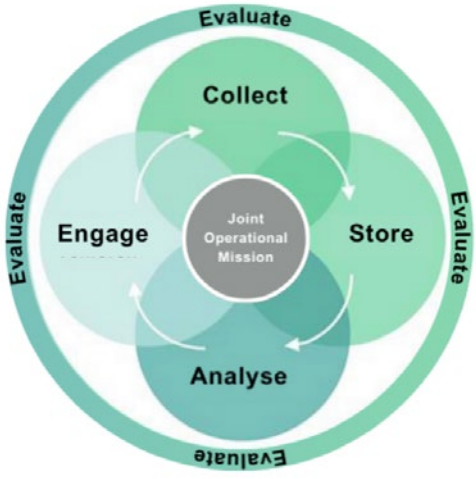


Figure 12.3. Business model for data-driven policing

In DDP, it is important to recognise that analysing big data with data science methods can reveal new patterns and trends that were previously invisible. However, it does not provide insight into the underlying reasons for these patterns (van der Zwet et al., 2022). In addition, the term 'big data' can give an unjustified sense of confidence in the completeness of the data (Dunietz, 2016). There are numerous examples where significant gaps in the data have been overlooked and/or the data are biased, for example, survey data and social media data (Bradley et al., 2021; Hargittai, 2020; Hargittai, 2015). The secrecy of criminal activities also results in a portion of crime remaining unseen and unregistered (i.e. dark number) (Barros et al., 2024).

Technology, human, organisational and ethical aspects

A well-known aspect of digital policing is its reliance on technology. However, technological, human, organisational and ethical aspects are equally important in the adoption of DDP. All four aspects are elaborated on in the next sections.

Technological aspects

DDP encompasses a broad range of technologies. Real-time identification technologies, for example, have transformed modern policing by making it possible to instantly identify people and objects. Tools such as ANPR, automated facial recognition and voice identification systems collect data in public areas without needing consent. Unlike traditional methods such as fingerprinting or DNA analysis, these systems allow live tracking and identification by comparing data with existing databases (Jansen et al., 2018).

Human aspects

A crucial aspect of DDP is the combination of both data-driven insights and human experience in decision-making. Officers often rely on their judgement and experience, sometimes overriding or modifying algorithmic suggestions to maintain their professional discretion. Officers heavily rely on their experience, which can sometimes clash with data-driven insights. For DDP to work well, officers need to combine their expertise with the data to recognise criminal patterns effectively (Buscariolli, 2023).

Challenges arise when tensions occur between data analysts and police officers, as officers tend to trust their own experience more than the data, which can hinder teamwork. For DDP to be effective, proper training and resources are needed, because officers and analysts sometimes lack the necessary skills or up-to-date knowledge (Afzal and Panagiotopoulos, 2024). Effective leadership is key to encouraging the use of data in policing. Leaders who inspire and involve others in their decisions can foster a culture of progress, while unclear objectives and poor management can hinder the successful adoption of data-driven strategies (Afzal and Panagiotopoulos, 2024).

Organisational aspects

On an organisational level, DDP changes the structure of how information and knowledge is exchanged (Marciniak, 2021). Policy and implementation do not always coincide. Data-driven policing has found its way into a network organisation, often alongside the traditional organisation (Dutch National Police, 2023). To what extent DDP is effectively implemented significantly depends on the resources and structure of police organisations. Having the right tools and properly trained staff is key to success. Smaller police departments often struggle with limited budgets, outdated technology and insufficient training. In contrast, larger organisations with more funding can

afford modern equipment, skilled data analysts and better training programmes. Furthermore, since HRCNs operate as network structures and quickly adapt to external factors (such as interventions by LEAs or other criminal networks), it is crucial for LEAs to also function as network organisations. They must be flexible in working with a diverse range of employees with various areas and levels of expertise (Schreurs and Martens, 2021).

Ethical aspects

The use of data-driven technologies in policing has made operations more efficient, improved decision-making and helped allocate resources better. However, these benefits come with ethical and privacy concerns, especially regarding the potential worsening of existing biases and harm to civil liberties. One major issue is the reliance on biased historical crime data, which often targets minority groups unfairly. For example, algorithms using factors like zip codes or minor offences can lead to over-policing in marginalised areas (Afzal and Panagiotopoulos, 2024). Predictive policing tools, despite being labelled as objective, risk creating cycles where biases are repeated and strengthened.

Real-time surveillance tools, like facial recognition and social media monitoring, add to privacy concerns. These technologies can undermine the presumption of innocence by flagging people based solely on their behaviour rather than solid, comprehensive evidence (Williams and Kind, 2019). Another challenge is the lack of transparency in machine learning systems, often called 'black box' algorithms. Policing tools created by private companies (like Palantir and PredPol), are protected by trade secrets, which make it hard for the public to hold them accountable (Afzal and Panagiotopoulos, 2024). These tools are also complicated, making it difficult for law enforcement officers to critically analyse their results. Hence, the ethical concerns of DDP go beyond technical problems and impact society.

Methodology

Study design

This study employed a mixed-methods qualitative design, combining desk research with empirical qualitative research to explore key perspectives within the Dutch police. In-depth interviews were conducted to gather rich, contextual data from key players involved in DDP. A semi-structured interview format was chosen to allow for flexibility while ensuring consistency across interviews. This approach was chosen to bridge the gap between theoretical frameworks and operational reality.

Participants

A total of 13 key players within the Dutch police organisation were selected by purposive sampling. These participants were identified based on their roles, expertise and involvement in DDP. As the Dutch police is a relatively small organisation, specific key players in the field of DDP-adoption are easily identifiable in a system search. In addition, interviewees were also asked for relevant key players within their networks and potential new interview subjects. The sample included a diverse range of individuals, such as project managers on DDP, legal advisors within the police organisation and employees of the national DDP programme, ensuring a comprehensive view of the organisation's structure regarding DDP.

To capture shared organisational insights, some sessions were conducted as group interviews; in total, nine interviews were held with the thirteen participants.

Data collection

The interviews took place between August and December 2024, either in person or virtually. Each interview lasted between 45 and 90 minutes. The interview focused on exploring the role of DDP in the Dutch National Police. The interview protocol was designed with a set of open-ended questions to explore the participants' views regarding the benefits, barriers and future developments of DDP across four primary dimensions: technological, human, organisational and ethical. The interview also addressed international collaboration, scientific research needs and any blind spots in current police practices related to DDP.

Interviews were audio-recorded with participants' consent and transcribed verbatim for subsequent analysis.

Data analysis

The transcribed interviews were analysed using thematic analysis to identify recurring patterns, themes and insights. To increase interrater reliability, the initial coding of one interview was performed independently by two researchers, after which the codes were compared and refined through an iterative process. Subsequently, the researchers each coded half of the remaining interviews. All data were anonymised to maintain participant confidentiality. The coding scheme can be found in Appendix 12.1. Quotes reported from the interviews were translated from Dutch to English, ensuring the preservation of the participants' original content.

Ethical considerations

The study adhered to standard ethical guidelines and all participants provided informed consent prior to their involvement. Participants were assured of their anonymity and the confidentiality of their responses, and they were given the option to withdraw from the study at any stage without any repercussions.

Results

This section presents a comprehensive analysis of the interviews, structured around the five key themes: defining DDP, and its technological, human, organisational and ethical dimensions, supplemented by additional relevant aspects.

Defining data-driven policing

Respondents offered diverse definitions of DDP but agreed that it is not a new concept. As one noted: 'We have always gathered information, from the moment we were a police force. And we register it all very carefully. However, nowadays we shove everything into specific bookcases and drawers, of which we have forgotten that they even exist.' Another respondent indicated that DDP is almost the same as intelligence-led policing, the only difference being the increased involvement of technology and big data, as it is difficult to ignore the impact of algorithms and AI in extracting valuable information from the data.

Despite the implication of the term 'data-driven', respondents emphasised that the data alone cannot lead decision-making in police practice. Current data systems cannot adequately account for contextual factors and risks, making

exclusive reliance on data undesirable. Some respondents differentiated between 'data-driven work', meaning the systematic analysis of existing data before an investigation, and 'working with data', which refers to combining data sources in the CSAE model. However, a consistent distinction did not clearly emerge. One respondent highlighted the importance of making critical choices about what data to specifically collect and how to use them. Others described data as 'the new weapon of the police'. The comparison being that as a baton or pepper spray are current weapons of the police, digital operations and interventions could be the weapons of the future, requiring similar levels of training, authorisation and evaluation before use.

Type of crime

Respondents generally agreed that DDP is applicable across a wide range of offences, particularly highlighting HRCNs and serious crime, and is useful across all phases of investigation, including prevention, detection and strategic intelligence.

Crimes with a clear start and finish, like robbery or homicide, may require different data-driven analytical approaches than ongoing, open-ended crimes, like drug trafficking networks (e.g. crime scripting, social network analysis). Several respondents remarked that focused questions (e.g. 'Who did it?') tend to feel more concrete and satisfying than open-ended intelligence questions (e.g. 'Who else is involved in a criminal network?').

Technological aspects

Views on technological development varied. One respondent claimed that technological advancements are almost already at their peak, and that the speed of developments will likely slow down. However, others see a future of increasing and continuing technological developments. For the police, technology is primarily about accessing new data sources, connecting systems and supporting analysis. A technical barrier mentioned by a respondent is the outdated ICT infrastructure, which limits the ability to share seized data and accommodate growing computational needs.

With new tools such as dashboards and large language models (e.g. ChatGPT), data are becoming more easily accessible to a larger proportion of employees. However, this carries the risks that employees without proper training and education regarding the use and risks of data tools may trust the results of these tools and adopt them as facts more easily than others.

Data quality, or data hygiene, was cited as a significant risk. Police reports, registrations and existing databases form the base of DDP, but the quality of the output is determined by the quality of the data, reinforcing the 'garbage in, garbage out' principle, as some respondents mentioned. Every person working with data within the police force should have a basic understanding and level of awareness that even a small registrational error could have big effects. For example, multiple respondents noted that once people are registered in police systems, whether they are involved, suspected or convicted, they will be more prone to police scrutiny and thus keep 'reappearing' in police systems. In addition, other respondents mentioned the limited data storage capacity of the police, and how the police must be more critical of what data to gather, what data to keep, and more importantly, what data to permanently delete and when.

Another technological development is the rise of misinformation, which has become a constant cat-and-mouse game between those who create and spread it digitally and those developing technologies to detect and counter it. One respondent mentioned: 'That was, for example, the case with deep fakes, where people made deep fake detectors, but those [deep fake detectors] were then used to improve the deep fakes. This can also be very dangerous.' The risks are that these technological advancements also enhance the expertise of criminals. Another respondent feared how the police will be able to deal with data (e.g. pictures, images, videos) that are automatically generated by a citizen or suspect. Questions arise as to whether the police can detect them as fake, how these data will be interpreted and to what extent it is illegal to provide this 'false' information to the police.

Due to the ever-growing and overwhelming amount of information and data that are involved in police work nowadays, respondents agree that it has become impossible for humans to analyse them all by themselves. Additionally, respondents mentioned the current personnel and capacity shortage within the Dutch police organisation, stressing the critical need for efficient data management. Respondents speculated that, through AI, large amounts of data could be analysed to identify which data points should be further examined by humans. It is repeatedly emphasised that a human should still provide the interpretation of the data to avoid making incorrect decisions.

Human aspects

Mindset

In recent years, with the increase of the amount and the importance of data, the necessity for change has become unavoidable. According to one respondent's personal experience, organisational change only occurs when there is both a sense of urgency and necessity on a strategic level. For years, this respondent experienced that, at first, there was no perceived need to change or improve work processes: 'I think that the insights generated by the crypto communication data have led to the realization that we, as an organisation, need to take action and ... anticipate what is coming'. Additionally, respondents noted that pressure from the media and societal discourse were also seen as significant factors of organisational change.

Although the sampled respondents are enthusiastic about DDP and mentioned many different, local DDP initiatives, at the same time, the sense of success and satisfaction among colleagues differs. The traditional police mindset is described as being focused on 'catching kilos, cash and crooks' and less on effect-based interventions or the prevention of crime. The latter being less tangible. As an example, a respondent mentioned that a lot of information can be collected and endlessly analysed in a criminal investigation about a HRCN, but this is not perceived as a success by the detectives if no criminal has been arrested.

Respondents note that a part of the Dutch police culture revolves around people and data being compartmentalised, which hinders people from thinking beyond their own domain. This is improving according to the respondents, partly because colleagues are collaborating more and, as they work in different teams throughout their careers, they learn to understand each other's expertise better (with the CATs as a leading example). One respondent mentioned that, while the Dutch police want to work more flexibly as an organisation, employees quickly interpret that as the dissolution of existing teams. People like having stability and feeling connected to a team. A respondent described that, on an operational level, the organisation is currently not designed for flexibility. The example was

given that, when determining when an intervention should take place, intelligence is sometimes not the leading factor, but whether there is enough staff available at that moment.

An often-mentioned aspect of the DDP mindset is how police personnel should be very critical about the use of data in their investigations. As mentioned earlier, DDP-practitioners believe that, with so many data available, a shift in mindset is needed to focus on asking the right questions: what data and information do we really need for this investigation? What are we going to do with the data we collected? Some respondents used the example of smartphones to illustrate this. The average smartphone contains about 128 to 256 gigabytes of data. In a stalking case, would all the data on that phone be necessary? Or just the phone logs, messaging apps and recent photos? Respondents call for both a shift in mindset and proper internal checks and balances in this age of DDP.

Multiple respondents argue that other areas of police work, such as emergency services, are also valuable as information and data sensors. Respondents also commented on the mindset of street patrolling officers, who want to catch criminals, but do not see themselves as part of the 'intelligence organisation'. However, when these colleagues are motivated to gather information, and accurately register data in police systems, their input can be a valuable additional source and yield significant results.

Lastly, respondents noted how people like to remain critical as the 'human-in-the-loop'. At all levels – strategic, tactical and operational – people are perceived to be sceptical about sharing data: 'Should I share this?', 'Why would I share my data with you?'. The most reported value in operations is still: 'Then I'll lose my case!'. This leads to reluctance in sharing information.

Skills and expertise

To operate in a data-driven manner, officers need to be skilled enough to handle large amounts of data and specific tooling. One respondent discussed that colleagues often know how to investigate 'the traditional way', through tapping phones, surveillance and other labour-intensive manners but, as mentioned before, investigators are less likely to think about what data are already available in the systems, and what data are still needed to solve a case. Hence, multiple respondents argue that analytical and critical thinking skills are increasingly important for detectives and intelligence analysts.

The respondents agree that a human is always needed as the 'man in the middle' between technology and operations, with the focus on human qualities like integrity and empathy. In addition, according to the respondents, more experts, such as data scientists, legal advisors and ethicists, are needed. As the data are still too unreliable, and technology and algorithms are not (yet) sufficiently reliable, the police organisation will need to maintain human control in the near future.

In conclusion, current employees will need to be trained to work effectively with both data and people, and expert skills will need to be brought in. As one respondent put it: 'it should soon become a basic rule that criminal investigators need to know a certain amount of tooling. They do not need to be an expert in everything, but DDP will become a standard way of working'.

Organisational aspects

Structure

As mentioned earlier, a topic that often came up in the interviews is that teams need to remain flexible for DDP to work. As one respondent described: 'As an organisation, we are still really at the foot of a high mountain, the organisation is sluggish and change is slow'. Multiple respondents argue that, to become a data-driven organisation, the organisation needs to be able to respond to rapid changes. To keep up with developments in society, and therefore also in crime, it is important to make effective choices regarding the organisational structure.

Most of the respondents mentioned the 'golden triangle', where intelligence departments, criminal investigation and 'specialist criminal investigation' – which entails specific expertise such as forensics or digital expertise – work together. As this has increased, for example in the CATs, the value of this multidisciplinary collaboration has proven itself and led to success stories. Currently, this collaboration does come with its hardships as, for example, intelligence analysts and investigators within the same team report to different supervisors who do not always share the same operational or strategic goals. A suggestion made by two respondents is to have thematic multidisciplinary teams at both the operational and strategic levels with a single supervisor, where, at the strategic level, disciplines can remain separate. These thematic teams can also assist in making the transition from the 'analyse' phase to the 'engage' phase (see Figure 12.3), as both employees work closely together in the same team.

As the Dutch police is a national police organisation with ten regional and two national units, the collaboration between these units is also discussed. Respondents argue that the regional units are structured similarly; however, in practice they still experience large differences between the units. One respondent mentions the increasing role of the two national units in the acquisition and distribution of knowledge and experience.

Human resources

When discussing the organisational needs for DDP, human resources issues were discussed on two levels: regional cases and organisation-wide cases. On a regional level, respondents repeated their views on strong, local leadership and the consequences for DDP implementation. Leaders with a clear vision and means to act on that vision are allowed to combine and even hire personnel to create multidisciplinary teams. These teams seem to thrive, but are threatened by overall personnel shortages and shifting priorities, and often are not sustainable. Respondents call for a flexible human resources policy that would allow leaders to create their own teams according to their needs, and to be able to keep these people on for as long as necessary, and for organisational flexibility, in the sense that the organisation can foster successful teams and change their structure, rather than ending them prematurely.

On a national scale, respondents foremostly mentioned the structural personnel shortage within the Dutch police, regardless of DDP implementation. Generally speaking, although there are regional differences, despite all the data that are available, there is a shortage of (data) analysts who can work with (big) data to generate actionable outcomes. In addition, even when such analysts are available and do generate results, there is a shortage of personnel who can act on those results.

In addition to the general personnel shortage, respondents describe how diversity in personnel and multidisciplinary teams are essential for DDP. Different backgrounds, specifically data sciences or OSINT skills, are mentioned as being important. However, respondents acknowledge that these often highly specialised people are scarce, and the Dutch police organisation must compete with corporate companies and other services. It is urged to challenge these highly sought individuals to work together with the police and build a resilient organisation.

Leadership

The role of management and leadership was brought up by the respondents in almost every interview. Several respondents reported that they noticed how individual team leaders determine the success of DDP integration. They agree that if a strong-willed leader has a clear vision of how DDP should be implemented, and he or she is given the space and means to express that vision in, for example, personnel changes and priority shifting, DDP is better adopted in the workplace. However, because this implementation is largely reliant on the efforts of individual leaders, respondents also noted that there are large differences between regional units.

As mentioned earlier, DDP activities, such as big data intelligence analysis, might not generate immediate tangible results. It was noted that police success is traditionally defined more by quantifiable results, like the amount of drugs or money seized, or the number arrests made. This apparent delay in traditional, tangible results might lead to feelings of dissatisfaction and frustration among personnel. It was noted that leaders should be able to defend their DDP vision and implementation to both their superiors and their team.

When asked about the role of strategic management and the national data-driven cooperation programme, respondents noted how the programme started off with a strong vocal presence and vision of what DDP should look like in the Dutch National Police. Several regional units were selected for pilots. Respondents observed that if their unit was not selected as one of the pilot units, their involvement in the national programme gradually diminished. Several respondents shared the thought that, to successfully implement DDP, strategic management should not only rely on the top-down flow of vision and practice but should also work together with (all) regional units to create a shared understanding of DDP implementation. Another respondent added that a new paradigm is needed, because thinking in terms of 'bottom-up' and 'top-down' traps you in a mindset of duality.

Education

Several respondents addressed the desire for more formal education regarding DDP. Regional units often organise local educational activities, ranging from a workshop day to their own educational courses. Respondents praise these initiatives but warn that knowledge gained and lessons learned in these courses should be more properly integrated into police education, as they seem to lack professional checks and guidance. Respondents agree that police educational institutions, like the Dutch Police Academy, should be involved in developing and providing such education.

Some respondents noted that new personnel seem to differ from 'regular' police personnel in terms of education and knowledge needs. For example, a data scientist might have sufficient knowledge of data and tooling but might lack domain-specific police knowledge. On the other hand, police personnel might be experts in their field or domain but could lack basic knowledge of data and data analyses to properly understand and interpret results. As mentioned under 'Skills and expertise', respondents call for a basic understanding of the uses and risks of data.

However, it is yet to be determined what this basic, general understanding of domain, data and tooling knowledge should consist of.

Ethical aspects

Only a few respondents mentioned the ethical aspects of DDP. Hence, the following results are mainly from one interview with an ethics expert. The respondent argues that organisations have generally transitioned from a functional structure to process optimisation, and eventually to a customer-centric approach. Now, the respondent argued, data are seen as the starting point. In DDP, the respondent described ethics as 'the current biggest challenge'. The recently experienced 'techno-optimism' in organisations ensures that new technologies are used enthusiastically without thoroughly considering the consequences.

Respondents advocated for early ethical considerations via structured methods such as the guidance ethics approach. For the police, the tension between AI and ethics is even more relevant because of budget, time and workforce shortfalls, and the ongoing search for more efficient working methods. According to this respondent, even though police officers must make ethical decisions daily, there is a need for more awareness and professional governance. The expectation is that the impact of AI will only increase in the coming decades. Fundamental values will not change, but the rapid technological development requires continuous monitoring and adjustment to maintain a balance between people and technology. Aspects such as surveillance, privacy and democracy will become increasingly urgent. Data awareness requires analysis of processes, practices and possible biases. These considerations should be made at a strategic level, with input from both internal (police) and external experts. Although ethics and sustainability are considered important, concrete actions are often lacking.

Additional aspects

Several interviews touched upon additional aspects affecting DDP, for instance, societal involvement and legal developments. A few respondents noted how the Dutch society has yet to debate to what extent they value their fundamental rights of freedom and privacy over police authority and security. Both the Dutch and the European political climate, along with increasing societal polarisation, are expected to play a role in this debate and to shift the balance toward more freedom and less security in the near future.

Some respondents share the view that the current Dutch legal framework is not yet up to date with technological developments and their implications for police work. New technologies or data sources, such as civilian cameras (i.e. smart doorbell), could have a major impact on criminal investigations. However, the current legal framework (despite the approval of the EU AI Act) is not yet adapted to such technological advancements and is either ambiguous or reserved about the adoption of technological advancements in police work. According to the respondents, this leads to misunderstanding and frustration for both police personnel and civilians. Dutch criminal law is currently under major supervision, but respondents agree that the rate of legislation and jurisprudence development is too slow and already behind current technological developments.

Some respondents call for levels of authority or control of data and corresponding, proportional authorisation rights. Respondents believe the examining magistrate (*rechter-commissaris*) might play a role in this data authorisation in the future.

Discussion and conclusion

The rapid digitalisation of society has fundamentally altered the operating environment of LEAs. In particular, the widespread use of encrypted communication by criminals, especially within HRCNs, has generated unprecedented volumes of data, as criminals need communication to organise their business. This has led to the concept of DDP. This study combined desk research and interviews to gain better insight into the role and the current status of DDP in the Dutch police with regard to HRCNs. The use of data, algorithms and AI in policing raises technological, human, organisational and ethical challenges that must be addressed to develop an effective strategy against crime.

The current state of data-driven policing in the Netherlands

Recent research and respondents from the current study provide varied interpretations of what DDP entails, and there is no clear definition provided by the Dutch police. There is general agreement that DDP is not a new concept, but rather an evolution of intelligence-led policing, distinguished by the scale, complexity and speed of the data available through digitalisation and encryption. Within DDP, there is need for multidisciplinary collaboration between, among others, AI experts, domain experts and intelligence analysts. Therefore, we propose that a clear definition of what DDP entails should be introduced within the Dutch police organisation. In this way, the organisation can align expectations and create collaborative goals. It also enables them to work in a universal manner and systematically learn from it. By discussing learning points with different teams, the DDP approach can also be continuously improved throughout the whole organisation.

While encryption enables criminals to conceal their activities, it simultaneously produces highly structured datasets once law enforcement gains lawful access. Respondents emphasised that these datasets offer substantial investigative value but also introduce new risks. Data extracted from encrypted communication require interpretation, contextualisation and critical assessment, as automated systems cannot adequately account for investigative, legal and ethical nuances. This reinforces the central finding that DDP cannot be reduced to algorithmic decision-making: human judgement remains essential throughout the intelligence and investigative cycle, including with regard to prevention and detection. Operational practice should therefore formally embed 'human-in-the-loop' principles at all stages of data-driven investigations, ensuring that analytical outputs from encrypted data are validated, contextualised and authorised by trained personnel before operational action is taken.

The emergence of the CATs has been a catalyst for DDP within the Dutch police. The successes and barriers these teams have experienced increased their awareness of the potential, necessity and risks of the use of big data, algorithms and AI by the police. Additionally, since the start of the national programme of data-driven policing, it has become a key strategic issue in the police organisation. Change in the organisation has also been driven by the increasing volume of data and external pressures, partly from media and society. The realisation that action is necessary, spurred by insights from crypto communication data, has created an urgent need to adapt work processes. As technological advancements continue, new opportunities and threats will emerge (e.g. quantum computing (European Union Agency for Law Enforcement Cooperation, 2024b)), which LEAs will have to anticipate and prepare for.

Aspects and challenges

Technological advancements in policing are progressing at different rates, with some respondents noting slowdowns while others anticipate continued growth. The Dutch police face challenges such as outdated ICT systems and insufficient server capacity, hindering data accessibility and the full transition to DDP. New tools like dashboards and large language models (e.g. ChatGPT) have become widely available to many employees, but this could increase the risk of people unconsciously relying on unreliable data without having received proper training and with a lack of internal authorisation systems. Respondents call for a basic understanding of the uses and risks of data. The increased volume of data and the rise of misinformation, such as deepfakes, further complicates the situation, as these advancements also enhance criminal expertise.

The overwhelming amount of data available requires a shift in mindset, with a focus on asking the right questions about what additional data are necessary alongside the already comprehensive databases. The data quality and importance of correct registration in police systems ('garbage in, is garbage out') needs more attention. Ethical and legal considerations must guide data collection and their timely removal, but this awareness is not yet sufficiently present among employees working with data. There is a need to foster a mindset where information gathering is seen as a part of the broader police effort, not just the intelligence community. While technology and data sharing are crucial, there is reluctance among staff, which is often driven by the fear of losing control. A flexible authorisation model could be of assistance in structurally storing and sharing data, with a foreseen increased role for the examining magistrate.

Trust in data tooling and the outcomes of algorithms still impedes efforts to fully integrate DDP on all levels. This barrier is two-sided: on the one hand, police staff need to be aware of the shortcomings of data, presence of biases and lack of transparency of algorithms. Although all these data seem to be a gold mine, we argue that a critical mindset is needed to assess whether we are dealing with actual gold or 'gilded gold'. As LEAs will have to deal with deepfakes, misinformation and manipulation and the challenges they pose to data integrity and decision-making, we recommend that LEAs introduce an additional, manual approach in tooling to assess how reliable systems and algorithms are. Discussions need to be held on an organisational – and societal – level as to what degree of system (un)reliability to accept. A 95 % or even a 99 % accurate system will still generate mistakes. On the other hand, staff need to trust the outcomes of data enough to be willing to make data-based decisions and reduce human workload. This delicate balance can be achieved through awareness, training and experience over time.

Results showed that the integration of DDP within the Dutch police requires significant attention to organisational structure, leadership, and human resources to effectively leverage data analytics in operational contexts. One key aspect emerging from the interviews is the need for organisational flexibility to adapt to the demands of a data-driven, highly valued multidisciplinary approach. Respondents emphasised that, to respond to rapid societal and criminal developments, the organisation must adjust its structure to ensure efficient use of capacity and expertise. Data-driven decision-making necessitates the breakdown of silos between different disciplines. However, challenges persist, like aligning leadership goals across teams, as individual supervisors often set different operational or strategic objectives for analysts and investigators. An organisational mindset shift is needed to create a more adaptable workforce that can respond to changing demands.

Leadership plays a critical role in the success of DDP integration, with respondents noting that individual leaders' visions for DDP significantly influence the implementation process. Clear leadership with the ability to allocate resources and manage personnel changes has been shown to foster more successful DDP adoption, although discrepancies between regional units remain. We argue that a national collaborative approach is essential for the success of data-driven initiatives, as regional units, particularly those not involved in pilot projects, reported feeling sidelined as the national programme progressed. In the future, it would be beneficial to keep all regional units in the loop of current experiments and developments.

On the human resources front, a structural shortage of personnel, particularly data analysts with the necessary skills to handle big data, was noted as a significant barrier to effective DDP implementation. Despite the availability of data, there is an insufficient number of analysts who can transform it into actionable intelligence, and even when such individuals are available, a lack of personnel to act on these insights further limits effectiveness. However, they acknowledged that attracting such highly specialised individuals is a challenge due to competition from the private sector and other governmental organisations. To address these shortages, it was suggested that the police organisation must adopt strategies to attract and retain these professionals, fostering a resilient workforce capable of navigating the complex demands of DDP.

The current Dutch legal framework is not yet up to date with technological developments. Modern technologies or data sources could have a beneficial impact on criminal investigations, but the legal framework needs to be adapted to such technological advancements. Dutch criminal law is currently under major supervision, but respondents agree that the rate of legislation and jurisprudence development is too slow and already behind on current technological developments. With new legislation, such as Dutch law and the EU AI Act, education on these changes is necessary.

The police face significant tension between AI and ethics due to limited resources, unclear legal guidelines and the ongoing search for more efficient methods. In the interviews, ethical topics did not come up very easily. Police officers must make ethical decisions daily, but there is a need for greater awareness and professional governance to ensure that these ethical standards also apply in DDP contexts. The growing impact of big data and AI require ongoing monitoring and adjustment. Issues like surveillance, privacy and democratic values will become more pressing, making data awareness essential among police officers at all levels. Hence, we argue for increasing ethical awareness, for example, by including an ethical advisor in a flexible team or by establishing a compliance officer or an ethical (data) committee.

Data-driven policing also sparks a societal debate about the extent to which the public values their fundamental rights of freedom and privacy over police authority and security. The Dutch, but also European, political climate and societal polarisation are expected to play a role in this debate, and the outcome of this delicate balance will likely affect police legitimacy in the future.

In conclusion, this study highlights both the potential and the challenges of DDP within the Dutch police, particularly in the context of HRCNs. While DDP offers promising opportunities for addressing HRCNs, significant obstacles remain. Its success depends on the integration of technology, human judgement, organisational design, ethical governance and legal clarity. Operationally, this requires a clear and consistent definition of DDP, and greater

organisational flexibility and leadership. There is an urgent need for better training, collaboration and ethical awareness to ensure that data-driven approaches are used responsibly and effectively. Moving forward, LEAs should foster an adaptable, well-resourced and ethically conscious workforce to navigate the complexities of modern policing in an increasingly digital world. Future research and policy development should focus on bridging gaps in data reliability, improving education on DDP, conducting empirical evaluations of its effectiveness, adapting legal frameworks and strengthening human resources development to optimise the potential of DDP in combating crime while safeguarding civil liberties.

Acknowledgments

We would like to thank Femke van 't Hoff for her assistance in the literature review.

Artificial intelligence statement

During the drafting process, AI tools such as Copilot were used only for language improvement. All intellectual contributions, analysis and literature synthesis were made by the authors. The final manuscript reflects the authors' academic interpretation and critical evaluation of the reviewed studies.

References

Afzal, M. and Panagiotopoulos, P. (2024), 'Data in policing: An integrative review', *International Journal of Public Administration*, Vol. 28, Issue 7, pp. 411–430, https://doi.org/10.1080/01900692.2024.2360586.

Barros, A. I. (2022), *De Kracht van Intelligence: Bezint eer ge moet bijsturen*, Politieacademie, Apeldoorn, https://mediatheek.politieacademie.nl/pdf/102452.PDF.

Barros, A. I., Doeleman, R. and Schreurs, W. (2024), 'Intelligence', in: Kop, N., Muller, E. R. and van der Torre, E. J. (eds), *Politie – Organisatie en functioneren van de politie in Nederland*, Wolters Kluwer, Deventer, pp. 395–416.

Bradley, V. C., Kuriwaki, S., Isakov, M., Sejdinovic, D., Meng, X.-L. et al. (2021), 'Unrepresentative big surveys significantly overestimated US vaccine uptake', *Nature*, Vol. 600, pp. 695–700, https://doi.org/10.1038/s41586-021-04198-4.

Buscariolli, A. (2023), 'Making crime visible in the digital age: The ethnomethods of data policing', *Critical Criminology*, Vol. 31, No 2, pp. 545–562, https://doi.org/10.1007/s10612-023-09683-y.

Davis, J., Purves, D., Gilbert, J. and Sturm, S. (2022), 'Five ethical challenges facing data-driven policing', *AI and Ethics*, Vol. 2, pp. 185–198, https://doi.org/10.1007/s43681-021-00105-9.

Den Hengst, M. and Wijsman, O. (2023), 'Datagedreven politiewerk – Een organisatorisch en juridisch perspectief', in: Snaphaan, T., Hardyns, W., Van Dijk, A., Spithoven, R. and van Brakel, R. (eds), *Big Data Policing*, Vol. 1, No 66, Gompel en Svacina, pp. 71–90, https://nscr.nl/app/uploads/2023/02/2023-den-Hengst-Wijsman-Datagedreven-politie-accepted.pdf.

Dunietz, J. (2016), 'How big data creates false confidence', *Nautilus*, 22 April, https://nautil.us/how-big-data-creates-false-confidence-235908.

Dutch National Police (2023), *Landelijk programmaplan – Magazine Datagedreven Samen Werken*.

European Union Agency for Law Enforcement Cooperation (2024a), *Decoding the EU's Most Threatening Criminal Networks*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2813/811566.

European Union Agency for Law Enforcement Cooperation (2024b), *The Second Quantum Revolution – The impact of quantum computing and quantum technologies on law enforcement*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2813/42230.

Hargittai, E. (2015), 'Is bigger always better? Potential biases of big data derived from social network sites', *The ANNALS of the American Academy of Political and Social Science*, Vol. 659, Issue 1, pp. 63–76, https://doi.org/10.1177/0002716215570866.

Hargittai, E. (2020), 'Potential biases in big data: Omitted voices on social media', *Social Science Computer Review*, Vol. 38, Issue 1, pp. 10–24, https://doi.org/10.1177/0894439318788322.

Jansen, F. (2018), 'Data driven policing in the context of Europe', Data Justice Lab, 7 May, https://datajusticeproject.net/wp-content/uploads/2019/05/Report-Data-Driven-Policing-EU.pdf.

Jansen, J., Westers, S., Schreurs, W., Berkenpas, M., Alpár, G. et al. (2023), *De Rol van Encryptie in de Opsporing: Belemmeringen en mogelijkheden*, NHL Stenden Hogeschool: Cybersafety Research Group, https://open.overheid.nl/documenten/ronl-d497ea5bebe949b3cde930209d87e131413e6b09/pdf.

Marciniak, D. (2021), 'Data-driven policing: How digital technologies transform the practice and governance of policing', University of Essex: Department of Sociology, https://repository.essex.ac.uk/30103/1/Data-driven%20policing%20-%20how%20digital%20technologies%20transform%20the%20practice%20and%20governance%20of%20policing%20(Daniel%20Marciniak).pdf.

Ministry of Justice and Security (2019), *Datagedreven Werken – Wat is er voor nodig?*, https://open.overheid.nl/documenten/ronl-7cdd61bf-c43c-4cf8-a054-86dfe1a49951/pdf.

Roest, D. (2023), 'Big data en politiewerk, een onoverbrugbare kloof? Hoe TROI de brug slaat van big data naar politiewerk', in: Snaphaan, T., Hardyns, W., Van Dijk, A., Spithoven, R. and van Brakel, R. (eds), *Big Data Policing*, Vol. 1, No 66, Gompel en Svacina, pp. 91–106.

Schreurs, W. and Martens, P. (2021), 'De politie als anticiperende en adaptieve organisatie – De criminele context en politie-interventies beter begrijpen en beïnvloeden', in: Meershoek, G., Nap, J. and van Spijk, L. (eds), *In Naam der Wat? Reflecties op politie en politiewerk*, Boom, The Hague, https://doi.org/10.13140/RG.2.2.15492.55681.

United States Department of Defense: Joint Chiefs of Staff (2013), 'Joint intelligence', *Joint Publication 2-0*, 22 October, https://www.benning.army.mil/infantry/doctrinesupplement/atp3-21.8/PDFs/jp2_0.pdf.

Van de Sandt, E., van Bunningen, A., van Lenthe, J. and Fokker, J. (2021), *Towards Data Scientific Investigations: A comprehensive data science framework and case study for investigating organized crime and serving the public interest*, National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online, https://www.rephrain.ac.uk/wp-content/uploads/White-Paper-Towards-Data-Scientific-Investigations.pdf.

Van der Zwet, K., Barros, A. I., van Engers, T. M. and Sloot, P. (2022), 'Emergence of protests during the COVID-19 pandemic: quantitative models to explore the contributions of societal conditions', *Humanities and Social Sciences Communications*, Vol. 9, pp. 1–11, https://doi.org/10.1057/s41599-022-01082-y.

Williams, P. and Kind, E. (2019), *Data-driven Policing: The hardwiring of discriminatory policing practices across Europe*, European Network Against Racism, Brussels, https://www.statewatch.org/media/documents/news/2019/nov/data-driven-profiling-web-final.pdf.

Appendix 12.1.

Code	Sub-code
Affiliation	
DDP	Definition
	Work process
	Data sources
	Developments
Type of crime	Organised crime
	Drug-related crime (specific)
	Cybercrime
	Police patrol
	Sexual offences
	Crime prevention
	Other
Organisational	Structure
	Leadership
	Human resources
	Education
Technological	
Human factor	Skills and expertise
	Mindset
	Societal
Legal	
Ethical	
SWOT	Strength
	Weakness
	Opportunity
	Threat
	Developments
International	Collaboration
	Positioning
Research proposals	

Study on corruption vulnerabilities in EU seaports' supply chain

Jasmin Saarijärvi, Gabrielle op 't Hoog, Sabine Hellemons, Federica Genna, Victoria Tokatzian, Halima Guelai, Margarita Gasparinatou, Eirini Stamouli, Júlia Miralles-de-Imperial, Fernando Jiménez-Sánchez

https://doi.org/10.3013/sr700b64

Abstract

This article draws on the results of a study on corruption vulnerabilities in EU seaports' supply chains, developed within the framework of project POSEIDON (PortS unitED Against Corruption). POSEIDON is an EU-funded project (Grant Agreement No 10110337) that seeks to enhance anti-corruption practices in EU seaports. This is done through the mapping and identification of corruption vulnerabilities in the supply chains of EU seaports. Ports and their supply chains are crucial as enablers of trade, but they are also vulnerable to the exploitation of organised crime groups involved in the trafficking of illicit goods such as drugs or firearms. The identification of corruption vulnerabilities and anti-corruption practices is carried out through literature research, interviews, focus groups, surveys and study visits to selected ports in Belgium, Greece, Spain, Italy and the Netherlands. To contribute to EU-level actions against corruption and address vulnerabilities in the port supply chain system, POSEIDON also gathers practices from different public and private stakeholders. The project is still ongoing, but some anti-corruption practices have already been identified, namely digitalisation, training and awareness campaigns, and screening of port employees and staff, along with public–private cooperation. This process of exchange is fostered in the project by a cycle of six thematic dialogues, where different stakeholders from the public and private spheres are brought together to discuss current trends, challenges and good practices in this sector.

The identification and collection of anti-corruption practices is closely connected to the EU public–private network of port sector stakeholders that has been established during the project. The network fosters the exchange of anti-corruption practices and contributes to the mitigation of corruption vulnerabilities in the port sector. The transferability of good practices identified by the project – which will also be displayed via an interactive dashboard

available to the public – will be assessed within the project's life cycle, contributing to the definition of a series of recommendations for an EU port supply chain integrity standard.

Keywords: seaports, corruption, supply chain, vulnerabilities, good practices, port stakeholders, organised crime, infiltration, resilience.

Introduction

This article is a summary of a 2024 study by the POSEIDON Consortium on corruption vulnerabilities in EU seaports' supply chains drafted as part of the EU-funded project POSEIDON ([27]).

The article seeks to identify vulnerabilities for corruption in EU seaports' supply chains. In particular, it aims to contribute to the understanding of vulnerabilities for corruption and, as such, to provide a stepping stone for an improved EU-wide approach against this phenomenon.

The overall objective is to shed light on the vulnerabilities for corruption at different stages of the EU port supply chain. EU seaports are part of the critical infrastructure that enables the transport of goods across Europe (and beyond) and are an essential component of the supply chain that ensures the smooth functioning of the single market (Europol, 2023, p. 4). Corruption in seaports facilitates crime, disrupts trade and undermines the rule of law. As there is no universally agreed definition of corruption, perspectives and interpretations of corruption vary between cultures and countries (European Parliament: Directorate-General for Parliamentary Research Services et al., 2017, p. 5). However, corruption is regularly understood as 'the abuse of (entrusted) power for private gain', a relatively broad concept that covers offences such as active and passive bribery, conflict of interest, clientelism, favouritism and trading in influence (European Parliament: Directorate-General for Parliamentary Research Services et al., 2017, p. 5). The focus of the study at hand is on corruption intended as an 'enabler of organised crime'. While organised crime can exist with and without corruption, the focus of this study lies at the intersection between the two, with its scope delimited to the working mechanisms of EU seaports' supply chains.

Methodology

The research methodology applied includes desk research of over 30 sources at the international, EU and national levels, 12 interviews with public and private actors and 6 case studies (Port of Algeciras, Port of Antwerp-Bruges, Port of Cartagena, Port of Piraeus, Port of Rotterdam and Port of Venice). Additionally, a cycle of six thematic dialogues was organised to gather further input from stakeholders, and a targeted survey was developed and distributed to the law enforcement community across the EU. Further details on each data collection method are presented in the following sections. As outlined above, the scope of the article covers corruption as an enabler of organised crime, with a focus on corruption at the operational level (i.e. in the supply chain). The research has been focused on corruption related to the trafficking of illicit goods from ports located outside the EU into ports in the EU, predominantly through container trade.

([27]) Ports United Against Corruption – Grant Agreement No 101103337 – POSEIDON – ISF-2022-TF1-AG-CORRUPT, POSEIDON, 2023. See: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43252368/101103337/ISF?order=DESC&pageNumber=1&pageSize=10&sortBy=relevance&keywords=poseidon&frameworkProgramme=43252368.

Analytical framework

To facilitate the comprehensive and structured collection of data, an analytical framework was developed, based on a supply chain of legal trade of EU seaports. This draft supply chain was developed based on desk research, scoping interviews and detailed exchanges with the POSEIDON advisory board, supporting partners and relevant port stakeholders and experts on EU seaport supply chains. These activities yielded a comprehensive overview of the different steps in the EU seaport supply chain of legal trade and helped to identify a first set of vulnerabilities linked to these steps, as presented in the figure below.

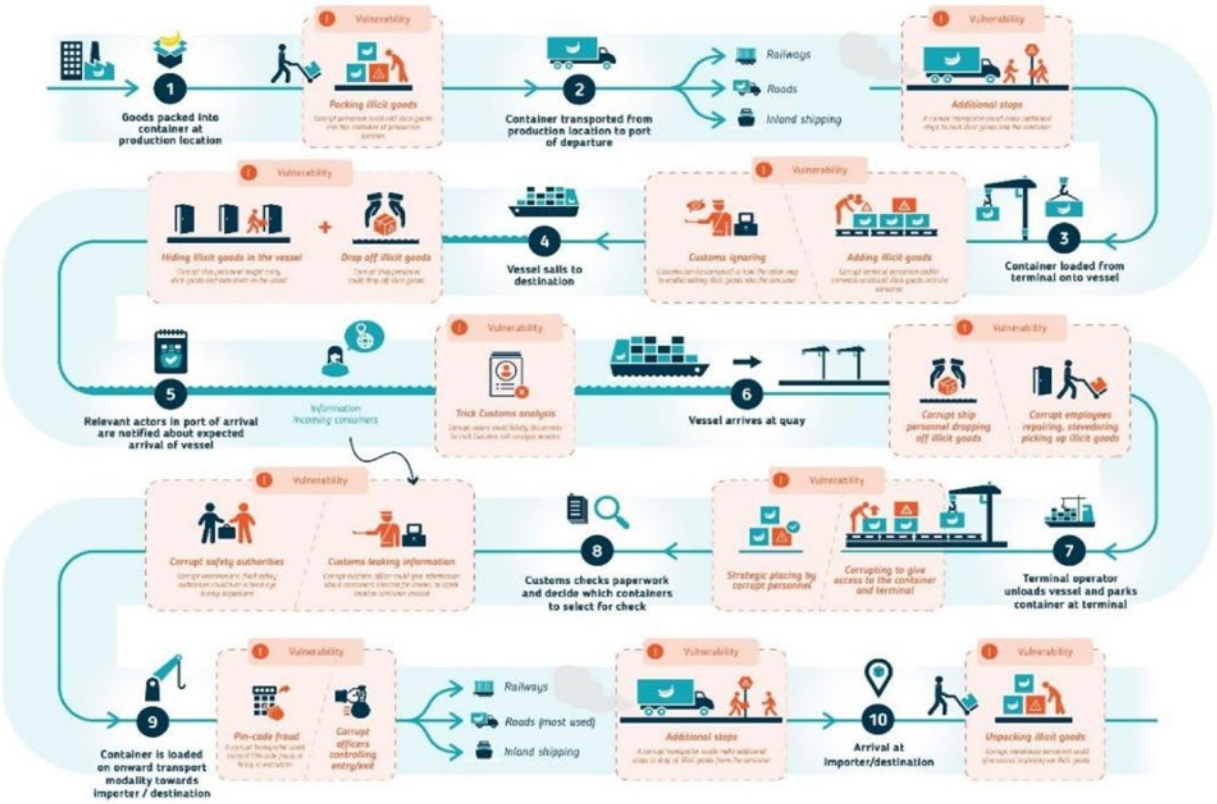


Figure 13.1. Visualisation of corruption vulnerabilities in the port supply chain

Source: POSEIDON.

Data collection

Desk research was conducted taking into account a wide array of documentation. Over 30 documents have been reviewed via desk research, including academic papers, policy documents and reports from (inter)national organisations and law enforcement agencies, at both the international and EU levels. An overview of relevant documentation considered is included in the references ([28]). Moreover, interviews with various seaport authorities, European policymakers and researchers have enriched the study with in-depth insights that complemented findings obtained through desk research.

([28]) This overview does not include the relevant documentation considered in light of the case studies.

Six case studies were conducted in the framework of the POSEIDON project ([29]) with a view to providing seaport-specific insights, illustrating findings with real-world examples. The case studies were selected in such a way to allow for a geographical spread of the seaports across the EU and to ensure a mix between larger and smaller seaports. Each case study involved desk research, interviews with stakeholders, focus groups with economic operators and study visits to seaports.

During the visits (as part of the case studies) to the Port of Antwerp-Bruges, the Port of Algeciras and the Port of Venice, thematic port dialogues were also held ([30]). The purpose of these thematic dialogues was to bring a variety of stakeholders together and to discuss a particular topic related to corruption in seaports with a diverse group of stakeholders. Central topics of the thematic dialogues were public–private cooperation, compliance systems and digitalisation in seaports, and corruption as an enabler of human smuggling.

Lastly, a survey was conducted with a dual objective. Firstly, the survey served as an opportunity to gather information on vulnerabilities for corruption in seaport supply chains outside the six seaports that serve as case studies. Secondly, the survey also provided an opportunity to validate the findings collected through the six case studies. Given the sensitivity of the topic at hand, the survey was only launched within the law enforcement community, within the framework of POSEIDON under the European multidisciplinary platform against criminal threats (Empact) high-risk criminal networks operational action plan (operational action 7.1) ([31]).

Validation of findings

Preliminary findings and conclusions have been verified and validated at several stages, including at a validation session with the POSEIDON advisory board, composed of academics, policymakers and law enforcement representatives, inter alia. Finally, the draft findings and conclusions were presented to the co-leaders and participants of operational action 7.1 of Empact's high-risk criminal network operational action plan, focusing on the prospective impact of these findings on the operational work of the law enforcement community.

Methodological limitations

The research encountered methodological limitations that warrant acknowledgment. First, the selection of seaports for case studies, limited to six, may restrict the generalisability of findings to a broader port context. Limitations in geographical focus are also present due to this, as the case studies only focus on seaports in north-western Europe and southern Europe. This limitation was mitigated by collecting additional data on seaports beyond the selected case study ports through desk research, in-depth interviews, the survey and validation sessions with different types of stakeholders. Second, distinguishing between organised crime and corruption posed a significant challenge. The intertwined nature of these phenomena, often due to blurred distinctions, complicates the assessment of individual contributions to corrupt practices within seaport environments. Due to the sensitivities surrounding corruption in countries, the tendency to apportion blame to organised crime instead of corruption emerged as a difficulty. These

([29]) Case studies have been implemented as follows: Port of Piraeus (September 2023), Port of Antwerp-Bruges (November 2023), Port of Algeciras (January 2024), Port of Rotterdam (February 2024), Port of Cartagena (March 2024), Port of Venice (April 2024).

([30]) The organisation of thematic dialogues is part of Poseidon's work package 4, and contributes to fostering inter-port exchanges and dialogues, supporting the establishment of a public–private port stakeholder network.

([31]) Poseidon serves as inspiration and driver for Empact's fight against high-risk criminal networks (operational action 7.1), which formally kicked off in February 2024.

limitations highlight the need for a cautious interpretation of findings and suggest ways in which this can be addressed in future research more comprehensively.

Key findings

The research has yielded many relevant and concrete insights into corruption vulnerabilities in the different ports in the case studies. Whereas the vulnerabilities for corruption in the supply chain tend to be relatively clearly demarcated, the more structural features in and around ports that increase vulnerability to corruption are less tangible, more complex and, likely, more difficult to address. Some of these vulnerabilities directly affect the possibility of corruption risks, while others have a more indirect effect on corruption risks.

This section first describes the vulnerabilities with a direct impact (i.e. types and origin of goods, the involvement of people, social communities around the port and the role of politics) before addressing the more indirect factors (i.e. the economic climate in the port, the type, size and location of the port, the cooperation between actors in the port, and legislation). Subsequently, the corruption vulnerabilities in each step of the port supply chain are highlighted.

Vulnerabilities related to corruption in seaports

Types and origin of goods and shipments

The ports examined in this article suggest that certain types of goods, modalities and trade routes pose more vulnerabilities related to corruption than others. Regarding the types of goods, perishable goods are particularly vulnerable (Europol, 2023; GI-TOC et al., 2021, p. 42; Roks et al., 2021, pp. 182–184; EMCDDA et al., 2019, p. 7) and are used to conceal different kinds of illicit goods such as drugs, illegal waste and counterfeit products. The limited scope for inspections of these shipments creates a vulnerability that can be exploited by corrupt personnel including both public authorities and/or private actors in the seaport (e.g. customs authorities, ship agents and freight forwarders) ([32]), as they can purposefully overlook parts of a container or shipment during the check and/or refrain from reporting suspicious items ([33]). Various types of shipments can be vulnerable to corruption, with container trade being among the most frequently mentioned (EMCDDA et al., 2022, p. 24; Roks et al., 2020, pp. 182–183; GI-TOC et al., 2021, pp. 38–40). Containers are attractive for illicit activities, inter alia, due to their size, limited visibility of their contents and the high volume of their throughput ([34]). The nature of trade routes connected to a seaport also impacts the corruption vulnerabilities. Some trade routes and thus, ports of origin, pose higher risks for trafficking of illicit goods and, therefore, require a degree of insider help to have shipments of illicit goods pass through the seaport supply chain (EMCDDA et al., 2019, p. 13; EMCDDA et al., 2022).

The human factor

One of the most vulnerable characteristics of the seaport and the supply chain is the human factor, which has been noted in all case studies and high-level interviews ([35]). More generally, this vulnerability is driven by the knowledge

([32]) Interviews with private and public stakeholders, February and March 2024 (Roks et al., 2020, p. 174).
([33]) Port of Piraeus, Port of Algeciras, Port of Antwerp-Bruges, Port of Rotterdam.
([34]) The high volumes of throughput were also mentioned by one respondent of the survey as a reason why it is difficult to tackle corruption risks.
([35]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Piraeus, Port of Algeciras, Port of Cartagena, Port of Venice; interviews with private and public stakeholders, February and March 2024.

of organised crime groups (OCGs) related to the actors that play a crucial role in processing containers, conducting checks and controlling entry to and exit from the seaport (Roks et al., 2021, pp. 56–57; Sergi, 2020, p. 197; Jancsics, 2019, pp. 3–4; Roks et al., 2020, pp. 182–183; Eski et al., 2017, pp. 3–4). Zooming into the specific corruption vulnerabilities of the human factor, three aspects stand out.

First, non-automated container processing requires more human involvement, which has been observed to increase corruption vulnerabilities and opportunities for OCGs ([36]). For example, during the offloading and placement of containers, stevedores and crane operators can be approached by OCGs to assist in placing containers in favourable and accessible locations in the terminal for picking up illicit goods later on ([37]).

Second, access to critical information such as containers selected for checks or the location of containers (with illicit goods) is not permanently restricted to a limited number of employees. In some cases, different teams working in the terminal have access to this information due to working in shifts ([38]). Broad access to critical information reduces oversight and might present more corruption opportunities for OCGs, as it is more difficult to link an employee to the leaked piece of information (Sergi, 2020, pp. 16–18, pp. 197–198; Europol, 2023, pp. 17–18). Third, transporters (e.g. truck drivers, train conductors, inland shipping captains), responsible for picking up the containers from the terminal for further transport, are particularly vulnerable and are therefore usually approached and bribed by OCGs. This has been identified specifically in relation to PIN codes ([39]) used to retrieve containers with illicit goods, or to bring in extractors to the port.

Social communities around the port

The role of the social communities in and around seaports is also relevant. The communities of people working in and for the seaport generally have long-standing relationships with the port and are generally proud and protective of the related seaport ([40]).

However, close-knitted seaport communities also pose substantial challenges and vulnerabilities related to corruption. It is not uncommon in certain seaports for staff to be hired through (in)direct family ties or recommendations. The connections of the close community also pose a vulnerability to corruption in light of procurement. Here, similar dynamics as those described above are at play whereby contracts are allocated to stakeholders that are part of the seaport community, rather than through transparent procurement procedures.

In addition to these vulnerabilities, there are socioeconomic factors that render the social communities around the port vulnerable to corruption. Examples of these factors are manifold but include, for example, high unemployment rates around the port ([41]), debt-related issues ([42]), poverty (Centrum Kinderhandel en Mensenhandel et al., 2021, p. 30) and a general sentiment of low trust in the government and its actions ([43]). These elements make some members of port communities susceptible to different forms of corruption.

([36]) Port of Algeciras, Port of Piraeus.
([37]) Port of Algeciras, Port of Piraeus.
([38]) Port of Algeciras; interviews with public stakeholders, February and March 2024.
([39]) Unique PIN codes are used by shippers and freight forwarders to securely release the container for onward transport by truck drivers at the port of arrival.
([40]) As seen in all case studies.
([41]) Port of Algeciras, Port of Piraeus, Port of Venice.
([42]) Port of Rotterdam, Port of Antwerp-Bruges (Eski et al., 2017, pp. 5–6, p. 17).
([43]) Port of Rotterdam, Port of Antwerp-Bruges.

Role of politics in the seaport

Whereas the focus of the study at hand is to identify corruption vulnerabilities in the operations of the seaport supply chain, it has become apparent that in some seaports the role of politics also creates vulnerabilities. These corruption vulnerabilities seem to predominantly impact the risk of procurement-related corruption and the ambitions of the seaport being driven by political interest ([44]).

Factors hindering an effective approach to the fight against corruption in seaports

In addition to the features in the seaport that pose direct vulnerabilities related to corruption, factors that hinder an effective approach against corruption have been identified. These factors indirectly contribute to the existence and persistence of corruption vulnerabilities in the supply chain. They concern the economic climate, the type, strategic location and size of the seaport, the cooperation between public and private actors in the seaport and legislation.

Economic climate

Seaports are hubs for (international) trade and transportation, serving as vital links in the logistical chain. In the pursuit of sustaining profitability, attracting business and maintaining a competitive position in the global trade, security considerations are occasionally overlooked, with efficiency taking precedence over security measures ([45]).

Some seaports struggle to keep pace with evolving modernisation while simultaneously upholding and enhancing all necessary security measures ([46]). The combination of these factors may lead to seaports prioritising economic interests over security considerations.

Size and location of the seaport

The size and location of a seaport indirectly impact the vulnerability to corruption in various ways. Firstly, the size of the seaport was mentioned as a key challenge in some of the larger seaports studied, such as in Rotterdam and Antwerp-Bruges ([47]), as it is virtually impossible to maintain complete oversight over the entire port premises and over personnel, companies and systems ([48]), thus creating vulnerabilities related to the trafficking of illicit goods both into and outside of the seaport ([49]).

While major seaports grapple with issues such as expansive terrain, smaller seaports face different challenges that impact their vulnerability to corruption. They face resource constraints that impact their ability to actually conduct controls of the physical terrain and patrols ([50]). Additionally, smaller seaports are more likely prone to the waterbed effect resulting from larger seaports around them stepping up security measures ([51]).

([44]) Port of Cartagena, Port of Algeciras; interviews with private stakeholders, March 2024 (GI-TOC et al., 2021, pp. 56–57; Sergi, 2020, pp. 22–23).
([45]) Interviews with private and public stakeholders, February and March 2024 (GI-TOC et al., 2021, pp. 40–45; Roks et al., 2020, pp. 182–184).
([46]) Port of Piraeus.
([47]) Rotterdam encompasses 467.4 million twenty-foot equivalent units and 12.5 hectares, and Antwerp-Bruges encompasses 13.5 million twenty-foot equivalent units and 14.65 hectares.
([48]) Interviews with public and law enforcement stakeholders, February and March 2024 (Roks et al., 2020, pp. 184–185). This was also mentioned by survey respondents.
([49]) Port of Piraeus.
([50]) Port of Piraeus, Port of Antwerp-Bruges.
([51]) Port of Cartagena (GI-TOC et al., 2021, pp. 39–40).

Secondly, the volumes of throughput affect the vulnerability to corruption in seaports ([52]). Seaports that see a higher throughput generally face more complex and elaborate processes and security measures, thus increasing the need for insider help ([53]). On the other hand, seaports with less throughput generally face fewer resources dedicated to security measures in the seaport and, as a result, tend to experience more weaknesses in their seaport landscape, providing opportunities for corruption ([54]).

Type of port

The main vulnerability linked to the ownership of the seaport is the varying degrees of obligations and policies for security, integrity and transparency. In privatised seaports, economic interests might prevail as the private entities owning the seaport are, naturally, inclined to favour efficiency over security.

Moreover, in privatised seaports, the public bodies tasked with fighting crime and corruption are dependent on the private stakeholders owning the seaport to implement their tasks ([55]) (Sergi, 2020, p. 18). The law enforcement authorities therefore rely on and are guided by the port management companies. This may delay the inspection and decrease the transparency of port operations ([56]). While landlord seaports might have more (harmonised) security policies, they remain vulnerable to crime and corruption, as the actual implementation and monitoring generally falls within the responsibility of private companies ([57]). This makes it challenging to ensure consistency in anti-corruption and security measures and may lead to an overlapping of accountability for security-related activities.

Public–private cooperation

Challenges in cooperation between public and public–private actors have been observed across the case studies and high-level interviews, as each port stakeholder has a demarcated responsibility in a specific part of the chain and therefore they rely heavily on each other ([58]) (Sergi, 2020, pp. 16–18, pp. 22–23). This configuration leads to a complicated basis for effective cooperation.

The principal corruption vulnerabilities concern the lack of oversight and transparency due to limited information sharing, trust issues and conflicting interests between public actors. These loopholes and inconsistencies in public–private and public–public cooperation impact the ability of public and private actors to effectively address crime (and corruption in particular). More controls and checks have significant economic effects on companies, which often bear the costs for these checks ([59]) (Sergi, 2020, pp. 16–18, pp. 26–27), thus underscoring the delicate balance between economy and security in seaports.

([52]) The high volume of throughput is also mentioned by one survey respondent as reason why corruption is difficult to tackle.
([53]) Port of Rotterdam, Port of Antwerp-Bruges (Antonelli, 2021, p. 164).
([54]) Port of Venice.
([55]) Port of Piraeus.
([56]) Port of Piraeus.
([57]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Venice.
([58]) Interviews with public and law enforcement stakeholders, February and March 2024.
([59]) Port of Algeciras, Port of Venice.

Legislation

Regarding corruption vulnerabilities posed by suitable legislation (or the lack thereof), two elements stand out. First, the International Ship and Port Facility Security Code (ISPS Code) (Regulation (EC) No 725/2004) is repeatedly mentioned as a weak link in seaports' anti-corruption (and anti-organised crime) approach ([60]). Given that the fundamentals of the ISPS Code lie in a counterterrorism response, the risks of OCGs' infiltration are not sufficiently covered by the code. The second vulnerability identified in terms of legislation is the restrictions with regards to information sharing. Due to these restrictions, cooperation is sometimes negatively affected ([61]).

Corruption vulnerabilities in the port supply chain

The following section of this article focuses on the corruption vulnerabilities in specific steps in the seaport supply chain, as presented in Figure 13.1 above.

It is essential to reiterate here that the supply chain has been designed based on trade from non-EU countries into EU seaports and with a prime focus on container trade. Furthermore, before corruption vulnerabilities are explained for each step of the supply chain, it is important to underline that the legitimate activities taking place at each step have also been presented to provide a clear overview of the supply chain.

Step 1: Goods packed into a container at the production location

Legitimate activities

The supply chain starts when the goods to be transported are packed into a container at the production location. In this instance, the goods are physically put into the container that will be shipped. Staff employed by the exporting company are involved in this step, physically packing goods into the container.

Corruption vulnerabilities

The key corruption risks in this step concern the lack of standardised rules and protocols for packaging at the production location. OCGs therefore use the prevailing modus operandi (MO) of hiding illicit goods among high-volume shipments. Corruption is used to gain the assistance of production and warehouse personnel to add the illicit goods to the containers ([62]).

Step 2: Container transported from production location to port of departure

Legitimate activities

After loading the goods into the container, the container is transported to the seaport of departure. The container is brought to the terminal, where it will be picked up by the vessel that will transport it to the intended destination. The person or company transporting the container plays a key role in this step.

([60]) Predominantly mentioned in Port of Rotterdam and Port of Antwerp-Bruges.

([61]) Port of Piraeus, Port of Antwerp-Bruges; interviews with private and public actors, February and March 2024.

([62]) Port of Rotterdam, Port of Antwerp-Bruges; interviews with private stakeholders, March 2024 (GI-TOC et al., 2021, pp. 44–45; OCCRP, 2019); 15 respondents in the survey (n = 16) also recognised this risk. According to the survey findings, transport companies and warehouse personnel emerged as the most susceptible to corruption.

Corruption vulnerabilities

The key vulnerability in this step is the physical transport of the container from the production location to the terminal. During this transport, OCGs might bribe the driver to make additional stops to load illicit goods into the container ([63]) (GI-TOC et al., 2021, pp. 43–45; OCCRP, 2019; Stockholm International Peace Research Institute et al., 2012, pp. 35–36). It is worth noting that OCGs could also approach the container without the active involvement of the driver, when the vehicle is stationary in a car park. ([64])

Step 3: Container loaded from the terminal onto the vessel

Legitimate activities

Once the container has been transported from the production location to the terminal, it is loaded into a vessel for transport. The customs authority oversees handling the export declaration of the goods and releasing the container for departure. The terminal personnel ensure the container transfer from the terminal onto the vessel.

Corruption vulnerabilities

In this step, the terminal personnel could be bribed by OCGs to add illicit goods into the container whilst it is stored in the terminal (i.e. the so-called rip-on/rip-off method). Alternatively, they could be bribed to look the other way and let criminals add illicit goods into the containers before loading them onto the vessel ([65]). In addition, the limited screening of exported goods (container loads and ro-ro loads) provides a bigger 'window of opportunity' for illicit goods to be loaded onto the vessel.

Step 4: Vessel sails to destination

Legitimate activities

This step focuses on what occurs on sea. After the container has been loaded onto the vessel, it starts its journey to the port of destination. The main actor in this step is the vessel's crew.

Corruption vulnerabilities

The corruption vulnerabilities identified in this step concern the vessel itself and its route. First, ship personnel are vulnerable to corruption, for example, allowing the hiding of illicit goods in cabins ([66]) (GI-TOC et al., 2021, pp. 44–45). Similarly, ship personnel can allow OCGs to weld underwater constructions to a ship's hull (e.g. dispatchable torpedoes), where illicit goods can be hidden. This allows the OCGs to evade security checks at the seaport and decreases the need to bribe dock workers to extract illicit goods (GI-TOC et al., 2021, pp. 44–45).

Second, it is evident that there is a risk of OCGs influencing ship personnel to make additional stops whilst at sea or diverting the vessel from its original route ([67]). In addition, corrupt ship personnel use the drop-off method whilst at sea. In this case, a corrupt ship employee drops illicit goods into the sea, for example, a package of cocaine (as

([63]) Fifteen respondents of the survey recognised this risk ($n = 16$).
([64]) Port of Piraeus.
([65]) Port of Algeciras (GI-TOC et al., 2021, pp. 43–45); 14 respondents of the survey recognised this risk ($n = 16$).
([66]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Algeciras, Port of Venice, interviews with law enforcement agencies, February 2024.
([67]) Port of Antwerp-Bruges.

cocaine floats), which are then picked up by OCGs in smaller speedboats ([68]) (Politico, 2021). This is particularly appealing for OCGs as the vessel is rather isolated at sea, and there are no authorities on site (Europol, 2023, pp. 13–14; GI-TOC et al., 2021, pp. 42–44).

Step 5: Relevant actors in the port of arrival are notified about the expected arrival of the vessel

Legitimate activities

The port authority, customs and other relevant authorities at the seaport of arrival receive information about the container from the port of origin. Customs authorities then start to prepare the clearance procedure for the container.

Corruption vulnerabilities

The corruption vulnerabilities in this step predominantly lie with customs authorities, shippers, ship agents and freight forwarders, who are the key actors involved in the documentation of shipments, making these groups vulnerable to corruption ([69]) (Roks et al., 2020, p. 182; Jancsics, 2019, pp. 3–4; Langlois et al., 2022, pp. 296–298; GI-TOC et al., 2021, pp. 42–43; Europol, 2023, p. 10; EMCDDA et al., 2019, p. 7) as they are responsible for sending the entry summary declaration (ENS) to the customs authorities at the seaport of arrival. There is a risk of OCGs bribing these private actors to falsify the ENS to import illicit goods.

Step 6: Vessel arrives at quay

Legitimate activities

In this step, the vessel arrives at the quay of the terminal. The container is now on the vessel at the quay of the seaport of arrival, waiting to be placed in the terminal.

Corruption vulnerabilities

Vulnerability to corruption involves the personnel overseeing or managing the vessels waiting at the quay, as OCGs could bribe them to turn a blind eye to other bribed personnel extracting illicit goods from the vessel ([70]) (Roks et al., 2020, p. 182; Jancsics, 2019, pp. 3–4).

Moreover, the drop-off of packages of drugs by corrupt ship personnel ([71]) into the water or in smaller speedboats, picked up by divers recruited by OCGs, is a prevalent MO also at this step ([72]) (GI-TOC et al., 2021, pp. 44–45).

([68]) Port of Piraeus, Port of Algeciras, Port of Venice; 14 respondents of the survey recognised this risk ($n = 16$).
([69]) Port of Piraeus, Port of Antwerp-Bruges, Port of Rotterdam, Port of Algeciras, Port of Venice. Findings from the survey: customs authorities in particular were perceived as vulnerable to corruption by the survey respondents (9 out of 14).
([70]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Piraeus, Port of Algeciras, Port of Venice; 13 respondents of the survey recognised this risk ($n = 15$).
([71]) Often the same ship personnel that has already been corrupted at the port of origin.
([72]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Piraeus, Port of Algeciras, Port of Venice; interviews with law enforcement agencies, February 2024.

Step 7: Terminal operator unloads the vessel and parks the container at the terminal

Legitimate activities

Once the vessel is moored at the terminal, the terminal operators unload the containers and place them in the terminal. The goods are then assigned to a specific customs procedure, depending on where the containers are coming from (intra-EU or non-EU country) (European Commission: Directorate-General for Trade and Economic Security, 2026).

Corruption vulnerabilities

The corruption vulnerabilities linked to the human factor seem rather critical at this step, as observed across the case studies and high-level interviews ([73]). Subcontracting and independent and occasional workers render terminal personnel an increasingly vulnerable group due to difficulties in screening them. Additionally, the monetary compensation offered by OCGs is very high (ranging from EUR 25 000–200 000) ([74]). This increases the attractiveness of engaging in corruption for terminal personnel.

Influencing terminal personnel in order to extract illicit goods from the containers is therefore attractive for OCGs. OCGs use forms of corruption with few widely known MOs, such as the rip-on/rip-off method, Trojan Horse containers and hotel containers ([75]). Notably, limited port surveillance grants potential access to OCGs to illicit goods prior to customs inspections.

Step 8: Customs checks paperwork and decide based on the risk management system which containers to select for checks

Legitimate activities

In this step, the container is parked in the terminal and is waiting for customs clearance. The customs authority check the necessary documents and decide whether to release the container to the transport company.

In addition, the customs authority uses a risk management system to determine which containers to check. If the container is selected for a check, it can be either moved to a customs inspection area or checked on the spot by authorities.

Corruption vulnerabilities

Corruption vulnerabilities in this step are mainly linked to customs authorities and other actors conducting checks in the seaport. Authorities might be bribed to 'turn a blind eye' if they spot suspicious activity or illicit goods. Additionally, customs officers sometimes have discretion over which containers to physically check due to shortages

([73]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Piraeus, Port of Algeciras, Port of Venice; interviews with private and public stakeholders, February and March 2024.
([74]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Piraeus.
([75]) Port of Rotterdam, Port of Antwerp-Bruges; interviews with public and law enforcement stakeholders, February and March 2024.

in personnel and time restrictions. This coupled with the lack of adherence to the four-eye principle and rotation of customs officers, contributes to the corruption vulnerabilities ([76]).

Second, customs authorities can also be bribed to select containers other than the containers containing illicit goods for checks or to speed up the processing of the container to avoid physical checks ([77]) (OCCRP, 2019). In some cases, the notification period of selecting a container for checks is relatively long, which allows corrupt employees to notify OCGs to extract the illicit goods before the checks are conducted (through the rip-on/rip-off method or the switch method) ([78]) (Jancsics, 2019, pp. 3–4).

Step 9: Container is loaded onto onwards transport towards importer/destination

Legitimate activities

The container is released to the transport company. The freight forwarder usually organises the transport of the container.

Corruption vulnerabilities

Regarding the transport of the container, the main vulnerabilities identified lie in road transport, non-automated access to the terminal and the lack of monitoring of railway systems. Authorities are not allowed to check the driver's cabin, which makes it harder to catch OCGs transporting illicit goods.

In addition, the use of PIN codes is often subject to fraud. This allows the OCGs to retrieve the container with illicit goods from the terminal either themselves or with the help of a bribed transporter ([79]) (Europol, 2023).

Step 10: Arrival at the importer/destination

Legitimate activities

After the transport company has picked up the container, it is transported to the importer. The importer then usually organises the unloading of the container at the final destination.

Corruption vulnerabilities

The main corruption vulnerability in this step concerns the importer and the warehouse personnel who may have been bribed or recruited by OCGs to add or remove illicit goods from the container.

([76]) Port of Antwerp-Bruges, Port of Rotterdam, Port of Venice. Respondents of the survey recognised this risk (n = 15).
([77]) Port of Rotterdam, Port of Antwerp-Bruges; interviews with private stakeholders, February and March 2024.
([78]) Port of Antwerp-Bruges, Port of Rotterdam, Port of Venice; interviews with public stakeholders, February and March 2024.
([79]) Port of Rotterdam, Port of Antwerp-Bruges; interviews with public and private sectors, February and March 2024.

Conclusion

Combining the findings across the different seaports studied, the insights gathered from beyond those case study seaports and the overarching desk research and interviews provides an overview of a variety of corruption vulnerabilities.

The identified vulnerabilities in seaports are directly linked to the supply chain, but also to more structural, indirect elements in and around the seaport that increase the vulnerability to corruption or, in turn, hinder an effective approach to corruption. Furthermore, this article has shown that there is a wide range of different seaports in the EU, with different features, facing different types of challenges.

One of the key conclusions from the article is that the vulnerabilities related to corruption in the seaport supply chain are manifold, but are only one piece of the puzzle. The vulnerabilities in the supply chain predominantly pertain to the involvement of personnel, loopholes in (legal) processes and systems, and lack of oversight.

Compared with corruption-related vulnerabilities in the supply chain, the underlying and more structural elements and features in and around seaports that create vulnerabilities for corruption are generally more difficult to address, but risk being more impactful. These vulnerabilities are the consequence of more transversal issues such as the degree of human involvement in the seaport, the degree of digitalisation, the type and origin of the cargo and throughput, the role and composition of social communities around the seaport and the role of politics in the seaport. These elements are not directly linked *per se* to specific steps of the seaport supply chain but instead affect multiple steps across the supply chain.

These difficulties are further intensified by a series of factors hindering an effective and efficient approach to corruption in seaports. Such factors include, among others, the size and location of the seaports, the prioritisation of efficiency over security, the ownership of seaports, cooperation between public authorities in the seaport, the degree of collaboration between public and private bodies, and legislation. While these factors do not directly translate into vulnerabilities to corruption in the seaport supply chain, they do affect the ability of addressing corruption in the seaport effectively.

These findings provide useful food for thought for the law enforcement community as it strives to respond effectively to the ever-growing phenomenon of corruption and infiltration of organised crime within European ports.

Overall, it has become evident that an all-encompassing set of corruption vulnerabilities applicable to all seaports across the EU is non-existent. Specific vulnerabilities, and their intensity and operational details, differ substantially between seaports. Taking this into account, four key findings must guide the efforts in addressing the vulnerabilities to corruption in EU seaports when moving ahead.

First, tailored approaches to address the vulnerabilities in the various seaports are required, as a generic strategy would overlook the specificities of the needs in seaports, such as the level of digitalisation, human involvement, the political priorities and available resources. Strategies to address corruption vulnerabilities in seaports must take these specificities into account and design tailor-made measures. Second, the vulnerabilities related to corruption

in seaports must not be addressed from the perspective of a single seaport or only at the national level. Instead, seaports should be understood as a broader group of logistical hubs across the EU. Indeed, an EU-wide approach and EU-level investments in port security would have to be adopted to ensure an equal level playing field, and thus an equal minimum level of resilience across the EU and single market. This rationale could be extended beyond EU seaports in the future to also include non-EU seaports.

Third, an effective approach to combating corruption in seaports would not only include repressive measures focused on specific operational vulnerabilities in the seaport supply chain, but would also address the more structural challenges present in and around seaports. In this sense, it could be beneficial to dedicate resources to prevention strategies.

Fourth, an update of the ISPS Code would allow more effective oversight of the implementation of appropriate security measures in the seaport ([80]). Such an update would be most effective to avoid a waterbed effect whereby OCGs shift activities to ports with less strict legislation.

These key findings and suggestions for a way forward shall be considered in the identification and selection of practices that aim to tackle corruption in EU seaports, and in the definition of recommendations for the establishment of an EU port supply chain integrity standard.

References

Antonelli, M. (2021), 'An exploration of organized crime in Italian ports from an institutional perspective – Presence and activities', *Trends in Organized Crime*, Vol. 24, pp. 152–170, https://doi.org/10.1007/s12117-020-09400-z.

Centrum Kinderhandel en Mensenhandel, Leito, T. L. M., van Bemmel, S. R. and Noteboom, F. (2021), *Het misdrijf voorbij – Een verkenning naar criminele uitbuiting in Rotterdam*, Capelle aan den IJssel, https://www.hetckm.nl/wp-content/uploads/2023/03/CKM-Rapport-2021-Het-misdrijf-voorbij.pdf.

EMCDDA and Saggers, T. (2019), 'An assessment of the extent of Albanian(-speaking) organised crime groups involved in drug supply in the European Union: characteristics, role and the level of influence', https://www.euda.europa.eu/system/files/attachments/12102/EDMR2019_BackgroundReport_Albania nSpeakingOCGs.pdf.

EMCDDA and Europol (European Union Agency for Law Enforcement Cooperation) (2022), EU Drug Market: Cocaine, https://www.euda.europa.eu/publications/eu-drug-markets/cocaine_en.

Eski, Y. and Buijt, R. (2017), 'Dockers in drugs: Policing the illegal drug trade and port employee corruption in the Port of Rotterdam', Policing: A Journal of Policy and Practice, Vol. 11, Issue 4, pp. 371–386, https://doi.org/10.1093/police/paw044.

([80]) It should be noted that Belgium EMCDDA (European Monitoring Centre for Drugs and Drug Addiction) introduced a new maritime security law on 1 January 2023 (*Wet tot wijziging van het Belgisch Scheepvaartwetboek betreffende de maritieme beveiliging*, Belgian Official Gazette, 26 October 2022), which lays down stricter measures than the ISPS Code.

European Commission: Directorate-General for Trade and Economic Security (2025), 'Customs clearance documents and procedures', Access2Markets website, https://trade.ec.europa.eu/access-to-markets/en/content/customs-clearance-documents-and-procedures.

European Parliament and Council of the European Union, Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6, ELI: http://data.europa.eu/eli/reg/2004/725/oj.

European Parliament: Directorate-General for Parliamentary Research Services, Bąkowski, P. and Voronova, S. (2017), *Corruption in the European Union – Prevalence of corruption, and anti-corruption efforts in selected EU Member States – In-depth analysis*, European Parliament, https://data.europa.eu/doi/10.2861/071091.

Europol (2023), 'Criminal networks in EU ports – Risks and challenges for law enforcement', https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Joint.

Europol (2021), European Union Serious and Organised Crime Threat Assessment – A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf.

GI-TOC (Global Initiative Against Organized Crime), InSight Crime, McDermott, J., Bargent, J., and den Held, D. (2021),, *The Cocaine Pipeline to Europe*, GI-TOC, Geneva, https://globalinitiative.net/wp-content/uploads/2021/02/The-cocaine-pipeline-to-Europe-GI-TOCInsightCrime.pdf.

Jancsics, D. (2019), 'Border Corruption', *Public Integrity*, Vol. 21, Issue 4, pp. 406–419, https://doi.org/10.1080/10999922.2019.1581043.

Langlois, F., Rhumorbarbe, D., Werner, D., Florquin, N., Caneppele, S. et al. (2022), 'International weapons trafficking from the United States of America: A crime script analysis of the means of transportation', *Global Crime*, Vol. 23, Issue 3, pp. 284–305, https://doi.org/10.1080/17440572.2022.2067847.

OCCRP (Organized Crime and Corruption Reporting Project) (2019), 'Albanian drug suspect's banana bonanza', OCCRP website, 16 December 2019, https://www.occrp.org/en/investigation/albanian-drug-suspects-banana-bonanza.

Poseidon, Saarijärvi, J., Helemons, S., op t' Hoog, G., Steensma, J. et al. (2024), 'Study on corruption vulnerabilities in the EU seaports supply chain', https://poseidon.safe-europe.eu/wp-content/uploads/2024/10/POSEIDON_Study-on-corruption- vulnerabilities-in-the-EU-seaports-supply-chain.pdf.

Poseidon (2023), 'POSEIDON – POrtS unitED Against corruption', Poseidon website, https://poseidon.safe-europe.eu/.

Roks, R., Bisschop, L. and Staring, R. (2021), 'Getting a foot in the door – Spaces of cocaine trafficking in the Port of Rotterdam', *Trends In Organized Crime*, Vol. 24, pp. 171–188, https://doi.org/10.1007/s12117-020-09394-8.

Sergi, A. (2020), *The Port-Crime Interface: A report on organised crime and corruption in seaports*, University of Essex, London, https://repository.essex.ac.uk/30303/1/EBOOK_PORT_CRIME.pdf.

Stockholm International Peace Research Institute, Griffiths, H. and Jenks, M. (2012), *Maritime Transport and Destabilizing Commodity Flows*, Stockholm, https://www.sipri.org/sites/default/files/files/PP/SIPRIPP32.pdf.

Too secure to fail? Anti-corruption policies in the Port of Antwerp-Bruges

Halima Guelai

https://doi.org/10.3013/wekgfz19

Abstract

In response to an increase in cocaine seizures and drug-related violence and growing evidence of corruption in Belgium, policymakers have strengthened maritime security measures in the Port of Antwerp-Bruges to address organised drug crime. However, corruption is not merely an enabler of such crime, but a phenomenon embedded within it.

This article draws on a 2013 assessment of the port, a literature review and 23 expert interviews. It explores current anti-corruption efforts in the port over the past decade through five key pillars: clearly defined roles within multidisciplinary collaboration, political support, evidence-based policymaking, a long-term focus and the flexibility to address emerging threats. The analysis highlights the motivations, objectives and challenges of involved actors, with particular attention to recent policy shifts.

Despite growing awareness, current measures remain largely focused on visible deterrence such as screening, port bans or technological tools, while overlooking the social, administrative and political dimensions of corruption. Addressing corruption requires moving beyond fragmented, short-term responses towards an integrity-based strategy that engages both public and private actors willing and able to drive organisational change. Pursuing the total eradication of corruption would be overambitious and risks undermining efficiency. Instead, progress should rest on shared responsibility, trust and sustained monitoring to prevent integrity fatigue. Belgium's advocacy for expanding the International Ship and Port Facility Security Code and the establishment of a national drugs agency offer opportunities for a more integrated approach.

Keywords: corruption, organised drug crime, Port of Antwerp-Bruges, maritime security, integrity.

1. Introduction

Corruption embedded in the Port of Antwerp-Bruges

At the national level, corruption is defined in the Belgian Criminal Code as active and passive bribery of public officials under Articles 246 to 252. These provisions cover the solicitation, acceptance and offering of undue advantages. Articles 504-bis and 504-ter extend criminal liability to active and passive bribery in the private sector ([81]). However, corruption extends beyond these legal definitions, existing on a continuum of unethical behaviour, ranging from intimidation, extortion, nepotism, embezzlement, abuse of functions and obstruction of justice. Multiple stakeholders including officials, politicians, lobbyists, private sector actors and citizens partake in such behaviours, making a unified definition challenging (European Commission, 2023). Meanwhile, Belgium has ratified several international treaties to address corruption, including the Organisation for Economic Co-operation and Development (OECD) Anti-Bribery Convention (1997), the Council of Europe's Criminal and Civil Law Conventions on Corruption (1999) and the UN Convention Against Corruption (2003). More recently, the 2024 EU directive on combating corruption aims to harmonise gaps in European anti-corruption measures by setting minimum standards for defining, punishing and preventing corruption, alongside guidelines for more effective investigations and prosecutions (European Council, 2024; European Parliament et al., 2024a).

The broader reality of corruption extends beyond legal definitions and is especially apparent in strategic locations such as the Port of Antwerp-Bruges. Since its merger in 2022, the port has grown in size, economic activity and throughput. In 2023, the port handled 271 million tonnes of maritime traffic, an increase of 100 million tonnes compared with 2013 (Cools et al., 2013; Garyfallidou, 2024; Port of Antwerp-Bruges, 2024). This growth, combined with its strategic location and rising global cocaine production ([82]), made Antwerp-Bruges a gateway for illicit activities such as drug trafficking (De Middeleer et al., 2017; Colman, 2018; Verodova et al., 2023; Garyfallidou, 2024; Zürcher et al., 2024; Paoli et al., 2025). Containers are particularly attractive for drug traffickers due to their volume, the nature of goods transported, the limited visibility of contents and their high turnover (Staring et al., 2021; Zürcher et al., 2024).

Since 2004, the port has complied with the International Ship and Port Facility Security (ISPS) Code, by implementing fencing, cameras, scanners and port facility security officers (PFSOs) responsible for security planning (Cools et al., 2013; Nelen et al., 2021; Port of Antwerp-Bruges, 2024). However, as the ISPS Code excludes inland ports, this creates a potential displacement effect to less regulated areas (Staring et al., 2021). In response, the Belgian Maritime Security Act of 2023 introduced technological and physical security measures for inland navigation, reflecting a political will to close security gaps (Team Justitie, 2024; Struys, 2024; De Wever, 2025). While these measures reduce opportunities for offenders, strengthen seaport security and enhance surveillance (Staring et al., 2021), they do not address the fragmentation of global port security standards. A more effective response would be to expand the ISPS Code itself, thereby strengthening the fight against organised crime. Although Belgium advocates this expansion (De Wever, 2025), the absence of reliable, evidence-based data makes it difficult to assess the necessity and likely effectiveness of these enhanced security standards.

([81]) Loi du 10 février 1999 relative à la répression de la corruption, Moniteur Belge, 10 février 1999.

([82]) Cocaine is the most prominent drug imported through the Port of Antwerp-Bruges, which is known as one of the gateways for cocaine into Europe (De Middeleer et al., 2017; Colman, 2018; Verodova et al., 2023; Garyfallidou, 2024; Zürcher et al., 2024; Paoli et al., 2025).

Although pioneering research identified barriers to a fully integrated approach to port security, the impact of corruption was often overlooked (Cools et al., 2013). For years, it was not considered a priority in combating illicit smuggling (Staring et al., 2021; Staring et al., 2023). However, as port security tightened, organised crime groups (OCGs) sought to bypass controls by gaining access to individuals or information systems (Depuydt et al., 2020; Staring et al., 2021; Nelen et al., 2021; Staring et al., 2023; Zürcher et al., 2024; Europol, 2025). The 2021 Sky ECC investigation exposed how OCGs used encrypted messaging to approach port insiders, such as dockworkers, transport operators, prosecutors and those working in law enforcement or customs (Federale Politie, 2021; Paoli et al., 2025). These so-called 'screen readers' have access to confidential data, such as national registers, licence plates, container locations or logistics data, making them vulnerable to corruption (Struys, 2024). Bribery has since become a key enabler for infiltrating ports and logistics chains, allowing OCGs to conceal illicit goods (Europol, 2023a; Verodova et al., 2023; Zürcher et al., 2024).

Too many hands, too little power?

The 2002 Ministerial Directive ([83]), assigns the Federal Police a leading role in investigating corruption. Within its structure, the Office Central pour la Répression de la Corruption (OCRC), established in 1998, is also mandated to address corruption. Although their resources have improved in recent years, its workforce has diminished from 120 in 2000 to just 66 in 2024 (Openbaar Ministerie, 2022; European Commission, 2024a; Federale Politie, 2024b). As a result, the unit remains largely reactive, relying on complaints or media reports to initiate corruption investigations (GRECO, 2020). Meanwhile, the Federal Maritime Police support corruption investigations through first-line assessments in the port, while also focusing on border control, illegal immigration, drug trafficking, environmental crimes, theft and terrorism. Despite their expertise, the growing workload and limited capacity hinder proactive and preventive measures, creating gaps that OCGs may exploit (Cools et al., 2013; Eski et al., 2020). Respondents voiced frustration over the Federal Police's limited capacity, especially when compared with the resources of the local police. The 181 local police zones maintain disparate integrity policies and smaller police zones are not maintaining an effective integrity policy (European Commission, 2025). Key recommendations such as a code of conduct for the entire police force proposed by the Group of States against Corruption (GRECO), have not been implemented, and overall, police integrity policies are still assessed as insufficient (European Commission, 2025). This fragmentation and lack of coordination within Belgian law enforcement have created opportunities for OCGs to expand their operations (Verodova et al., 2023).

Customs assists the Federal Police by conducting risk analyses based on the entry summary declaration ([84]) and the bill of lading ([85]) to identify suspicious high-risk shipments for inspection. If illicit activities are detected, the Federal Police take over to investigate the individuals or OCGs involved (Colman, 2018).

Judiciary actors are responsible for prosecuting corruption, with a federal prosecutor investigating corruption cases referred by the European Anti-Fraud Office (Openbaar Ministerie, 2022). However, following the merger of the ports, the port is located in three municipalities: East Flanders, West Flanders and Antwerp (Garyfallidou, 2024; Port of Antwerp-Bruges, 2024). This division poses challenges for legal proceedings, requiring coordination across different

([83]) Directive relative à la répartition des tâches, à la coopération, à la coordination et à l'intégration entre la police locale et la police fédérale en matière de missions de police judiciaire, Moniteur Belge, 1 mars 2002.

([84]) The entry summary declaration must be submitted for all goods on board a vessel entering the EU. Customs require this declaration to know the contents of the vessel (Colman, 2018).

([85]) A bill of lading serves as a document of title, a receipt for shipped goods and a contract between a carrier and a shipper (Colman, 2018).

prosecutorial priorities, and legal interpretations (see below). Nevertheless, the College of Prosecutors-General's network on corruption aims to overcome these barriers by facilitating information sharing among prosecutors (Openbaar Ministerie, 2023).

I still have the impression that public actors believe they can address corruption alone and view us as the enemy.
Port authority

Port authorities also play a key role in maintaining security and protecting the port's reputation (Cools et al., 2013). They serve as a node in the information chain, sharing intelligence with port companies, which are in turn encouraged to report suspicious activity to law enforcement, helping to identify OCGs operating in the port (see below). However, addressing corruption requires trust and the willingness to share information between public and private actors, along with legal frameworks and clear communication channels. Only through collective action can the private sector contribute to the systematic changes needed in the port environment (Depuydt et al., 2020; Torbrand, 2022; De Wever, 2025).

This article focuses on the role of corruption in relation to organised drug crime in the Port of Antwerp-Bruges. Corruption is a cross-border phenomenon with social and environmental implications, undermining economic growth and swiftly adapting to new opportunities (Torbrand, 2022; Verodova et al., 2023; European Commission, 2024a; Europol, 2025). Respondents indicate that OCGs continue to exploit vulnerabilities within the port supply chain (see below), prompting policymakers to call for immediate interventions. In addition, the 2024 Eurobarometer revealed that 66 % of 1 047 Belgian citizens consider corruption within government institutions is widespread, a 4 % increase from the previous year (European Commission, 2024b). The 2025 Special Eurobarometer on Corruption shows that 59 % of 1 006 respondents consider corruption widespread in Belgium (European Commission, 2025). Such perceptions erode public trust in governance and law enforcement (Europol, 2025). Therefore, public perceptions, political pressure and economic factors have shaped the evolving concept of corruption, which now drives proposals for international cooperation (Janssens and De Vos, 2019; European Commission, 2023). According to Transparency International, effective anti-corruption strategies rest on five key pillars: clearly defined roles within multidisciplinary collaboration, political support, evidence-based policymaking, a long-term focus and the flexibility to address emerging threats (Torbrand, 2022; Jenkins and Camacho, 2022). Following a brief explanation of the methodology, the main findings are presented chronologically according to the legislative periods during which anti-corruption measures were introduced or implemented in the Port of Antwerp-Bruges since 2013. Emphasis is placed on recent developments between 2019 and 2024, a period during which corruption (re)gained policy attention. Each measure is assessed in terms of its alignment with the five pillars. A concluding discussion draws together key sociological and criminological considerations.

2. Methodology

This research draws on data collected as part of the Poseidon (ports united against corruption) project, funded by the EU's Internal Security Fund. The project aims to enhance anti-corruption measures within EU seaports ([86]).

([86]) Between March 2023 and March 2025, the project assessed corruption vulnerabilities and identified good practices in the ports of Rotterdam, Antwerp-Bruges, Algeciras, Cartagena, Venice and Piraeus. It also established an EU network of public–private port stakeholders to improve communication and information exchange in the port sector.

Data collection

Between October 2023 and February 2024, the author conducted 23 in-depth expert interviews (see Annex 14.1). A semi-structured questionnaire guided the interviews, focusing on motivations, objectives and the challenges faced in implementing anti-corruption measures. Respondents were selected based on their involvement in anti-corruption efforts in the Port of Antwerp-Bruges, with additional participants identified through snowball sampling. The interviews were voluntary, lasted one to two hours and were conducted either online or in person. All participants were informed about the study, gave written consent and had the option to decline specific questions or withdraw at any time. Some individuals declined to participate due to concerns about reputational damage or prior negative experiences with similar research. In parallel, a scoping literature review was conducted, covering the period from 2013 to 2025. This review included both academic and grey literature, such as peer-reviewed articles, research reports, news media, policy papers and internal documents provided by respondents. Emphasis was placed on sources that capture the national context of anti-corruption efforts in the Port of Antwerp-Bruges. Relevant publications were identified using databases such as Google Scholar and the Web of Science, applying Boolean search strategies with keywords including 'corruption', 'seaports', 'integrity', 'organised crime', across both Dutch- and English-language publications.

Data management and analysis

The recorded interviews were transcribed and anonymised to ensure participant confidentiality. To ensure data reliability, certain quotes were adjusted for clarity while preserving their original meaning. The data were manually coded and analysed to identify recurring themes, without the use of digital software tools.

Limitations

This article is primarily exploratory and descriptive, which may limit its depth. Given the researcher's background in criminological science, the analysis is grounded mainly in sociological and criminological perspectives. The insights obtained from experts may also be influenced by their familiarity with the sector. Moreover, the voluntary nature of their participation may have limited diversity of perspectives, as those with negative experiences may not participate. Finally, the focus on recent policy priorities may have shaped public perceptions of corruption.

3. Drugs and corruption: implications for port security

2010–2014: caught between reluctance and inability

In 2013, the Port of Antwerp recorded five tonnes of cocaine seizures, an amount comparable to the drug seizures at the Port of Rotterdam in 2017 (Colman, 2018; Depuydt et al., 2020) ([87]). However, a lack of political will and insufficient resources hindered efforts to address corruption, fraud and financial crime. The growing focus on counterterrorism often led to investigations not being opened or to corruption cases expiring (OECD, 2013; European Commission, 2014; Openbaar Ministerie, 2015). As a result, national security plans ([88]) no longer prioritised these types of crime. Additionally, the absence of disciplinary measures in public services and a whistleblower protection system continued to hinder progress in corruption cases (Maesschalck, 2012). These shortcomings ultimately led to Belgium being criticised by the OECD in 2013 for its passive approach to cross-border corruption (OECD, 2013).

([87]) Seizure figures do not reflect the total volume of imported drugs, as the true figures are dark numbers. Although rising seizures may suggest increased enforcement or a more serious problem, they do not necessarily indicate a growth in drug trafficking (Staring et al., 2023).

([88]) The national security plan (*Nationaal Veiligheidsplan*) and the integrated security framework (*Kadernota Integrale Veiligheid*).

2014–2019: the limits of an unfinished fight

Cocaine seizures at the Port of Antwerp increased tenfold, reaching 60 tonnes in 2019, alongside a rise in drug-related violence (Colman, 2018; Staring et al., 2021) ([89]). This increase in seizures was driven by strengthened collaborations between Dutch and Belgian OCGs, who expanded their influence in the ports of Antwerp and Zeebrugge (Colman, 2018; InSight Crime, 2020). In 2018, the Belgian federal government introduced a local plan (*Stroomplan*) to address drug trafficking in the Port of Antwerp, through multidisciplinary collaboration among 60 partners, including law enforcement agencies, customs agencies, prosecutors, port authorities, inspection services and government agencies (Colman, 2018; Easton, 2018). The plan focused on four areas: (1) creating barriers within the port, (2) targeting OCGs and the underground economy, (3) enhancing investigations into organised crime and (4) developing anti-corruption policies within public services (Colman, 2018). A joint taskforce (KALI) was set up, with the Belgian Federal Police taking a more proactive role and reintroducing intelligence-led policing, a concept first introduced in 2007 to address shortcomings in information-driven policing. By collaborating with the involved partners, they sought to improve the understanding of corruption related to the financial flows of OCGs (Easton, 2018; Colman, 2018; Geens and Jambon, 2019). Additionally, the local police enhanced information-sharing within the port through a neighbourhood information network, raising awareness about suspicious activities among port companies and enabling targeted police actions (Eski et al., 2020). While this approach encouraged proactive information exchange, it largely remained reactive, focusing on targeted police interventions. Through memorandums of understanding and operational action plans with Latin American countries, information sharing was strengthened (Colman, 2018; InSight Crime, 2020). Despite these efforts, understaffing at the OCRC continue to impede corruption investigations (GRECO, 2020; Openbaar Ministerie, 2021; Federale Politie, 2024b). Moreover, sharing information between public and private actors is not always desirable or feasible without breaching confidentiality. A regulatory framework is needed to enable multidisciplinary cooperation. Respondents voiced criticism by questioning whether policymakers had overlooked this when announcing the *Stroomplan* and its measures.

> *There is a strong desire for immediate statements, but given the scale of the problem, patience is crucial.*
>
> Port company

The measures, including scanning equipment, automatic number plate recognition cameras, smart seals, fines for avoiding scans and awareness campaigns for drug extractors are primarily repressive, targeting the supply side rather than addressing the root causes of drug trafficking (Colman, 2018). Although necessary, integrity measures for the involved partners were perceived to slow logistics, and alongside high workloads and societal and political pressure, contributed to the ending of the development of an anti-corruption policy in 2019 (Atillah, 2020; InSight Crime, 2020). The evaluation of the *Stroomplan* called for a systematic, well-monitored approach to organised drug crime, one that ensures a chain-oriented strategy with both policy and operational capacity, while promoting information sharing (Colman, 2018; InSight Crime, 2020). While the *Stroomplan* takes several steps in the right direction with political support and establishing a multidisciplinary collaboration, policymakers should reconsider the focus on visible, reactive measures targeting the drug market, as they may undermine long-term impact.

([89]) Given the dark number, these quantities likely represent only a portion of the overall drug supply (Staring et al., 2021).

2019–2024: increased efforts, persistent gaps

Cocaine seizures in Belgian ports continued to increase, reaching a record of 121 tonnes in 2023 (Verodova et al., 2023; Federale Politie, 2024a). The COVID-19 pandemic did not disrupt this trade; instead, seizures increased as maritime shipping remained unaffected, allowing OCGs to continue trafficking (Depuydt et al., 2020). Furthermore, OCGs use visible violence, such as explosions and arson, or invisible violence, including threats, torture and kidnappings targeting law enforcement, journalists and bystanders (Verodova et al., 2023; Paoli et al., 2025). This violence ensures that corrupt actors remain compliant, but it also contributes to growing public unrest (Verodova et al., 2023; Zürcher et al., 2024; Europol, 2025; Paoli et al., 2025). The violence peaked with the tragic death of an 11-year-old girl in 2023, leading to, among other measures, stricter screening of dockworkers. In Belgium, port work is regulated and restricted to recognised dockworkers ([90]), who, according to respondents, are currently only required to present a certificate of good conduct. In some cases, family ties and friendships have formed the basis for access to the port. However, economic growth has increased reliance on temporary labour, which raises security concerns (Eski et al., 2020; Staring et al., 2021; Staring et al., 2023). Unlike dockworkers, occasional workers are not covered by the law and therefore are not subject to the same level of monitoring, making them vulnerable to criminal infiltration (Depuydt et al., 2020; Eski et al., 2020; Zürcher et al., 2024). Given that Sky ECC confirms nearly all port positions are vulnerable to such infiltration (see above), the Maritime Security Act now requires security clearance or advice for both public and private employees in high-risk port positions to access confidential information (Daems, 2021; Kir, 2023; Team Justitie, 2024; De Wever, 2025). These security verifications are conducted by the Federal Police, the State Security Service and the General Intelligence and Security Service (Federale Politie, 2024a). Although periodic screening enjoys political support, respondents argue that it once again lacks the long-term vision and flexibility needed to address threats across all 162 000 direct and indirect port positions. Moreover, increased scrutiny may heighten pressure on screened individuals, making them more susceptible to corruption or displace OCGs to less regulated areas. To mitigate this, information on screened individuals and database access must be shared with EU Member States (De Wever, 2025). Meanwhile, the Federal Police face ongoing resource shortages that hinder their core responsibilities, while structural vulnerabilities, such as reliance on temporary labour, negative media portrayals of port work and difficult working conditions that hinder recruitment, remain unaddressed.

> *Reliance on occasional workers is a risk: they may be a financial stopgap, but they know their way around the port very well.*
>
> Labour union

Respondents emphasised that technological measures could enhance compliance and integrity systems, improve coordination and increase transparency. By preventing unauthorised access to port areas and limiting leaks of sensitive information about port operations, these measures contribute to a more secure and efficient port environment. To address PIN code fraud ([91]), Antwerp, Rotterdam and Hamburg/Bremerhaven container terminals implemented Certified Pick up (CPu), a blockchain-based platform integrating identity verification, authorisation and customs approval to strengthen access control (Port of Antwerp-Bruges, 2024; Europol, 2023b). Previously, PIN codes were not tied to specific individuals and were often shared with OCGs (Europol, 2023b). With CPu, access to

([90]) Arrête royal du 5 juillet 2004 relatif à la reconnaissance des ouvriers portuaires dans les zones portuaires tombant dans le champ d'application de la loi du 8 juin 1972 organisant le travail portuaire, Moniteur Belge, 4 août 2004.

([91]) PIN codes are used by shippers and freight forwarders to release the container for onward transport by transport operators at the port of arrival (Europol, 2023b).

confidential information is now more restricted (Port of Antwerp-Bruges, 2024). However, this might shift corruption vulnerabilities to other professions with access to digital systems, such as transport operators, IT companies or customs authorities, who could face increased pressure to manipulate container checks or expedite approvals (European Commission, 2024a; Staring et al., 2023; Zürcher et al., 2024; Europol, 2025). CPu should be implemented nationwide and extended beyond container traffic to prevent displacement effects. Additionally, ongoing investment in digital infrastructure is needed to prevent outdated systems from being exploited by OCGs. Without adequate cybersecurity, these systems remain vulnerable to misuse. Furthermore, digital systems should be part of a broader anti-corruption strategy and supported by an organisational change for lasting impact.

OCGs find new ways to exploit digital systems because they can still corrupt people. While technology plays a crucial role, human psychology remains the key factor in prevention.
Law enforcement official

While technological security measures evolve in the port, they alone cannot prevent corruption without integrity policies that promote reporting and awareness (Easton, 2018; Eski et al., 2020). Eurobarometer data shows that 1 047 Belgian citizens are less willing to report corruption due to challenges in providing evidence (55 %), not knowing where to report (36 %), fear that reporting is futile (31 %), reluctance to betray others (28 %) and a lack of protection for whistleblowers (25 %) (European Commission, 2024b; Zürcher et al., 2024). By the end of December 2022 ([92]), anonymous external reporting platforms for government bodies and law enforcement agencies were introduced under the 2019 Whistleblower Protection Directive ([93]), offering legal safeguards against retaliation. PortWatch was launched to extend these protections to the maritime sector, streamlining existing reporting channels in Belgian ports and strengthening law enforcement investigations into corruption (Port of Antwerp-Bruges, 2024; Team Justitie, 2024). Meanwhile, on an international level, the Maritime Anti-Corruption Network (MACN) facilitates anonymous reporting through the Global Port Integrity Platform. The platform provides port integrity risk scorecards to identify corruption risks and support collective action (MACN, 2023). Future evaluations by the Federal Police are needed to assess whether PortWatch improves information flow and supports a systematic evidence-based anti-corruption approach.

These efforts must be regularly updated and monitored to remain relevant, as the lack of reporting creates a knowledge gap.
Law enforcement official

Meanwhile public–private campaigns like 'our port drug-free' empower port employees to recognise threats, resist coercion and report suspicious activities, thereby strengthening their resilience against criminal infiltration (Cepa and Alfaport Voka, 2024; Port of Antwerp-Bruges, 2024). Respondents emphasised that expanding these efforts to logistics students, management and operational staff promotes a culture of integrity within the broader port community. However, Transparency International warns that highlighting the prevalence or immorality of corruption can backfire, normalising it as an inevitable part of the system, instead of changing behaviour (Ishikawa, 2024; Europol, 2025). A victim-centred approach that focuses on positive role models and uses engaging, context-specific

([92]) Loi du 8 décembre 2022 relative aux canaux de signalement et à la protection des auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public federal et au sein de la police intégrée, Moniteur Belge, 8 décembre 2022.

([93]) Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, p. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

formats would be more beneficial (European Commission, 2024a; Ishikawa, 2024; European Commission: Directorate-General for Migration and Home Affairs et al., 2024).

Nevertheless, motivation for acting with integrity is often lacking, as institutional transparency is perceived as a significant hurdle that slows logistical processes (Atillah, 2020; Eski et al., 2020; Daems, 2021; Staring et al., 2021; Staring et al., 2023). While respondents emphasised measures such as dilemma training or codes of conduct, they often remain isolated, with limited monitoring and enforcement, leading to fragmented and outdated initiatives. Integrity efforts tend to be driven more by societal or political pressure, or concerns about staff well-being and organisational reputation, rather than by strategic priorities. As a result, excessive focus on integrity can generate fatigue and foster an 'ethics industry', while pursuing the total elimination of corruption may be overambitious and undermine efficiency. To be effective, anti-corruption strategies must therefore be evidence-based, regularly updated and structurally funded to enable cross-border implementation and long-term impact (Anechiarico and Jacobs, 1996).

4. When every actor moves alone

Judiciary

Follow the money, and you will find corruption? Criminals do not keep records of their corrupt activities.
Public prosecutor

The judiciary has been strengthened with criminologists, legal experts, liaison magistrates and a port prosecutor to implement a unified port security policy (Gezelle, 2024). Since October 2021, an amendment to Article 4 of the Act of 24 February 1921 ([94]) allows Belgian judges to impose port bans of up to 20 years on individuals or entities guilty of drug-related offences or maritime security violations (Team Justitie, 2024). These bans restrict access to and employment within the maritime sector, aiming to address criminal infiltration (Team Justitie, 2024). However, their enforcement remains inconsistent across three judicial districts (see above) and raises concerns about stigmatisation and hindering rehabilitation (De Rechter, 2020). Looking ahead, the new government plans to establish a specialised prosecution service for financial crime and corruption, enabling a 'follow-the-money' approach against OCGs (European Commission, 2025; De Wever, 2025).

Law enforcement

While corruption presents unique challenges in investigations (Federale Politie, 2022), there is growing public and political support for a 'follow-the-money' approach to dismantle OCGs (Cel voor Financiële Informatieverwerking, 2023; Gezelle, 2024). In response, the Federal Police will collaborate with the new financial crime division within the federal prosecutor's office, a multidisciplinary financial and tax investigation unit under the Ministers of Finance and Justice, the National Drugs Agency and the Financial Intelligence Processing Unit to address the financial flows of OCGs (De Wever, 2025). Although the Federal Police employed 13 979 employees as of December 2024, with 13.2 % of their resources dedicated to corruption, they still lack the resources and expertise in financial and economic investigations (Federale Politie, 2024a). Allegations of information leaks in corruption investigations and undue

([94]) Act of 27 March 2023 amending the Act of 24 February 1921 concerning the trade in toxic substances, hypnotics and narcotics, psychotropic substances, disinfectants and antiseptics, and substances that may be used for the illegal manufacture of narcotics and psychotropic substances, Moniteur Belge, 3 April 2023.

political influence concerning the work of the OCRC have raised concerns among civil society, potentially undermining public trust in law enforcement (European Commission, 2025). In response, the new government announced screening and integrity checks throughout police officers' careers, during recruitment, selection and training (De Wever, 2025).

In 2023, the National Drugs Agency, responsible for the coordination of the fight against drug-related crime ([95]), established a fund to reinvest confiscated criminal proceeds into law enforcement and healthcare (Kir, 2023; Cel voor Financiële Informatieverwerking, 2023; Gezelle, 2024). At the European level, the revision of the Asset Recovery Directive emphasises asset seizure as a cornerstone to addressing organised crime ([96]). Yet in practice, only 2.2 % of criminal assets are frozen and 1.1 % are confiscated (Transparency International, 2024). To support the Federal Maritime Police, the government established a Port Security Corps, adding 70 security officers to increase their first-line assessments (Kir, 2023; Federale Politie, 2024a). By mid 2024, only 49 officers were operational (Verlinden, 2024). Additionally, a new investigative service within the Federal Maritime Police was established to deter criminal activities in the port (Federale Politie, 2024a; Verlinden, 2024). However, deterrence alone does not discourage criminal behaviour (De Rechter, 2020). Recognising the undermining effects ([97]) of organised drug crime, both national and European authorities invested in an administrative approach aimed at disrupting the infiltration of OCGs into maritime logistics (Paoli et al., 2025). To better conceal their illicit goods, they exploit legal economic structures, increasing the risk of reputational damage to the legal sector (Staring et al., 2023; Verodova et al., 2023; Paoli et al., 2025). Therefore, the Law on Municipal Administrative Enforcement, introduced on 7 February 2024 ([98]), empowers local authorities to revoke or deny business licenses for companies linked to financial crimes, money laundering or the facilitation of criminal influence (Wittevrongel and De Jaeger, 2024). These decisions rely on advice from the Directorate for Integrity Assessment of Public Authorities, under the Ministry of Interior, which can introduce delays and administrative bottlenecks. Moreover, such measures must be carefully balanced, as OCGs adapt by displacing their activities to less regulated sectors (Staring et al., 2023; Wittevrongel and De Jaeger, 2024).

Customs

OCGs or corrupt employees can bypass, manipulate or falsify risk analyses, and tamper with or remove container contents (Colman, 2018). In response, the Belgian government has strengthened customs capabilities by investing in mobile scanners to screen 100 % of high-risk containers and additional personnel, allowing a more proactive, intelligence-driven approach (Kir, 2023; Team Justitie, 2024; Port of Antwerp-Bruges, 2024; De Wever, 2025). However, enforcement remains limited. First, monitoring 271 million tonnes of maritime traffic is unfeasible, with only 1.5 % of all incoming cargo being scanned (Verodova et al., 2023; Port of Antwerp-Bruges, 2024). Second, customs operations are divided between two departments: operations, responsible for goods declarations in ports, and investigations, which focuses on fraud and smuggling (Federale Overheidsdienst Financiën, 2022). Although both conduct risk analyses on the flow of goods, respondents emphasise that coordination between them is unclear, leading to fragmented information-sharing with other port stakeholders.

([95]) Loi du 7 avril 2023 relative à la création, aux missions et à la composition d'un commissariat national drogue, Moniteur Belge, 7 avril 2023.
([96]) Proposal for a Directive of the European Parliament and of the Council on asset recovery and confiscation, 25 May 2022.
([97]) Despite lacking a universally agreed definition, 'undermining' is frequently associated with the societal harms of organised drug crime (Staring et al., 2023; Paoli et al., 2025).
([98]) Loi du 7 février 2024 relative à l'approche administrative communale, à la mise en place d'une enquête d'intégrité communale et portant création d'une Direction chargée de l'Évaluation de l'Intégrité pour les Pouvoirs publics, Moniteur Belge, 7 février 2024.

It is not always clear which department within customs should be notified.

Port company

In response, efforts are underway to revise and clarify the customs criminal law (Cepa and Alfaport Voka, 2024). The European Commission proposes replacing existing IT systems with a centralised data hub to harmonise risk analyses and criteria across the EU (European Parliament et al., 2024b). Furthermore, a European customs authority will coordinate national efforts and support Member States in identifying high-risk shipments (European Parliament et al., 2024b). At the national level, the digital customs platforms of Antwerp and Zeebrugge ports will be integrated to improve information exchange and streamline logistics (Jacobus, 2025).

Port companies

Port companies are willing to cooperate, provided it is economically feasible.

Port company

It was not until 2023 that Belgium and the Netherlands agreed with five port companies to address organised crime through measures such as high-risk container seals, smart cameras, drones, screening policies and cross-border information exchange (Kir, 2023; Rijksoverheid, 2023; De Wever, 2025). In the port of Zeebrugge, a central security control room coordinates surveillance with port authorities and the local police (Port of Antwerp-Bruges, 2024). While these cameras are not inherently 'smart', they are connected to automatic number plate recognition databases, which improves the detection of suspicious activities (Fiers, 2023). However, these measures remain reactive, identifying activities only after they occur. The federal government has emphasised that responsibility for implementation lies with port companies (De Wever, 2025). However, the main challenge is balancing security with economic competitiveness, as stricter measures in one port may displace OCGs to other areas.

International partners

As global trade and organised crime became transnational, addressing corruption in seaports emerged as a priority for the EU, its Member States and international partners (Europol, 2025). Organisations such as the OECD, the European Union Agency for Law Enforcement Cooperation (Europol), the Group of States against Corruption (GRECO), the European Multidisciplinary Platform Against Criminal Threats (Empact), the World Customs Organization or the MACN highlight the need for knowledge sharing and constant vigilance to develop an integrated approach to port security, to identify corruption trends and enhance both security and trade efficiency (European Commission, 2023). However, caution is warranted: in 2024, only 40 tonnes of cocaine were intercepted. While this decline may reflect the success of improved enforcement and collaborations, it could also indicate that OCGs are adapting. By shifting their activities to inland waterways, bulk cargo, airports or using modi operandi such as the drop-off and rip-off method, they continue to evade detection (Staring et al., 2023; Verodova et al., 2023; Decré, 2025; Paoli et al., 2025). These methods usually depend on corruption to succeed (Verodova et al., 2023).

Our projects and support team focuses solely on gathering and exchanging information at national and international levels. Centralising this data allows us to identify patterns and enhance anti-corruption efforts in the port.

Law enforcement official

The federal government emphasised strengthening liaison officers in non-EU countries to enhance the sharing of preventive measures and security standards (De Wever, 2025). While law enforcement collaborates with (inter) national port authorities, common efforts should be made across the entire EU, and globally, to mitigate a displacement effect by the development of legal frameworks and policy guidelines. Belgium could benefit from a shared command entity to streamline and exchange anti-corruption efforts at the local, national and international levels (European Commission, 2024a). Although several initiatives, such as *Stroomplan* 2.0 ([99]), the European ports alliance ([100]), the Security Think Tank ([101]), the Security Steering Committee ([102]), the local maritime security committees ([103]), the EU network against corruption ([104]), the Europol Platform for Experts ([105]) or the Poseidon project, have been launched to improve information sharing, these efforts remain fragmented due to inconsistent participation from the involved actors. A systematic evaluation could ensure that new network initiatives are monitored and adjusted as needed.

5. Closing the gaps: concluding discussion

With the increasing size and throughput of the Port of Antwerp-Bruges, physical and technological security measures have been strengthened to address organised drug crime. To maintain access and control over logistics chains, OCGs increasingly rely on corruption. Although Belgian and European frameworks strongly focus on organised drug crime, they risk overlooking the specific dynamics and impact of corruption. Corruption is not merely an enabler of organised crime, but a criminal phenomenon embedded within it. Addressing this requires more than traditional law enforcement tools. A sustainable anti-corruption strategy should therefore ensure clear roles, political support, evidence-based decision-making, a long-term focus and the flexibility to respond to emerging threats. However, the current developments remain too focused on visible deterrence, such as screenings, port bans or the deployment of a port security corps, creating an overly securitised port environment. Likewise, technological solutions such as CPu and a central security control room offer potential but are prone to manipulation if not embedded in a broader framework of cybersecurity, integrity policies, staff training and organisational change. Otherwise, they risk being symbolic, shifting rather than addressing corruption vulnerabilities. Yet, the real challenge lies not only in recognising the need for change, but in ensuring that these efforts are structurally implemented, monitored and enforced. Belgium's advocacy for expanding the ISPS Code could serve as a catalyst for sharing evidence-based security measures across all ports, ensuring their regular evaluation, structural funding and preventing the shifting of illicit activities. While private port actors bear responsibility for implementing security measures and balancing them with

([99]) The evaluation of the *Stroomplan* resulted in *Stroomplan* 2.0, emphasising (international) cooperation and increased resources for public services (Openbaar Ministerie, 2022).

([100]) The European ports alliance is an EU initiative to enhance port security against drug trafficking and organised crime. It fosters a public–private partnership among EU agencies and Member States to safeguard logistics, information and staff in seaports.

([101]) The Security Think Tank, established in 2005 by the Port of Antwerp-Bruges, fosters collaboration between public and private actors to build a resilient network for port security (communication with Antwerp-Bruges Port Authority).

([102]) The Security Steering Committee of the ports of Antwerp, Hamburg and Rotterdam exchanges strategic information to enhance port security. This collaboration focuses on the implementation of the ISPS Code and container security (Europol, 2023b).

([103]) The local maritime security committees are supported by the National Maritime Security Authority and oversee collaboration among customs, law enforcement and defence agencies, and intelligence services, port authorities and external partners (Team Justitie, 2024).

([104]) The EU Network against Corruption, established in 2023, serves as a platform for EU Member States, national authorities, civil society, international organisations and EU agencies to collaborate, share best practices, identify trends and improve coherence in anti-corruption efforts (European Commission, 2024a).

([105]) The Europol Platform for Experts is a collaborative web platform for specialists in a variety of law enforcement areas (Europol, 2023a).

economic competitiveness, their engagement requires meaningful involvement, transparency and access to information. A more positive public perception of the port depends on their inclusion and support. Moving forward, multidisciplinary collaboration should make information sharing the norm, not merely by joining networks, but through active contribution and organisational readiness to act on shared insights. This depends not only on the ability but also the willingness of each actor to engage in meaningful change. The National Drugs Agency could provide the necessary operational and strategic coordination to mobilise both public and private stakeholders and streamline responsibilities.

Finally, as Europe moves towards a unified anti-corruption framework, Belgium must align its Criminal Code and port security policies with international standards while retaining flexibility to adapt to evolving criminal tactics. This requires critical reflection on the roles and responsibilities of all actors involved. A streamlined division of tasks and improved coordination are needed to avoid fragmentation and ensure recourses are used strategically rather than claimed reactively. Encouragingly, drug seizures in the port have recently declined. This may be seen both as a sign of progress and a reminder of the persistent vigilance required. However, without reliable, evidence-based data, and under public pressure for swift action, it remains difficult to assess whether existing measures lead to progress or shift the problem elsewhere, leaving both public and private actors uncertain about their effectiveness and responsibilities.

Overall, the Port of Antwerp-Bruges has made progress in implementing anti-corruption measures, yet gaps remain. Since 2019, growing political commitment and public scrutiny have encouraged multidisciplinary collaboration. However, unclear responsibilities among many partners continue to hinder the implementation of anti-corruption policies, resulting in *ad hoc* initiatives. Short-term, highly visible deterrent actions often take precedence over a long-term approach. This focus on visible outcomes enhances political legitimacy but does not necessarily strengthen resilience against corruption. Pursuing the total elimination of corruption is likely overambitious and may undermine organisational efficiency. These challenges highlight the need to prioritise anti-corruption efforts, clarify responsibilities and adopt a flexible, long-term strategy to prevent fragmented initiatives and integrity fatigue.

References

Anechiarico, F. and Jacobs, J. B. (1996), *The Pursuit of Absolute Integrity – How corruption control makes government ineffective*, University of Chicago Press, Chicago, https://press.uchicago.edu/ucp/books/book/chicago/P/bo3633806.html.

Atillah, S. (2020), 'Anti-corruptiebeleid binnen Antwerp's anti-drugsteam "on hold" gezet', Apache, 2 June, https://apache.be/2020/06/02/anti-corruptiebeleid-kali-team-on-hold.

Cel voor Financiële Informatieverwerking (2023), *Activiteitenverslag 2023*, Brussels, https://www.ctif-cfi.be/images/documents/Dutch/Jaarverslagen/JV2023_NL.pdf.

Cepa and Alfaport Voka (2024), 'Zo maakten Alfaport Voka and Cepa voor u het verschil – Verslag oktober 2023–september 2024', https://alfaportvoka.be/wp-content/uploads/2024/10/Jaarverslag2024_AlfaportVokaCepa-DEFLOWRES.pdf.

Colman, C. (2018), 'Naar een geïntegreerde aanpak van de invoer en doorvoer van cocaïne via de haven via Antwerpen', *Panopticon*, Vol. 39, Issue 2, pp. 130–140, http://hdl.handle.net/1854/LU-8564445.

Cools, M., Reniers, G., Easton, M., van den Herrewegen, E. and De Boeck, A. (2013), *Integrale Veiligheid in de Haven van Antwerpen*, Maklu, Antwerp, http://hdl.handle.net/1854/LU-3222849.

Daems, R. (2021), 'Schriftelijke vraag nr. 7-1240 – Minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing', 12 May, https://www.senate.be/www/?MIval=Vragen/SchriftelijkeVraagandLEG=7andNR=1240andLANG=nl.

Decré, H. (2025), '"Historische daling" van cocaïnevangsten in de haven van Antwerpen in 2024: Alleen maar reden tot juichen of is voorzichtigheid geboden?', VrtNws, 9 January, https://www.vrt.be/vrtnws/nl/2025/01/09/jaarcijfers-drugs-2024-haven-antwerpen/.

De Middeleer, F. and De Ruyver, B. (2017), 'De verschuiving van illegale drugsmarkten van Nederland naar België: perceptie of realiteit?', *Justitiële Verkenningen*, Vol. 43, Issue 2, pp. 103–119, http://hdl.handle.net/1854/LU-8520400.

Depuydt, P., Bové, L. and Segers, T. (2020), 'In de greep van de cocaïnemaffia', *De Tijd*, https://www.tijd.be/dossiers/de-cokelijnen/in-de-greep-van-de-cocainemaffia/10269817.html?_sp_ses=b1b4ff18-ea2d-4256-86d7-5d9dc8e176ee.

De Rechter, B. (2020), 'De relatie tussen afschrikking en criminaliteit – Een verkennende literatuurstudie', Universiteit Gent, https://eu-st01.ext.exlibrisgroup.com/32RUG_INST/storage/alma/DB/02/58/57/B3/09/89/0B/67/21/AC/12/3D/EC/F3/F2/RUG01-002835977_2020_0001_AC.pdf?Expires=1775819140&Signature=aXaFyz33bYbkH-DymR4fopfcYpiY0XIIKD~RAmVHk26pCquvzR3mbry9xlX8oUAw4TrYgMiiPwEbNJYMRsCrcKD5BrPSfvcGLKM-FV8MTapBzbY1h897ZjLnRI5Wu2dgE25z6dkpgip5RFShdtCXg7Kf85bVYUFXdL7lb4D-vXzcEpf0KQORMN2e-dn8Ln-lKpu7i9yz0493oacs-1yDlqsSY-y2Nf-hAIMuHG-1s8ZjQKCel8b-OY3PnySJFtmFZzFUPLhV0tSjLo9qlbdVpxS3mfvAi-Kq0rL0Umev1S7dJ5GLQEjkitMW7ComlwnS1F6jV10hXZ3IS2X62rVt98NCQw__&Key-Pair-Id=APKAJ72OZCZ36VG-VASIA.

De Wever, B. (2025), 'Federaal regeerakkoord 2025–2029', https://www.belgium.be/sites/default/files/resources/publication/files/Regeerakkoord-Bart_De_Wever_nl.pdf.

Easton, M. (2018), 'Reflecties over nodaal en netwerkend politiewerk: De aanpak van cocaïnestromen in de haven van Antwerpen', *Cahiers Politiestudies*, Vol. 2, Issue 47, pp. 91–110, http://hdl.handle.net/1854/LU-8565708.

Eski, Y., Boelens, M. and Boutellier, H. (2020), 'Gezamenlijke richting tegen maritieme ondermijning: Strategische aanbevelingen voor de aanpak van ondermijnende (drugs)criminaliteit in Nederlandse havens', Vrije Universiteit Amsterdam, https://research.vu.nl/en/publications/gezamenlijke-richting-tegen-maritieme-ondermijning-strategische-a/.

European Commission (2014), Annex 1 – Belgium to the EU anti-corruption report, COM(2014) 38 final of 3 February, https://www.parlament.gv.at/dokument/XXV/EU/10940/imfname_10436400.pdf.

European Commission (2023), Joint communication from the European Commission to the European Parliament, the Council, and the European Economic and Social Committee on the fight against corruption, JOIN(2023) 12 final of 3 May 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023JC0012.

European Commission (2024a), Commission staff working document – 2024 rule of law report – Country chapter on the rule of law situation in Belgium – Accompanying the document 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – 2024 rule of law report – The rule of law situation in the European Union', SWD(2024) 801 final of 24 July 2024, https://commission.europa.eu/document/download/ac09a9ad-63c4-4c65-bf36-d032b605a015_en?filename=7_1_58050_coun_chap_belgium_en.pdf.

European Commission (2024b), 'Special Eurobarometer 548 – Citizens' attitudes towards corruption in the EU in 2024', https://europa.eu/eurobarometer/surveys/detail/3217.

European Commission (2025), Commission staff working document – 2025 rule of law report – Country chapter on the rule of law situation in Belgium – Accompanying the document 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – 2025 rule of law report – The rule of law situation in the European Union', SWD(2025) 901 final of 8 July 2025, https://commission.europa.eu/document/download/5fe5bb71-2898-4079-ad5a-19a3ff595a62_en?filename=5_1_63936_coun_chap_belgium_en.pdf.

European Council (2024), 'Combatting corruption: Council adopts position on EU law', 14 June, https://www.consilium.europa.eu/en/press/press-releases/2024/06/14/combatting-corruption-council-adopts-position-on-eu-law/.

European Parliament: European Parliamentary Research Service and Bąkowski, P. (2024a), 'Directive on combating corruption', PE 762.406, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762406/EPRS_BRI(2024)762406_EN.pdf.

European Parliament: European Parliamentary Research Service and Baert, P. (2024b), 'Establishing an EU customs data hub and a customs authority', PE 753.931, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)753931.

Europol (2023a), 'Europol Platform for Experts (EPE)', Europol website, https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts.

Europol (2023b), *Criminal Networks in EU Ports – Risks and challenges for law enforcement*, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Joint-report_Criminal %20networks %20in %20EU %20ports_Public_version.pdf.

Europol (2025), *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2813/0758057.

Federale Politie (2021), 'Enorme hoeveelheid ontcijferde berichten geeft unieke kijk in de werking van criminele organisaties', 10 March, https://www.politie.be/5998/nl/nieuws/enorme-hoeveelheid-ontcijferde-berichten-geeft-unieke-inkijk-in-de-werking-van-criminele.

Federale Politie (2022), *Nationaal Veiligheidsplan 2022–2025 – Een veerkrachtige geïntegreerde politie, ten dienste van de samenleving*, https://www.politie.be/5998//sites/5998/files/media/file/2022-04/NVP2022-2025.pdf.

Federale Politie (2024a), 'Drugstrafiek via de haven: enkele jaarcijfers 2023', Federale Politie website, 17 January, https://www.politie.be/5998/nl/nieuws/drugstrafiek-via-de-haven-enkele-jaarcijfers-2023.

Federale Politie (2024b), 'Achter de schermen bij de Federale Gerechtelijke Politie in de strijd tegen corruptie', 9 December, https://www.politie.be/5998/nl/nieuws/achter-de-schermen-bij-de-federale-gerechtelijke-politie-in-de-strijd-tegen-corruptie.

Federale Overheidsdienst Financiën (2022), 'De algemene administratie van de douane en accijnzen', https://financien.belgium.be/sites/default/files/Customs/Over-de-AADA/Organisatie/Presentatie_%20corporate_%20NL_%20_%28externe_%20versie_%202022_%29.pdf.

Fiers, D. (2023), 'Federale regering investeert fors in ANPR-camera's, maar is dat wel een goed idee? "Drogreden dat cameraschil ons land veiliger zal maken"', VrtNws, 10 October, https://www.vrt.be/vrtnws/nl/2023/10/10/regering-de-croo-investeert-fors-in-anpr-camera-s-maar-experten/.

Garyfallidou, F. (2024), *China's Overseas Port Investments: Unravelling the nexus between economic strategies and potential political influence in NATO nations*, Univerzita Karlova, http://hdl.handle.net/20.500.11956/197721.

Geens, K. and Jambon, J. (2019), *Kadernota Integrale Veiligheid – 2016–2019*, https://justitie.belgium.be/sites/default/files/downloads/2016-06-07_kadernota_integrale_veiligheid_nl_0.pdf.

Gezelle, H. (2024), 'Ministerraad keurt toewijzing van budgetten uit drugsfonds goed', Nnieuws website, 3 May 2024, https://nnieuws.be/artikel/ministerraad-keurt-toewijzing-van-budgetten-uit-drugsfonds-goed.

GRECO (2020), 'Fifth evaluation round – Preventing corruption and promoting integrity in central governments (top executive functions) and law enforcement agencies – Evaluation report – Belgium', https://rm.coe.int/fifth-evaluation-round-preventing-corruption-and-promoting-integrity-i/1680998a40.

InSight Crime (2020), 'Samenvatting wetenschappelijke evaluatie stroomplan', https://insightcrime.org/wp-content/uploads/2020/02/Samenvatting_pers_onderzoek_UGent.docx.

Ishikawa, Y. (2024), 'Anti-corruption awareness raising – Effective messaging and best practices', Transparency International, https://knowledgehub.transparency.org/helpdesk/anti-corruption-awareness-raising-effective-messaging-and-best-practices.

Jacobus, R. (2025), 'Digitale platformen RX/SeaPort en NxtPort gaan samenwerken', Flows, 6 June, https://www.flows.be/douane/2025/06/digitale-platformen-rx-seaport-en-nxtport-gaan-samenwerken/.

Janssens, J. and De Vos, A. (2019), 'The European Union: Organised crime policies, politics and the EU', in: Allum, F. and Gilmour, S. (eds), *Handbook of Organised Crime and Politics*, Edward Elgar Publishing, Cheltenham, pp. 437–454, https://doi.org/10.4337/9781786434579.00042.

Jenkins, M. and Camacho, G. (2022), 'Core principles for the development of anti-corruption strategies – Practices from around the world', U4 Anti-Corruption Resource Centre: Chr. Michelsen Institute, Bergen, https://cdn.sanity.io/files/1f1lcoov/production/4a18911be17c93e5fd7115a89377bb2de6669cd6.pdf.

Kir, E. (2023), 'Plan om drugssmokkel in Antwerpen aan te pakken', De Kamer van Volksvertegenwoordigers, https://www.stradalex.com/nl/sl_src_publ_div_be_chambre/document/SVbkv_55-b108-1192-1755-2022202319216.

Maesschalck, J. (2012), 'Anti-corruptie initiatieven', *Evaluatie van het Nationaal Integriteitssysteem – België*, Transparency International, Brussels, pp. 47–48, https://lirias.kuleuven.be/1908583?&lang=en.

MACN (2023), *MACN Annual Report 2023 – From sanctions to sustainability: Evolving dynamics in global trade management*, https://macn.dk/wp-content/uploads/2024/05/MACN_Annual_Report_2023_SinglePages.pdf.

Nelen, H., Noack, J. and Spapens, A. C. M. (2021*), Druggerelateerde Criminaliteit in de Euregio Maas-Rijn: Fenomeen en aanpak*, Maastricht University, https://cris.maastrichtuniversity.nl/en/publications/druggerelateerde-criminaliteit-in-de-euregio-maas-rijn-fenomeen-e/.

OECD (2013), *Phase 3 report on implementing the OECD anti-bribery convention in Belgium*, OECD Publishing, Paris, https://www.oecd.org/daf/anti-bribery/BelgiumPhase3ReportEN.pdf.

Openbaar Ministerie (2015), *Jaarverslag 2015*, https://www.om-mp.be/sites/default/files/u1/nl_jaarverslag_2015_def.pdf.

Openbaar Ministerie (2021), *Jaarverslag 2021*, https://www.om-mp.be/sites/default/files/Jaarverslag %202021.pdf.

Openbaar Ministerie (2022), *Jaarverslag 2022*, https://www.om-mp.be/sites/default/files/Jaarverslag %202022.pdf.

Openbaar Ministerie (2023), *Jaarverslag 2023*, https://www.om-mp.be/sites/default/files/Jaarverslag %202023.pdf.

Paoli, L., Greenfield, V. A. and Gabriëls, L. (2025), 'Is cocaine trafficking in Belgium becoming more harmful?', *Cahiers Politiestudies*, Vol. 74, pp. 163–198, https://lirias.kuleuven.be/4254519?&lang=en.

European Commission: Directorate-General for Migration and Home Affairs, Persson, A., Worth, M. and Jeney, P. (2024), *High-Risk Areas of Corruption in the EU – A mapping and in-depth analysis*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2837/5907939.

Port of Antwerp-Bruges (2024), *2024 Feiten and Cijfers*, https://media.portofantwerpbruges.com/m/2b2df2df48d5141e/original/BROCHURE_Cijferboekje_NL_2024.pdf.

Rijksoverheid (2023), 'Maritieme sector strijdt samen met België en Nederland tegen narcoterrorisme', 17 February, https://www.rijksoverheid.nl/documenten/publicaties/2023/02/17/maritieme-sector-strijdt-samen-met-belgie-en-nederland-tegen-narcoterrorisme.

Staring, R., Bisschop, L., Colman, C., Janssens, J. and Roks, R. (2021), 'De Scheldestad of Manhattan aan de Maas? Een vergelijkende analyse van de Antwerpse en Rotterdamse havens bij de in- en doorvoer van cocaïne', *Tijdschrift Voor Criminologie*, Vol. 63, Issue 2, pp. 146–166, http://doi.org/10.5553/tvc/0165182x2021063002003.

Staring, R., Bisschop, L., Roks, R., Brein, E. and van de Bunt, H. (2023), 'Drug crime and the Port of Rotterdam: About the phenomenon and its approach', in: Nelen, H. and Siegel D. (eds), *Organized Crime in the 21st Century: Motivations, opportunities, and constraints*, Springer International Publishing, Cham, pp. 43–61, https://doi.org/10.1007/978-3-031-21576-6_4.

Struys, B. (2024), 'Hoe de ondermijnende criminaliteit onze economie infiltreert via de kleine handelaar: "Het cliché bij uitstek is de kapperszaak"', DeMorgen, 1 October, https://www.demorgen.be/nieuws/van-de-kapper-tot-de-visboer-overal-probeert-de-drugsmaffia-geld-wit-te-wassen-de-meest-perverse-hr-dienst~b5dec36b/.

Team Justitie (2024), 'Nieuwe maatregelen voor een betere beveiliging van onze havens', https://mobilit.belgium.be/nl/news/nieuwe-maatregelen-voor-veiligere-havens.

Torbrand, C. M. (2022), 'Tackling corruption in the maritime industry', Global Maritime Forum, 19 September, https://globalmaritimeforum.org/insight/tackling-corruption-in-the-maritime-industry/.

Transparency International (2024), 'Guide to strengthening the EU's asset recovery framework', https://www.google.com/url?sa=tandsource=webandrct=jandopi=89978449andurl=https://transparency.eu/wp-content/uploads/2024/03/Asset_recovery_briefing_2022.pdfandved=2ahUKEwjm6YmukPGNAxURZqQEHRBQDLoQFnoECDMQAQandusg=AOvVaw02JpemkwmLb03XL8kHBeki.

Verlinden, A. (2024), '1 jaar na start Havenbeveiligingskorps in Antwerpse haven: Meer controles, minder drugsuithalers', Federale Politie, 8 May, https://www.politie.be/5998/nl/nieuws/1-jaar-na-start-havenbeveiligingskorps-in-antwerpse-haven-meer-controles-minder#:~:text=U%20bent%20hier%3A-,1%20jaar%20na%20start%20Havenbeveiligingskorps,haven%3A%20meer%20controles%2C%20minder%20drugsuithalers&text=Begin%20mei%20is%20het%20precies,strijd%20tegen%20de%20georganiseerde%20drugscriminaliteit.

Verodova, A., Apriani, D., Annindya, J., Aulia, S. and Satria, R. (2023), 'The Mexico-Belgium drug trafficking on the rise of criminal: Belgium as the new drug capital of Europe', *Mandala: Jurnal Ilmu Hubungan Internasional*, Vol. 6, No 2, pp. 43–66, https://ejournal.upnvj.ac.id/JM/article/view/8132/2964.

Wittevrongel, F. and De Jaeger, T. (2024), 'Het spanningsveld tussen het vrij ondernemerschap en het criminele ondernemerschap in België: Een eerste blik op enkele opportuniteiten voor, en recente initiatieven tegen, malafide ondernemers', *Panopticon*, Vol. 45, Issue 4, pp. 305–350, https://backoffice.biblio.ugent.be/download/01J0T7XFNHDMS3PAFWE684VN4P/01J0T7XNQDJ4HSXCF0AE0KCJHX.

Zürcher, E., Pardal, M., Leussink, I. and Hoorens, S. (2024), *Drugsgerelateerde corruptie op Schiphol en in de Rotterdamse haven – Een analyse van corruptiedreigingen, impact en beleidsinstrumenten op basis van de methodologie voor national risk assessment*, RAND Europe, https://www.rand.org/pubs/research_reports/RRA2870-1.html.

Annex 14.1. List of interviewees

Interviewees (organisations)	Customs (1) Judicial authorities (7) Law enforcement (2) Government agencies (2) Labour unions (2) Port authorities (4) Port companies (5)

Islamic terrorism in Germany – The use of social network analysis to detect high-risk criminal networks

Kristin Weber ([106])

https://doi.org/10.3013/57bdcd15

Abstract

This article pays particular attention to the networks of homegrown terrorists in Germany who were engaged in conflicts and war zones in Iraq, Syria and African states by the Islamic State in Iraq and Syria (and other terrorist organisations). Based on the combination of court file and social network analysis it was possible to highlight a network of 255 people and 650 connections, the key actors and the infrastructure of the network itself. This article presents social network analysis as a possible tool for police investigations on how to identify terrorist networks as high-risk networks. Using the example of a terrorist network from Germany, it is possible to explain how terrorist networks are organised and how they can be destabilised or even disrupted. By identifying relevant key players and subgroups, their connections and positions within the network, it is possible to gain a deeper understanding of radicalisation and create more effective counterterrorism strategies.

Keywords: radicalisation, terrorism, covert networks, social network analysis, police training.

Introduction

Terrorism represents a dynamic and constantly evolving phenomenon. Security authorities and researchers continue to face major challenges in analysing and countering terrorism and radicalisation and in developing effective counterterrorism strategies. Terrorist organisations, recruitment mechanisms and narratives continually adapt to changing social and political environments. Between 2015 and 2017 ([107]), members of the Islamic State in Iraq and

([106]) The results presented are based on findings published in Weber (2023).

([107]) Terrorist acts included the following: in January 2015, attacks in Paris on Charlie Hebdo and a kosher supermarket; in November 2015, attacks in Paris on the Stade de France, bars and restaurants in the 10th arrondissement and the Bataclan theatre in the 11th arrondissement; in 2016, attacks in Brussels at Zaventem Airport and on the subway, attacks in Nice, France and at a Christmas market in Berlin, Germany; and in 2017 on Las Ramblas in Spain.

Syria (ISIS) carried out a series of terrorist attacks that profoundly affected Europe. The proclamation of the ISIS's caliphate in 2014 marked a significant turning point, sparking a wave of departures from Europe – particularly from Germany – towards war zones in Syria to join the caliphate. The Federal Office for the Protection of the Constitution estimates that over 1 060 jihadist Islamists from Germany travelled to war zones in Syria and Iraq until 2020 (the Federal Office for the Protection of the Constitution, n.d.). Many of these individuals maintained direct links to ISIS and actively engaged in combat operations. The appeal of the conflict zones and of ISIS's activities in Syria and Iraq extended far beyond Germany's borders. In 2014, approximately 1 130 individuals from France joined the conflicts in Syria and Iraq, followed by around 1 000 from Turkey, 800 from Russia, 550 from Germany, 500 from the United Kingdom and 300 each from Belgium and Sweden. From North Africa and the Middle East about 3 000 Tunisians, 2 500 Saudi Arabians, 2 090 Jordanians, 1 500 Moroccans and 890 Lebanese travelled to jihadist-held territories (cf. Salloum, 2014; Weber, 2023, pp. 31–33). Since the destruction of the caliphate in 2019, movement patterns have shifted, but ISIS has not disappeared. ISIS has retreated underground and created offshoots in different areas of the world, such as the Islamic State Khorasan Province (ISKP) in Afghanistan. Understanding the organisation's network processes, dynamics, logistics, important key players and their roles, along with detecting these covert connections, plays an important role in law enforcement and counterterrorism efforts. Strengthening investigative capacities not only requires identifying central figures and their roles but also analysing how these hidden networks operate and sustain themselves. Even after the fragmentation of ISIS in Syria, network structures and radicalisation processes continue to demand systematic research – particularly in light of ISKP's growing influence and regional expansion.

This present research ([108]) draws on a court file and social network analysis of 36 court records provided by the Federal Public Prosecutor General at the Federal Court of Justice, and other public prosecutors and the Federal Bureau of Criminal Investigation. The files offered rich insights into the radicalisation processes of the perpetrators and their network (cf. Weber, 2023, pp. 7–10).

The article highlights social network analysis as a valuable tool for law enforcement to identify and analyse underground networks, assess their risk potential and develop strategies to disrupt or destabilise them.

Data pool

This research draws on an analysis of 36 court records concerning completed legal proceedings that resulted in final convictions of the perpetrators. The dataset excludes individuals affiliated with Al-Qaeda. The analysed cases involve convictions between 2014 and 2017 for offences such as forming, participating in, or supporting a terrorist organisation abroad; preparing a serious act of violence endangering the state; establishing contacts to plan such acts; and financing terrorism ([109]). All personal identifiers of the perpetrators were anonymised to ensure confidentiality ([110]). The court files include interrogation transcripts, chat logs, telecommunications and surveillance records, arrest warrants, photographs, indictments and judgments (cf. Weber, 2023, pp. 7–10).

([108]) This research was part of the project 'X-Sonar: Extremist endeavours in social media networks: Identification, analysis and management of radicalisation processes' by the German Police University in Münster, Germany. For more information, see Weber (2023).

([109]) German Criminal Code (Strafgesetzbuch, StGB): § 129(a) StGB 'Formation of a terrorist organisation', § 129(b) StGB 'Criminal and terrorist organisations abroad', § 89(a) StGB 'Preparation of a serious act of violence endangering the state', § 89(b) 'Establishing relations for the commission of a serious act of violence endangering the state' and § 89(c) 'Financing of terrorism' (Federal Ministry of Justice, 2025). Relevant international counterterrorism frameworks include the EU Directive 2017/541 on combating terrorism (European Parliament and Council of the European Union, 2017), which harmonises legal definitions across the EU, and UN Security Council Resolutions 1373 (2001) and 2178 (2014), which establish global standards for criminalising and preventing terrorism, including the phenomenon of foreign terrorist fighters.

([110]) A comprehensive data protection framework was established and implemented throughout the X-Sonar research project and the dissertation (Weber, 2023). Measures included restricted access to case files, prohibition of third-party access, secure storage in a fireproof, lockable cabinet, the use of a coded key list for offenders and full anonymisation of offender identities. Further details are provided in Weber (2023).

The analysis identified 58 individuals (53 men and 5 women) and categorised them according to their actions.

- **Foreign terrorist fighters (*n* = 40).** These individuals travelled to war zones in Iraq, Syria or African states, received military training, and repeatedly returned to and departed from Germany.
- **Individuals intending to leave (*n* = 14).** These individuals planned to travel to war zones but were arrested or prevented from carrying out their plans.
- **Supporters (*n* = 4).** These individuals provided financial or material support (e.g. clothing) to terrorist organisations, produced propaganda and/or offered assistance to imprisoned members. They joined and supported different terrorist organisations (Jabhat al-Nusra, Jaish al-Muhajireen wal-Ansar, Jabhat al-Sham) but mostly ISIS (cf. Weber, 2023, pp. 8, 97).

All individuals investigated were affiliated with the (inter)national Salafist-jihadist milieu. The analysis shows that the individuals actively participated in Islamic seminars, Qur'an distribution campaigns and rallies organised by prominent preachers in Germany and across the EU. They also attended demonstrations, religious services, prayers and religious missionary activities. Most of them regularly frequented radical mosques and many engaged in fundraising efforts for extremist causes. Furthermore, all perpetrators were members of radical Salafist-jihadist organisations or communities based in Germany. They formed part of an international terrorist network that extended its connections to Iraq, Syria and African states (cf. Weber, 2023, pp. 156–159).

Literature review

The pioneering studies conducted by Krebs (2002), Sageman (2004), Bakker (2006), Koschade (2006), Magouirk et al. (2008), and also more recent studies by Weber and Hamachers (2020), and Weber (2023) among others exemplify the valuable use of network analysis based on open-source material and court records. Krebs (2002) conducted an analysis of open-source media to examine the communication patterns used by the al-Qaeda attackers during the World Trade Center attacks on 11 September 2001. His findings highlight the challenges of detecting covert networks and underscore the importance of identifying key actors (e.g. critical nodes, such as brokers) to effectively disrupt them. In addition, he identified not only the connections among the attackers but also the flow of information and money from other network members that supported the planning and execution of the 11 September attacks. Bakker (2006) focused on European terror networks building on Sageman's (2004) research on global terrorism. In the comparison of 172 global and 242 European terrorists he highlights their connection through kinship and friendship (Bakker, 2006). This result is also reflected in the research by Weber and Hamachers (2020) and Weber (2023).

Koschade (2006) and Magouirk et al. (2008) analysed the communication networks underlying the 2002 Bali bombings conducted by Jemaah Islamiyah. Koschade (2006) identified key players and weak points within the Jemaah Islamiyah network, demonstrating how targeting these nodes could fragment the organisation and disrupt the flow of information. He also emphasised the value of social network analysis as a tool for intelligence services. Magouirk et al. (2008) demonstrated how the network's structure shifted over time from a centralised hierarchy to a decentralised configuration, distributing critical functions across a wider set of actors.

Weber and Hamachers (2020) investigated foreign terrorist fighters from Germany by combining court record analysis and social network analysis. Their study identified three types of networks: online, offline and key-player networks, revealing the absence of a real online network and underscoring the importance of the offline sphere and active key players as critical nodes within it.

Weber (2023) applied the same methodological approach as Weber and Hamachers (2020) to examine preachers as key players and their role in the radicalisation and mobilisation of foreign terrorist fighters from Germany. She emphasised the value of social network analysis as a powerful tool for investigating underground and covert networks, particularly when using court records.

Researchers can employ this method to illuminate structures, hierarchies and key actors, and to identify strategies for weakening networks and developing effective counterterrorism measures (Mullins, 2013). However, obtaining comprehensive and reliable data, especially court records, remains a major challenge (Weber and Hamachers, 2020, p. 230).

Methodology

I employed a mixed-methods approach to analysing these files, combining qualitative content analysis by Mayring (2015), grounded theory methodology by Glaser and Strauss (1967), Strauss and Corbin's methodology (1996) and network analysis to uncover patterns and relationships (cf. Weber, 2023, pp. 90–100) ([111]).

The advantages of utilising court files are evident: experts from the police and public prosecutors meticulously collected and evaluated the data during their preliminary investigations. Consequently, they provide a wealth of detailed information, enabling in-depth individual case analyses. Combining content analysis with social network analysis proves highly beneficial in this research. It provides valuable insight into complex social processes and dynamics, such as individual radicalisation processes and group mobilisation/recruitment: why and how people became members of terrorist organisations and the international network. In addition, it allows researchers to analyse the structure of the jihadi network in Germany and its connections to members of a terrorist organisation abroad (cf. Weber, 2023, pp. 101, 106–118).

A cross-file analysis identified 255 individuals with more than 650 connections to other network actors. The analysis revealed that members of this network assumed various key roles and responsibilities to sustain and expand it (cf. Weber, 2023, pp. 263–265).

Examining the relationships (edges) between actors/individuals (nodes) within a network is the primary focus of a social network analysis (Wassermann and Faust, 1994, pp. 94–95; Weber, 2023, p. 120). A network is defined as a group of individuals who share a connection through relationships (Sageman, 2004, p. 137). The analysis treats a relationship as established when the files explicitly mention it or when the contained records provide verifiable evidence (e.g. chat records, telecommunication and observation protocols). To sum up: 'the study of networks is, in essence, the study of relationships' (Arsenault, 2011, p. 260). The size of each node reflects the strength of its connections: the larger the node, the more connections an individual has, indicating their potential significance

([111]) For more information regarding the use of content analysis and grounded theory methodology, see Weber (2023).

within the network (Figure 15.1). In any network, certain individuals play pivotal roles in its existence, maintenance, growth and overall success (cf. Weber, 2023, pp. 121–124). These roles include group or organisation leader, recruiter, preacher, propagandist, trafficker, marriage broker, recruits, organisers of a terroristic attack, terrorist attacker/assassins, supporter, contact person and exit supporter (cf. Weber, 2023, pp. 121–124).

The position of a node within the network matters too: the more central the node, the higher its importance. A node positioned at the centre of the network suggests that the individual may play a key role, potentially acting as a central figure within the network. Nodes located on the periphery can also hold significant importance. These actors function as critical nodes and fulfil different roles, such as controlling the flow of information or serving as informational hubs for subgroups distant from the centre (Figure 15.1). Such nodes facilitate the flow of information between different parts of the network and even influence its dynamics (cf. Weber, 2023, pp. 290–291). To identify critical nodes within a network, statistical measures are important.

I visualised the network with the software Gephi (Bastian et al., 2009), applying the Fruchterman–Reingold algorithm (Fruchterman and Reingold, 1991), combined with the no-overlap function. This algorithm ensures a clear arrangement of nodes, positioning those with connections closer together. This approach helps to identify distinct network structures and subgroups effectively. By using statistical centrality measures (degree, betweenness and closeness) provided by Gephi, it is possible to analyse the structure and even key players within the network (cf. Weber, 2023, pp. 121–124).

Centrality provides insights into the significance of nodes within a network, including their number of connections, the extent to which they are connected with other members, and their influence or control over the flow of information. Degree centrality represents the number of connections of a node. This number allows for determining how important a node is for the network. Betweenness centrality is a common measure used to identify potential influencers within a network. Closeness centrality gives information about how close a node is to all other nodes in the network. This measure ranges from 0 to 1. Values close to 1 indicate that nodes (individuals) are central in the network and are close to most other nodes. Values close to 0 indicate that nodes (individuals) lie far from the centre and require more steps to connect with other members of the network. Nodes with higher closeness measures are able to communicate and share information more easily because they are close to other nodes (Chau and Xu, 2007; see Medina, 2014; Fuhse, 2016; Weber and Hamachers, 2020; Weber, 2023, pp. 121–124, 290–291).

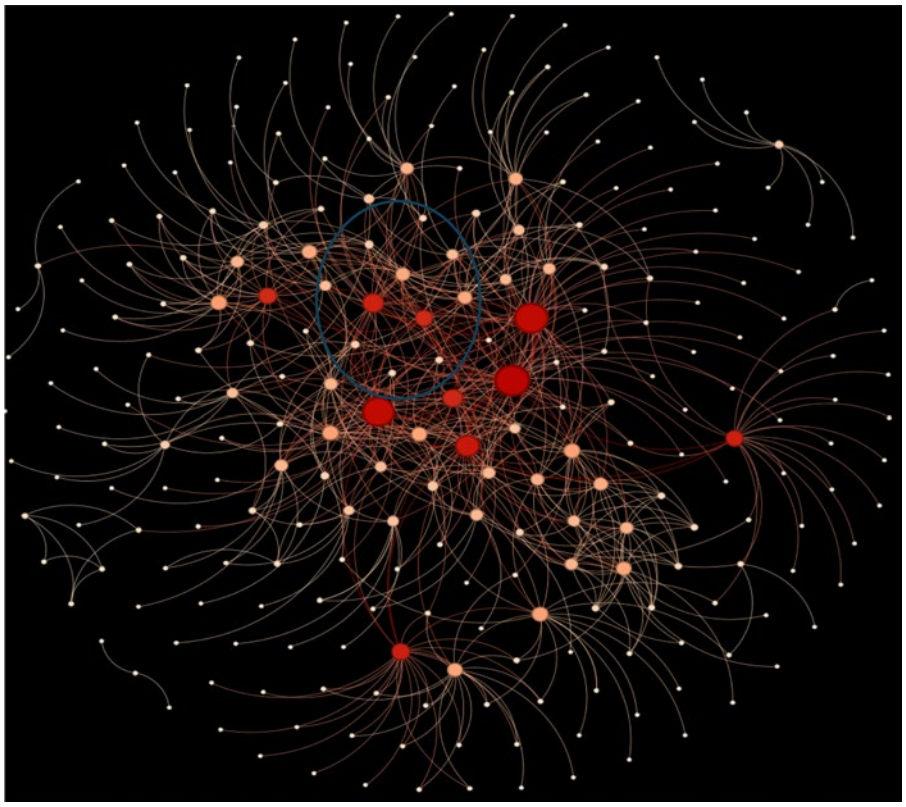


Figure 15.1. Visualised network by Gephi
NB: Fruchtermann–Reingold logarithm, no overlap.
Source: Weber, 2023.

The figure shows the complete network identified by Weber (2023). It shows a number of nodes and connections, differentiating central nodes and nodes in the periphery. Nodes with a higher degree (number of connections) are bigger than nodes with fewer connections. The blue oval highlights as an example a subgroup that will be explained next. Figure 15.1 is based on Weber (2023).

By identifying key players, such as information hubs or bridging nodes (bridges) linking peripheral and central positions, it becomes possible to strategically destabilise or disrupt the network by isolating or removing these crucial individuals. The fragmentation of the network or a slowing down in its information dynamic could result by removing important key players.

Even nodes positioned at the periphery or those without direct connections can play pivotal roles within the network. Some actors may actively cut their ties to conceal their activities, resulting in nodes that appear isolated. Peripheral nodes with long-distance connections can function as covert intermediaries, hubs, bridges or supporters, linking actors between the network's centre and its periphery.

Although this paper provides relevant insights on social network analysis and the connection between different actors in the network, it focuses on directly connected nodes and their surroundings ([112]). However, it provides a useful initial

([112]) For more information about nodes in the periphery and long-distance connections, see Weber and Hamachers (2020), Weber (2023).

heuristic for risk assessment. Focusing only on direct connections may overlook indirect relational pathways through which information, resources or influence circulate within terrorist networks. Future analyses should therefore consider higher-order connections to capture the broader structural risks embedded in indirect ties, adopting a multilevel network perspective (e.g. k-step neighbourhoods: explaining indirect range and influence of an actor). Using social network analysis combined with qualitative material, such as court records, like Weber (2023), within an interdisciplinary team (security authorities, researchers, prosecutors) can heighten the validity and the results of the analysis.

Results

To better understand the strategy of detecting and removing key players, we can take a closer look at a subnetwork of active recruiters (SR49 ([113]), SR50, SR51, SR52) as an example (blue oval, Figure 15.1, zoom: Figure 15.2) (cf. Weber, 2023, pp. 292, 297–300).

Figure 15.2. Zoom on SR49–SR52 and their connections

NB: Füh indicates leaders; P, preacher; R, recruits; and U, supporters. The filter applied is an ego network focus on SR49.

In terms of centrality measures, SR49 and SR52 score high, SR50 mediocre and SR51 low (Table 15.1).

Table 15.1. Centrality measures for SR49–SR52

Name	Degree	Betweenness	Closeness
SR49	23	1 999.00	0.40233
SR52	21	1 235.25	0.38746
SR50	15	243.442	0.34877
SR51	13	456.79	0.37774

Source: The statistical values used in this analysis are based on findings published in Weber (2023, p. 292).

([113]) SR stands for Syria returnee (foreign terrorist fighter). This abbreviation is part of the strategy to anonymise all perpetrators.

These four nodes occupy peripheral positions within the network but remain relatively easy to access (closeness). It is important to note at this point that SR49, SR50 and SR52 shared kinship ties. SR49 and SR52 demonstrate strong connectivity within the network, with degree ([114]) values of 23 and 21, respectively, indicating high levels of activity. SR49, in particular, exhibits a high betweenness centrality, highlighting his significant role as an intermediary within the network. This makes SR49 crucial for the flow of information (hub), as many connections pass through him. His strong integration into the network's core is evident through links to SR45 and P4 (see Figure15.1 and Figure15.2) (Weber, 2023, pp. 298–299). SR49 acts as a critical bridge into jihad (cf. Sageman, 2004, p. 169; Weber, 2023, p. 299).

The analysis of connections involving SR49, SR50, SR51 and SR52 reveals that SR49 maintains close links to a subnetwork of recruits. Court file analyses confirm SR49's active role as a recruiter for ISIS, directly engaging with 10 recruits. He facilitated their recruitment into violent jihad and ISIS operations by providing guidance on how and when to leave the country to join ISIS. Among these recruits were four young men (R1, R6, R7 and R9) who later died in Syria while fighting for ISIS. SR49, together with SR50 and SR52, played a crucial role in enabling these individuals to join ISIS and therefore bear direct responsibility for the deaths of these recruits (cf. Weber, 2023, pp. 289–299).

Disrupting the subnetwork formed by SR49, SR50 and SR52 could have prevented the departure of these 10 young men, or possibly more, since the exact total remains uncertain. Targeting SR49, SR50 and SR52 would likely have dismantled the network because they maintained direct links to Preacher 4 (P4). P4, as the central figure in the network, belonged to ISIS and provided multifaceted support, including facilitating departures, mediating contacts and issuing letters of recommendation ([115]). Severing the links from SR49, SR50 and SR52 to P4 would have cut the network off from crucial information (cf. Weber, 2023, pp. 292–303).

Conclusion and implications

Using a social network analysis can be beneficial for security authorities and researchers. It enables the identification, visualisation and assessment of relationships and structures within a network, helping to uncover hidden support systems, trace flows of information and resources, and improve inter-agency communication, for example, by exploring links between organised crime and the financing of terrorism.

Numerous studies have demonstrated the practical benefits of applying social network analysis in counterterrorism contexts. Krebs (2002), for example, revealed the structural vulnerabilities of the 11 September al-Qaeda network and showed how information sharing across agencies could generate a more comprehensive understanding of potential threats – an observation that remains highly relevant today. Similarly, Koschade (2006) and Magouirk et al. (2008) illustrate how the disruption of key intermediaries can significantly reduce an organisation's operational capacity. In a European context, Bakker (2006) and Sageman (2004, 2008) highlighted the decentralised but resilient structure of jihadist networks, informing strategies that prioritise disruption over dismantlement. More recent research in Germany (Weber and Hamachers, 2020; Weber, 2023) applied social network analysis to court records of foreign terrorist fighters from Germany and their connections to ISIS, revealing radicalisation and recruitment strategies, and the pivotal role of radical preachers. Collectively, these studies underscore the continued value of

([114]) Number of connections.
([115]) For more information about criminally relevant actions of P4, see Weber (2023).

social network analysis for identifying key actors, mapping hidden infrastructures and designing targeted prevention and disruption strategies in the fight against terrorism.

Social network analysis reveals the underlying social structures that shape (inter)actions among individuals within terrorist networks and provides insights into the overall behaviour and dynamics of the network. It provides a deeper understanding of how a covert network operates, identifies significant key players and reveals how different members contribute in various roles to its persistence and growth. It also exposes the structural vulnerabilities of covert networks and provides strategies to target critical points, enabling their disruption or even complete dismantling. By pinpointing and targeting key players, analysts can disconnect actors and subnetworks from the network's core and its strategically relevant members. This approach disrupts the flow, exchange and dynamics of information and can ultimately fragment the network. However, because networks are inherently dynamic and adaptive, other members may quickly replace removed actors. Future research should therefore focus on monitoring structural changes over time to detect reconfigurations after interventions and anticipate new or renewed mobilisation efforts, especially on social media ([116]).

Another benefit of applying social network analysis lies in its ability to enhance understanding of recruitment strategies and processes. Specifically, how individuals become integrated into radical milieus and, consequently, into broader networks (e.g. Weber, 2023). Such insights enable the development of more effective prevention and counterterrorism strategies. To leverage these capabilities effectively, security agencies need continuous training in social network analysis, expertise in managing big data and access to advanced analytical software tools. Recent developments in Horizon 2020 projects, such as Appraise (facilitating public and private security operators to mitigate terrorism scenarios against soft targets) ([117]) (European Commission, 2021), demonstrate how the integration of new technologies, including AI-supported network analytics and automated risk assessment frameworks, can further enhance the detection, monitoring and disruption of terrorist networks.

However, one limitation of this approach lies in the exclusive consideration of 'next neighbours' when assessing risk. Focusing only on direct connections may overlook indirect relational pathways through which information, resources or influence circulate within terrorist networks. Future analyses should therefore consider higher-order connections to capture the broader structural risks embedded in indirect ties.

References

Arsenault, A. (2011), 'Networks: The technological and the social', in Delanty, G. and Turner, S. (eds) *Handbook of Contemporary Social and Political Theory*, Routledge, London, pp. 259–269.

Appraise Consortium (2024), "Appraise achievements – Plot summaries and key results', Horizon 2020 Research and Innovation Programme (grant agreement No 101021981), https://appraise-h2020.eu/sites/default/files/2024-02/APPRAISE %20Brochure %20 %28website %29.pdf.

([116]) When using social media data for network analysis, researchers must be aware of legal restrictions and data protection regulations, including the safeguarding of personal rights and privacy.

([117]) Appraise (Horizon 2020 project, grant agreement No 101021981) develops AI-driven analytics and collaborative decision-support tools to strengthen counterterrorism capabilities and protect public spaces across Europe (cf. European Commission, 2021; Appraise Consortium, 2024).

Bakker, E. (2006), *Jihadi Terrorists in Europe – Their characteristics and the circumstances in which they joined the jihad: An exploratory study*, Netherlands Institute of International Relations Clingendael, The Hague.

Bastian, M., Heymann, S. and Jacomy, M. (2009), 'Gephi: An open-source software for exploring and manipulating networks', in: *Proceedings of the Third International AAAI Conference on Weblogs and Social Media* (ICWSM'09), AAAI Press, San Jose, pp. 361–362.

Chau, M. and Xu, J. (2007), 'Mining communities and their relationships in blogs: A study of online hate groups', *International Journal of Human-Computer Studies*, Vol. 65, No 1, https://doi.org/10.1016/j.ijhcs.2006.08.009.

European Commission (2021), 'Appraise: fAcilitating Public and Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts', European Commission website, https://cordis.europa.eu/project/id/101021981.

European Parliament and Council of the European Union (2017), Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, p. 6, ELI: http://data.europa.eu/eli/dir/2017/541/oj).

Federal Ministry of Justice (Germany) (2025), German Criminal Code (Strafgesetzbuch, StGB), https://www.gesetze-im-internet.de/stgb.

Federal Office for the Protection of the Constitution (no date), Daten und Fakten, https://www.verfassungsschutz.de/DE/themen/islamismus-und-islamistischer-terrorismus/zahlen-und-fakten/zahlen-und-fakten_node.html#doc678982bodyText4.

Fruchterman, T. M. J. and Reingold, E. M. (1991), 'Graph drawing by force-directed placement', *Software: Practice and Experience*, Vol 21, No 11, pp. 1129–1164, https://doi.org/10.1002/spe.4380211102.

Fuhse, J. (2016), *Soziale Netzwerke: Konzepte und Forschungsmethoden*, 1st Kindle edition, UVK Verlagsgesellschaft mbH, Konstanz.

Glaser, B. G. and Strauss, A. L. (1967), The Discovery of Grounded Theory, Aldine, Chicago.

Koschade, S. (2006), 'A Social Network Analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence', *Studies in Conflict and Terrorism*, Vol. 29, pp. 559–575.

Krebs, V. E. (2002), 'Mapping networks of terrorist cells', Connections, Vol. 24, No 3, pp. 43–53.

Magouirk, J., Atran, S. and Sageman, M. (2008), 'Connecting terrorist networks', *Studies in Conflict and Terrorism,* Vol. 31, No 1, pp. 1–16, https://doi.org/10.1080/10576100701759988.

Mayring, P. (2015), *Qualitative Inhaltsanalyse: Grundlagen und Techniken*, 12th edition, Beltz Verlag, Weinheim.

Medina, R. M. (2014), 'Social Network Analysis: A case study of the Islamist terrorist network', Security Journal, Vol. 27, No 1, pp. 97–121, https://doi.org/10.1057/sj.2012.21.

Mullins, S. (2013), 'Social network analysis and counter-terrorism: Measures of centrality as an investigative tool', *Behavioral Sciences of Terrorism and Political Aggression*, Vol. 5, No 2, pp. 115–136, https://doi.org/10.1080/19434472.2012.718792.

Sageman, M. (2004), *Understanding Terror Networks*, University of Pennsylvania Press, Philadelphia.

Sageman, M. (2008), *Leaderless Jihad: Terror networks in the twenty-first century, University of Pennsylvania Press, Philadelphia*.

Salloum, R. (2014), 'Rekruten für den Islamischen Staat: Die Weltkarte des Terrors', *Der Spiegel*, 28 November, https://www.spiegel.de/politik/ausland/is-islamischer-staat-zehntausende-auslaendische-kaempfer-machen-mit-a-1001193.html#bild-e3b6d3b3-0001-0004-0000-000000782535.

Strauss, A. and Corbin, J. (1996), *Grounded Theory: Grundlagen Qualitativer Forschung*, Beltz Verlag, Weinheim.

United Nations Security Council (2001), Resolution 1373 (2001), Adopted by the Security Council at its 4385th meeting, on 28 September 2001, United Nations, https://undocs.org/S/RES/1373(2001).

United Nations Security Council (2014), Resolution 2178 (2014), Adopted by the Security Council at its 7272nd meeting, on 24 September 2014, United Nations, https://undocs.org/S/RES/2178(2014).

Wasserman, S. and Faust, K. (1994), *Social Network Analysis: Methods and applications*, Cambridge University Press, Cambridge, https://doi.org/10.1017/CBO9780511815478.

Weber, K. (2023), *Islamistischer Terrorismus in Deutschland: Analyse der Täterprofile deutscher Syrienrückkehrer auf Basis von Gerichtsakten*, Springer, Berlin, https://doi.org/10.1007/978-3-658-42830-3.

Weber, K. and Hamachers, A. (2020), 'Aus dem radikalen Netzwerk in den Jihad: Radikale Prediger als Schlüsselakteure im Umfeld deutscher Syrienreisender', in: Hamachers, A., Weber, K. and Jarolimek, S. (eds), Extremistische Dynamiken im Social Web: Forschungsbefunde zu den digitalen Katalysatoren politisch und religiös motivierter Gewalt, Verlag für Polizei und Wissenschaft, Frankfurt am Main, pp. 225–270.

Risk of mafia infiltration abroad

Marco Garofalo, Cristian Maffongelli, Fabrizio Sbicca, Luca Turchi,

Giovanni Nicolazzo, Marco Dugato, Alessandra Porcu, Francesca Basso

https://doi.org/10.3013/7v3b9n17

Abstract

As part of the European multidisciplinary platform against criminal threats, the Central Operations Service of the Central Anticrime Directorate of the Italian National Police led an operational action focused on the priority 'high risk criminal networks'.

The action was carried out in partnership with the Joint Research Centre on Innovation and Crime of the Università Cattolica del Sacro Cuore ([118]) and with the participation of the Guardia di Finanza and the Anti-mafia Investigative Directorate, along with the support of the European Union Agency for Law Enforcement Cooperation (Europol). It was designed to test the possibility of indexing the risk of mafia infiltration abroad on the basis of specific 'indicators' shared with the participants ([119]) by the various Italian institutional stakeholders called upon to contribute to the project.

The analysis, which is innovative and based on the expertise acquired by Italy in the fight against the mafia, has therefore provided an interesting overview, resulting from the comparison between the contextual findings developed by the university and the in-depth studies on the subjects carried out by the investigative agencies involved (National Police, Guardia di Finanza and the Anti-mafia Investigative Directorate).

([118]) Transcrime is the joint research centre on innovation and crime of the Università Cattolica del Sacro Cuore, the Alma Mater Studiorum Università di Bologna and the Università degli Studi di Perugia (www.transcrime.it).

([119]) Participants took part in the project by filling in a questionnaire specially developed in consultation with the university.

The findings of the study, summarised in a series of charts, are therefore the result of a productive interaction established at an international level and provide useful insights into the need to create stable forms of information exchange and analysis that can enhance the ability to prevent and combat mafia infiltration.

1. The start of the project

The aim of the project is to measure the extent of mafia infiltration abroad, without taking into account the parameters of classic 'sentinel crimes' (extortion, damage, etc.) or, rather, profit-oriented crimes (drug trafficking, etc.) that traditionally characterise mafia operations.

These crimes are difficult to interpret in contexts lacking an awareness of the issue at the regulatory and investigative levels or cannot always be clearly attributed to a single mafia organisation, given the cross-cutting nature of the interests that often characterise the behaviour of 'brokers' in drug trafficking.

To this end, and with the aim of encouraging participants to reflect on the ability of mafias to infiltrate foreign economies, we wanted to investigate whether domestic organised crime groups could have launched targeted business initiatives in countries other than Italy based on 'reinvestment' or capitalisation of resources, thereby also acquiring a (potential) ability to distort the regular competitive mechanisms of the market (Savona and Riccardi, 2015; Pinotti, 2015; UNICRI, 2016).

A first explanatory meeting was therefore organised and held in Rome on 1 December 2022. At the meeting, the main characteristics of the mafia network were brought to the attention of the representatives of the countries participating in the project, with the valuable contribution of qualified speakers from the National Anti-Corruption Authority, the Financial Intelligence Unit of the Bank of Italy and the Customs and Monopolies Agency.

At the same meeting, the characteristics and peculiarities of the analytical approach characterising the contribution of the Joint Research Centre on Innovation and Crime of the Università Cattolica del Sacro Cuore (UCSC-Transcrime) were also presented.

1.1. The mafia network: characteristics

Unique features of Italian legislation were the starting point for describing the relational and organisational characteristics of the mafia organisation.

To this end, the characteristics of Article 416 bis of the Italian Criminal Code were highlighted, recalling the elements qualifying a criminal organisation as 'mafia-type'.

In this regard, the traditional mafia sources of income (drug trafficking, extortion and usury) were highlighted and the various reasons that may foster the need or the opportunity for this type of organised crime group to extend its business abroad were highlighted, along with its ability to establish links with professionals and/or trusted individuals that can facilitate its infiltration and/or its entrenchment in the economic and business network (Paoli, 2003; Varese, 2011; Calderoni et al., 2016).

It was pointed out how the diversification of relationships allows the organisation to gain credibility in a specific territory, thanks to its ability to find solutions that avoid the slowness and complexity of bureaucracy (Varese, 2011; Paoli, 2003).

In this context, the characteristics of the globalisation strategies adopted by the Cosa Nostra, Camorra and Apulian mafias were also presented, highlighting the impact of contextual factors (such as the socioeconomic, cultural and political–institutional factors) that may facilitate the globalisation of the mafias and favour the operation of the so-called *fattori di agenzia* (criminal skills, resources, social relations and organisational structure of the criminal organisation) (Varese, 2011; Calderoni et al., 2016).

1.2. The financial intelligence unit study: characteristics of the mafia enterprise

The analysis takes into account the work of Marco De Simoni (2022). The aim of this study is to investigate the infiltration of legitimate businesses by the mafia and the resulting financial profile of criminal firms. De Simoni addresses some of the shortcomings of the existing economic literature in the field (namely, uncertainty regarding the unlawful nature of the businesses analysed, and the limited geographical span) by relying on a unique sample of 237 firms that were seized by the judiciary as part of organised-crime-related prosecutions and are located in most Italian regions (De Simoni, 2022).

He identifies four different types of infiltrated firms and focuses on the two most common ones: 'investment firms' (used as conduits to invest illicit proceeds through legal activities) and 'competition firms' (which are run to gain control of the market of interest, deploying mafia methods to harm competitors) (De Simoni, 2022).

Overall, De Simoni finds that infiltrated firms, despite their higher revenues compared with legal businesses, appear to be less profitable, as they may be pursuing goals other than mere economic performance. Moreover, while all criminal firms feature low inventory levels, investment firms have a larger stock of tangible assets than competition firms, which prefer relying on leased facilities and equipment. That may be because competition firms are more at risk of detection and consequently adopt appropriate strategies to reduce any harmful consequences from potential seizures by law enforcement. Both classes of criminal firms also feature larger cash holdings than non-infiltrated firms in order to have more readily disposable assets in case of detection. Financing costs are lower for competition firms and higher for investment firms when compared with the control sample. Finally, some evidence shows that competition firms have higher costs of labour, suggesting that they may be providing job opportunities to local people and associates so as to gain support for the criminal organisation (De Simoni, 2022).

1.3. Corruption in public procurement: alerts and risk of mafia infiltration

Corruption is considered one of the main obstacles to positive economic, political and social development in various countries, due to higher transaction costs, barriers to entrepreneurship, limited access to finance, resource misallocation and so on (OECD, 2016; Decarolis and Giorgiantonio, 2020).

The specificity of this phenomenon, which appears latent and elusive by its very nature, prevents its clear and accurate measurement and, consequently, a precise understanding and awareness of its real impact on national economies and social systems (Decarolis and Giorgiantonio, 2020).

Cases of corruption that we learn about (e.g. through judgments) represent just the tip of the iceberg, making it difficult to understand the size and characteristics of the submerged parts of the phenomenon.

As a matter of fact, at an international level we observe a profound lack of structured scientific data on corruption that makes it difficult to go beyond a 'surface-level work' or some *ad hoc* work, which is certainly very interesting and full of ideas, but whose contents and results are difficult to extrapolate (Fazekas et al., 2016; Decarolis and Giorgiantonio, 2020).

Corruption is a multidimensional phenomenon influenced by numerous variables, and this characteristic was also confirmed by the analysis of public procurement data. It was observed that public procurement data do not always follow unambiguous trends at the territorial and sectoral levels, thus highlighting the complex dynamics presumably related to the different ways in which corruption can occur (Fazekas et al., 2016; Decarolis and Giorgiantonio, 2020).

1.4. Mafia operations in the gaming and betting sector

The role of the Italian gaming regulator, the Customs and Monopolies Agency (ADM), is fundamental to the gaming sector for the purpose of monitoring games in order to prevent and fight crime, to protect the community and to safeguard risk-exposed individuals.

Throughout the years, the ADM has developed a set of analytical tools for monitoring games in real time. Moreover, the ADM's employees are qualified judicial police officers; therefore they are entitled to lead criminal investigations.

Data analysis of gaming accounts and investigation activities, carried out together with the National Police, show a significant involvement of criminal groups in gaming, especially through organised crime groups (OCGs). Such involvement consists of managing the illegal gambling market through non-authorised operators and controlling gambling shops in the land-based network (Savona and Riccardi, 2017; UNODC, 2021; Europol, 2025).

The cooperation between the ADM and the National Police has been crucial in combating illegal activities and in protecting the market and its players.

1.5. The questionnaire developed by the Central Operations Service and by UCSC-Transcrime

During a meeting held in Rome on 1 December 2022 aimed at explaining the characteristics of mafia operations in the business sector and the scope of the phenomenon of corruption, especially in the field of public procurement, the Central Operational Service (SCO) and UCSC-Transcrime explained the structure of the questionnaire specifically designed to encourage the necessary interaction between the participants in view of the subsequent analysis phase.

UCSC-Transcrime ensured the prior identification of companies – located in the countries involved in the project – that met the two criteria established during the planning phase, namely:

- companies whose managers and/or beneficial owners were born in Sicily, Campania or Apulia, where some of the Italian mafia organisations are historically rooted;

- companies operating in the earth-moving, catering or gaming and betting sectors, traditionally controlled by the mafia and considered, according to investigative experience, to be more profitable for money laundering (Savona and Berlusconi, 2015; Savona and Riccardi, 2015, 2017).

The list of legal entities meeting the above criteria was then sent to the participants, via Secure Information Exchange Network Application messages, so that each representative could select at least three companies considered to be potentially at risk, including on the basis of the information shared during the meeting. The questionnaire requested specific detailed information on each reported company: the full personal details of managers and/or beneficial owners, data to be further investigated by Italian law enforcement agencies, and some background data, relating to the business sector ([120]), to be further studied by UCSC-Transcrime.

Data collection started in January 2023 and was completed in September 2023. The subsequent analysis phase began in September 2023 and ended in December 2023.

2. The sample of examined companies

As mentioned above, the sample of legal entities provided by USCS-Transcrime to the participants relates to the following business sectors:

- catering,
- earth moving,
- gaming and betting.

Participants were asked to report companies considered to be potentially at risk of mafia infiltration, whose managers and/or beneficial owners were of Italian origin and native to the regions of Campania, Apulia and Sicily.

Based on the data obtained through the questionnaire, and taking into account the legal restrictions that did not allow the Netherlands ([121]) to provide the requested data, the sample of companies analysed consists of a total of 59 legal entities (companies). The analysis of the different legal entities reported to the action leader initially revealed a preference for the catering and earth-moving sectors, the latter including building construction and the material transport sector.

([120]) These include the company's annual turnover, percentage of funds allocated, shareholdings in other companies, percentage of taxation based on income, average start-up time, etc.

([121]) The only exception is the Netherlands, where judicial regulations do not allow the acquisition of sensitive data except for limited investigative activities, upon authorisation of the judicial authority.

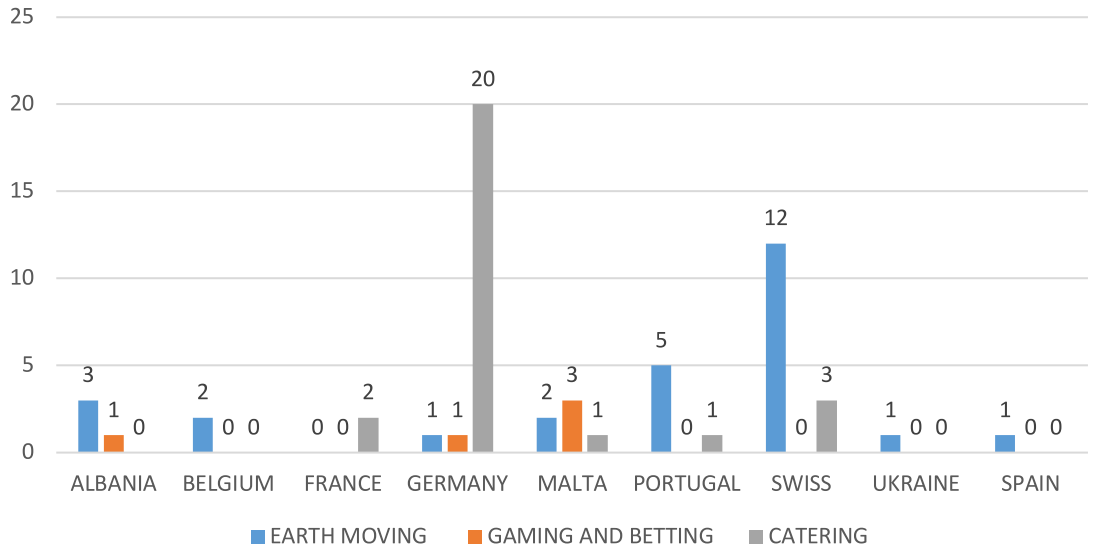


Figure 16.1. Number of companies by sector and country

The data show that the northern European countries are mainly focused on the catering sector, while the central and southern European participants are mainly interested in the earth-moving sector.

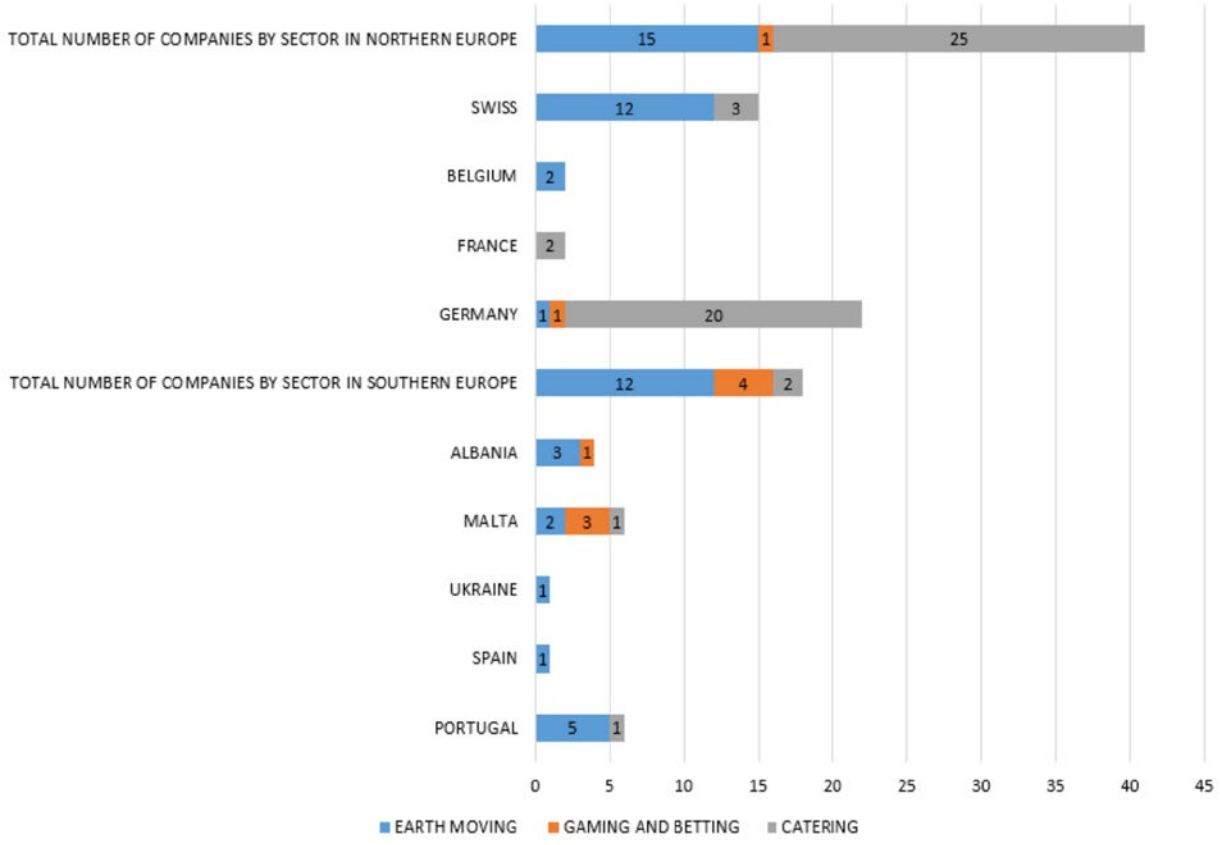


Figure 16.2. Companies by geographical area

3. The analysis process

3.1. The Central Operational Service's approach: method and procedures

The processing method proposed by the SCO of the National Police stems from a series of subjective and objective in-depth analyses based on a complex and multifactorial approach (Savona and Berlusconi, 2015; Bosisio et al., 2021).

To this end, the professional skills of the national law enforcement agencies (LEAs) that joined the operational action – the Anti-mafia Investigative Directorate (DIA) and the Guardia di Finanza Servizio Centrale di Investigazione sulla Criminalità Organizzata – have been duly used, taking advantage of the specific expertise of both investigative agencies.

At the same time, the National Police set up 43 investigative units at the National Police headquarters of the provinces where the subjects involved in the management of or owning the investigated businesses were residing. These subjects included third parties in the corporate structure, even when they did not come from the three regions under consideration (Campania/Sicily/Apulia).

In particular, the analysis provided by the territorial investigative bureaus was based on a series of indicators, developed by the SCO, aimed at analysing individual targets in depth in the following frameworks.

A) Relationships

1. Family relations with organised crime group members (limited to relatives and/or second-degree relatives by marriage).
2. Police checks in which the subject was found together with people who have police records (it is necessary to specify whether they are organised crime group members or connected to organised crime, or whether they have previous records of a different nature).
3. Police checks showing the subject's regular presence in Italy (checks on the owners of the vehicles possibly in use are necessary).

B) Judicial framework

1. Previous records in the LEAs database.
2. The target appeared in judicial contexts.

C) Working/professional framework

1. National Social Security Institute data (work history and area of employment).
2. Chamber of Commerce data (any corporate positions or ownership of legal entities). In case of a positive finding, it is necessary to ascertain:

- the source of the registered capital, through the articles of incorporation;
- whether the registered and operational office really exists.

3. Income ascertained/declared in the past five years.

The subject's profile was then completed with the following.

D) Confidential information

1. Confidential sources.
2. Any mentions of the target in confidential correspondence.

E) Open sources

1. News reports.
2. Analysis of social media accounts (if public).

In this regard, in line with business processes based on a horizontal organisation approach – considered as better suited to a possible infiltration – we intended to carry out the analysis of the data acquired by fostering the equivalence of the targets examined, regardless of the role played in the corporate structures.

Each of the above items was therefore given a numerical value between 0 and 4, according to the principle of the 'reliability' of the source and data (i.e. previous records = 4, police checks proving a regular presence in Italy = 2).

It follows that the overall value attributed to each target is given by the sum of the scores expressed by each item, independent of discretionary factors that would expose the analysis to subjective evaluations (i.e. regardless of the nature and number of the target's police records, the risk factor would always be 4).

Consequently, each business's 'risk value' is the result of the average risk values of individual managers / beneficial owners of the company.

Based on the overall data, four risk categories were identified linked to 'threshold values' in a range between 0 and 23 (identified as the maximum value that is obtained when all risk factors would reach the maximum value).

Table 16.3. Example table

PAESE SOCIETA'	NOME SOCIETA'	SETTORE PRODUTTIVO	NOME SOCIO	A) AMBITO RELAZIONALE			B) AMBITO GIUDIZIARIO		C) AMBITO LAVORATIVO/PROFESSIONALE			D) NOTIZIE FIDUCIARIE		E) FONTI APERTE:		TOTALE INDICE	MEDIA ARITMETICA INDICE DI RISCHIO
				1. Relazioni familiari con esponenti della C.O. (limitata a parenti e/o affini di 2° grado)	2. Controlli del territorio con soggetti gravati da precedenti di polizia (specificando se si tratta di esponenti della C.O. – o ad essa contigui – ovvero se si tratta di precedenti di altra natura)	3. Controlli del territorio comunque sintomatici di un'assidua presenza in Italia (con verifica sui titolari dei mezzi eventualmente in uso).	4. Precedenti SDI	5. Emergenze da atti giudiziari	6. INPS (precedenti lavorativi e settore di occupazione)	7. CAMERA DI COMMERCIO eventuali cariche societarie o titolarità persone giuridiche)	8. Redditi censiti/dichiarati nell'ultimo quinquennio	9. Fonte confidenziale	10. Eventuali cenni a pregressi riferimenti con corrispondenza riservata.	11. Eventuali notizie di cronaca	12. Analisi profili social (qualora "aperti")		
BELGIO	NOME	EARTH MOVIE	COGNOME Nome	0	0	0	0	0	0	0	0	0	0	0	0	0	
			COGNOME Nome	0	0	0	0	0	0	0	0	0	0	0	0	0	
			COGNOME Nome	0	0	0	0	0	0	0	0	0	0	0	0	0	
			COGNOME Nome	0	0	0	0	0	0	0	0	0	0	0	0	0	
			COGNOME Nome	0	0	0	0	0	0	0	0	0	0	0	0	0	
			COGNOME Nome	0	0	0	0	0	0	0	0	0	0	0	0	0	
			COGNOME Nome	0	2	2	4	3	2	2	2	1	1	0	0	19	
			COGNOME Nome	0	2	2	4	0	2	2	2	0	0	0	0	14	
			INDICE DI RISCHIO													33	4,12
FRANCIA	NOME	CATERING	COGNOME Nome	2	2	2	0	3	0	0	0	0	0	0	2	11	
			COGNOME Nome	0	0	0	0	3	0	0	0	0	0	0	0	3	
			COGNOME Nome	0	0	2	0	0	2	0	2	0	0	2	2	10	
			COGNOME Nome	0	0	0	4	0	0	0	0	0	0	0	0	4	
			INDICE DI RISCHIO													28	7

Table 16.4. Threshold values identified by different colours

From 0 to 5	From 6 to 11	From 12 to 17	From 18 to 23
Low	Medium	High	Top

3.2. Transcrime processing

The present chapter includes the results of an analysis of a sample of companies performed by UCSC-Transcrime. The list of target companies to be analysed was provided to UCSC-Transcrime by the Direzione Centrale Polizia Criminale following actors in the operation action having been alerted to the companies and refers to companies believed to be infiltrated or controlled by Italian organised criminal groups ([122]).

Information about operational, financial and ownership characteristics of these target companies was collected by UCSC-Transcrime from the Orbis database by Bureau van Dijk using as input the company names, the countries of registration and, when available, the unique company identifiers (e.g. VAT (value added tax) code). This allowed UCSC-Transcrime to identify 42 of the 59 companies in the list (71 %). The remaining companies could not be uniquely identified and were consequently excluded from the analysis.

Starting from the collected information, a set of risk indicators was defined for each company, allowing the identification of the firms at higher risk of criminal infiltration or misuse for illicit purposes (Bosisio et al., 2021; FATF, 2023).

3.2.a. Selection of the relevant risk indicators

Initially, an extensive array of 466 risk indicators was considered and tested, including alternative specifications of the same indicator or variables regarding different aspects and characteristics of the companies ([123]) (Bosisio et al., 2021). The indicators belong to different risk dimensions, namely:

([122]) Excluding the 'Ndrangheta.

([123]) These risk indicators were developed by UCSC-Transcrime and its spin-off Crime&tech. Specifically, some of the analysis included in this report was produced using the Datacros tool, a real-time analytical platform developed by UCSC-Transcrime, and designed for (and hand-in-hand with) law enforcement agencies, anticorruption authorities, competition authorities and investigative journalists, to support the identification of companies at high risk of corruption, money laundering, tax fraud and financial crimes (for more information, see www.transcrime.it/datacros2).

1. ownership structure risk,
2. territorial risk,
3. anomalous features of key officers (e.g. very high/low age of owners or anomalous gender balance with respect to peers),
4. anomalous financial features (e.g. indicators of shell company activity),
5. adverse events,
6. political exposure.

Each indicator was attributed a value between 0 and 4, where 0 indicates a minimal difference of the recorded value from the average observed among companies in the same country and economic sector, and 4 a very large deviation. These indicators were calculated for all the companies in the sample and for a control group of active companies having similar characteristics ([124]). In particular, the control group was generated by randomly selecting for each company 10 other companies operating in the same statistical classification of economic activities sector and in the same country. As a result, a total of 354 companies were included in the control group ([125]).

The following tables show the number of target and control companies by country and economic sector (Table 16.5 and Table 16.6).

Table 16.5. Number or target and control companies by country

Country	Target	Control	Total
Albania	4	40	44
Belgium	2	20	22
Switzerland	14	109	123
Germany	8	69	77
Spain	1	10	11
France	2	20	22
Malta	6	42	48
Netherlands		1	1
Portugal	4	34	38
Ukraine	1	10	11
Total	42	354	396

([124]) Due to insufficient data, the calculation of risk scores was not possible for all companies. This issue arises from the incompleteness of Bureau van Dijk data regarding, for example, information on the ownership structure of the company or its financial variables.

([125]) The number of companies in the control group is slightly lower than 420 (i.e. 42 target companies multiplied by 10) because some companies were included in the control group for more than one target company operating in the same country and statistical classification of economic activities sector.

Table 16.6. Number or target and control companies by economic sector

Economic sector	Target	Control	Total
Construction	16	132	148
Wholesale and retail trade	6	51	57
Accommodation and food service activities	10	100	110
Gambling and betting activities	3	21	24
Other	7	50	57

From this preliminary assessment, a restricted set of 13 relevant risk indicators was selected following two main criteria: (a) including the indicators that allow us to better discriminate between the target and the control groups; (b) ensuring the presence of at least one indicator for each risk dimension. Table 16.7 summarises and describes the selected risk indicators (Bosisio et al., 2021).

Table 16.7. Selected risk indicators

Selected risk indicators	Dimension	Description
Vertical complexity	Ownership structure risk	Number of layers between a company and its beneficial owners (BOs)
Horizontal complexity – natural person	Ownership structure risk	Number of natural persons with direct or indirect ownership links with the company
Legal arrangements	Ownership structure risk	Number of legal arrangements at the end of the ownership structure that do not allow identification of BOs
Shareholding anomalies	Ownership structure risk	Number of shareholders with a shareholding percentage between 24.90 % and 24.99 %, namely just below the BO disclosure threshold
Active address	Territorial risk	Average of the risk scores associated with the number of other active companies registered at the same address as the target company and with the ratio of active companies on the total number of companies registered at the same address
Previous roles	Anomalous features of key officers	Number of roles previously held in other companies by the key officers of the company (considering the highest value among BOs, directors and shareholders)
BO old age	Anomalous features of key officers	Ratio of BOs who are 80 years old or older
Days for creditors	Anomalous financial features	The average time taken for the company to pay creditors as observed for the last five available periods

The mafia presence index

UCSC-Transcrime and its spin-off Crime&tech defined a composite indicator aiming at measuring the presence of Italian organised crime groups in all Italian municipalities. The index processes public information (provided by the DIA, National Anti-Mafia and Anti-Terrorism Directorate, Italian National Institute of Statistics, Ministry of the Interior and the Agenzia Nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata) and is inspired by the methodology developed by Transcrime for the analysis of the presence of the Italian mafias (Dugatoet al., 2020; Calderoni, 2011). Information included in the index regards evidence of the presence or activities of mafia groups and indicators of political and economic infiltration. Cross-checking this index with information about companies and their BOs or directors, it is possible to identify the companies operating or linked to high-risk Italian municipalities in terms of mafia presence or infiltration. This indicator is particularly helpful for identifying the potential risk of mafia infiltration into the legitimate economy outside the regions where mafias are traditionally present. In this project, the mafia index was used by UCSC-Transcrime at an early stage to identify a preliminary list of companies to be provided to the participants in order to assist in the identification of the target companies.

3.2.b. Definition of the overall risk score

The overall risk score is defined as a composite indicator following the methodology developed by UCSC-Transcrime in previous research (Bosisio et al., 2021). Each risk indicator is attributed to a specific risk dimension. In particular, the exposure dimensions include the risk indicators related to:

- ownership structure risk,
- territorial risk,
- key members' anomalous features,
- anomalous financial features,
- adverse events.

The vulnerability dimension corresponds to the risk indicator related to:

- political exposure.

For each dimension, an aggregated risk score is defined. Then, the overall risk score is the result of the weighted average of those dimensions' risk scores. The score for the risk elements is increased in relation to the exposure elements and further raised in relation to the vulnerability elements. When a company has the same exposure components but different indicators of vulnerability, the company in a more vulnerable context will present a higher overall risk. If a company has maximum risk in all core exposure components, the overall risk will be the highest, regardless of the vulnerability of the environment. Conversely, if only the environment is vulnerable, but the company does not present any exposure components, the overall risk will be 'lower' (Bosisio et al., 2021; FATF, 2023).

The overall risk value is translated into four classes: low, medium, high, very high.

3.2.c. Results of the UCSC-Transcrime risk analysis

By aggregating the values of the different risk dimensions, it is possible to identify 4 companies at very high risk out of the 42 indicated by the participants in the operational action, while the majority of these companies (67 %) are categorised as companies at high risk (Figure 16.1) ([126]).

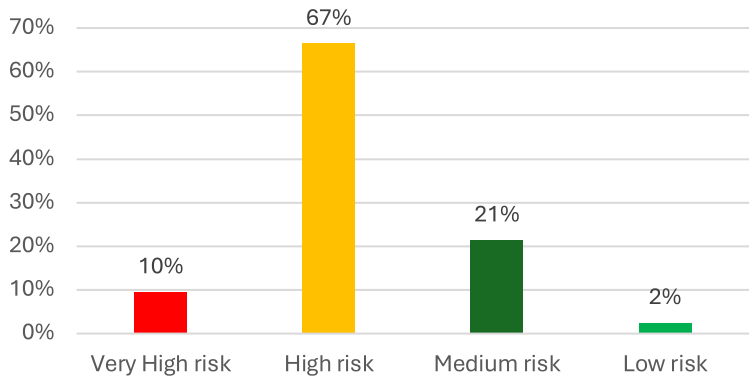


Figure 16.3. Percentages of the target companies by overall risk value

However, considering the scores of the single risk indicators, it emerges that 26 companies out of 42 (62 %) show high risk values (3 or 4) for one risk indicator and 11 (26 %) show a high risk value for at least two different risk indicators. These percentages are about double the ones recorded in the control group (37 % and 14 %, respectively). This suggests the presence of different profiles/types of infiltrated companies that may be better captured by focusing on specific risk dimensions separately (Table 16.9).

([126]) UCSC-Transcrime has diligently and professionally collected the data and information necessary to produce this report, according to the rules of the Italian Civil Code without any obligation of result. The information contained is provided on an 'as is' basis, without warranties of any kind. The user of this report acknowledges that the information communicated to UCSC-Transcrime may be incomplete and may not contain unique identifiers (e.g. date of birth, tax code, VAT number, Chamber of Commerce registration number or equivalent). UCSC-Transcrime does not take any responsibility for cases of homonymy resulting from the absence of such information. The information contained in the reports provided by UCSC-Transcrime should in no case be interpreted as definitive evidence of infiltration of organised crime, money laundering or any type of illegal conduct from a specific company or any connected individual and/or entity. Under no circumstances will UCSC-Transcrime be liable to any person or legal entity for any loss, damage, cost, expense or any other damage connected to any error (due to negligence or other cause), or any other circumstance under or outside the control of UCSC-Transcrime, in relation to the acquisition, collection, elaboration, analysis, interpretation, communication, publication or delivery of any information.

Table 16.4. Number of target companies by risk score for each risk indicator and risk dimension

		Risk score					
		0 (minimum)	1	2	3	4 (maximum)	Data not available
Risk indicators	Vertical complexity	8	12	4	4	1	13
	Horizontal complexity – natural person	16	7	2	3	1	13
	Legal arrangements	28	0	0	0	1	13
	Shareholding anomalies	27	0	0	0	2	13
	Address active	4	3	21	12	0	2
	Previous roles	9	16	8	5	4	0
	BO old age	25	0	0	0	2	15
	Days for creditors	4	2	2	3	1	30
	Financial exposure ratio (standard deviation)	6	0	0	2	0	34
	Fixed asset ratio (standard deviation)	3	6	0	3	1	29
	Personnel expenses on revenue (standard deviation)	5	0	3	1	0	33
	Leaks	33	3	1	0	5	0
	Local administrators	40	1	0	0	1	0
Risk dimensions	Ownership structure risk	6	9	10	4	0	13
	Territorial risk	4	3	21	12	0	2
	Anomalous features of key officers	9	8	18	4	3	0
	Anomalous financial feature	3	1	4	6	2	26
	Adverse events	33	3	1	0	5	0
	Political exposure	40	1	0	0	1	0

Comparing the values of the selected risk indicators calculated for the target companies and the ones estimated for the control group, some distinctive characteristics of the target companies emerge (Figure 16.2).

— **Key officers.** Target companies are 12.9 times more likely to have a high number of elderly beneficial owners. Furthermore, their key individuals are 1.7 times more likely to have been involved in many other companies before.

— **Ownership structure.** Target companies are about 2 times more likely to have complex ownership structures, with more ownership layers between the company and its BOs (vertical complexity) and more

individuals with direct or indirect ownership links with the company (horizontal complexity). Furthermore, target companies are 2.3 times more likely to have more ownership links with opaque legal arrangements (e.g. trust, fiduciaries, funds). Finally, they are 2.8 times more likely to have a high number of shareholders with a shareholding percentage just below the BO disclosure threshold.

— **Territorial risk.** Target companies are about 2.1 times more likely to have a higher number of other active companies registered at the same address.

— **Financial features.** Target companies are about 3 times more likely to take more days to pay creditors and to have a higher variability in their financial exposure. These companies are also 1.9 times more likely to have a higher variability in human resources expenses as a percentage of revenues and 1.6 more likely to have an inconsistent fixed asset ratio, which indicates a higher volatility of the company.

— **Political exposure.** Target companies are more likely to have a public administrator among owners or directors of the company.

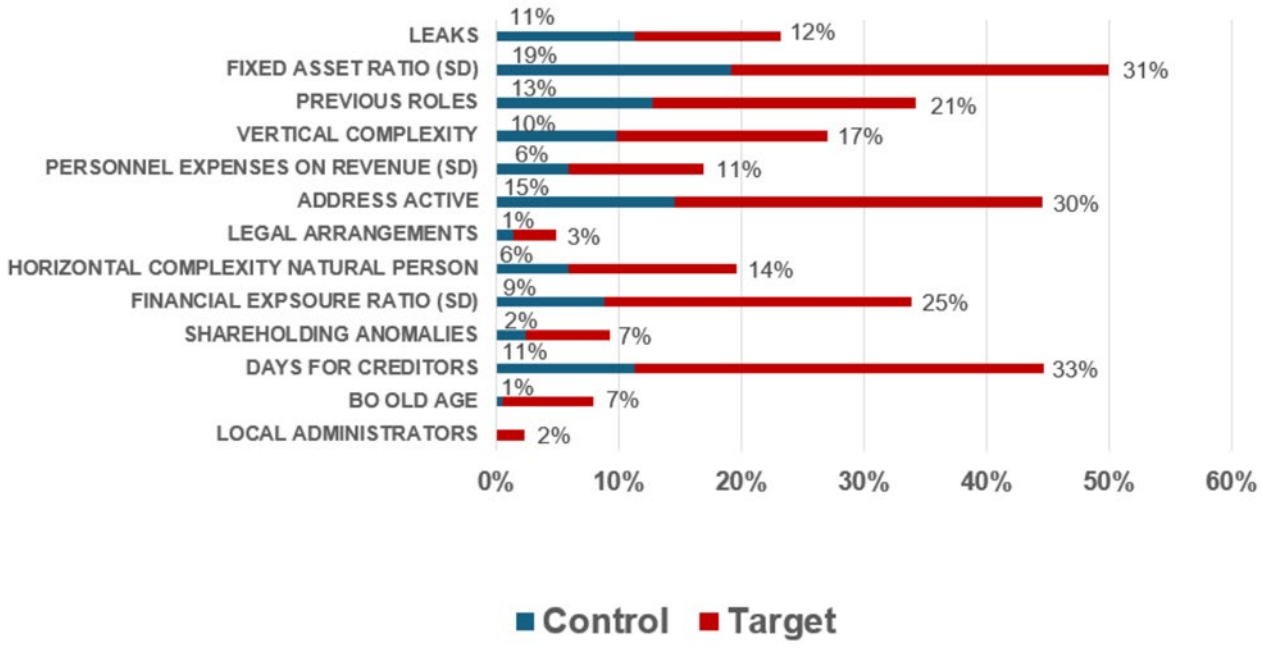


Figure 16.5. Percentages of companies at high or very high risk for each risk indicator among the target companies and in the control group

The results of the study

Firstly, it can be observed that the participants' choices seem to be at least partly influenced by past investigations carried out in the reference countries.

In this respect, we can observe, for example, how Germany – already concerned by the well-known investigations following the Duisburg massacre and the police operation known as Brodo Pollino – preferred to report several catering activities already reported as being carried out by Italians. Similarly, Malta focused its reports on the gaming sector, which had already been the subject of several investigations involving the Italian subjects.

With regard to the composition of the legal entities examined, it was established that in 35.60 % of the cases the companies are managed/owned by individuals from the same region.

In particular:

- 8.48 % of the companies are solely managed/owned by individuals from Campania;
- 11.87 % of the companies are solely managed/owned by individuals from Sicily;
- 15.25 % of the companies are solely managed/owned by individuals from Apulia;
- 44.07 % of the companies are solely managed/owned by individuals from the three regions mentioned above, together with nationals of the countries where the company is physically located;
- 20.33 % of the companies are managed/owned by individuals from the three regions mentioned above, together with third parties who apparently come from outside the state where the company is physically located. It should be noted that South American nationals (5 Brazilians and 1 Argentinian) participate in 50 % of companies.

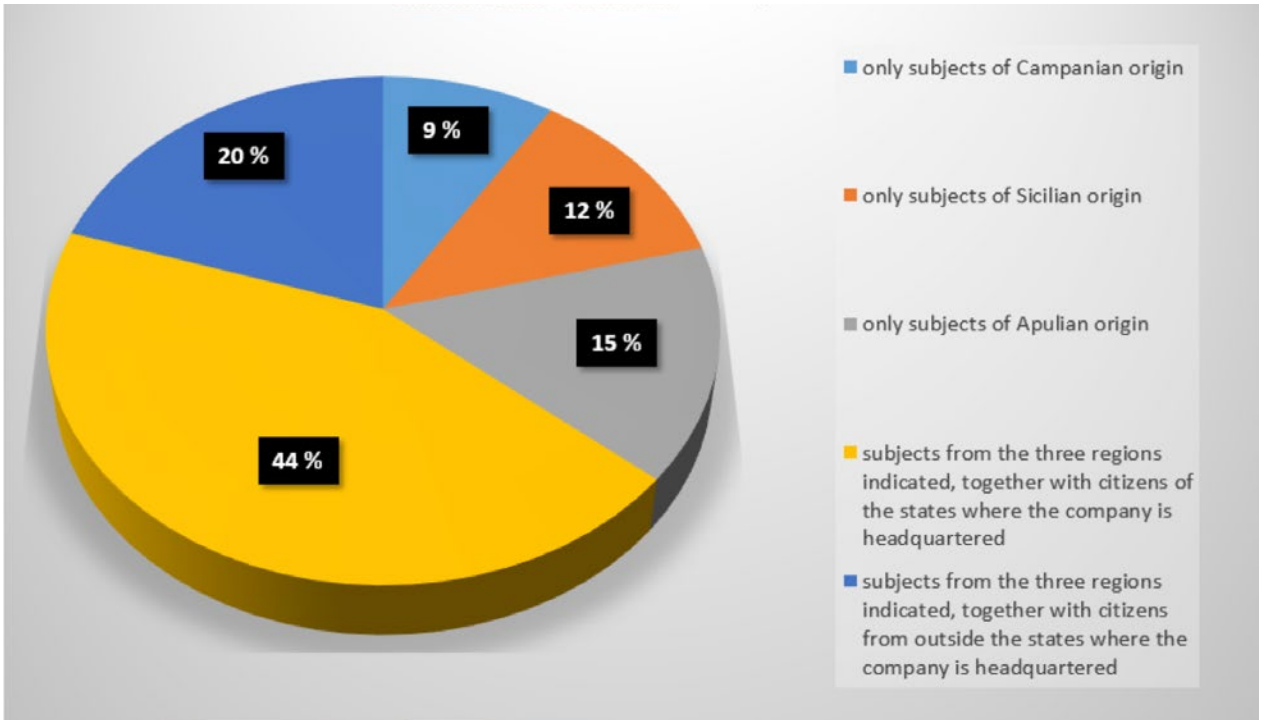


Figure 16.6. Managed/owned companies

Furthermore, it was established that:

- companies solely managed/owned by individuals from Campania prefer to operate in the catering and gaming and betting sectors;
- companies solely managed/owned by individuals from Sicily are active in the catering sector;

- companies solely managed/owned by individuals from Apulia are concentrated on the construction sector;
- companies managed/owned by individuals from the three regions mentioned above, together with nationals of the countries where the company is physically located, prefer operating in the catering sector;
- companies managed/owned by individuals from the three regions mentioned above, together with third parties who apparently come from outside the state where the company is physically located, mainly operate in the construction sector.

Finally, in terms of geographical distribution, it can be noted that:

- companies wholly or partly owned by individuals from Campania are mostly based in Germany;
- companies wholly or partly owned by individuals from Sicily are mostly based in Malta;
- companies wholly or partly owned by individuals from Apulia are mostly based in Switzerland;
- companies managed/owned by individuals from the three mentioned regions, together with foreign nationals, are mostly concentrated in Portugal.

Figure 16.7. Geographical distribution

On the basis of the analysis of the 59 companies reported by the participants, 169 subjects were profiled, divided by their geographical origin in the following chart.

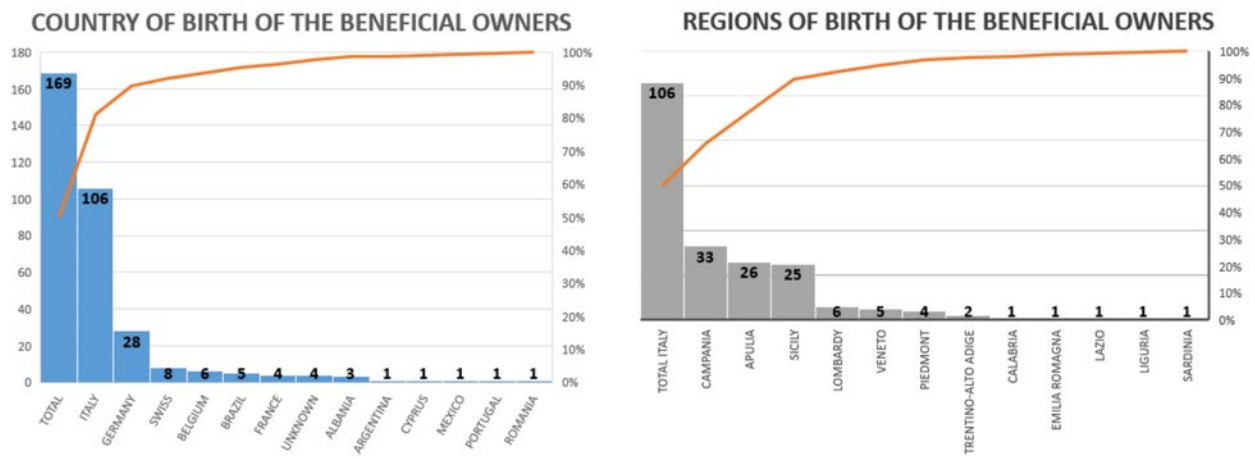


Figure 16.8. Country and regions of birth of the beneficial owners

With regard to this, the following is a preliminary regional projection by sector.

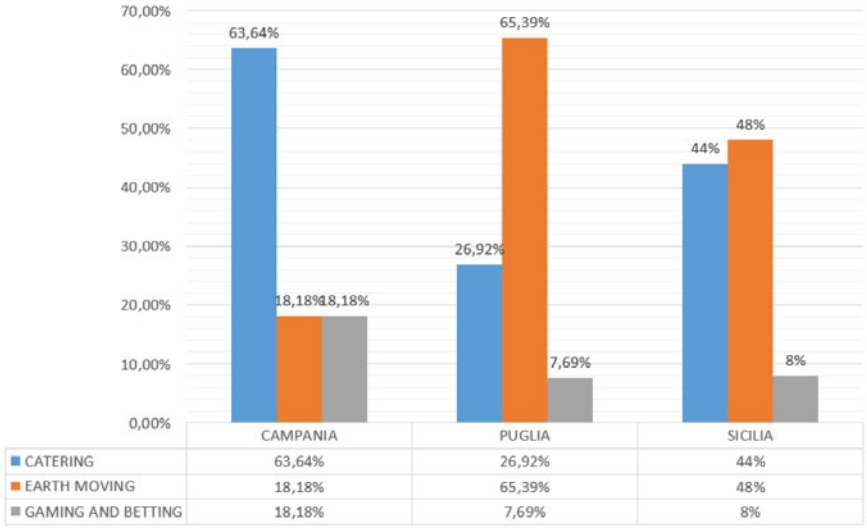


Figure 16.9. Sector by region

In this framework, checks on managers and beneficial owners revealed that an overall 21.30 % of subjects have previous police records in Italy.

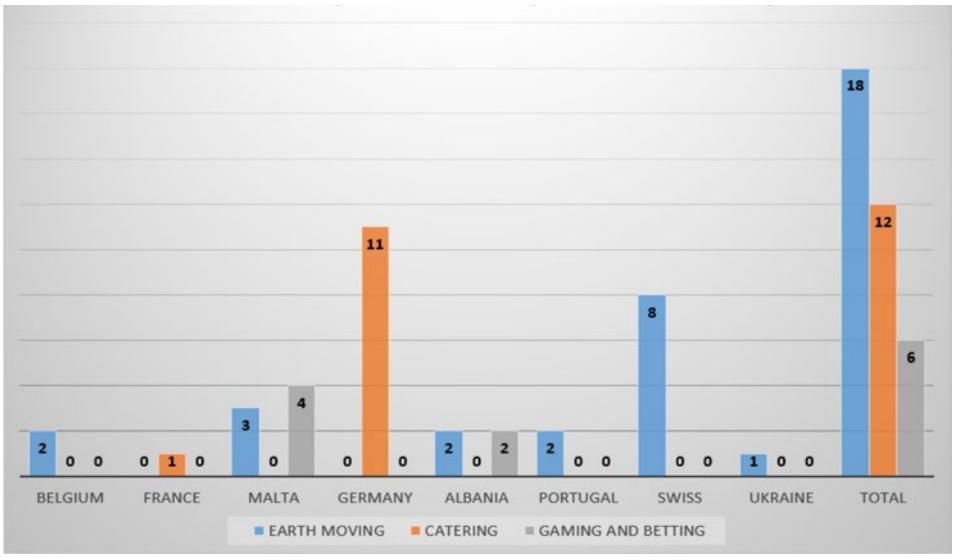


Figure 16.10. Incidence of police records by sector and country

19.44 % out of 21.30 % are involved in mafia-type conspiracy or other mafia crimes.

These companies operate in the following fields:

– 3 in the earth-moving sector;

– 3 in the catering sector;

– 1 in the gaming and betting sector.

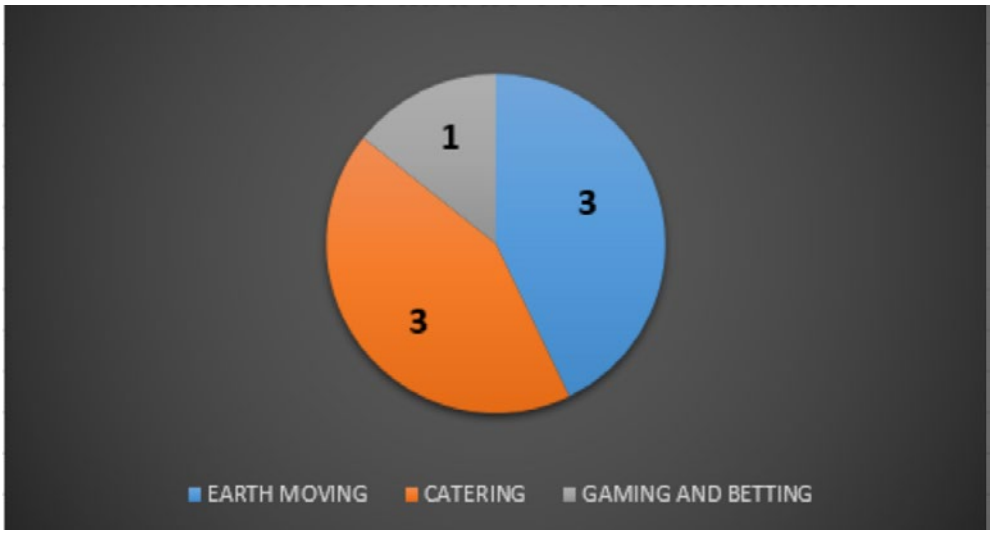


Figure 16.11. Incidence of mafia-type conspiracy

According to the above indicators, the companies in Figure 16.11 are within the following risk ranges.

High	Construction
High	Construction
Medium	Construction
Medium	Catering
Low	Catering
Low	Catering
Medium	Gaming and betting

Figure 16.12. Risk range by sector

The projection is then consistent with the potential risk of infiltration (by sector) revealed by the analysis.

On the other hand, it was found that 8.28 % of the subjects examined had kinship/connections with subjects having previous police records for mafia crimes.

In this case, the sectors concerned are the following.

Figure 16.13. Incidence of kinship with mafia members

Therefore, it follows that in the case of companies that are only indirectly linked to individuals with police records for mafia crimes, the potential risk (by sector) identified by the analysis does not match that of the companies owned by these individuals. In particular, the chart shows a greater interest in the catering sector, which actually has a low-risk potential. This figure suggests that these companies pursue a policy of prospective reinvestment, and that the choice to keep a low profile is related to the need to avoid investigations (and assets seizures).

The results of the study conducted by the SCO, taken as a whole, allowed us to draw up a preliminary figure showing the level of infiltration risk identified for each sector examined.

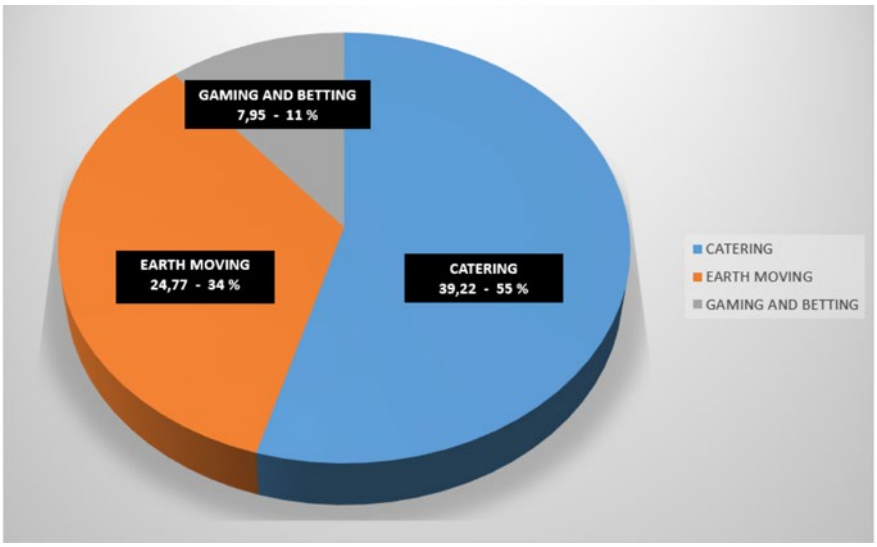


Figure 16.14. Risk index by sector

Furthermore, the comparative analysis of the findings with the checks conducted by the DIA and the Guardia di Finanza Servizio Centrale di Investigazione sulla Criminalità Organizzata allowed us to establish the following.

— In four cases, the companies subject to suspicious transaction reporting are included among those more at risk. In particular, the managers of the two companies more at risk (company 1 and company 2), have been subject to suspicious transaction reporting: the former in 2008, 2018 and 2019 and the latter in 2020, 2021 and 2022.

— Only 15.97 % of the 169 managers / beneficial owners included in the business structure of the 59 companies examined participate in other companies that mostly have the same corporate purpose as the target company.

— Lastly, 11.83 % of the managers / beneficial owners have at least one online gaming account.

Finally, the study also revealed a more than 50 % match between the top 10 at-risk companies identified by the SCO study and the Transcrime analysis. This also shows that the risk of mafia infiltration into the economy can be detected by the combination of subjective and objective factors.

Conclusions and practical implications

The exercise therefore highlighted the possibility of identifying companies at risk of mafia infiltration using a combined approach of both subjective and objective analysis factors (Savona and Berlusconi, 2015; Bosisio et al., 2021; Europol, 2021).

On this point, the data – limited to the framework of the analysis – confirm the involvement of individuals associated with or connected to Italian mafias in many foreign companies, taking advantage of the absence of preventive regulations that would require further investigation into the origin of the capital invested and the past of managers and partners of Italian origin.

The methodology, validated in the ongoing study by further results acquired on the potential interests of the 'Ndrangheta in the foreign economic network, therefore constitutes a valid basis to elevate the analysis technique to a prevention tool aimed at strengthening international cooperation in the fight against the globalisation of mafias (Calderoni et al., 2016; Varese, 2011; Europol, 2025).

This approach, which is useful for raising participants' awareness of the potential of traditional Italian organised crime groups, could also facilitate a process to develop a common definition of organised crime that also includes the hybrid threat posed by the mafia.

References

Bosisio, A., Carbone, C., Jofre, M., Riccardi, M. and Guastamacchia, S. (2021), Project Datacros – Developing a tool to assess corruption risk factors in firms' ownership structure: Final report, Transcrime and Università Cattolica del Sacro Cuore, Milan.

Calderoni, F., Berlusconi, G., Garofalo, L., Giommoni, L. and Sarno, F. (2016), 'The Italian mafias in the world: A systematic assessment of the mobility of criminal groups', European Journal of Criminology, Vol. 13, No 4, pp. 413–433, https://doi.org/10.1177/1477370815623570.

Decarolis, F. and Giorgiantonio, C. (2020), 'Corruption red flags in public procurement: New evidence from Italian calls for tenders', Questioni di Economia e Finanza (Occasional Papers), No 544, Bank of Italy, Rome.

De Simoni, M. (2022), 'The financial profile of firms infiltrated by organised crime in Italy', Quaderni dell'antiriciclaggio, Analisi e studi, No 17, Unità di Informazione Finanziaria per l'Italia, Bank of Italy, Rome.

Dugato, M., Calderoni, F. and Campedelli, G. M. (2020), 'Measuring organised crime presence at the municipal level', Social Indicators Research, Vol. 147, Np 1, pp. 237–261, https://doi.org/10.1007/s11205-019-02151-7.

Europol (European Union Agency for Law Enforcement Cooperation) (2021), European Union Serious and Organised Crime Threat Assessment – A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg.

Europol (2025), European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg.

FATF (Financial Action Task Force) (2023), Guidance on Beneficial Ownership of Legal Persons, Paris.

Fazekas, M., Tóth, I. J. and King, L. P. (2016), 'An objective corruption risk index using public procurement data', European Journal on Criminal Policy and Research, Vol. 22, No 3, pp. 369–397, https://doi.org/10.1007/s10610-016-9308-z.

OECD (Organisation for Economic Co-operation and Development) (2016), Preventing Corruption in Public Procurement, OECD Publishing, Paris.

Paoli, L. (2003), Mafia Brotherhoods: Organized crime, Italian style, Oxford University Press, New York.

Pinotti, P. (2015), 'The economic costs of organised crime: Evidence from Southern Italy', The Economic Journal, Vol. 125, No 586, pp. F203–F232, https://doi.org/10.1111/ecoj.12235.

Savona, E. U. and Berlusconi, G. (eds) (2015), Organized Crime Infiltration of Legitimate Businesses in Europe: A pilot project in five European countries – Final report of project ARIEL, Transcrime and Università degli Studi di Trento, Trento.

Savona, E. U. and Riccardi, M. (eds) (2015), From Illegal Markets to Legitimate Businesses: The portfolio of organised crime in Europe – Final report of project OCP, Transcrime and Università degli Studi di Trento, Trento.

Savona, E. U. and Riccardi, M. (eds) (2017), Assessing the Risk of Money Laundering in Europe – Final report of project IARM, Transcrime and Università Cattolica del Sacro Cuore, Milan.

UNICRI (United Nations Interregional Crime and Justice Research Institute) (2016), Organized Crime and the Legal Economy – The Italian case, Turin.

UNODC (United Nations Office on Drugs and Crime) (2021), Global Report on Corruption in Sport, Vienna.

Varese, F. (2011), Mafias on the Move: How organized crime conquers new territories, Princeton University Press, Princeton.

Innovative business modelling for understanding criminal networks and illicit markets

Ana Isabel Barros, Koen van der Zwet, Eldine Verweij, Louis Weyland

https://doi.org/10.3013/fqkj4c83

Abstract

Financial incentives serve as a primary motivator and enabler for organisations to engage in illicit activities, like drug trafficking. Such illicit activities often involve coercion and the use of violence. Drug trafficking, recognised as one of the most profitable criminal enterprises, also demonstrates extreme resilience and adaptability in the face of law enforcement interventions. Nonetheless, most law enforcement efforts focus primarily on disrupting the underlying logistics process and the associated criminal network.

To better capture the complexity and underlying dynamics of criminal organisations, insight is needed into the relationship between the criminal value chain (financial, logistical and social) and the impact of interventions over time. In this paper we illustrate how a computational system approach based on criminal business modelling can be used to create insight on the resilience of illicit markets. The explorative computational approach simulates how criminal organisations may adapt to different intervention strategies grounded in their underlying criminal business models. Its purpose is to stimulate critical reflection and support the development of more innovative and effective interventions.

Keywords: criminal networks, business modelling, modus operandi, critical thinking, double-loop learning.

Introduction

Criminal networks are often deeply embedded in society, seamlessly integrating illicit activities, such as drug trafficking, with legitimate operations, like investments in real estate (Dekkers, 2023) or sports (Europol, 2016). Moreover, drug trafficking is often accompanied by violence, threats and corruption, leading to a significant impact on society (Gerell et al., 2021; UNODC, 2024).

The activities of criminal networks are diverse and interconnected. For instance, drug trafficking requires a supply chain that encompasses production, transport and sales. Each of these activities is often entangled with corruption and/or intimidation (to facilitate production) and money laundering (to handle illicit proceeds). Additionally, criminal networks continuously try to stay under the radar by operating covertly and often in a decentralised manner. As a result, criminal networks are resilient (Ayling, 2009) and can adapt their modus operandi as a reaction to external factors such as law enforcement interventions. For instance, the interdiction of cocaine smuggling routes in Central America has led to adjustments in these routes to evade detection, as described by Magliocca et al. (2022). Another example of structural and functional changes in the criminal networks after law enforcement interventions can be found in O'Reilly et al. (2020). This yields a cat-and-mouse game between criminal networks and law enforcement, with both sides trying to outsmart each other.

In this sense, the embedding of criminal networks in society can be considered a complex adaptive system (Eidelson, 1997; Duijn et al. 2014). This complexity makes criminal networks resilient and challenging to disrupt. In fact, efforts to counter these criminal networks can also cause undesired effects like displacement (Magliocca et al., 2022) and even corruption (O'Reilly et al., 2020), retaliation and violence escalation. To cope with this inherent complexity, it is crucial to first analyse the system as a whole and in all its dimensions, logistical, social and financial, as highlighted by Spapens (2010). System analysis seeks to unveil the intricacies of a system, in all its dimensions, including its underlying components and interrelationships (Conger and Mason, 2013).

One component of the criminal system is the underlying financial drive. This is particularly true for organised criminal networks, as highlighted by Lotspeich (2000). Drug trafficking is particularly considered one of the most profitable criminal enterprises, as noted by May (2017). However, this perspective is often overlooked, even though criminal activities seek to make profit and rely heavily on investments, which are frequently funded by previous proceeds from other criminal activities. Recently, the need to consider more explicitly the financial aspect has been highlighted by, among others, Snaphaan and Ruitenburg (2024), Manzi and Calderoni (2024), Albanese (2023) and the Dutch Procureurs Office (Openbaar Ministerie, 2023). As suggested in Barros et al. (2024), the analysis of the criminal business model, which includes the financial, logistical and social dimensions of the criminal network, creates new insights into how these networks will adapt to protect their operations when facing law enforcement interventions. The need to develop computational models to simulate this resilience is also emphasised, promoting critical thinking to support the development of effective interventions capable of disrupting criminal networks over the long term. Van der Zwet et al. (2025) proposed an agent-based model to understand how opportunistic behaviour in criminal groups contributes to the adaptive capacity of illicit supply chains by considering these dimensions. However, such computational approaches tend to be highly abstract, whereas practitioners require models that enhance awareness and foster critical thinking. This paper responds to that need by presenting an explorative computational model.

The aim of the proposed model, rather than prediction (Epstein, 2008), is to uncover core dynamics and discover new questions that enhance awareness of the resilience of criminal networks, thereby supporting the development of more effective interventions. Furthermore, it aims to challenge law enforcement decision-makers to consider the criminal organisation as a complex adaptive system. Our model simulates different possible reactions of a criminal network to different types of interventions based on the underlying criminal business model as introduced by Barros et al. (2024). This computational approach is inspired by exploratory modelling that focuses on the development of models to enable exploring a range of possible dynamics and outcomes for decision support given the available

information (Steinmann et al., 2024). It differs from the traditional modelling approach that focuses on one model to accurately describe all system characteristics and behaviour (Bankes, 1993). As such, our computational approach offers the opportunity to simulate the evolving nature of the modus operandi of criminal networks and to explore the possible impact of different intervention strategies to counter these networks over the long term. In this way, the model serves as a vehicle to stimulate double-loop learning (Argyris, 1977). Double-loop learning is particularly suitable for understanding complex criminal networks with sophisticated and evolving modus operandi. It stimulates law enforcement organisations to continuously reflect on the possible effect of their interventions and their underlying assumptions, based on new insights, changing circumstances and evolving tactics of the criminal networks. The proposed computational model supports decision-makers to better grasp the inherent complexity, which stimulates the development of more effective and sustainable law enforcement interventions.

The proposed explorative computational model differs from existing approaches like Manzi and Calderoni (2024), who examined the resilience of a cocaine trafficking organisation against law enforcement efforts targeting specific key actors. Unlike Duijn et al. (2014) and Duxbury and Haynie (2019), who analysed network characteristics to define resilience, Manzi and Calderoni (2024) propose an agent-based model to analyse the effect of police interventions targeting specific roles in the criminal network (e.g. acquisition, trafficking, packaging and selling) on the revenue of the criminal network. Each agent has a specific role and strives to successfully complete it, generating revenue for the organisation. However, the model does not consider that a criminal organisation can employ various modus operandi to adapt to policing pressure and sustain its revenue. Magliocca et al. (2024) accounted for the adaptability of the criminal organisation by formulating a coupled agent-based model with a spatial interdiction optimisation model to assess the efficiency of law enforcement interventions. In this model, agents assess the trafficking costs based on the perceived risk of a particular modus operandi. This, in turn, influences the agents' decisions regarding which trafficking routes to use for shipping drugs, thereby altering the modus operandi of the criminal organisation. However, these authors do not consider how different law enforcement interventions influence the dynamics of the costs associated with each modus operandi. Finally, Weyland et al. (2023) took the financial perspective into account, to analyse the circumstances under which an individual joins a criminal organisation based on their societal environment and financial/societal situation. This computational model used a cost–benefit agent-based model wherein the financial component was implicitly represented through a fitness function that included power, money and success. The cost–benefit trade-off analysis can also be used to analyse changes in criminal organisation activity, adaptation and resilience, as shown by van Elteren et al. (2025).

This paper is structured as follows: first, we introduce the explorative computational model using cocaine trafficking as an example. Next, we present an illustration of its potential using an example. Finally, we draw some conclusions and recommendations for future research.

Methodology

In this paper, we introduce an explorative computational model that enables the exploration of how the criminal business model is affected when subjected to different types of law enforcement interventions. The model supports decision-makers in reflecting on the underlying assumptions that guide their decisions, along with exploring the potential effects of various law enforcement intervention strategies. This approach is built on the premise of double-loop learning. Introduced by Argyris (1977) in the late 1970s, double-loop learning goes beyond simply refining the current strategy by adjusting it based on past outcomes (single-loop learning). Instead, it involves a critical reflection

and reassessment of the underlying assumptions, goals and norms that drive those interventions. Double-loop learning can be stimulated through computer simulation, as shown by Kim et al. (2013). By engaging with a computer model, decision-makers can explore different strategies and obtain insight into the broader implications of their strategies within a complex environment.

The illicit market exhibits a high degree of complexity that defies intuitive comprehension of its dynamics. As discussed throughout this paper, the financial aspect plays a significant role in the dynamics of a criminal business model. To gain a better grip on this complexity, it is essential to understand the intricacies of the entire system and to encourage decision-makers to rethink their strategies or, in other words, to engage in double-loop learning. This modelling approach builds on the criminal business analysis approach proposed by Barros et al. (2024).

In this section we will first briefly describe how to conduct the analysis of the criminal business. This analysis will be used to develop our explorative computational model.

Analysis of a criminal business model

Cocaine trafficking can be viewed as a value chain involving various parties, subject to the laws of supply and demand and associated price formation mechanisms. To analyse this criminal business model, Barros et al. (2024) propose a methodology consisting of three steps. In the first step, the methodology describes how to conduct a stakeholder and value network analysis. Understanding the roles, interests and added value of each party in the value chain clarifies the relationships between the parties involved. Using these insights, the business model is further analysed for each party using a business model canvas (Osterwalder and Pigneur, 2010). The canvas provides insight into how the criminal network in question creates value, which activities and resources are needed to achieve this, what the costs are, and through which channels the product is sold and how this yields benefits. As such, the canvas offers an overview of how the business model of the criminal network works. Finally, the business model is quantified using a cost–benefit analysis that considers uncertainty. A cost–benefit analysis maps out the costs and benefits offering a method to assess the financial aspects of the business model. In this case, it focuses on analysing the total costs and benefits of the individual parties in the value chain of cocaine trafficking, for example producers, traders, dealers and brokers. This analysis is carried out by first mapping out all relevant cost and benefit items and then preferably monetising these items, that is, putting a monetary value on them, or at least quantifying them. For further detail, see Barros et al. (2024).

The analysis of the criminal business model provides insight into the areas where the parties involved can be most financially impacted. Since criminal networks are driven by financial gain, these insights can be used to identify interventions that counteract the underlying criminal business model. Additionally, it allows for the comparison of different criminal business models (and the corresponding modus operandi). This comparison can be used to identify more attractive business models and potential future frictions in the value chain in a timely manner. By doing so, it supports law enforcement intelligence and enhances its early warning capability.

Modelling criminal business models requires access to relevant data sources. Data can be retrieved, among others, from law enforcement documents and law court sentences, and from open sources like the European Union Drugs Agency (former European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)), the European Union Agency

for Law Enforcement Cooperation (Europol) (EMCDDA and Europol, 2022) and the United Nations Office on Drugs and Crime (UNODC) (UNODC, 2023). The data for the current modelling efforts was collected through an analysis of relevant literature for three illustrative examples of a modus operandi. In practice, the diverse and fragmented nature of the different data sources poses a challenge for the collection and structuring of the data. Moreover, to challenge the adaptiveness of criminal networks, it is required to develop rapid data collection and analysis. Advancements in AI and increased computing power provide support in the automatic extraction and analysis of unstructured sources of information to efficiently make sense of large amounts of textual information sources and extract characteristics of different modus operandi (Barros et al., 2022).

Explorative computational model

An explorative computational model has been developed to gain a deeper understanding of the dynamics of a drug trafficking criminal network. The aim of this approach is to create insight into the cost–benefit dynamics of the criminal business model, considering external factors such as law enforcement intervention. The computation model builds on the criminal business modelling approach proposed in Barros et al. (2024). The criminal business modelling methodology was applied using open sources like Europol (2024), UNODC (2023), EUDA (former EMCDDA) and Europol (2022) and Roks et al. (2021) to create three illustrative examples of cocaine trafficking business models in the Netherlands ('Dutch port', 'Dutch cocaine laundry' and in another, non-Dutch port ('EU port')). Using the model, an interactive simulation tool has been created that enables interactive analysis. This tool includes visual illustration to enhance the understanding of the possible financial evolution of the criminal business model. The proposed explorative computer simulation model invites law enforcement practitioners to explore how criminal networks might respond to different law enforcement intervention strategies. By creating a space for reflection and discovery, the use of the model encourages decision-makers to revisit underlying assumptions about cocaine trafficking and fosters double-loop learning.

Examples of criminal business models

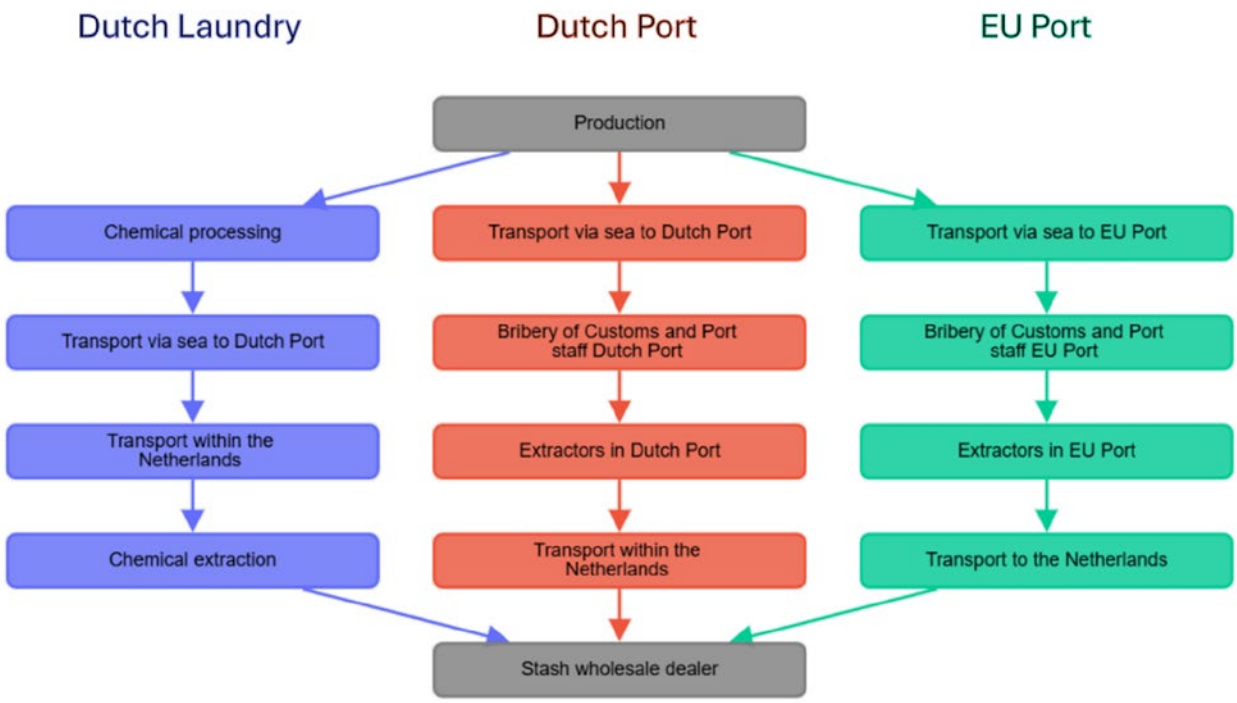


Figure 17.1. Overview of three examples of cocaine trafficking business models

Dutch port represents the first modus operandi, whereby the cocaine is concealed in ship containers and shipped from the origin country to a port in the Netherlands (see Figure 17.1). At the port, the drugs are extracted covertly from the shipping containers and taken outside of the port. This smuggling modus operandi often relies on the cooperation of the shipping company and/or port authorities and customs to avoid container inspections and to locate the containers containing cocaine, essentially involving corruption (Roks et al., 2021). The cost–benefit analysis based on open sources, using the methodology described in the previous section, shows that the costs involved with shipping container extraction are estimated to be smaller than the costs associated with the required corruption activities (Europol, 2024), and that the largest profit margins are achieved by the wholesale dealer (Barros et al., 2024).

An alternative modus operandi is the EU port, which involves adding an extra waypoint in the transportation chain to avoid arrival at a Dutch port (see Figure 17.1). In this case the shipment containing concealed drugs arrives at another EU port, which is assumed to be less monitored by law enforcement. The drugs are then extracted and transported by road to the Netherlands. The cost–benefit analysis shows that, similarly to the Dutch port business model, the costs involved with shipping container extraction are estimated to be smaller than the costs associated with the required corruption activities and that the largest profit margins are still achieved by the wholesale dealer. Due to reduced monitoring at this port, it is assumed that the costs of smuggling the cocaine into this location are smaller than at the Dutch port. However, additional transportation costs from the EU port to the Netherlands are necessary, resulting in higher overall expenses compared with the initial Dutch port business model.

Finally, to reduce the risks at the port, another modus operandi involves hiding the cocaine by impregnating it into an innocent-looking product, such as clothing, in the country of origin. This 'hiding in plain sight' strategy makes detection more difficult and eliminates the need for immediate extraction at the port. However, it requires the incorporation of the cocaine in the origin country and its extraction in the Netherlands. This extraction process corresponds to the reverse impregnation process and requires a specialised facility known as a 'laundry'. The cost–benefit analysis shows that this modus operandi, Dutch laundry, yields less costs at the port but requires additional expenses associated with the incorporation and extracting of the drugs.

The three different modus operandi result in different criminal business models and value chains that were derived using the cost–benefit analysis described in the previous section. As the price of cocaine has been stable for the last decades (RTL Nieuws, 2022), we will assume that the benefit component of the analysis is constant for the three criminal business models. Law enforcement interventions can impact the profitability of these criminal business models differently. Law enforcement interventions targeting a specific step of the value chain can increase the costs and therefore decrease the profitability of the criminal business model. For example, if law enforcement focuses on reducing corruption at the port, the risk of engaging in an illicit activity increases, pushing the bribery costs up. Similarly, for the drug extractors, the more that are caught, the higher the perceived risk becomes, which in turn can increase the costs of their illicit activities. In such a case, the Dutch port business model becomes less attractive, prompting the criminal network to adapt its cocaine trafficking modus operandi to develop a more lucrative business model, as financial gain is a major driving force.

Computational model

To analyse the dynamics of illicit drug trafficking and shed light on how targeted law enforcement interventions impact the business model, we introduce an explorative computation model based on the concept of agent-based modelling (ABM) (Bonabeau, 2002). ABM enables capturing non-linear emergent effects by simulating simple interactions between individual agents and their environment. Furthermore, ABM has proven to be a powerful tool for studying complex social systems and understanding how micro-level effects can trigger macro phenomena (Bonabeau, 2002). Therefore, ABM will be used to model how, under a specific law enforcement strategy, the business model that ultimately becomes the most lucrative can emerge over time.

The agent-based model developed is based on the criminal business models (and associated value chains) depicted in Figure 17.1. Each agent is associated with one of the criminal business models and with a specific step within the corresponding value chain. Each agent has the following attributes:

- criminal business value chain: name of the criminal business to which the agent belongs;
- initial cost: associated cost of the value chain step at the beginning of the simulation;
- current cost: current cost of the value chain step at a given iteration of the simulation;
- cost increase rate: the rate at which costs change following a law enforcement intervention (this can be linear or non-linear).

The initial cost and the cost increase rates are based on Barros et al. (2024). The initial cost is expressed as a percentage of the product's total cost, and the resulting criminal business chain value is updated linearly by simply multiplying the current cost by the corresponding cost increase rate. When an exponential rate applies, the costs are updated in a way that makes them rise progressively over time following an exponential pattern. The model parameters can be found in Table 17.1.

Table 17.1. Overview of the model parameters

Business chain value	Cost increase rate
Transport by sea to EU port	Linear
Bribery of customs and port staff in EU port	Exponential
Extractors in EU port	Linear
Transport to the Netherlands	Linear
Transport by sea to Dutch port	Linear
Bribery of customs and port staff in Dutch port	Exponential
Extractors in Dutch port	Linear
Transport within the Netherlands	Linear
Chemical processing	Linear
Transport by sea to Dutch port	Linear
Transport within the Netherlands	Linear
Chemical extraction	Exponential

The aggregation of the agents of a given criminal business model and their actions is modelled as a meta-agent. This meta-agent models the overall criminal business value chain and its overall costs. Finally, a smuggler meta-agent is modelled to represent the criminal network. For the sake of simplicity, it is assumed that this meta-agent's behaviour is rational. The smuggler will always choose the cheapest modus operandi.

In the explorative computational model, the decision-maker can choose between different law enforcement interventions for each of the three criminal business models:

- Dutch port: targeting drug extractors and/or targeting corruption at the Dutch port;
- EU port: intensifying collaboration with EU law enforcement agencies to increase monitoring and decrease corruption at the EU port;
- Dutch laundry: targeting drug laboratories responsible for the cocaine extraction.

Once the decision-maker has defined which strategies to use, including their frequencies, the explorative computational model simulates the corresponding law enforcement interventions over a two-year period. These interventions are distributed uniformly across the two-year period, using a daily time step. When a law enforcement

intervention is carried out, it is assumed that the costs of the targeted criminal business step increase. The rationale behind this dynamic is that potential corrupt individuals are harder to recruit, and/or that criminals will increase their prices due to increased probability of being caught. Therefore, if the law enforcement interventions stop, this will impact the costs of the target criminal business step. In fact, if there is less risk of a law enforcement intervention, there is less need for extra mitigating measures and, as such, the associated costs will decrease. These fluctuations depend on the value of the criminal business chain step. For instance, the costs associated with employment of drug extractors (often unskilled youngsters (The Brussels Times, 2024)) to extract the cocaine from shipping containers remain relatively stable, as the supply of volunteers to carry out this illicit activity is relatively high. On the other hand, the costs associated with customs corruption can vary significantly. Contrary to the drug extractors, the customs activities that need to be corrupted are conducted by a smaller number of skilled professionals (NL Times, 2019). Additionally, an increase in law enforcement interventions targeting corruption is expected to intensify their risk perception, thereby increasing the costs associated with carrying out these illicit activities.

Each simulation of the explorative computational model covers a period of two years and models the impact of the different chosen law enforcement interventions on the profitability of the different criminal business models. Additionally, the computational model makes it possible to review the timeline and identify the criminal business model most frequently chosen over the two-year period.

As the model is intended to illustrate its potential for stimulating double-loop learning, we rely on a single simulation run at this stage. For more in-depth exploratory analysis, additional simulation runs can be easily introduced (Steinmann et al., 2024).

Results

In this section we will show how the introduced explorative computational model can be used to facilitate double-loop learning. As mentioned before, three illustrative examples of criminal business models have been implemented to prompt decision-makers to analyse potential effects of disruption strategies and gain a deeper understanding of the repercussions of their interventions against criminal networks.

The results of the different simulations are visualised to create a better awareness of how the costs, profit margins and market share of each criminal business model may evolve over time under the selected law enforcement strategy. To encourage critical reflection, decision-makers are deliberately provided with limited law enforcement resources. This constraint is intended to prompt them to think strategically about their approach and to explore how different prioritisation choices may influence the criminal business models. In this scenario, law enforcement interventions are capped at 10 units, with each unit representing an arbitrary measure of law enforcement effort. Consequently, the decision-maker can allocate these efforts across various criminal activities.

Initial scenario

The initial scenario consists of the situation where a criminal network has the means to conduct its cocaine smuggling operations via the described three different modus operandi. When no law enforcement interventions take place, the most profitable criminal business model is Dutch port (which has the largest market share), followed by EU port and finally Dutch laundry.

Drugs extractors intervention focus

Facing the initial scenario, the decision-maker is prompted to choose, for instance, whether to focus on targeting drug extractors or on countering corruption. Figure 17.2 shows that a strategy wherein all law enforcement efforts are focused on drug extractors in the Dutch port has no effect. If we assume that all the simulated interventions (against drugs extractors) result in arrests, the overall costs associated (Dutch port) remained unchanged. This outcome might be surprising, as it could be expected that successful interventions over a two-year period would decrease the attractiveness of the Dutch port business model. However, it is assumed that the extraction of drugs does not require specific knowledge or skills, resulting in a large pool of potential drugs extractors, making replacement easy. This assumption keeps the costs required to hire drug extractors stable. Consequently, the market share is expected to remain the same.

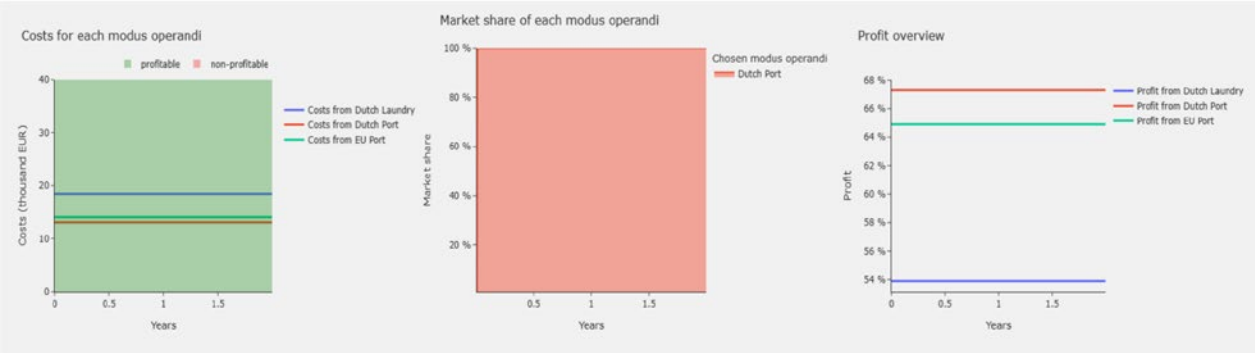


Figure 17.2. Visualisation of the simulation results based on only targeting drug extractors in the Dutch Port
NB: The evolution of the criminal business models costs (left), market share (centre) and profits (right) are shown**.**

These results suggest that a repressive intervention focusing on drugs extractors may not have the desired effect. They should trigger the decision-maker to consider other alternative possibilities, like exploring preventive interventions to deter individuals from engaging in drug extraction. In this sense they stimulate double-loop learning (challenge current approach and seek new strategies).

Corruption focus

Based on the previous insights, the decision-maker might be inclined to change the strategy by now targeting corruption at the Dutch port. As countering corruption requires more resources, which are usually scarce, only a limited number of law enforcement interventions can take place, for instance 10. Assuming that these investigations have led to arrests, corruption at the port will be more difficult to establish, which leads to extra costs, see Figure 17.3, for a timeline of up to two years. This also suggests that the overall costs of the Dutch port modus operandi may increase. The explorative computational model points out that this strategy may yield a shift in the market share as the alternative criminal business model via other EU ports has become now more attractive (waterbed effect).

These insights hint at the need to consider other intervention strategies. In particular, they can prompt the decision-maker to readjust the chosen strategy and switch the law enforcement efforts completely to collaboration with foreign equivalents over the following two years. These adaptations in the law enforcement strategy may yield an adaptation of the criminal business model, as Figure 17.3 shows. Between the fourth and sixth years, the EU port criminal business costs increased. As the focus on corruption at the Dutch port was stopped, the Dutch port business

model costs slowly decrease. However, after six years of law enforcement interventions, the Dutch laundry business model, which had previously been spared by such interventions, becomes as attractive as the other two criminal business models (as the three yield very similar profits) (see Figure 17.3).

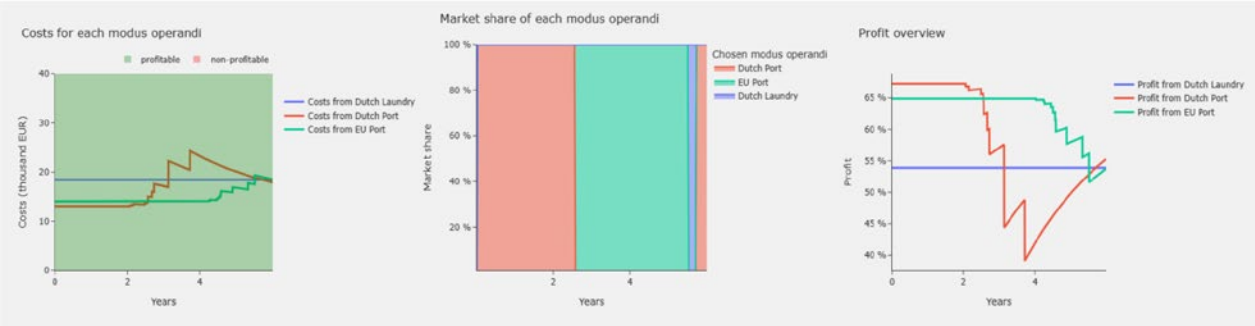


Figure 17.3. Visualisation of the simulation results when the focus of first two years of law enforcement efforts is on corruption at the Dutch Port

NB: After two years, the law enforcement strategy focuses solemnly on intensifying the collaboration with foreign law enforcement in other EU ports. The evolution of criminal business costs (left), market share (centre) and criminal business profits (right) are shown.

Contrary to the usual lean manufacturing assumption that focusing on one area of improvement at a time will achieve significant gains, the explorative model shows that with resilient criminal networks this might not lead to the expected results. Moreover, it suggests that it is important to consistently execute a given strategy to avoid creating an opportunity for the criminal network to use another modus operandi. This exemplifies the added value of this approach in questioning assumptions and stimulating double-loop learning.

Combined intervention strategy

The previous results can trigger the decision-maker to distribute the scarce law enforcement efforts evenly across the three criminal business models. As such the decision-maker can explore the possible effect of combined law enforcement strategy, wherein law enforcement efforts focus on corruption in Dutch port and EU port, and on Dutch laundry criminal business models. In this manner, the decision-maker hopes to prevent Dutch laundry from becoming the next profitable criminal business model. However, the results in the timeline between years six to eight show that a complicated pattern emerges, see Figure 17.4.

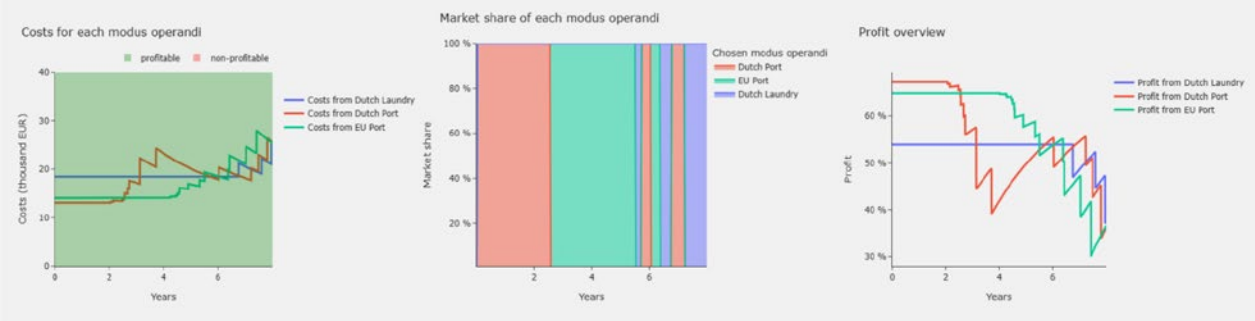


Figure 17.4. Visualisation of the simulation results when using a mixed law enforcement strategy between years six and eight on the collaboration with EU ports, countering corruption at the Dutch port and countering Dutch laundry

NB: The evolution of the criminal business costs (left), market share (centre) and criminal business profits (right) are shown.

In fact, after seven years it seems that no criminal business model remains predominant for longer than three months. One can see that after five years, the criminal business share market changes every three months, making it very difficult to anticipate which market will dominate in the future, which was not anticipated. These results stimulate reflection on the chosen strategy and, as such, double-loop learning.

Discussion

The goal of the developed explorative computational modelling approach is to support double-loop learning by encouraging decision-makers to reflect on, and explore, the possible effects of law enforcement interventions. The model helps decision-makers to think about what law enforcement interventions might lead to by letting them interact with the system's key dynamics. The possibility to conduct 'what if' analysis to explore different possible outcomes of the chosen intervention stimulates reflection and critical thinking, as explained in the results section. It is important to underline that the proposed modelling approach is designed to explore the complexity inherent in drug trafficking systems, acknowledging that the highly dynamic and adaptive nature of these social systems limits the possibility of precise prediction.

The current model assumptions and analysis show that, for the given scenario, focusing efforts on a single policy strategy and targeting a specific criminal business step might achieve the desired outcome in the short term. However, this approach may inadvertently make alternative criminal businesses models more attractive. As the results suggest, redirecting efforts to the newest lucrative criminal business model might make previously less lucrative business models attractive. Again, these results challenge the common assumption that concentrating on a single strategy yields the best results. Moreover, they also prompt the decision-maker to realise that efforts to disrupt a criminal network might unintentionally make another criminal business model more attractive, creating a cat-and-mouse dynamic. In addition, they also highlight the importance of long-term commitment and consistent execution of the chosen strategy. Finally, they also suggest that when financial gain is the primary driver for criminal networks, it may be worthwhile to consider reducing the profitability of the entire criminal business model or, in other words, to explore ways of destabilising the supply–demand system. This can be achieved not only through repressive measures but also, for instance, by demotivating consumers to using cocaine for recreational purposes.

Conclusions

This paper proposes an explorative computational modelling approach that enables law enforcement agencies to gain deeper insight into the complexity of disrupting criminal networks, using a double-loop learning approach.

The current model explicitly focuses on the financial component and the logistics associated with the criminal business model. This integrated approach provides further insight into the resilience of criminal networks, as it fills a gap in research that has been focused independently on logistics, financial transactions or the social network. Despite the profit-driven nature of criminal activities, there remains a significant gap in analysing criminal business models and the effects of criminal network disruption strategies.

The paper's contributions are built on a holistic approach that encompasses multiple aspects of the crime system. It demonstrates the potential of a simple explorative computational model to challenge decision-makers and enhance their awareness of the resilient behaviour of the entire system. By exploring the possible impact of different law enforcement strategies, the model exposes decision-makers to the possible consequences of short-term or inconsistent strategies. It also helps them realise that, rather than focusing on a single component, it may be necessary to reduce the overall attractiveness of the underlying criminal business model. In doing so, it can encourage them to consider alternative interventions, such as demotivating consumers from acquiring illicit products. Such interventions are not yet included in the explorative computational model but can be easily added. In this manner, the computational model supports double-loop learning by encouraging innovative thinking and the exploration of effective preventive and repressive law enforcement interventions capable of disrupting criminal networks over the long term.

Additionally, in contrast to other valuable analysis efforts focused on understanding and disrupting criminal networks based on either data analysis or simulation models, this interactive explorative modelling approach stimulates decision-makers to reflect on the adaptive and resilient behaviour of the criminal business models using a scenario that feels familiar and relatable. This approach enhances the potential for simultaneously stimulating double-loop learning for decision-makers who will face the complexity of criminal business models and are urged to anticipate possible (undesired) effects. It also stimulates co-creation, as it involves decision-makers in modelling efforts of future disruption strategies. The explorative modelling approach enables the incorporation of new and relevant aspects and perspectives into the explorative computation model, bridging the gap between data analysis and complex systems modelling.

Finally, further research is necessary to further fulfil the computational modelling potential, particularly for creating more detailed models, stimulating double-loop learning and identifying possible effective interventions. For example, the explorative computational model should be extended with the social network dimension to better capture the resilience of the criminal networks. Incorporating the dynamics at a social dimension would provide the possibility to further understand the effects of disruption efforts on the functioning of criminal networks. Moreover, criminal networks might merge or split to maintain covertness or increase effectiveness. Other extensions of the model could focus on including stochasticity and explicitly modelling the connections and dependencies between different illicit markets and illicit supply chains, thereby causing the tool to evolve from supporting double-loop learning toward supporting decision-making. In particular, extending the modelling approach to include multiple simulation runs

could support decision-makers in generating a range of possible scenarios, enabling them to explore in more detail potential disruption efforts before these are put into practise, that is *ex ante* (Steinmann et al., 2024).

References

Albanese, J. S. (2023), 'Development and surges of organized crime: An application of enterprise theory', in: Nelen, H. and Siegel, D. (eds), Organized Crime in the 21st Century, Springer, Cham, pp. 11–24, https://doi.org/10.1007/978-3-031-21576-6_2.

Argyris, C. (1977), 'Double-loop learning in organizations', Harvard Business Review, Vol. 55, No 5, pp. 115–125.

Ayling, J. (2009), 'Criminal organizations and resilience', International Journal of Law, Crime and Justice, Vol. 37, No 4, pp. 182–196.

Bankes, S. (1993), 'Exploratory modeling for policy analysis', Operations Research, Vol. 41, No 3, pp. 435–449.

Barros, A. I., van der Zwet, K., Westerveld, J. and Schreurs, W. (2022), 'AI-potential to uncover criminal modus operandi features', European Law Enforcement Research Bulletin, Special Issue 6, pp. 23–31.

Barros, A. I., Verweij, E. D. N., van der Zwet, K. and Wemmers, S. M. (2024), 'Dynamische crime scripts: systeemanalyse van ondermijnende criminaliteit', in: Snaphaan, T. and Klerks, P. (eds), Crime Scripting Theory and Practice, BoomCriminologie, The Hague, pp. 525–548.

Bonabeau, E. (2002), 'Agent-based modeling: Methods and techniques for simulating human systems', Proceedings of the National Academy of Sciences, Vol. 99, Supplement 3, pp. 7280–7287.

Conger, S. A. and Mason, R. O. (2013), 'Systems analysis', in: Gass, S. I. and Fu, M. C. (eds), Encyclopedia of Operations Research and Management Science, Springer, Boston, pp. 1523–1536.

Dekkers, I. (2023), 'The palpability of undermining crime: Injections of drug money into the real estate sector', JASON Institute website, https://jasoninstitute.com/the-palpability-of-undermining-crime-injections-of-drug-money-into-the-real-estate-sector/.

Duijn, P. A., Kashirin, V. and Sloot, P. M. (2014), 'The relative ineffectiveness of criminal network disruption', Scientific Reports, Vol. 4, No 1, p. 4238.

Duxbury, S. W., and Haynie, D. L. (2019), 'Criminal network security: An agent-based approach to evaluating network resilience', Criminology, Vol. 57, No 2, pp. 314–342.

Eidelson, R. J. (1997), 'Complex adaptive systems in the behavioral and social sciences', Review of General Psychology, Vol. 1, No 1, pp. 42–71.

EMCDDA and Europol (2022), EU Drug Market: Cocaine https://www.euda.europa.eu/publications/eu-drug-markets/cocaine_en.

Epstein, J. M. (2008), 'Why model?', Journal of Artificial Societies and Social Simulation, Vol. 11, No 4, p. 12.

Europol (2016), 'Police dismantle Russian money laundering ring operating in the football sector, Europol website, https://www.europol.europa.eu/media-press/newsroom/news/police-dismantle-russian-money-laundering-ring-operating-in-football-sector.

Europol (2024), Criminal Networks in EU Ports: Risks and challenges for law enforcement, Europol_Joint-report_Criminal networks in EU ports_Public_version.pdf.

Gerell, M., Sturup, J., Magnusson, M. M., Nilvall, K., Khoshnood, A. and Rostami, A. (2021), 'Open drug markets, vulnerable neighbourhoods and gun violence in two Swedish cities', Journal of Policing, Intelligence and Counter terrorism, Vol. 16, No 3, pp. 223–244.

Kim, H., MacDonald, R. H. and Andersen, D. F. (2013), 'Simulation and managerial decision-making: a double-loop learning framework'. Public Administration Review, Vol. 73, No 2, pp. 291–300.

Lotspeich, R. (2000), 'The nature of organized crime: An economic perspective', Low Intensity Conflict and Law Enforcement, Vol. 9, No 3, pp. 35–66.

Manzi, D. and Calderoni, F. (2024), 'The resilience of drug trafficking organizations: Simulating the impact of police arresting key roles', Journal of Criminal Justice, Vol. 91, 102165.

May, C. (2017), Transnational Crime and the Developing World, Global Financial Integrity, Washington, DC, https://globalinitiative.net/wp-content/uploads/2017/12/GFI-Transnational-Crime-and-the-Developing-World-2017.pdf (Accessed: 30 December 2024).

Magliocca, N. R., Summers, D. S., Curtin, K. M., McSweeney, K. and Price, A. N. (2022), 'Shifting landscape suitability for cocaine trafficking through Central America in response to counterdrug interdiction', Landscape and Urban Planning, Vol. 221, 104359.

Magliocca, N. R., Price, A. N., Mitchell, P. C., Curtin, K. M., Hudnall, M., and McSweeney, K. (2024), 'Coupling agent-based simulation and spatial optimization models to understand spatially complex and co-evolutionary behavior of cocaine trafficking networks and counterdrug interdiction', IISE Transactions, Vol. 56, No 3, pp. 282–295.

NL Times (2019), 'Three Rotterdam customs officers arrested for money laundering', NL Times website, https://nltimes.nl/2019/03/05/three-rotterdam-customs-officers-arrested-money-laundering.

Openbaar Ministerie (2023), 'Crimineel geld, de kurk waar alles op drijft', Openbaar Ministerie website, http://www.om.nl/actueel/nieuws/2023/02/27/crimineel-geld-de-kurk-waar-alles-op-drijft.

O'Reilly, M. J. A., Hughes, C. E., Bright, D. A. and Ritter, A. (2020), 'Structural and functional changes in an Australian high-level drug trafficking network after exposure to supply changes', International Journal of Drug Policy, Vol. 84, 102797.

Osterwalder, A. and Pigneur, Y. (2010), Business Model Generation: A handbook for visionaries, game changers, and challengers, Wiley, Hoboken.

Roks, R., Bisschop, L. and Staring, R. (2021), 'Getting a foot in the door – Spaces of cocaine trafficking in the Port of Rotterdam,' Trends in Organized Crime, Vol. 24, pp. 171–188.

RTL Nieuws (2022), 'Drugs blijkt zeer inflatie-bestendig: Coke kost al decennialang 50 euro', RTL Nieuws website, https://www.rtl.nl/economie/artikel/5350823/waarom-worden-drugs-niet-duurder.

Spapens, T. (2010), 'Macro networks, collectives, and business processes: An integrated approach to organized crime', European Journal of Crime, Criminal Law and Criminal Justice, Vol. 18, No 2, pp. 185–215.

Snaphaan, T. and van Ruitenburg, T. (2024), Financial Crime Scripting: an Analytical Method to Generate, Organise and Systematise Knowledge on the Financial Aspects of Profit-Driven Crime, European Journal on Criminal Policy and Research [Preprint]. https://doi:10.1007/s10610-023-09571-9.

Steinmann, P., van der Zwet, K. and Keijser, B. (2024), 'Simulation-based generation and analysis of multidimensional future scenarios with time series clustering', Futures and Foresight Science, Vol. 6, No 4, e194.

The Brussels Times (2024), 'Three Belgian teenagers arrested for drug trafficking at Rotterdam Port', The Brussels Times website, https://www.brusselstimes.com/860508/three-belgian-teenagers-arrested-for-drug-trafficking-at-rotterdam-port.

UNODC (2023), Global Report on Cocaine 2023 – Local dynamics, global challenges, UNODC Research and Trend Analysis Branch, Vienna, https://www.unodc.org/documents/data-and-analysis/cocaine/Global_cocaine_report_2023.pdf.

UNODC (2024), UNODC World Drug Report 2024 – Key findings and conclusions, UNODC Research and Trend Analysis Branch, Vienna, https://www.unodc.org/unodc/en/data-and-analysis/wdr2024-key-findings-conclusions.html.

van der Zwet, K., Barros, A. I., van Engers, T. M. and Sloot, P. M. (2025), 'Opportunistic organization of illicit supply chains', Journal of Quantitative Criminology, pp. 1–24.

van Elteren, C., Vasconcelos, V. V., and Lees, M. H. (2025), 'The paradox of intervention: Resilience in adaptive multirole coordination networks', Proceedings of the National Academy of Sciences, Vol. 122, No 51, e2509856122.

Weyland, L. F., Barros, A. I. and van der Zwet, K. (2023), 'Longitudinal analysis of the topology of criminal networks using a simple cost–benefit agent-based model', in: Mikyška, J., de Mulatier, C., Paszynski, M., Krzhizhanovskaya, V. V., Dongarra, J. J. and Sloot, P. M. (eds), International Conference on Computational Science, Springer Nature Switzerland, Cham, pp. 10–24.

Navigating the shadows: Content analysis of organised crime recruitment in the *Ozark* series

Sónia Maria Aniceto Morgado, Sérgio Felgueiras

https://doi.org/10.3013/a48wtz86

Abstract

This study explores the multifaceted dynamics of organised crime recruitment through a qualitative and quantitative content analysis of the first season of the television series *Ozark*. By utilising a theoretical framework grounded in rational choice theory, social learning theory and strain theory, this research examines how fictional narratives reflect and shape societal perceptions of criminal networks. The analysis identifies three primary recruitment drivers: the exploitation of socioeconomic vulnerabilities; the manipulation of familial and social ties; and the gradual normalisation of criminality through moral disengagement and techniques of neutralisation. Findings reveal that recruitment is often an informal, opportunistic process leveraging existing social capital and financial desperation, particularly among marginalised individuals. The study highlights the role of 'calculated risk-taking' and the 'denial of the victim' in the decision-making processes of key characters. While acknowledging the limitations of fictional portrayals – including the risks of glamourisation and stereotyping – it is argued that the research demonstrates that series like *Ozark* can serve as a valuable pedagogical tool for law enforcement and criminology training. By bridging the gap between media studies and criminology, this paper provides insights into the psychological and sociological underpinnings of criminal involvement. Ultimately, it advocates for targeted interventions that address structural inequalities and promote media literacy to mitigate the allure of illicit opportunities.

Keywords: organised crime, recruitment, criminology, social impact of the media, socioeconomic conditions.

Introduction

The exploration of the dynamics of organised crime and of the recruitment processes within organised crime, a multifaceted area within criminology, psychology and sociology, has long intrigued scholars and is often enriched by analysing fictional narratives, such as television series.

Fictional narratives, particularly television series, offer a unique lens through which to explore this shadowy world, reflecting societal anxieties and offering insights into the complexities of criminal behaviour. The Netflix television series *Ozark* presents a compelling case study for examining the recruitment processes and psychological underpinnings that draw individuals into criminal networks. This analysis aligns with a growing body of scholarship examining the media's role in shaping public perceptions of crime, particularly organised crime (Cornish et al., 1986; Marsh et al., 2019).

By focusing on the first season of *Ozark*, this study seeks to answer the following research question: how does the series portray the dynamics of organised crime recruitment, and to what extent do these portrayals align with established criminological frameworks like strain theory and social learning theory? Answering this question will contribute to the academic discourse on media representations of crime, offering insights into the narratives presented to mass audiences. *Ozark* (2017–2022) centres on financial advisor Marty Byrde, who is forced to relocate his family to the Missouri Ozarks to launder money for a Mexican drug cartel. There, the Byrdes' lives become intertwined with local criminal entities, including the disenfranchised but resourceful Langmore family, particularly the young and ambitious Ruth, and the established Snell crime family. This analysis will focus on the recruitment and decision-making processes of these key characters.

Organised crime recruitment: theoretical foundations

Organised crime recruitment is a multifaceted process that cannot be explained solely through individual decision-making. Instead, it emerges from a complex interplay of socioeconomic, psychological and cultural factors. Theoretical frameworks from criminology and sociology provide critical insights into understanding the mechanisms that draw individuals into criminal organisations. These frameworks highlight how social structures, personal vulnerabilities and learned behaviours contribute to recruitment dynamics, offering academic and practical avenues for addressing this pervasive issue.

For approaching this element, there are key theoretical frameworks, such as (i) rational choice theory (RCT); (ii) social learning theory (SLT), (iii) strain theory (ST); and (iv) differential association and peer influence (DAPI).

RCT posits that individuals engage in crime after a calculated assessment of risks and rewards. Cornish et al. (1986) and van Gelder et al. (2013) argue that potential recruits weigh the benefits of joining organised crime, such as financial gain and social status, against potential costs like arrest or harm. These elements are reinforced by contemporary authors such as Raets (2024), Neuendorf (2017) and Weaver (2019). In the context of *Ozark*, characters frequently grapple with moral dilemmas, yet their ultimate decisions to engage in criminal activities often stem from perceived necessity or survival, reflecting RCT principles. This theory underscores the importance of understanding how socioeconomic pressures shape perceived cost–benefit analyses. As for SLT, it emphasises the role of association and reinforcement in adopting criminal behaviour. Akers (1973) expands on Bandura's (1999) foundational work to suggest that individuals learn behaviours by observing and imitating others, particularly those within their social circles. Organised crime networks often recruit members from familial or community connections, as demonstrated in *Ozark*, where criminal knowledge and justifications are transmitted across generations. This framework highlights how criminal organisations use social bonds to normalise illegal activities, fostering loyalty and cohesion. Lastly, Merton (1938) developed ST. The author highlights socioeconomic disparities as a driving force behind criminal behaviour. According to this framework, individuals facing structural barriers to legitimate

opportunities may resort to crime as an alternative means of achieving societal success. *Ozark* illustrates this through its portrayal of financially desperate individuals who, unable to access lawful avenues for stability, are coerced or tempted into criminal enterprises. ST reveals how systemic inequalities and economic deprivation create fertile ground for recruitment into organised crime. The DAPI of Sutherland and Cressey's (1978) theory delves into the influence of peer groups on criminal behaviour. The theory posits that individuals are more likely to engage in crime when exposed to frequent, intense interactions with those who hold deviant values. In *Ozark*, the characters' gradual immersion into crime is facilitated by their associations with established criminals, demonstrating how proximity to deviance fosters acceptance of illegal behaviour. This perspective emphasises the role of mentorship and social networks in recruitment processes.

These theories, along with concepts such as Bandura's (1999) moral disengagement and Bourdieu's (2018) social capital, underscore the multifaceted nature of crime recruitment, particularly when coercion, manipulation and societal alienation are involved. They provide a foundational understanding of the complex interplay between individual vulnerabilities, social structures and learned behaviours that contribute to the recruitment dynamics within organised crime.

Media portrayals and public perceptions of crime

Media serves as a powerful lens through which society interprets and understands crime, including the dynamics of organised crime. Fictional narratives, particularly in television series and movies like *Ozark* (2017–2022), *Peaky Blinders* (2013–2022), *Sicário* (2015) and *The Godfather* (1972) offer both a reflection of real-world practices and a dramatised version that influences public perception. The intricate portrayal of recruitment strategies in *Ozark* provides a unique opportunity to examine how media shapes societal attitudes toward organised crime, law enforcement and preventive measures.

Series and movies can provide a reinforcement of stereotypes, as presented by some studies. It has been shown that dramatised portrayals both reflect and reinforce stereotypes about organised crime in the following ways: (i) media as a reflection of reality; (ii) stereotypes and simplification; and (iii) impact on public perception.

Media narratives often mirror real-world practices, providing viewers with a dramatised but familiar perspective on crime. According to Surete (2015), Marsh et al. (2019), Hu et al. (2024) and Gomes et al. (2022), media content is not created in a vacuum but is influenced by actual crime trends, societal anxieties and historical contexts. In *Ozark*, the recruitment strategies depicted – such as leveraging financial desperation or familial loyalty – align with documented tactics used by criminal organisations. While dramatisation may embellish these practices for entertainment, the foundational elements often stem from reality. This reflective quality allows media to serve as an educational tool, albeit one that must be critically analysed for accuracy, such as *Ozark* characters potentially reinforcing stereotypes about criminals and their motives. Fictional portrayals shape societal attitudes toward crime, justice and law enforcement (Dowler et al., 2006; Muzzatti et al., 2023). *Ozark*'s nuanced depiction of moral ambiguity challenges viewers to reconsider their preconceptions.

These illustrations often involve oversimplifications, stereotyping and ethical issues that distort public understanding and policymaking by synthesising findings from various studies.

Media representations of crime, whether fictional or journalistic, shape public understanding of criminality and justice. However, these portrayals are often fraught with limitations that perpetuate stereotypes, neglect systemic causes and misrepresent the complexities of criminal behaviour, such as the following.

— **Oversimplification and stereotyping**

Crime representations often reduce complex social phenomena to simplistic narratives. In films, characters are frequently characterised as one-dimensional, with far-right domestic terrorists exemplifying a common oversimplification in which nuanced motivations are disregarded (Rich, 2020). Similarly, media coverage frequently reinforces racial and socioeconomic stereotypes, depicting marginalised communities disproportionately as perpetrators, thus perpetuating systemic biases. Studies also indicate that this stereotyping extends to gender dynamics, where men dominate as offenders and women are sidelined as victims or secondary characters (Hosford et al., 2021; Welsh et al., 2011; Zeppa, 2014).

— **Neglect of structural causes**

A significant limitation of crime media is the lack of focus on structural causes. For instance, systemic issues such as economic inequality, social injustice and institutional racism are often overlooked in favour of narratives centred on individual criminal behaviour (Rich, 2020; Pfeiffer et al., 2005). Media narratives about organised crime, such as those surrounding the 'Ndrangheta, often attribute criminal activities to personal greed or moral failings, neglecting broader sociopolitical contexts (Phillips, 2016).

— **Glorification and desensitisation**

Films and television shows often glamourise crime, presenting criminal activities as exciting or heroic while downplaying their consequences. This can desensitise audiences to violence, reducing their empathy for victims (Reiner et al., 1997; Welsh et al., 2011). The repetitive exposure to glorified violence normalises aggressive behaviour, potentially influencing public attitudes and diminishing engagement in preventative social measures (Pfeiffer et al., 2005; Zeppa, 2014).

— **Impact on public perception and policy**

Sensationalised crime representations contribute to a public perception that overestimates the prevalence of crime. Media often focus disproportionately on violent crimes, creating a false impression that crime rates are increasing, even when data shows otherwise (Pfeiffer et al., 2005; Reiner et al., 1997). This skewed perception pressures policymakers to adopt punitive measures, such as stricter sentencing or increased policing, rather than addressing the root causes of crime through social reforms (Hosford et al., 2021; Welsh et al., 2011).

— **Ethical issues and sensationalism**

Economic motivations often drive media representations of crime, leading to sensationalism that prioritises entertainment value over accuracy. This approach can trivialise the realities of criminal behaviour and justice while influencing audience perceptions (Zeppa, 2014). Moreover, journalistic crime reporting often relies on state and law enforcement sources, which can introduce biases that align with institutional agendas, further distorting the public's understanding of crime dynamics (Hosford et al., 2021).

— **Marginalisation of victims and gender bias**

Media narratives frequently marginalise the experiences of victims, focusing instead on the perpetrator's story. This trend minimises the impact of crime on individuals and communities (Reiner et al., 1997; Zeppa, 2014). Gender representation remains problematic, as crime media perpetuates traditional roles by underrepresenting women's perspectives, both as offenders and as victims, while overlooking the unique dynamics of gendered violence (Hosford et al., 2021; Rich, 2020; Welsh et al., 2011).

While influential, the representation of crime in the media is fraught with significant limitations. By oversimplifying narratives, perpetuating stereotypes and neglecting systemic causes, these portrayals contribute to misinformed public perceptions and policymaking. Addressing these concerns requires more nuanced, inclusive and evidence-based approaches to crime storytelling that prioritise accuracy and social responsibility. Media portrayals can also influence perceptions of law enforcement and policy discussions around crime prevention, along with raising ethical implications by potentially glamourising criminal behaviour. Despite potential pitfalls, media remains a powerful catalyst for public discourse around organised crime, increasing awareness and amplifying marginalised voices. By bringing complex issues to the forefront, series like *Ozark* encourage audiences to engage with topics they might otherwise overlook. This engagement can lead to increased awareness of the systemic issues contributing to crime, fostering a more informed and proactive citizenry.

Moreover, media can amplify marginalised voices and perspectives, shedding light on the lived experiences of those affected by organised crime. By presenting diverse narratives, creators can challenge dominant stereotypes and promote a more holistic understanding of crime and justice.

Media portrayals of organised crime, such as those in *Ozark*, play a dual role as both mirrors of reality and shapers of public perception. While they provide valuable insights into the dynamics of criminal recruitment, they also risk reinforcing stereotypes and glamourising illegal activities. By critically analysing these portrayals, audiences and policymakers can extract meaningful lessons while remaining vigilant against the potential distortions inherent in dramatisation. Through responsible representation and media literacy initiatives, the power of media can be harnessed to foster a deeper understanding of organised crime and its societal implications.

Bridging the gap between media studies and criminology requires analysing how narratives like *Ozark* shape public understanding of organised crime (Gomes et al., 2022; Hu et al., 2024; Marsh et al., 2019; Surete, 2015). By examining the specific techniques used to depict organised crime in *Ozark*, we can uncover how media narratives shape public discourse and influence real-world behaviours (Dowler et al., 2006).

Psychological and sociological approaches: factors and roles

Understanding the psychological and sociological factors that underpin vulnerability to organised crime recruitment is crucial for developing effective prevention strategies. Theories such as RCT, SLT, ST and DAPI provide a framework for analysing the decision-making processes and social influences that draw individuals into criminal networks (Akers, 1973; Merton, 1938; Sutherland et al., 1978).

Individuals who have been victims of inequality or who come from economically vulnerable backgrounds are more susceptible to criminal involvement as they often perceive illegal activities as a necessary survival strategy

(Adamse et al., 2024; Calderoni et al., 2021; Kleemans et al., 2008; Morgado, 2013), as previously mentioned. This dynamic aligns with ST (Merton, 1938), which emphasises the role of structural inequality in pushing individuals toward illegitimate means of achieving success. Intertwined, and in an elusive way, criminal organisations coercively manipulate ties and familial loyalty to secure compliance and loyalty (Dickie, 2024; Gambetta, 1993). This interplay of coercion and loyalty highlights the relational aspects of crime recruitment, emphasising the importance of trust and obligation in maintaining criminal networks.

Additionally, concepts like moral disengagement (Bandura, 1999) and social capital offer insights into how individuals rationalise unethical actions and the role of social connections in facilitating or hindering criminal involvement.

Social isolation and alienation are additional sociological factors that influence criminal recruitment. Criminal networks target individuals who feel disconnected from mainstream society, offering them a sense of belonging and purpose. This mirrors real-world recruitment strategies that capitalise on individuals' need for connection and acceptance. By creating an alternative social structure, organised crime offers recruits a community that fills the void left by societal exclusion. This dynamic aligns with SLT (Akers, 1973), which emphasises the role of association and reinforcement in adopting deviant behaviours (Goode, 2022).

Threats and violence are used to instil fear. This is another psychological tool leveraged by criminal organisations, both as a method of coercion and as a means of control. Women are often recruited through familial ties or as extensions of male-dominated networks, reflecting broader patterns of gendered recruitment in organised crime. Exploring these dynamics offers critical insights into how gender roles shape the experiences and vulnerabilities of recruits.

Cultural norms play a significant role in shaping the recruitment process. In societies where corruption and crime are normalised, individuals may view participation in organised crime as a pragmatic choice rather than a moral failure. Understanding the cultural contexts that facilitate recruitment can inform culturally sensitive interventions and policies.

The interplay of these psychological and sociological factors creates a potent environment for recruitment into organised crime. Economic pressures, social isolation and psychological vulnerabilities do not operate in isolation but reinforce each other. Addressing these overlapping factors requires a holistic approach that integrates psychological support with socioeconomic reform.

The contemporary nature of *Ozark* provides a unique opportunity to analyse how organised crime is rendered in the digital age, considering the specific characteristics of new media and its potential influence on recruitment.

Bridging research and policy

Bridging the gap between research and policy requires translating academic insights into actionable strategies for crime prevention and law enforcement. This involves drawing explicit connections between media illustration and developing targeted interventions to address the vulnerabilities and recruitment tactics depicted (Kleemans et al., 2008; van Koppen et al., 2022). Research on the effectiveness of various crime prevention strategies, such as early

intervention programmes, community-based initiatives and media literacy campaigns, can inform policy recommendations. Van Koppen et al. (2010) emphasise the importance of strengthening social ties and community resilience to counter the appeal of criminal networks. Additionally, examining the role of law enforcement in addressing the challenges posed by media portrayals of organised crime can lead to more effective training programmes and operational strategies. By integrating these perspectives, policymakers and practitioners can develop a multifaceted approach to counter the appeal and influence of organised crime, fostering a more informed and resilient society.

Methodology

This study employed a sophisticated approach to content analysis, integrating a qualitative technique to provide a comprehensive examination of the TV series *Ozark*. The qualitative component drew upon thematic analysis (Braun et al., 2006) and discourse analysis (Gee, 2014) to uncover the intricate ways in which the series renders the recruitment processes and decision-making dynamics within organised crime. The dialogue scripts were subjected to the systematic coding and identification of recurrent patterns. Subsequently, a quantitative analysis, drawing on the traditions of Krippendorff (2019) and Neuendorf (2017), provided a more nuanced understanding of the frequency and prevalence of specific themes and patterns.

The thematic analysis, as described by Braun and Clarke (2006, 2023), served as a primary tool for identifying and interpreting recurring motifs within *Ozark*. This involved a systematic process of familiarisation with the data, generating initial codes, searching for themes, reviewing themes, defining themes and naming themes and producing the final report. The analysis focused on identifying salient themes related to recruitment, such as socioeconomic vulnerability, exploitation, manipulation, moral disengagement and the normalisation of criminality. By meticulously coding and categorising these themes, the research sought to draw connections between the fictional representations in *Ozark* and real-world sociopolitical issues related to organised crime.

Complementing the content analysis, the examination of the power dynamics and ideology was performed using discourse analysis. Discourse analysis, as outlined by Gee (2014), was employed to delve into the intricate ways in which language, dialogue and storylines within *Ozark* construct social realities and reflect power dynamics. The analysis focused on how the series depicts the recruitment process, paying particular attention to the language used by recruiters to manipulate and coerce potential recruits. This involved examining the dialogue between characters, analysing how they rationalise their criminal behaviour and identifying the underlying power structures and ideological frameworks that shape these interactions.

Corpus

The corpus for this investigation consisted of the complete first season of the TV series *Ozark*. This included all dialogue scripts and visual elements relevant to the characterisation of organised crime and recruitment dynamics. The selection of a specific season of a television series for academic analysis requires careful justification, particularly when aiming for publication in a high-impact journal. In the case of *Ozark*, focusing on the first season offers compelling advantages for an investigation into organised crime and recruitment dynamics. Firstly, it provides a pristine portrayal of the genesis of Marty Byrde's criminal enterprise, allowing for a detailed examination of his initial immersion into the *Ozark*'s underworld. This includes analysing his early strategies for money laundering, his

navigating of nascent relationships with local criminals, and the initial moral compromises he undertakes. Studying these foundational elements offers valuable insights into the trajectory of his criminal development.

Secondly, the first season meticulously establishes the complex web of relationships between the Byrdes, established criminal organisations (the Snells), opportunistic newcomers (the Langmores) and law enforcement agencies. These initial interactions lay the groundwork for the subsequent evolution of alliances, betrayals and power struggles that fuel the narrative. Analysing these foundational dynamics within a contained time frame allows for a more focused understanding of power structures within the criminal milieu.

Furthermore, the inaugural season is crucial for delineating the core motivations driving each character. By concentrating on this early stage, the analysis can penetrate the unadulterated desires and anxieties that propel their actions before these motivations become obscured by subsequent events and moral compromises. This provides a clearer lens for examining the psychological and sociological factors that contribute to individual involvement in organised crime.

Finally, while *Ozark* maintains overarching themes of violence, corruption and moral ambiguity throughout its run, the first season exhibits a degree of narrative closure. Several key plotlines and character arcs reach a resolution within this time frame, allowing for a comprehensive analysis of specific themes without the risk of redundancy or the need to account for narrative developments in later seasons that might shift the analytical focus. This self-contained structure enhances the methodological rigor of the study.

In sum, the first season of *Ozark* serves as a microcosm of the series' broader exploration of criminal activity. It effectively encapsulates the core thematic concerns, establishes the foundational relationships and showcases the initial motivations driving the characters. This concentrated focus allows for a more manageable and in-depth analysis, contributing to a nuanced understanding of organised crime and recruitment dynamics within a clearly defined narrative framework.

Data analysis

The data analysis process involved a multi-stage approach grounded in the principles outlined by Bardin (2018). First, the researchers conducted a thorough review of the corpus, familiarising themselves with the characters, storylines and overall narrative arc of the series. Next, they employed a combination of thematic and discourse analyses to identify and interpret recurring motifs and patterns related to recruitment and decision-making within organised crime. This involved systematically coding and categorising dialogue scripts and visual elements, following Bardin's (2018) guidance on formulating context units and registration units, to identify salient themes and analyse the use of language and its implications for power dynamics and ideology.

Throughout the research process, careful attention was paid to ethical considerations. The researchers maintained a critical distance from the fictional narrative, recognising the importance of distinguishing between the entertainment value of the series and its potential real-world implications. They avoided overinterpreting or decontextualising the data, ensuring that their analysis remained grounded in a nuanced understanding of the complexities of organised crime and its portrayal in media.

This study represents a significant contribution to the field of media studies and criminology. By employing a sophisticated mixed-methods approach to content analysis, the research provides a comprehensive and nuanced examination of the TV series *Ozark*. The integration of thematic analysis, discourse analysis and quantitative techniques ensures a high level of rigour and allows for a deeper understanding of the complex dynamics of organised crime as rendered in the series. Furthermore, the study's focus on recruitment dynamics and decision-making processes within organised crime offers valuable insights for policymakers, law enforcement agencies and researchers seeking to understand and address this complex social phenomenon.

For the analysis, the following categories and subcategories were used. It is to be noted that the elements are grounded in the literature review, consolidated by authors such as Barlow et al. (2010), Morgado (2013), Morgado et al. (2022) and Weisburd et al. (2020), among others.

The analysis was guided by a structured coding framework grounded in the literature. The framework's primary categories were the following.

- **Category A: recruit characteristics.** Coding for attributes such as age, gender, education and prior criminal history to build a profile of recruits within the narrative (see Appendix 18.1).
- **Category B: decision-making process.** Identifying motivations for criminal involvement (timelines, biological determinants, valuing status, prestige, respect), with codes for 'cost–benefit analysis' (RCT), 'familial obligation' and 'pursuit of status' (see Appendix 18.2).
- **Category C: recruitment tactics.** Categorising the methods used by recruiters, including 'financial inducement', 'coercion and threats' and 'exploitation of skills' (see Appendix 18.3).
- **Category D: justification and rationalisation.** Capturing dialogue where characters justify their actions, aligning with 'techniques of neutralisation'. The spontaneous explanatory system and its subcategories are applied to the recruit and recruiter (see Appendix 18.4).

Results and discussion

The analysis of *Ozark*'s first season indicates that the series portrays organised crime recruitment as a process driven by three primary dynamics: the exploitation of socioeconomic vulnerability, the manipulation of familial and social ties and the gradual normalisation of criminality through rationalisation. The context is depicted through the characters' dilemmas, showing how economic pressures are weaponised by criminal organisations, leading to coercion, emotional manipulation and promises of security as core strategies. The series blurs the moral lines, offering insights into how individuals rationalise involvement in crime over time.

Preliminary analyses suggest that *Ozark* effectively encapsulates the complex interplay between socioeconomic vulnerabilities and recruitment strategies. Most of the characters are male, with the most common age range being 16–19 years old. Educational backgrounds and job statuses are diverse, with 'no formal education', 'high school student' and 'no steady job' being the most frequent employment statuses.

In this sense, the results are presented considering some basic elements, such as (i) recruitment dynamics: pathways to criminality; (ii) decision-making in organised crime: a complex interplay; (iii) recurrent patterns: unveiling the dynamics of organised crime; and (iv) implications for policy and law enforcement.

Recruitment dynamics: pathways to criminality

This study identified key factors contributing to the recruitment of individuals into organised crime. From the scripts we can unveil that the characters exhibit a range of criminal experiences, with 42.86 % involved in theft and petty crimes, 28.57 % engaged in broader illegal activities, and 14.29 % having either criminal records or no prior offences. The recruitment process is influenced by factors such as age, economic circumstances and family ties. For instance, Marty's financial expertise is central to his recruitment, while the recruitment of the youngest is precipitated by exposure to criminogenic factors within the familial unit and the potential value they offer in specific tasks. Recruitment methods vary depending on the presence of a family criminal network, ranging from gradual integration to direct recruitment based on specific skills or vulnerabilities. For instance, Wyatt Langmore's recruitment into criminal activities is often informal and opportunistic, primarily through his family. As noted in the opening monologue:

> *Marty Byrde (voiceover): Deciding to miss the ball game, the play, the concert, because you've resolved to work and invest in your family's future.* (Episode 1, 00:01:56)

This opening voiceover immediately establishes the 'appeal to higher loyalties' as a primary technique of neutralisation. By framing sacrifice for family as the ultimate virtue, the narrative provides Marty with a powerful justification for the criminal actions he undertakes in the name of 'investing in his family's future'.

Meanwhile, Boyd Langmore is deeply embedded in the Langmore family's criminal network, and his recruitment is an ongoing process within that existing structure, as he evidenced by his own testimony:

> *Boyd Langmore: Well ... How long we gotta feel bad about what we did?* (Episode 3, 00:06:36)
> *Russ Langmore: Don't start with that again... There's gotta be a statute of limitations about this shit.* (Episode 3, 00:06:42)
> *Boyd Langmore: You're damn right there does.* (Episode 3, 00:06:50)

Boyd's casual question while preparing an instrument of torture demonstrates the complete normalisation of extreme violence within the Langmore family. For other family members present, this is a clear example of observational learning, where deviant methods are taught and reinforced as routine problem-solving.

Consistent with ST (Agnew, 1992; Merton, 1938), many characters, particularly the Langmore family, are driven to criminal activity due to economic hardship and limited legitimate opportunities. This vulnerability is explicitly exploited by criminal organisations, who offer financial incentives and a sense of belonging to those marginalised by society. The series effectively illustrates how economic pressures are weaponised to lure individuals into criminal networks, namely by Boyd Langmore:

Boyd Langmore: Guy who runs a drug cartel's a smart man… He wouldn't trust damn near $3 million to someone like you. (Episode 2, 00:31:01)

Here, Boyd Langmore weaponises Russ Langmore's perceived low social status and financial desperation. This dialogue illustrates that manipulation based on 'strain' is not unique to criminals; law enforcement is shown using the exact same psychological tactics to 'recruit' an informant.

Marty Byrde: But what is money?… It's everything if you don't have it, right? (Episode 1, 00:00:40)
Wendy Byrde: Sometimes we don't think we're gonna like something, but then you try it, and then suddenly you realize that you're having fun. Think about your trampoline. (Episode 1, 00:07:35)

Marty's first question explicitly frames his world view through the lens of ST; money is not about greed, but about the absence of 'strain'. Wendy follows the logic by using the 'trampoline' analogy, a manipulative tactic that reframes a high-stakes, illicit financial decision as a low-stakes, exciting consumer purchase, thereby minimising the perceived risk for the potential recruit.

Furthermore, the series highlights the powerful role of family ties and loyalty in the recruitment process. In this season of *Ozark*, the Byrde family recruits Ruth Langmore to aid in their operations, but they face significant opposition from a rival family, the Snells. Characters like Wyatt and Three Langmore are drawn into criminal activity due to their family environment, supporting the notion of intergenerational crime and the role of SLT (Bandura, 1977; Sutherland et al., 1978). This underscores the importance of addressing familial patterns of criminality to disrupt the cycle of recruitment.

Charlotte Byrde: Wyatt, is it? … I really don't want to have to get you fired today, okay? (Episode 2, 00:11:21)

This polite threat is a clear act of coercion. Charlotte leverages Wyatt's economic vulnerability (his job) to gain control over him and his family, demonstrating her own rapid adaptation to the coercive methods required by the criminal enterprise.

Charlotte Byrde: This isn't your boat, is it? The house? College? Any of it? (Episode 2, 00:21:18)

Charlotte's dialogue signifies a rupture in the normalisation process. Her questioning directly confronts the 'techniques of neutralisation' her parents are using, highlighting the internal family strain that emerges when criminal activity is introduced to a previously non-deviant social group.

Ruth Langmore: Who knows how much pain and misery he's caused?
Russ Langmore: Would cause …
Ruth Langmore: Would cause ... To kids, even. (Episode 2, 00:32:09)

This serves as a textbook example of the denial victim technique (Sykes et al., 1957). Ruth Langmore recasts Marty as someone whose potential for causing pain and misery justifies his exploitation, allowing her and her family to morally disengage from the reality of criminal intent.

The pursuit of power, status and respect within the criminal underworld emerges as a significant motivator for characters like Ruth Langmore. This aligns with differential association theory (Sutherland et al., 1978), which emphasises the role of social groups and peer influence in shaping individual behaviour. The series depicts how criminal organisations offer a sense of identity and purpose to those seeking recognition and control.

Finally, characters frequently rationalise and justify their criminal involvement as a means of survival, protection or providing for their families. This finding supports the concept of techniques of neutralisation (Sykes et al., 1957), where individuals engage in crime while maintaining a positive self-image. *Ozark* effectively illustrates how the lines between right and wrong become blurred as characters gradually normalise their criminal behaviour.

Decision-making in organised crime: a complex interplay

The analysis further explored the decision-making processes of individuals involved in organised crime, revealing a complex interplay of factors. Marty Byrde, the central character, consistently demonstrates a calculated approach to risk-taking, weighing potential gains against potential losses.

> *Marty Byrde: Or do you want to just role-play it? … Okay, I'm Detective Whoever The Fuck, and you're the wife of the top money launderer for the second largest drug cartel in Mexico. Go.* (Episode 1, 00:30:36)

This quote is a direct illustration of RCT in action. Marty is not acting impulsively; he is identifying a significant 'cost' (getting caught) and attempting to mitigate that risk through preparation, demonstrating a calculated, cost–benefit approach to his criminality. However real-world security operations increasingly recognise the limited rationality of human decisions under pressure, advocating for AI-driven platforms like Marple to provide sound intelligence and decision support tools to mitigate human error (Felgueiras et al., 2026; Morgado et al., 2026).

> *Ruth Langmore: Watch me… What the …? …*
> *Russ Langmore: Now, Ruth, we were all involved.* (Episode 3, 00:04:58)
> *Marty Byrde: Money Laundering 101. (…) The dirty money is too clean. (…)* (Episode 4, 00:04:56)

Instead of challenging Ruth's threat, Russ's response, 'we were all involved', is a manipulative tactic to create shared culpability. By reminding her of their mutual entanglement, he binds her to him, making betrayal riskier for her – a clear form of social control. Moreover, as Marty Byrde is framing the criminal process as a pedagogical exercise for Jonah Byrde, he is able to neutralise moral inhibitions, providing the necessary justification for deviant behaviour and facilitating his formal integration into the criminal business.

This aligns with RCT (Cornish et al., 1986), which suggests that offenders make deliberate choices based on a cost–benefit analysis. The series portrays the strategic decision-making involved in navigating the complexities of organised crime. Marty also frequently engages in moral disengagement to justify his actions, particularly when

they involve harm to others. This resonates with Bandura's (1999) theory of moral disengagement, which explains how individuals can detach themselves from moral standards to justify harmful behaviour. *Ozark* provides a compelling illustration of the psychological mechanisms that allow individuals to compartmentalise their criminal activities.

> *Marty Byrde: They're not her friends… She didn't know that this boat was stolen… She thought a teenager running a leaf blower at a prom night motel lived in a $5 million home?* (Episode 2, 00:22:25)

Marty's sarcasm is a form of moral disengagement. By highlighting the obviousness of their criminal lifestyle, she dismisses her daughter's concerns as naive, thereby rationalising the family's exposure to danger and normalising their association with the Langmores.

Furthermore, Marty displays remarkable adaptability and resilience in the face of adversity, consistently adjusting his strategies to navigate the challenges of the criminal world. This adaptability is crucial for survival and success in the unpredictable environment of organised crime. The series showcases the resourcefulness and strategic thinking required to thrive in a criminal underworld.

> *Wyatt Langmore: Manager wanted me to make sure you still had one of these in your room.*
> *Wendy Byrde: Yeah, we're all set.*
> *Charlotte Byrde: Sure?* (Episode 2, 00:11:21)

> *Ruth Langmore: You gotta be kidding me …*
> *Marty Byrde: If I was kidding, I would've said you're witty and handsome.* (Episode 3, 00:04:50)

Finally, Marty exhibits a pattern of manipulating and exploiting others to achieve his goals, using charm, persuasion and intimidation to maintain control. This manipulative behaviour is central to his recruitment strategies and his ability to manage his criminal enterprise. The series shows the coercive tactics and emotional manipulation employed by organised crime to recruit and control individuals, expressed by the characters.

> *Marty Byrde: Deposit this [...] just do it*
> *Ruth Langmore: Okay. Good.*
> *Marty Byrde: You, Ruth Langmore, just committed an overt act ... See this camera? It sees you. And it saw you just make that deposit. Now if I'm ever arrested [...] so do you*. (Episode 3, 00:12:51)

This backhanded compliment is a key example of Marty's manipulative leadership style. He simultaneously asserts his dominance and keeps Ruth off balance. This psychological control is central to how he 'recruits' and retains her, building a complex relationship that is part mentorship, part-coercion.

Recurrent patterns: unveiling the dynamics of organised crime

Beyond individual motivations and decision-making, this study identified recurrent patterns that illuminate the dynamics of organised crime. The recruitment process is often informal and opportunistic, relying on existing social

connections and trust. In fact, the primary recruitment locale is the workplace, while family circumstances and interactions are the second main reason for recruitment instances.

Marty Byrde (voiceover): But what is money? It's everything if you don't have it, right? (Episode 1, 00:00:40)
Money as a measuring device (Episode 1, 00:01:31)

By framing money as a 'score' – language associated with games and sports – the narration immediately trivialises and normalises the criminal pursuit of it. This rationalisation detaches the money from its violent source and reframes it as a simple measure of success.

Marty Byrde: I mean, I guess I get it. You're scared. (Episode 3, 00:00:23)

This statement is not an expression of empathy but a tactical manoeuvre. Marty identifies Ruth's vulnerability (fear) and acknowledges it, positioning himself as an understanding figure. This builds a form of dependency that he leverages to secure her loyalty and recruit her more deeply into his operations.

Marty Byrde: A family is like a small business. (Episode 2, 00:00:45)

This quote is perhaps Marty's core rationalisation. By equating 'family' with a 'business,' he reframes his criminal actions as pragmatic, amoral 'managerial' decisions. This serves as an 'appeal to higher loyalty,' justifying any illicit act as necessary for the 'business' (his family) to survive.

This finding is consistent with research on recruitment to organised crime, which highlights the role of social networks (Calderoni et al., 2021; Morselli, 2009; Weisburd et al., 2020). The series demonstrates how criminal organisations leverage existing relationships to expand their networks.

Young characters like Wyatt Langmore and Charlotte Byrde are susceptible to exploitation due to their limited opportunities and desire for acceptance. This aligns with research on the involvement of young people in crime, which emphasises the role of social and economic marginalisation (Argueta et al., 2020; Bernburg, 2009; Klein, 1986; Mowen et al., 2023; Tannenbaum, 1938; Tannenbaum et al., 2021). *Ozark* illustrates the specific vulnerabilities that make young people attractive targets for recruitment into organised crime.

Marty Byrde: Del just has a few questions. He's…
Bruce Liddell: Yeah? What's going on? …
Marty Byrde: Hey, Del. Didn't know you were coming in town. (Episode 1, 00:17:05)

Business owner: Am I speaking Greek? …
Marty Byrde: I don't like to give extraneous details. There's is a safe. And I need the contents. (Episode 3, 00:13:30)

Wyatt Langmore: So, you're, um … you're still promising to buy us suits for the funeral? …
Marty Byrde: Yeah …
Wyatt Langmore: Okay, then. (Episode 1, 00:30:36)

This exchange perfectly captures the exploitation of youth vulnerability. Wyatt, in a moment of grief and need, is forced into a transactional relationship with Marty. Marty, by becoming a provider (of funeral suits), creates a social debt and a bond that further entangles the young, vulnerable Langmores in his criminal world.

Moreover, characters experience shifting loyalties as they navigate the complexities of the criminal world, highlighting the dynamic nature of relationships and power structures within organised crime (Topalli, 2005; van Gelder et al., 2013; Weisburd et al., 2020). The series depicts the shifting alliances and betrayals that characterise the internal dynamics of criminal organisations.

> *Marty Byrde: Or do you want to just role-play it? … Okay, I'm Detective Whoever The Fuck, and you're the wife of the top money launderer for the second largest drug cartel in Mexico. Go.* (Episode 1, 00:30:38)

Finally, Marty's criminal involvement escalates throughout the series, demonstrating the slippery slope often associated with criminal careers. This progression underscores the gradual desensitisation and increasing entanglement in criminal activities that can occur over time. *Ozark* provides a compelling case study of how individuals can become increasingly entrenched in a criminal lifestyle.

> *Ruth Langmore: I guess you're right. Stripping isn't for everyone.* (Episode 4, 00:19:17)

The study of media narratives like *Ozark* offers valuable insights for crafting effective law enforcement and crime prevention strategies. Addressing socioeconomic disparities and vulnerabilities before they lead to criminal involvement is crucial. By providing educational opportunities, job training and social support programmes, communities can reduce the susceptibility of individuals to recruitment by criminal organisations.

Strengthening social ties and community resilience can help counteract the appeal of criminal networks. Fostering a sense of belonging and providing positive alternatives can reduce the influence of criminal organisations within communities.

Educating audiences, particularly young people, to critically engage with fictional portrayals of crime can help reduce the undue influence of media on public perception. By promoting media literacy, individuals can better understand the complexities of crime and make informed choices.

Discussion: *Ozark*'s recruitment process analysis

The series *Ozark* provides a compelling case study for examining the intricate dynamics of recruitment into organised crime. As our analysis has shown, characters are drawn into Marty Byrde's money-laundering operation through a complex interplay of factors, including coercion, economic vulnerability, ambition and the manipulation of familial bonds.

Marty, with his financial expertise, becomes a tool for the cartel, highlighting how specialised skills can be exploited within criminal networks, echoing the assertion by Morgado et al. (2022) that fictional portrayals of crime offer valuable data. Wendy's trajectory showcases the fluid nature of recruitment, where initial coercion, driven by a need

to protect her family, can evolve into a quest for power and autonomy. This aligns with Morgado's (2013) framework, which emphasises the role of economic factors in shaping criminal behaviour. The Byrde children, Charlotte and Jonah, illustrate the vulnerability of youth within families entangled in criminal activity. Jonah's curiosity and adaptability lead him to an active role, while Charlotte grapples with a sense of entrapment. Ruth Langmore's story exemplifies the allure of upward mobility and the compromises individuals make in pursuit of it, reflecting the findings by Kleemans et al. (2008) on financial instability and susceptibility to recruitment. Rachel, the owner of the Blue Cat Lodge, demonstrates how economic hardship can create susceptibility to criminal offers, underscoring the insights of Agnew's (1992) GST.

The Snells, including Jacob and Darlene, represent a different dynamic: strategic alliances formed between established criminal actors. Their partnership with Marty highlights that recruitment is not always predicated on vulnerability. Meanwhile, Buddy Dieker's unique motivations highlight how recruitment can intersect with personal desires for meaning and purpose. Finally, Pastor Mason Young's tragic downfall underscores the corrosive effects of economic pressure and moral compromise.

These fictional narratives resonate with real-world observations. *Ozark* reinforces the importance of social cohesion and community resilience in crime prevention, echoing the findings of van Koppen et al. (2010) and the principles of social disorganisation theory (Shaw et al., 1942), a concept further explored by Morgado et al. (2023).

Ozark also serves as a cautionary tale about the influence of media on perceptions of crime, aligning with the concerns raised by Gomes et al. (2022), Hu et al. (2024), Marsh et al. (2019) and Surete (2015). This underscores the need for media literacy to foster critical engagement with such narratives, echoing Morgado's (2022) analysis of improving police communication with the media.

The series offers valuable insights for policymakers and law enforcement. It highlights the need for targeted interventions to address socioeconomic disparities and support at-risk populations, as proposed by Morgado et al. (2021). Strengthening community bonds and providing positive alternatives are also crucial.

For law enforcement agencies, *Ozark* underscores the importance of early intervention and multi-agency collaboration, mirroring the recommendations by Morgado et al. (2019). The series can even serve as a training tool to enhance officers' understanding of the complex factors driving organised crime, fostering empathy and improving community policing efforts, as suggested by Moura et al. (2022).

Finally, the transnational nature of the cartel's operations in *Ozark* emphasises the need for international cooperation in combating organised crime, supporting the arguments by Allum et al. (2012), Buckley et al. (2024) and Shelley (2018a; 2018b) for collaborative efforts between nations. This includes information sharing, joint operations and harmonised legal frameworks, reflecting the interorganisational approach discussed by Felgueiras et al. (2019) and Machado et al. (2021), and the development of technological tools for tackling organised crime and terrorism (Morgado et al., 2024a; Morgado et al., 2024b).

In conclusion, *Ozark* provides a compelling lens through which to analyse the complexities of organised crime recruitment. By integrating these fictional narratives into existing research, we can gain a deeper understanding of the phenomenon and inform more effective prevention and intervention strategies.

Conclusion

By meticulously dissecting the intricate tapestry of *Ozark*, this research illustrates the recruitment dynamics and decision-making processes inherent to organised crime. The findings illuminate the potent interplay of socioeconomic vulnerabilities, familial influences and the allure of power and status in shaping individual pathways to criminality. Moreover, the study elucidates the narrative's use of calculated risk-taking, moral disengagement and manipulative tactics employed by individuals entrenched in organised crime.

While an analysis of a fictional narrative cannot be used to directly formulate law enforcement policy, its implications are valuable within specific educational and training contexts. The practical value of this study, therefore, lies in its potential as a pedagogical tool. For instance, law enforcement or criminology training modules could utilise key scenes from *Ozark* as case studies to stimulate discussion on (i) identifying community vulnerabilities, such as how the depiction of the Langmore family illustrates the real-world socioeconomic indicators – such as poverty and a lack of legitimate opportunities – that academic research links to recruitment risk; (ii) understanding offender rationalisation, through analysing the 'techniques of neutralisation' in the Byrdes' dialogue to help trainees recognise how offenders justify their actions to themselves and others; (iii) the dynamics of coercion, through examining how Marty Byrde blends financial inducement with subtle threats to control recruits like Ruth, providing a clear illustration of complex manipulation tactics.

This study underscores the value of using popular culture as a critical lens through which to discuss complex social phenomena. By integrating insights from media studies and sociology and criminology, this analysis demonstrates how *Ozark*'s narrative reflects established criminological theories. Ultimately, its contribution is not a direct blueprint for policy, but a illustrative resource that can foster a more nuanced and critical understanding of organised crime dynamics for students, trainees and the public.

The implications of this research extend beyond the realm of academia, offering potential discussion points for policymakers and law enforcement agencies. By recognising the socioeconomic underpinnings of criminal recruitment, targeted interventions can be developed to mitigate the allure of illicit opportunities. Strengthening community resilience by fostering social support networks and providing positive alternatives can further diminish the influence of criminal organisations. Additionally, promoting media literacy empowers individuals to critically engage with fictional portrayals of crime, thereby mitigating the undue influence of media on public perception.

Acknowledgments

This research is supported by Portuguese national funds, administered by the Foundation for Science and Technology (FCT), Public Institute, under grant agreement, https://doi.org/10.54499/UID/04915/2025.

References

Adamse, I., Veroni, E., Blokland, A. and Schoonmade, L. (2024), 'The risk and protective factors for entering organized crime groups and their association with different entering mechanisms: A systematic review using ASReview', European Journal of Criminology, Vol. 21, No 6, https://doi.org/10.1177/14773708241250278.

Agnew, R. (1992), 'Foundation for a general strain theory of crime and delinquency', Criminology, Vol. 30, No 1, pp. 47–88, https://doi.org/10.1111/j.1745-9125.1992.tb01093.x.

Akers, R. L. (1973), Deviant Behavior: A social learning approach, Wadsworth Publishing Company, Belmont.

Allum, F. and Gilmour, S. (2012), 'Introduction', in: Allum, F. and Gilmour, S. (eds), Routledge Handbook of Transnational Organized Crime, 2nd edition, Routledge, New York, pp. 1–17.

Argueta, J. J. and Lonergan, H. (2020), 'Labeling theory: A theoretical and empirical overview', in: Conyers, A. and Calhoun, T. C. (eds), Deviance Today, 2nd edition, Routledge, London, pp. 53–62.

Bandura, A. (1977), Social Learning Theory, Prentice-Hall, Hoboken.

Bandura, A. (1999), Moral disengagement in the perpetration of inhumanities, Personality and Social Psychology Review, Vol. 3, No 3, pp. 193–209, https://doi.org/10.1207/s15327957pspr0303_3.

Bardin, L. (2018), Análise de conteúdo, Edições 70, Lisbon.

Barlow, H. D. and Kauzlarich, D. (2010), Explaining Crime: A primer in criminological theory, Rowman & Littlefield, Lanham.

Bernburg, J. (2009), 'Labeling theory', in: Krohn, M., Lizotte, A., and Hall, G. H. (eds), Handbook on Crime and Deviance, Springer, New York, pp. 187–207, https://doi.org/10.1007/978-1-4419-0245-0_10.

Bourdieu, P. (2018), 'The forms of capital', in: Granovetter, M. (ed.), The Sociology of Economic Life, 3rd edition, Greenwood Press, Westport https://doi.org/10.4324/9780429494338.

Braun, V. and Clarke, V. (2006), 'Using thematic analysis in psychology', Qualitative Research in Psychology, Vol. 3, No 2, pp. 77–101, https://doi.org/10.1191/1478088706qp063oa.

Braun, V. and Clarke, V. (2023), 'Toward good practice in thematic analysis: Avoiding common problems and be(com)ing a knowing researcher', International Journal of Transgender Health, Vol. 24, No 1, pp. 1–6, https://doi.org/10.1080/26895269.2022.2129597.

Buckley, P. J., Enderwick, P., Hsieh, L. and Shenkar, O. (2024), 'International business theory and the criminal multinational enterprise', Journal of World Business, Vol. 59, No 5, 101553, https://doi.org/10.1016/j.jwb.2024.101553.

Calderoni, F.Campedelli, G. M., Szekely, A., Paolucci M. and Andrighetto, G. (2021), 'Recruitment into organized crime: An agent-based approach testing the impact of different policies', Journal of Quantitative Criminology, Vol. 38, pp. 1–41, https://doi.org/10.1007/s10940-020-09489-z.

Cornish, D. B. and Clarke, R. V. (1986), The Reasoning Criminal: Rational choice perspectives on offending, Springer-Verlag, Berlin.

Dickie, J. (2024), 'Ginsborg, Gambetta, and the Mafia', in: Foot, J. M. and Gundle, S. (eds), Paul Ginsborg and the Historiography of Modern Italy: Revolutions, revolt and resistance, Springer International Publishing, Cham, pp. 33–52.

Dowler, K., Fleming, T. and Muzzatti, S. L. (2006), 'Constructing crime: Media, crime, and popular culture', Canadian Journal of Criminology and Criminal Justice, Vol. 48, No 6, pp. 837–850, https://doi.org/10.3138/cjccj.48.6.837.

Felgueiras, S., Pais, L. G. and Morgado, S. (2019), 'Interoperability: Diagnosing a novel assessment model', European Law Enforcement Research Bulletin, Special Conference Edition No 4, pp. 255–260.

Gambetta, D. (1993), The Sicilian Mafia: The business of private protection, Harvard University Press, Cambridge, Massachusetts.

Gee, J. P. (2014), An Introduction to Discourse Analysis: Theory and method, 4th edition, Routledge, London.

Gomes, S., Sardá, T. and Granja, R. (2022), 'Crime, justice and media: Debating (mis)representations and renewed challenges', Comunicação e Sociedade, Vol. 42, pp. 7–24, https://doi.org/10.17231/comsoc.42(2022).4467.

Goode, E. (2022), Deviant Behavior, 13th edition, Routledge, London, https://doi.org/10.4324/9781003285304.

Hosford, K., Aqil, N., Windle, J., Gundur, R. V. and Allum, F. (2021), 'Who researches organised crime? A review of organised crime authorship trends (2004–2019)', Trends in Organized Crime, Vol. 25, pp. 249–271, https://doi.org/10.1007/s12117-021-09437-8.

Hu, X. and Lovrich, N. P. (2024), Social Media and Criminal Justice, Taylor & Francis, London https://doi.org/10.4324/9781003360049.

Kleemans, E. R. and De Poot, C. J. (2008), 'Criminal careers in organized crime and social opportunity structure', European Journal of Criminology, Vol. 5, No 1, pp. 69–98, https://doi.org/10.1177/1477370807084225.

Klein, M. W. (1986), 'Labeling theory and delinquency policy', Criminal Justice and Behavior, Vol. 13, No 1, pp. 47–67, https://doi.org/10.1177/0093854886013001004.

Krippendorff, K. (2019), Content Analysis: An introduction to its methodology, 4th edition, Sage, Newcastle upon Tyne, https://doi.org/10.4135/9781071878781.

Machado, P., Pais, L. G., Morgado, S. and Felgueiras, S. (2021), 'An inter-organisational response to domestic violence: The pivotal role of police in Porto, Portugal', European Law Enforcement Research Bulletin, Vol. 21, pp. 121–139, https://www.cepol.europa.eu/api/assets/CEPOL_European_Law_Enforcement_Research_Bulletin_Issue_21.pdf.

Marsh, I. & Melville, G. (2019), Crime, Justice and the Media, 3rd edition, Routledge, London, https://doi.org/10.4324/9780429432194.

Merton, R. K. (1938), 'Social structure and anomie', American Sociological Review, Vol. 3, No 5, pp. 672–682, https://doi.org/10.2307/2084686.

Morgado, S. (2013), Crime and Socioeconomic context: A framework approach, Publishing Institution of the University of Zilina, pp. 139–142.

Morgado, S. M. A. (2022), 'Improving communication with media: Portuguese national public police case', in: Reis, J. L., Parra López, E., Moutinho, L. and Marques dos Santos, J. P. (eds), Marketing and Smart Technologies – Smart innovation, systems and technologies, Springer, Singapore, pp. 105–119, https://link.springer.com/chapter/10.1007/978-981-16-9268-0_9

Morgado, S. and Alves, R. (2019), 'Core capabilities: Body-worn cameras in Portugal', European Law Enforcement Research Bulletin, Vol. 18, pp. 105–119.

Morgado, S.M.A., Carvalho, M., Felgueiras, S. (2024). Diagnosis Model for Detection of e-threats Against Soft-Targets. In: Rocha, A., Adeli, H., Dzemyda, G., Moreira, F., Colla, V. (eds) Information Systems and Technologies. WorldCIST 2023. Lecture Notes in Networks and Systems, vol 800. Springer, Cham. https://doi.org/10.1007/978-3-031-45645-9_24

Morgado, S. M. A., Neves, L. and Sequeira, P. (2023), 'Policing in sport hall sporting events: A look through several lenses', Lecturas: Educácion Física Y Deportes, Vol. 28, No 299, pp. 101–118, https://doi.org/10.46642/efd.v28i299.3494.

Morgado, S. M. A. and Felgueiras, S. (2022), 'Technological policing: Big data versus real data, Politeia – Revista Portuguesa de Ciências Policiais, Vol. 19, pp. 139–151, https://doi.org/10.57776/0pep-xz31.

Morgado, S. M. A., Nabais, T. & Felgueiras, S., 2024b. Unveiling the project facilitating Public & Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts – APPRAISE: the future for preventing and providing security for soft targets. In: *40 anos das Ciências Policiais em Portugal.* Lisboa: ICPOL (pp. 277-285).

Morselli, C. (2009), Inside Criminal Networks, Springer, New York.

Moura, R., Birges, A., Morgado, S. and Ramalho, N. (2022), 'Police leadership 2.0: A comprehensive systematic review of the literature', Policing: A Journal of Policy and Practice, Vol. 17, pp. 1–11, https://doi.org/10.1093/police/paac068.

Mowen, T. J. and Heitkamp, A. (2023), 'The label of looks: Physical attractiveness, stigma, and deviant behavior', Sociological Focus, Vol. 56, No 4, pp. 407–423, https://doi.org/10.1080/00380237.2023.2239733.

Muzzatti, S., Colaguori, C. and Smith, E. (2023), 'Cultural criminology and popular media representations of crime', in: Colaguori, C. (ed.), Crime, Deviance, and Social Control in the 21st Century: A justice and rights perspective, Canadian Scholars, Toronto, pp. 115–152.

Neuendorf, K. A. (2017), The Content Analysis Guidebook, 2nd edition, Sage Publications, Newcastle upon Tyne.

Ozark (2017–2022), [Television series] directed by Bateman, J., Mundy, C., Dubuque, B. and Williams, M., produced by MRC Television and Aggregate Films, United States.

Peaky Blinders (2013–2022), [Television series] directed by Caryn Mandabach Productions and Tiger Aspect Productions, produced by Caryn Mandabach Productions and Tiger Aspect Productions, United Kingdom.

Pfeiffer, C., Windzio, M. and Kleimann, M. (2005), 'Media use and its impacts on crime perception, sentencing attitudes, and crime policy', European Journal of Criminology, Vol. 2, No 3, pp. 259–285, https://doi.org/10.1177/1477370805054099.

Phillips, A. (2016), 'Corrado Alvaro and the Calabrian Mafia: A critical case study of the use of literary and journalistic texts in research on Italian organized crime', Trends in Organized Crime, Vol. 20, pp. 179–195, https://doi.org/10.1007/s12117-016-9285-0.

Raets, S. (2024), 'Desistance, disengagement, and deradicalization: A cross-field comparison', International Journal of Offender Therapy and Comparative Criminology, Vol. 68, No 4, pp. 389–426, https://doi.org/10.1177/0306624X221102802.

Reiner, R. and Livingstone, S. (1997), Discipline or Desubordination? Changing media images of crime, ESRC, London.

Rich, P. B. (2020), 'Hollywood and cinematic representations of far-right domestic terrorism in the U.S.', Studies in Conflict & Terrorism, Vol. 43, No 2, pp. 161–182, https://doi.org/10.1080/1057610X.2018.1446295.

Shaw, C. R. and McKay, H. D. (1942), Juvenile Delinquency and Urban Areas, University of Chicago Press, Chicago.

Shelley, L. I. (2018a), Dark Commerce: How a new illicit economy Is threatening our future, Princeton University Press, Oxford.

Shelley, L. I. (2018b), 'Corruption & illicit trade', Daedalus, Vol. 147, No 3, pp. 127–143 https://www.jstor.org/stable/48563085.

Sicário(2015) [Film] directed by McDonnell, E., Smith, M., Luckinbill, T., Luckinbill, T. and Iwanyk, B., produced by Thunder Road Pictures, Black Label Media and Lionsgate, United States / Mexico.

Surete, R. (2015), Media, Crime and Criminal Justice: Images, realities and policies, Cengage Learning, Boston.

Sutherland, E. H. and Cressey, D. R. (1978), Criminology, 10th edition, Lippincott Williams & Wilkins, Philadelphia.

Sykes, G. M. and Matza, D. (1957), 'Techniques of neutralization: A theory of delinquency', American Sociological Review, Vol. 22, No 6, pp. 664–670, https://doi.org/10.2307/2089195.

Tannenbaum, F. (1938), Crime and the Community, Columbia University Press, New York https://doi.org/10.7312/tann90782.

Tannenbaum, L. Lemert, C., Goffman, B., Becker, H. S. and Braithwaite, J. (2021), 'Societal reactions and labeling of deviance', in: Behl, J. D. and Steverson, L. A. (eds), Criminal Theory Profiles: Inside the minds of theorists of crime and deviance, Taylor and Francis, New York.

The Godfather (1972), [Film] directed Coppola, F. F., produced by Paramount Pictures and Alfran Productions, United States.

Topalli, V. (2005), 'When being good is bad: An expansion of neutralization theory', Criminology, Vol. 43, No 3, pp. 797–835, https://doi.org/10.1111/j.0011-1348.2005.00024.x.

van Gelder, J. L., Elffers, H., Reynald, D. and Nagin, D. (2013), Affect and Cognition in Criminal Decision-making: Between rational choices and lapses of self-control, 1st edition, Routledge, Berlin.

van Koppen, M. V., De Poot, C. J. and Blokland, A. A. (2010), 'Comparing criminal careers of organized crime offenders and general offenders', European Journal of Criminology, Vol. 7, No 5, pp. 356–374, https://doi.org/10.1177/1477370810373730.

van Koppen, V., van der Geest, V., Kleemans, E. and Kruisbergen, E. (2022), 'Employment and crime: A longitudinal follow-up of organized crime offenders', European Journal of Criminology, Vol. 19, No 5, pp. 1097–1121, https://doi.org/10.1177/1477370820941287.

Weaver, B. (2019), 'Understanding desistance: A critical review of theories of desistance', Psychology, Crime & Law, Vol. 25, No 6, pp. 641–658, https://doi.org/10.1080/1068316X.2018.1560444.

Weisburd, D., Uchida, C. D. and Lum, C. (2020), The Law of Crime Concentration, Oxford University Press, Oxford.

Welsh, A., Fleming, T. and Dowler, K. (2011), 'Constructing crime and justice on film: Meaning and message in cinema', Contemporary Justice Review, Vol. 14, No 4, pp. 457–476, https://doi.org/10.1080/10282580.2011.616376.

Zeppa, C. J. (2014), 'Entertaining media representations of crime and the criminal justice system: A review essay', Critical Criminology, Vol. 23, pp. 209–213, https://doi.org/10.1007/s10612-014-9263-2.

Appendices

Appendix 18.1. Subcategories of Category A – Recruit

Subcategory	Description
	Information describing the characteristics of the recruit.
A.1. Age	Information on the age of the recruit (e.g. young people).
A.2. Gender	Information on the gender of the recruits.
A.3. Ethnicity	Information on the influence of ethnic factors (e.g. ethnic homogeneity).
A.4. Level of education/ experience	Information on the level of education and experience of those recruited (e.g. illiteracy).
A.5. Employment	Information on factors such as the recruit's job or profession (e.g. employees of logistics companies).
A.6. Economic conditions	Information on the recruit's economic situation (e.g. poverty).
A.7. Social ties	Information about the recruit's social relationships (e.g. family connection or groups to which they belong).
A.8. Group affiliation	Information on the values and culture shared by the recruit and the groups to which they belong.
A.9. Psychological factors	Information about the recruit's psychological characteristics (e.g. being antisocial).
A.10. Criminal record	Information about the recruit's criminal record (e.g. risky behaviour).
A.11. Code of silence	Information about the recruit's ability to comply with the code of silence.
A.12. Addictions	Information about the recruit's addictions (e.g. drugs, sex, gambling).

Appendix 18.2. Subcategories of Category B – Decision-making process

Subcategory	Description
B.1. Timelines	Description of the role that opportunities play in the recruitment process (i.e. considering that the opportunity is the recruit's perception of gaining an advantage).
B.2. Biological determinants	Information on the hereditary aspects that influence the recruitment process.
B.3. Cultural transmission	Information on the learning and acculturation processes that influence recruitment process.
B.4. Feeling of failure and frustration associated with traumatic event	Information on the influence or facilitation that feelings of failure and/or frustration and the presence of a traumatic event have on recruitment.
B.5. Valuing status, prestige and respect	Information on the perception that status, prestige and respect have on the individual's recruitment process.
B.6. Profit, power and influence	Information on the importance of profit, power and influence on the individual's recruitment process.
B.7. Exclusion of young people from the labour market	Information on the influence that the lack of opportunities associated with the exclusion of young people from the labour market has on the recruitment process.
B.8. Gender inequality	Information on the role that inequality plays in the recruitment process.

Appendix 18.3. Subcategories of Category C – Recruitment

Subcategory	Description
C.1. Organisation	Information on the organisation promoting the recruitment (e.g. centralised or decentralised).
C.1.a. Centralised recruitment	
C.1.b. Decentralised recruitment	
C.2. Place of occurrence	Information on the location of the recruitment process.
C.2.a. Public place	
C.2.b. Private place	
C.3. Type of recruitment	Information on the type of recruitment (e.g. individual or block).
C.3.a. Individual	
C.3.b. In block	
C.4. Modus operandi	Information on the recruitment strategy used by criminal organisation.
C.5. Role in the organisation	Information on the role played in the organisation by the recruit.
C.6. Time of recruitment	Information on the time of recruitment.
C.7. Allied systems	Information on the organisations collaborating with the recruiting organisation.

Appendix 18.4. Subcategories of category D – Spontaneous explanatory system

Subcategory	Description
D.1. Recruit	Information explaining the recruit's decision to join the organisation.
D.2. Recruiter	Information explaining the actions of the organisation's recruiters in the recruitment process.

Two-way crimes, parallel economies and professional enablers: Dissecting corruption in the EU's financial sector

Jasmin Saarijärvi, Mark Worth

https://doi.org/10.3013/rr4v5t41

Abstract

The European Union is in the midst of developing an anti-corruption strategy to achieve the multi-part goal of pre-empting corruption, improving oversight, strengthening enforcement and reducing the damage that corruption causes to public institutions, companies, communities and citizens. To further this undertaking, we have identified areas and sectors that are especially prone to corruption. This entailed a three-step process of identifying a broad list of high-risk areas, narrowing these to six areas for in-depth study and examining the character, causes and consequences of corruption in these six sectors.

One of these areas is the financial sector. A significant portion of corruption in the EU either originates from the financial sector or is inflicted upon it; sometimes the line between perpetrator and victim is blurred. As the most serious corruption-related crimes, money laundering and tax evasion involve many types of people and organisations including banks, investment advisors, wealth managers and organised crime groups. With the help of professional enablers such as lawyers, notaries, accountants and real estate agents, organised crime groups have built a 'parallel criminal economy' in the EU. This complex and overlapping landscape complicates interdiction, as the epicentre of any particular corrupt act is not always easy to pinpoint.

Keywords: European Union, anti-corruption, corruption risks, financial sector, financial regulation, organised crime, financial crime.

Introduction: towards a new EU anti-corruption strategy

Two thirds of EU citizens and EU-based companies believe corruption is widespread in their country (Eurobarometer, 2024). Citizens' pessimistic views on corruption have remained unchanged for the past two decades, indicating that most Europeans are unsatisfied with official measures to stop it or that corruption is not declining – or both. The economic costs of corruption in the EU are estimated at up to EUR 990 billion per year (Fernandes et al., 2023), reducing the EU's gross domestic product by about 6 % annually (Greens/EFA Group in the European Parliament, 2018).

A significant portion of this corruption originates from, or is inflicted upon, the financial sector. Corruption in the financial industry is everywhere and is being committed at every level of society – from individual scammers on laptops to unscrupulous banks and investment houses, to international money-laundering and terrorism-financing networks. It is an enormous, ever-evolving industry that is both perpetrator and victim of corruption. Serious corruption crimes include money laundering, tax evasion, hidden assets, consumer fraud, terrorism financing and cybercrimes.

As the financial sector becomes more decentralised, unwieldy and IT-driven, the opportunities to become a perpetrator and/or a victim continue to grow. As an example of such two-way crimes, banks both condone and are victimised by money laundering, tax evasion and other crimes.

Sensing the need to better tackle these problems, the EU is developing an anti-corruption strategy. As part of this effort, the European Commission released the study, 'High-risk areas of corruption in EU Member States: A mapping and in-depth analysis' (European Commission: Directorate-General for Migration and Home Affairs et al., 2024). The study's goal is to provide a deeper knowledge base regarding the sources of corruption in EU Member States and explore particularly vulnerable areas. The study feeds into tasks anticipated in the Commission's joint communication on the fight against corruption (European Commission, 2023).

The Commission's study identified six areas that necessitate urgent responses – those responses being, improvements in regulation, oversight, investigation, enforcement and prosecution. In addition to the financial sector, these high-risk areas are public procurement, construction and infrastructure, healthcare, defence and security, and sports. Though virtually all areas of society can expect some degree of corruption, many experts expressed the view that these areas already are, or are likely to become, more prone to serious crimes.

This paper, which focuses on the financial sector, is an excerpt of the Commission's study, published by the Directorate-General for Migration and Home Affairs in November 2024. As a follow-up, work began in autumn 2024 on a report for the Commission on successful measures to mitigate corruption. Scheduled for completion in 2025-2026, the report will outline and analyse measures in Member States that could be replicated EU-wide.

The nature of corruption in the financial sector

An interplay of crimes

The EU's financial sector is a diverse, continuously evolving industry that provides an increasingly complex set of financial services and informational tools to commercial and retail customers. Financial companies include investment and commercial banks, insurance companies, investment houses, money managers, mortgage and other lenders, fintech and cryptocurrency companies, payment services and foreign exchange firms.

As the financial sector is becoming more decentralised and unwieldy, the opportunities to become a perpetrator and/or a victim continue to grow. Corruption enablers, including lawyers, notaries, accountants, real estate agents and other professionals, sell their expertise to help criminals hide their money, avoid paying taxes and evade detection. Organised crime groups (OCGs) have built a 'parallel global criminal economy' in the EU, which lies at the heart of much of the corruption.

Perhaps more than any other area, assessing the types and methods of corruption in the financial sector is just as important as examining the perpetrators and venues. Granted this, money laundering and tax evasion are the most serious corruption-related crimes in the EU and those that receive the most attention of policymakers and criminal justice agencies. These crimes involve many different types of people and organisations, including banks, investment advisors, OCGs and professional enablers. This complex and overlapping landscape complicates the corruption assessment, as the epicentre of any particular corrupt act is not always easy to pinpoint. Further, the 'financial sector' does not have a precise definition, and the terms 'financial corruption' and 'financial crime' often are interchanged by practitioners and researchers.

Corruption costs

Estimating the scale and costs of corruption is challenging because much available research and many statistics combine financial and economic crimes. It can be difficult to differentiate the cost of crimes that utilise or victimise the financial sector from the cost of economic crimes in general. The European Union Agency for Law Enforcement Cooperation (Europol) notes that corruption in the sector remains systematically under-investigated (Europol, 2020).

Moreover, transferring criminal proceeds online and using cash for lower-level bribery can make it difficult to detect financial flows and uncover corruption (Europol, 2020). For this and other reasons (including the fact that more than 60 % of OCGs in Europe use 'corruptive methods to achieve their illicit objectives'), less than 2 % of OCGs' proceeds are seized each year (Europol, 2023b). Making matters more difficult, nearly 70 % of criminal networks operating in the EU use at least one form of money laundering to fund their activities and conceal their assets (AML Intelligence, 2023). The lines between the illicit and licit world become increasingly blurred (Europol, 2023a).

OCGs are drawn to the EU, among many reasons, because of its strong economy and high standard of living. Europe is an attractive terrain for investment in real estate (Cotici, 2024). They also target countries and jurisdictions with gaps in international anti-money-laundering (AML) standards and law enforcement cooperation (Europol, 2023a).

The European Public Prosecutor's Office (EPPO) had 226 active money-laundering cases at the end of 2023, making up 5 % of its total caseload (EPPO, 2024). The European Union Agency for Criminal Justice Cooperation (Eurojust) recorded 2 870 money-laundering cases in 2016–2021, representing 12–14 % of all cases. The annual total doubled during this period. The top five Member States involved with these cases are Germany, Spain, France, Italy and the Netherlands (Eurojust, 2022).

Given these shortcomings, kleptocrats and their family members use European banks to launder their criminal proceeds, along with their reputations. Even when malpractice is identified, national authorities often do not take appropriate action, according to Transparency International, which stated that the European Central Bank's supervision of banks' AML activities is 'very limited' because many issues are handled by national authorities (Martini, 2019).

Causes of corruption in the financial sector

Upperworld and underworld

There are large gaps in understanding the nexus between corruption and money laundering, as well as the structures and mechanisms that allow these crimes to be committed, according to the Basel Institute on Governance. In general terms, it is known that secrecy jurisdictions and service providers such as financial intermediaries, lawyers, bankers and accountants 'have emerged as constant actors in corruption and money-laundering cases of all types, all over the world' (Costa, 2021).

These players make up webs of cross-border links and financial transactions that 'disguise illicit connections between corrupt political elites and the businesses that thrive by bribing these individuals', according to the Basel Institute. These transnational networks also include offshore companies, corporate vehicles, intermediaries, service providers and financial institutions that conspire to move illicit assets and hide them from the public and law enforcement. These financial and legal service providers manage these networks and lower the transactional costs of international corruption (Costa, 2021).

Offshore financial centres are uniquely skilled to simultaneously ensure the ownership and non-ownership of assets. This means they guarantee the indirect and mediated control of assets by their ultimate beneficiaries, all the while disguising the connections between offshore financial centres and their beneficial owners. This is done via service providers, surrogates, frontmen and cross-border chains of offshore vehicles.

In addition, these structures simultaneously occupy both the 'upperworld' of formality and the 'underworld' of informality. This is achieved by switching between the legal facade of their business and political activities and the hidden financial infrastructure that helps to disguise their illicit transactions (Costa, 2021).

Aided by globalisation and under-regulated online platforms, money launderers can quickly move illicit funds in and out of the EU, from and to anywhere in the world. About 70 % of OCGs operating in the EU use basic money-laundering techniques, while the rest work with professional money-laundering networks or underground

banking systems that operate in multiple jurisdictions (Europol, 2020; Europol, 2023a). Various investigative agencies describe money laundering as perhaps the most widespread financial crime in the EU.

Outmatched regulators and black holes

Because of the industry's complexity, enormous size and the number of transactions it handles, suspicious and illegal transactions can be difficult to identify, monitor and remedy. The inadequacy of mechanisms to watchdog transactions can lead to fraud, bribery, money laundering and other types of corruption (Ragazou et al., 2022). Europe's financial industry has shown signs of improvement with regard to the fight against corruption in recent years, but considerable challenges remain. One reason is executives' limited ability to thoroughly evaluate and comprehend market trends and corruption indicators (Zafeiriou et al., 2023).

Another major reason, according to Europol, is the low-risk and high-reward nature of financial crimes, which makes them 'very attractive' to OCGs. Additionally, the complexity of these crimes and the sophisticated expertise required to commit them makes them difficult to detect and investigate. This problem has grown worse because of technical innovation and the digitalisation of financial transactions. Because of this, 'many of these crimes are now even less visible than before and more challenging to investigate' (Europol, 2020).

In particular, Eurojust said it is challenged by differences in national laws used to identify predicate offences for money laundering. Other challenges include the increased use of cryptocurrencies, shell companies that hide the identity of beneficial owners of criminal assets, difficulties in identifying who is a victim and who can apply for compensation, and difficulties tracing money transfers to and from the EU (Europol, 2022).

New concepts of financial services, including fintech, artificial intelligence (AI), virtual international bank account numbers (vIBANs), and decentralised finance such as cryptocurrencies and blockchain, are increasingly being exploited by criminal networks to launder money and commit fraud and other crimes (AML Intelligence, 2023).

Risks to citizens also are on the rise. An estimated 58 % of banking customers in the EU regularly carry out transactions via online tools such as websites and apps. These platforms provide significant benefits to customers and companies alike. However, many customers lack the technical knowledge and experience to protect them from cybercriminals who use phishing and malware to burrow into their online accounts (Europol, 2020).

These risks to consumers have been fuelled by the huge expansion of online shopping. The proliferation of digital payment systems and the reduced ability to verify customers due to cross-border trade are making fraud prevention more complex. 'No merchant, bank or payment service provider has all the data necessary to determine whether a transaction has been executed by the customer or a fraudster' (Forster, 2019).

The industry is not free of political corruption. There are 'significant' risks of corruption in the context of financial companies that do business with public banks or sovereign wealth funds, according to Association Europe-Finances-Régulations (Montigny, 2016).

Consequences of corruption in the financial sector

Parallel underground societies

Financial crime is a 'highly complex, significant threat that affects millions of citizens and thousands of companies in the EU every year', according to Europol. These crimes destabilise economies and undermine social security systems, depriving society of prosperity, economic growth and employment. 'Although indirect, the impact these crimes have on society cannot be underestimated' (Europol, 2020).

Financial crimes, especially money laundering, not only infiltrate the legal economy but also foster the growth of a parallel underground society dominated by OCGs. 'Vulnerable demographics, and especially vulnerable youngsters who are lacking trust in societal institutions and confidence in the rule of law, are the perfect target pool for such parallel underground society' (Europol, 2023a).

Fraud is one of the main ingredients, to a lesser or greater extent, in virtually every type of financial crime. Its economic impact is 'staggering', stated the International Criminal Police Organization (Interpol), noting that tech-savvy fraudsters stay one step ahead of law enforcement by exploiting new vulnerabilities and 'circumventing security measures' (Interpol, 2024).

Both the volume and methods of financial fraud are increasing and diversifying significantly. Financial fraud, which Interpol calls a 'pervasive, global threat', is a predatory crime perpetrated in anonymity and across borders. In Europe, the most prevalent types are investment fraud, business email compromise, romance fraud and telecom fraud. A hybrid scheme known as 'pig butchering' combines romance and investment fraud, often using cryptocurrencies. Victims of these swindles are often hesitant to come forward. Another new type of scam is the 'rug pull', when a cryptocurrency outfit suddenly abandons their investors (Interpol, 2024).

Within banks and other financial companies, the 'fraud tree' has three main branches: asset misappropriation, corruption and tax evasion. All of these, individually or in unison, can be a cause of another type of fraud: the misstatement of financial statements. 'All the aspects of the fraud tree have become widespread in the past ten years in both the business and banking worlds'. Moreover, corruption and fraud in banking are 'complex problems that confound researchers' (Zafeiriou et al., 2023).

A growing area of fraud is internet and cross-border card swindles, which reached EUR 1.8 billion as of 2016, according to the European Central Bank. That year, three fourths of all fraud losses on cards issued in the single euro payments area (SEPA) were from 'card-not-present payments' – namely, payments made by post, telephone or over the internet (Forster, 2019).

Many investment fraud schemes are now carried out exclusively online or via advertising on social media platforms. These schemes use tools such as foreign exchange trading platforms, binary options and online crowdfunding. Advance-fee fraud schemes, in which people are promised a large sum of money in return for a small upfront payment, are increasingly being perpetrated with alternative payment methods such as online vouchers (Europol, 2020).

Other tools used by fraudsters and money launderers are digital or 'neo' banks. These virtual financial institutions have no physical branches and are growing quickly. With IBANs, international payments can be made quickly while masking the identity of the master account, issuer and country of origin. This makes suspicious transactions tougher to detect and adds extra steps to investigations. In all EU Member States, digital payments are being used for money laundering (Europol, 2023a).

Another major risk area is value added tax fraud. Based on investigations by the EPPO, OCGs finance value added tax fraud schemes with illicit funds from other criminal activities. These groups easily can be set up in any country and recruit people with local connections and knowledge of the local market and law. They choose EU Member States with weaker detection and investigation capabilities, spot loopholes and use professional enablers, high-level brokers and financial channels outside the formal financial system (EPPO, 2024).

References

BankTrack, Les Amis de la Terre and National Committee to Combat Climate Change (2017), 'Odebrecht corruption in Dominican Republic – Five European banks urged to pull out of dirty coal plant financing', BankTrack website, 18 January, https://www.banktrack.org/news/odebrecht_corruption_in_dominican_republic_five_european_banks_urged_to_pull_out_of_dirty_coal_plant_financing.

Basquill, J. (2021), 'Germany's KfW Ipex-Bank fined over loan linked to Angolan corruption scandal', *Global Trade Review*, 8 September, https://www.gtreview.com/news/europe/germanys-kfw-ipex-bank-fined-over-loan-linked-to-angolan-corruption-scandal/.

Costa, J. (2024), personal interview, Basel Institute on Governance.

Costa, J. (2021), 'Revealing the networks behind corruption and money laundering schemes: An analysis of the Toledo-Odebrecht case using social network analysis and network ethnography', Basel Institute on Governance, Working Paper 36, July, https://baselgovernance.org/sites/default/files/2021-07/Working %20Paper %2036 %20Odebrecht %20Toledo.pdf.

Cotici, R. (2024), personal interview, International Development Law Organization.

de Andrés, P., Polizzi, S., Scannella, E. and Suárez, N. (2022), 'Corruption-related disclosure in the banking industry: Evidence from GIPSI countries', *The European Journal of Finance*, Vol. 30, Issue 4, 20 December, https://doi.org/10.1080/1351847X.2022.2153073.

Eurobarometer (2024), 'Citizens' attitudes towards corruption in the EU in 2024', https://europa.eu/eurobarometer/surveys/detail/3217.

Eurojust (2024), 'Full-scale action against EUR 2 billion money laundering network via Lithuanian financial institution', Eurojust website, 27 February, https://www.eurojust.europa.eu/news/full-scale-action-against-eur-2-billion-money-laundering-network-lithuanian-financial.

Eurojust (2023), 'Economic crimes', Eurojust website, https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/economic-crimes.

Eurojust (2022), *Eurojust Report on Money Laundering*, Eurojust, The Hague, October, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-report-money-laundering-2022.pdf.

European Banking Authority (2022a), 'EBA Report on competent authorities' responses to the 2020 Luanda leaks', EBA/REP/2022/05, 22 February, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2022/1027361/Report%20Risk%20assessment%20on%20Luanda%20Leaks%20under%20art%209a.pdf.

European Banking Authority (2022b), 'EBA concludes its Luanda leaks investigation and points to significant differences in competent authorities' responses to emerging money laundering and terrorist financing risks', European Banking Authority website, 22 February, https://www.eba.europa.eu/publications-and-media/press-releases/eba-concludes-its-luanda-leaks-investigation-and-points.

European Commission: Directorate-General for Migration and Home Affairs, Persson, A., Worth, M. and Jeney, P. (2024), *High-Risk Areas of Corruption in the EU – A mapping and in-depth analysis*, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2837/5907939.

European Parliament and European Council (2023), Proposal for a directive of the European Parliament and of the Council on combating corruption, COM(2023) 234 final of 3 May 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A234%3AFIN.

European Parliament and European Council (2018), Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law (OJ L 284, 12.11.2018, p. 22, ELI: https://eur-lex.europa.eu/eli/dir/2018/1673/oj).

EPPO (2024), *EPPO Annual Report 2023*, Publications Office of the European Union, Luxembourg, https://www.eppo.europa.eu/document/download/23b0f21c-c43a-4aec-8f47-4af07cc712e3_en?filename=EPPO_Annual_Report_2023.pdf.

Europol (2023a), European Financial and Economic Crime Threat Assessment 2023 – The other side of the coin: An analysis of financial and economic crime, Publications Office of the European Union, Luxembourg, https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf.

Europol (2023b), 'New Europol report shines light on multi-billion euro underground criminal economy', Europol Newsroom, 11 September, https://www.europol.europa.eu/media-press/newsroom/news/new-europol-report-shines-light-multi-billion-euro-underground-criminal-economy.

Eurojust (2022), 'Eurojust Casework on Corruption: 2016–2021 Insights', May, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-casework-on-corruption-2016-2021-insights-report.pdf.

Europol (2020), 'Enterprising criminals: Europe's fight against the global networks of financial and economic crime', https://www.europol.europa.eu/cms/sites/default/files/documents/efecc_-_enterprising_criminals_-_europes_fight_against_the_global_networks_of_financial_and_economic_crime_.pdf.

Fernandes, M. and Jančová, L. (2023), 'Stepping up the EU's efforts to tackle corruption: Cost of non-Europe report', European Parliamentary Research Service, PE 734.687, https://www.europarl.europa.eu/RegData/etudes/STUD/2023/734687/EPRS_STU(2023)734687_EN.pdf.

Forster, H. (2019), 'European fraud report – Payments industry challenges', Nets Group, https://www.nets.eu/solutions/fraud-and-dispute-services/Documents/Nets-Fraud-Report-2019.pdf.

Freedberg, S. P., Alecci, S., Fitzgibbon, W., Dalby, D. and Reuter, D. (2020), 'Luanda leaks: How Africa's richest woman exploited family ties, shell companies and inside deals to build an empire', International Consortium of Investigative Journalists, 19 January, https://www.icij.org/investigations/luanda-leaks/how-africas-richest-woman-exploited-family-ties-shell-companies-and-inside-deals-to-build-an-empire/.

Green, R. (2019), 'The fight against corruption: Europe's black hole', International Bar Association, https://www.ibanet.org/article/7616EA92-EC08-4610-8DF4-99A4845903A9.

Greens/EFA Group in the European Parliament (2018), 'The Costs of Corruption Across the EU', https://www.greens-efa.eu/files/assets/docs/the_cost_of_corruption_across_the_eu_final_report_07.12.2018.pdf.

Gronholt-Pedersen, J. and Guarascio, F. (2019), 'EU states force clearing of Estonian, Danish regulators over Danske Bank', Reuters, 17 April, https://www.reuters.com/article/us-danske-bank-moneylaundering/eu-states-force-clearing-of-estonian-danish-regulators-over-danske-bank-idUSKCN1RT0VZ/.

Group of States against Corruption (2024), '24th General Activity Report (2023) of the Group of States against Corrpution (GRECO): Anti-corruption trends, challenges and good practices in Europe and the United States of America', Council of Europe, May, https://rm.coe.int/general-activity-report-2023-greco-060424-gbr-web/1680afd7f2.

Guarascio, F. (2019), 'Explainer – Europe's money laundering scandal', Reuters, 4 April, https://www.reuters.com/article/idUSKCN1RG1XB/.

Interpol (2024),Interpol Global Financial Fraud Assessment, Interpol General Secretariat, Lyon, https://www.interpol.int/content/download/21096/file/24COM005563-01_%20-_%20CAS_Global_%20Financial_%20Fraud_%20Assessment_Public%20version_2024-03%20v2-1.pdf.

Interpol (n.d.), 'Our role in fighting financial crime', Interpol website, https://www.interpol.int/en/Crimes/Financial-crime/Our-role-in-fighting-financial-crime.

Martini, M. (2019), 'European banks in money laundering scandals: What lessons for the EU?', Transparency International, 26 February, https://www.transparency.org/en/blog/european-banks-in-money-laundering-scandals-what-lessons-for-the-eu.

Montigny, P. (2016), 'Anti-corruption challenges for the financial sector', Association Europe-Finances-Régulations, 19 May, https://www.aefr.eu/en/news/4369/anti-corruption-challenges-for-the-financial-sector.

Ragazou, K., Passas, I. and Garefalakis, A. (2022), 'It is time for anti-bribery: Financial institutions set the new strategic "roadmap" to mitigate illicit practices and corruption in the market', *Administrative Sciences,* Vol. 12, No 4, https://hdl.handle.net/10419/275436.

Transparency International (2020), 'Transparency International EU reveals the murky tax affairs of Europe's biggest banks', 26 October, https://transparency.eu/tax-affairs-of-europes-biggest-banks/.

Transparency International (n.d.), 'Illicit financial flows', Transparency International EU website, https://transparency.eu/priority/financial-flow-crime/.

United States Department of Justice (2024), 'Four men charged in Philippine bribery and money laundering scheme', 8 August, https://www.justice.gov/opa/pr/four-men-charged-philippine-bribery-and-money-laundering-scheme.

Woodman, S. (2021), 'Deutsche Bank agrees to pay $130 million in latest major US penalty', International Consortium of Investigative Journalists, 12 January, https://www.icij.org/investigations/fincen-files/deutsche-bank-agrees-to-pay-130-million-in-latest-major-us-penalty/.

Zafeiriou, E., Garefalakis, A., Passas, I. and Ragazou, K. (2023), 'Illicit and corruption mitigation strategy in the financial sector: A study with a hybrid methodological approach', *Sustainability*, Vol. 15, No 2, 11 January, https://doi.org/10.3390/su15021366.

Strengthening the integrity and independence of police and prosecution institutions in the Western Balkans

Ioannis Vlassis

https://doi.org/10.3013/55qnnh79

Abstract

This article examines the integrity and independence of police and prosecution services in the Western Balkans, focusing on structural and operational factors that continue to undermine their capacity to prevent and prosecute corruption and organised crime. Drawing on comparative, multi-country research conducted between 2023 and 2024, the analysis combines normative and institutional review, with case studies and expert interviews across the Western Balkans six. While the region has undertaken extensive legal and institutional reforms to more closely align themselves with the European Union and international standards, the findings indicate that political interference, weak oversight mechanisms, operational constraints and persistent gender imbalances remain significant challenges. By situating national-level dynamics within a broader regional framework, the article identifies common patterns of vulnerability affecting police and prosecutorial independence. The paper concludes by reflecting on the practical limitations of reform implementation and outlining priority areas where institutional safeguards, professional capacity and accountability mechanisms require strengthening to ensure sustainable progress in the rule of law.

Keywords: police integrity, prosecutorial independence, rule of law, corruption, organised crime, Western Balkans, institutional reform.

Introduction

The Western Balkans six (WB6), made up of Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia, have undergone profound political and legal transformations since the 1990s, moving from totalitarian systems to democratic governance models underpinned by the rule of law. Within this context, police forces were among the first institutions targeted for reform. Shifting from instruments of state power to professional bodies mandated to maintain public order and serve citizens, these reforms aimed to instil principles of accountability,

impartiality and integrity (Zvekic et al., 2024). In recent years and in the context of the EU accession process, additional organisational changes and anti-corruption measures have been introduced to align national legislation with the EU *acquis* and international standards relating to the independence of the police and judiciary.

Despite these efforts, persistent reports from the United Nations (UN), European Commission and prominent civil-society organisations highlight that corruption and weak rule of law remain significant obstacles to democratic consolidation in the region. The inadequate implementation of legislation, combined with external and internal risks to police and prosecutorial independence, continues to undermine the integrity and impartiality of criminal justice institutions. Organised crime and systemic corruption exert influence over state structures and the economy, normalising a degree of tolerance for unethical behaviours, further eroding public trust and contributing to a culture of impunity (Zvekic et al., 2024).

This article draws on recent regional research conducted by the Observatory of Illicit Economies in South Eastern Europe of the Global Initiative Against Transnational Organized Crime (GI-TOC), with a particular focus on police and prosecution services. While grounded in a broader comparative research effort, the article adopts an analytical perspective that foregrounds systemic vulnerabilities affecting institutional integrity and independence across the Western Balkans. Rather than providing an exhaustive account of national reforms, it examines recurring patterns of political influence, weak accountability mechanisms, operational constraints and gender disparities that shape the functioning of criminal justice institutions. In doing so, it seeks to contribute to ongoing debates on the practical limits of institutional reform in environments characterised by entrenched corruption and organised crime.

Methodology

This article draws on research conducted under the anti-corruption portfolio of GI-TOC's Observatory of Illicit Economies in South Eastern Europe, which between 2023 and 2025 focused on the integrity and independence of criminal justice institutions in the WB6. The analysis presented here is derived from a multi-country research programme carried out between June 2023 and January 2024 that centred on police and prosecution services, while selectively foregrounding findings most relevant to institutional independence, integrity risks and governance challenges.

The research design combined qualitative and comparative methods. A common methodological framework was developed at the outset of the study by the regional coordination team to ensure conceptual coherence and cross-country comparability. This framework was informed by international standards on police and prosecutorial independence, integrity and accountability, including relevant European Union *acquis*, Council of Europe instruments and UN norms. It established shared definitions, analytical categories and data-collection protocols to guide national-level research.

Data collection was conducted by national experts in each Western Balkan country, with each component supported by three regional coordinators responsible for quality control and analytical consistency.

The research relied on three primary sources: first, a normative and institutional analysis of legal frameworks governing police and prosecution services; second, qualitative case studies illustrating integrity and independence

challenges in practice; and third, semi-structured interviews with key stakeholders. Interviewees included serving and former police officers, prosecutors, representatives of oversight bodies, civil-society stakeholders, journalists and independent experts with direct knowledge of the criminal justice system. These interviews were used to contextualise formal rules and identify discrepancies between legal provisions and institutional practice. Draft country-level reports were subsequently reviewed by independent external reviewers with relevant professional or academic expertise. Their feedback was incorporated to strengthen factual accuracy and balance.

The article adopts a comparative regional perspective rather than a comprehensive country-by-country assessment. Its analytical focus lies in identifying recurring patterns and systemic vulnerabilities affecting police and prosecutorial independence across the Western Balkans. While the methodology allows for triangulation across legal analysis, empirical cases and stakeholder perspectives, the findings remain subject to certain limitations. These include uneven access to sensitive institutional data, the reliance on qualitative interviews that may reflect subjective perceptions, and the political sensitivity of corruption-related cases, which can constrain transparency. Acknowledging these constraints, the article nevertheless provides a grounded assessment of structural and operational risks that continue to shape the functioning of criminal justice institutions in the region.

Integrity and independence of the police in the Western Balkans

Political pressure and corruption

Police institutions in the Western Balkans operate in a complex post-transition environment shaped by legacies of centralised state control, incomplete institutional reform and persistent political contestation. Although formal reforms have sought to redefine policing as a professional, service-oriented function aligned with European standards, these efforts continue to be undermined by structural vulnerabilities that expose police institutions to political and criminal influence (Zvekic et al., 2024). Rather than manifesting primarily through overt interference, such influence is often exercised indirectly, through appointment powers, disciplinary mechanisms and informal networks linking political elites, economic players and organised crime groups.

Empirical evidence drawn from publicly available surveys and targeted interviews conducted by GI-TOC consultants indicates that public trust in police institutions remains low across much of the region, driven largely by perceptions of corruption and external interference from both political actors and organised crime groups (Zvekic et al., 2024). While corruption cases and scandals are frequently framed internally as the actions of isolated individuals, this narrative obscures the more systemic nature of the problem. By focusing predominantly on lower-level misconduct, such as cases involving individual officers accepting small bribes, institutions often divert attention away from higher-level wrongdoing that is more difficult to detect and address at an institutional scale (Zvekic et al., 2024). This tendency contributes to a culture of tolerance toward structural corruption and weakens incentives to pursue complex cases involving powerful actors.

The consequences of political pressure are most visible in the handling of sensitive investigations. Interviews and documented cases suggest that charges against individuals with close ties to political elites or criminal networks are sometimes delayed, downgraded or quietly dropped, reinforcing public sentiments of mistrust (Zvekic et al., 2024; Civil Rights Defenders, 2023). Such practices not only undermine the credibility of police institutions but also distort operational priorities, discouraging officers from pursuing politically sensitive or resource-intensive cases.

A prominent example illustrating these dynamics emerged in Albania in July 2023, when footage circulated showing relatives of a governing party member of parliament assaulting two individuals who had reported property damage linked to the member of parliament's family (Erebara, 2023; Doci, 2023). Initial institutional responses, including the dismissal of senior police officials, appeared to signal accountability (Euronews Albania, 2023; A2 CNN, 2023). However, subsequent developments, including the downgrading of charges and the relatively lenient treatment of those involved, raised serious concerns regarding the consistency and independence of law enforcement action (Politiko, 2024).

More broadly, the persistence of such cases highlights the limits of reform processes that prioritise legislative alignment over institutional practice. While legal frameworks governing police independence have improved across the Western Balkans, their implementation remains uneven and vulnerable to informal influence (Zvekic et al., 2024). Without credible safeguards protecting operational autonomy, particularly in relation to appointments, disciplinary proceedings and case management, police institutions remain exposed to political capture. Addressing corruption in policing therefore requires not only stricter enforcement of ethical standards, but also a deeper reconfiguration of governance arrangements that currently allow political and criminal interests to intersect with law enforcement functions.

Oversight, cooperation and stakeholder engagement

Weak and fragmented oversight remains a central challenge to ensuring the integrity and independence of police institutions in the Western Balkans. Although international and European standards – including the European Convention on Human Rights and the UN Code of Conduct for Law Enforcement Officials – envisage independent, transparent and effective accountability mechanisms, national oversight frameworks in the region continue to function unevenly in practice. Responsibility for monitoring police conduct is typically dispersed across multiple bodies, including interior ministries, prosecutors' offices, ombuds institutions and parliamentary committees. In the absence of clear coordination and information-sharing arrangements, this fragmentation often results in diluted accountability rather than mutual oversight (Zvekic et al., 2024).

Internal control units are formally mandated to prevent, detect and address misconduct within police services, yet their effectiveness is frequently constrained by insufficient staffing, limited professional autonomy and inadequate training. These limitations are compounded by weak engagement with external stakeholders such as civil-society organisations and independent media, whose potential role in identifying misconduct and strengthening public accountability remains underutilised (Zvekic et al., 2024). As a result, oversight mechanisms often react to scandals *ex post* rather than functioning as preventive instruments capable of identifying systemic risks.

The experience of North Macedonia following the 2015 wiretapping scandal illustrates both the potential and the limits of accountability mechanisms in the region. The establishment of a special prosecutor's office created a dedicated institutional response to allegations of high-level corruption and abuse of power, leading to indictments against senior political figures, including a former prime minister (Zvekic et al., 2024; Magleshov, 2023). While these developments demonstrated that accountability structures can emerge in response to systemic failures, the subsequent challenges, including political obstruction, concerns over lenient sentencing and ongoing questions regarding judicial integrity, continue to highlight the fragility of such mechanisms once the initial political momentum is gone.

Beyond national oversight structures, cooperation in combating organised crime and corruption remains uneven. Western Balkan police services participate in information exchange with international partners such as the European Union Agency for Law Enforcement Cooperation (Europol) and the International Criminal Police Organization (Interpol), yet joint investigations are often constrained by practical barriers, including language gaps, outdated information technology systems, limited analytical capacity and persistent political sensitivities that limit the full participation of certain jurisdictions in international policing frameworks. At the domestic level, cooperation between police and prosecution services is frequently undermined by unclear divisions of responsibility, insufficient communication and limited engagement with other relevant authorities, such as customs, financial intelligence units and regulatory bodies (Zvekic et al., 2024).

Strengthening oversight and cooperation therefore requires more than formal institutional redesign. It demands sustained investment in professional capacity, clearer mandates for oversight bodies, and structured mechanisms for interinstitutional collaboration. Without addressing these underlying governance and coordination issues, efforts to enhance police integrity risk remaining procedural rather than substantive, with limited impact on public trust or institutional resilience.

Training and capacity building

Effective safeguards against corruption and undue influence within police institutions depend not only on formal rules and oversight mechanisms, but also on the professional capacities and ethical orientation of individual officers. Training and education therefore play a central role in shaping institutional integrity, particularly in contexts where law enforcement agencies are required to respond to increasingly complex forms of organised crime and corruption while operating under political and operational constraints.

As noted above, strengthening institutional integrity requires sustained investment in human resources through comprehensive training and education. This includes ensuring that police academies responsible for recruiting and training future officers are equipped not only to address established forms of crime, but also to anticipate emerging threats such as cybercrime and increasingly sophisticated financial offences. Although anti-corruption components are formally incorporated into training curricula across the Western Balkans, these efforts often remain fragmented and insufficiently reinforced throughout officers' careers. As a result, ethical standards are frequently treated as abstract principles rather than operational norms guiding day-to-day decision-making.

While officers in the region receive instructions and supplementary training focused on detecting and documenting corruption and organised crime, significant gaps persist. Training programmes tend to place greater emphasis on procedural compliance than on developing the analytical, technological and interdisciplinary skills required to investigate complex cases. In particular, deficits remain in areas such as ethics-based decision-making, foreign-language proficiency, information and communication technology skills, forensic methodologies and awareness of gender equality and discrimination risks. Although equal-opportunity frameworks formally exist, tailored leadership development programmes for female officers remain limited, contributing to persistent gender imbalances in senior positions.

Moreover, the identification of training needs is often slow and reactive, while the quality and consistency of instructors vary significantly across institutions. In the absence of systematic needs assessments and standardised evaluation mechanisms, training risks becoming disconnected from operational realities. This limits its effectiveness

in strengthening institutional resilience against corruption and political pressure, particularly in specialised units tasked with investigating organised crime.

A recent case in Serbia illustrates the consequences of these gaps. A former inspector from a specialised organised crime unit was charged with leaking confidential police information to a criminal network through the encrypted Sky ECC communication platform (Vojinović, 2021). Although international cooperation played a critical role in intercepting the communications, the subsequent prosecution encountered substantial legal and political challenges. Questions regarding the admissibility of intercepted digital evidence, combined with public and political debate surrounding the case, complicated proceedings (Đorđević, 2023). While the inspector was ultimately convicted in 2024, appeals and retrial proceedings exposed persistent weaknesses in the integration of advanced investigative technologies into domestic legal frameworks (Vojinović, 2024).

This case underscores the importance of aligning training, legislation and operational practice. Strengthening officers' technical skills must be accompanied by clearer procedural standards, closer coordination between police and prosecution services and sustained engagement with international partners. Without such alignment, investments in training risk producing limited returns, as institutional weaknesses continue to constrain the effective investigation and prosecution of corruption and organised crime.

Integrity and independence of the prosecution in the Western Balkans

Over recent decades, Western Balkan countries have undertaken extensive legislative and institutional reforms to strengthen their prosecution services, align themselves with EU and international standards and enhance their independence and professionalism. Although these reforms – guided by instruments such as the UN Convention against Corruption, recommendations by the Council of Europe and evaluations by the Group of States against Corruption – have advanced legal frameworks on paper, their implementation remains uneven. Political interference, both direct and indirect, continues to influence senior prosecutorial appointments and prosecutorial decision-making, undermining the impartiality and effectiveness of criminal justice in the region. Internal and external corruption risks persist, weakening prosecutors' integrity and diminishing their capacity to pursue high-level corruption and organised crime cases. While some progress has been noted, the urgent need for robust accountability, clear internal policies and adequate resource allocation to the prosecution offices cannot be overstated. Ensuring genuine political will and implementing meaningful control mechanisms is critical, not only to dismantle entrenched networks of corruption, but also to foster a prosecutorial culture capable of resisting undue pressure and safeguarding the rule of law in the region (Zvekic et al., 2024).

Political interference and case selection

Despite extensive legislative reforms aimed at strengthening prosecutorial independence in the Western Balkans, political interference continues to affect key aspects of prosecutorial decision-making. Rather than operating primarily through direct instructions, such interference is more commonly exercised through structural levers, including appointment procedures, career advancement, disciplinary mechanisms and control over case allocation. These forms of influence are less visible but no less consequential, as they shape incentives within prosecution services and condition prosecutors' willingness to pursue sensitive cases (Zvekic et al., 2024).

One of the most significant manifestations of political interference concerns case selection and prioritisation. In several Western Balkan jurisdictions, discretionary powers over the allocation of cases, particularly those involving corruption, abuse of office or politically exposed individuals, remain weakly regulated or lack transparency. This creates opportunities for selective prosecution, whereby some cases are delayed or deprioritised, while others are fast-tracked or quietly resolved through abbreviated procedures. Such practices not only shield specific individuals from scrutiny but also narrow the scope of public debate by limiting the judicial exposure of systemic corruption risks (Zvekic et al., 2024).

Political influence over senior prosecutorial appointments further exacerbates these vulnerabilities. Non-merit-based selection processes and prolonged vacancies in leadership positions weaken institutional cohesion and delay the development of specialised expertise, particularly within units responsible for complex financial and corruption-related investigations. In this context, prosecutors may face implicit pressure to avoid cases perceived as politically sensitive, especially where institutional support is uncertain or where career prospects depend on discretionary decisions taken by politicised bodies (Zvekic et al., 2024).

The experience of Kosovo illustrates how institutional design can amplify these risks. The re-election of the chair of the Kosovo Prosecutorial Council beyond the legally prescribed term, despite clear statutory limitations, raised concerns regarding the council's commitment to legality and accountability (Official Gazette of the Republic of Kosovo, 2019). These concerns were reinforced by the Kosovo Prosecutorial Council's limited openness to external scrutiny and its frequent dismissal of input from media and civil society. Subsequent attempts to reform the council were blocked following constitutional review and critical opinions from the Venice Commission, effectively entrenching existing governance arrangements and constraining prospects for reform (Kosovo Constitutional Court, 2023; Venice Commission, 2023).

These institutional dynamics are reinforced by managerial and procedural weaknesses within prosecution services. The limited accountability of leadership, particularly where appointments are politically influenced, contributes to unclear chains of command between police and prosecutors, leading to mismanaged investigations, inconsistent case allocation and prolonged proceedings. The absence of standardised operating procedures further constrains effective decision-making, while limited transparency in handling politically sensitive corruption cases allows discretionary practices to persist. In some instances, expedited legislative procedures have been used to grant immunity or procedural advantages to politically connected individuals, further undermining prosecutorial independence and public confidence in the justice system (Zúñiga, 2020; Magleshov et al., 2023).

Operational constraints

A range of operational shortcomings continues to undermine prosecutorial effectiveness and public confidence in the Western Balkans. The inconsistent enforcement of disciplinary measures and frequent leaks of confidential information erode the fairness of investigations and trials, while lengthy pre-investigations often proceed without anyone taking clear responsibility for delays. These systemic weaknesses are intensified by outdated digital infrastructure and weak case-management practices, making it difficult to process complex cases efficiently. Prosecutors frequently lack both the specialised expertise and the resources needed to investigate financial crimes, recover assets and handle complex cross-border offences. Together, these factors slow the pace of justice, reduce the likelihood of securing convictions in high-level corruption cases and ultimately undermine the rule of law.

For example, the 'tunnel' case uncovered at the High Court in Podgorica, Montenegro, in September 2023 highlights how operational vulnerabilities can be exploited (Zvekic et al., 2024). A 30-metre tunnel, dug from a nearby building directly into the court's evidence depot, went undetected and led to the theft of critical evidence for organised crime trials. Although arrests were made, no indictments were issued. This incident was similar to a 2016 arson case targeting trial documents and underscores how inadequate security and oversight can jeopardise entire proceedings (Kajosevic, 2023).

Gender equality in criminal justice institutions

Gender inequality remains a significant issue within the criminal justice systems of the Western Balkans, particularly within law enforcement and prosecution services. Policing is predominantly a male-dominated profession, influenced by enduring stereotypes that associate policing with traits traditionally attributed to men, such as physical strength and authority (Zvekic et al., 2024). Consequently, women are underrepresented in police services, especially in leadership positions. While some Western Balkan countries, like Serbia and North Macedonia, have achieved female representation levels that exceed the EU average of 18.5 %, others – including Albania, Bosnia and Herzegovina, Kosovo and Montenegro – remain below that level, with women constituting as little as 9 % of the police force in Bosnia and Herzegovina (Zvekic et al., 2024).

This disparity in gender representation not only reflects societal attitudes but also impacts the effectiveness and inclusivity of policing strategies. A gender-balanced police force benefits from diverse perspectives and skills, particularly in communication, conflict resolution and community engagement, which are essential for effective law enforcement and for building public trust (Zvekic et al., 2024). Women also play a crucial role in handling cases involving domestic violence and sexual assault, where their empathy and communication skills significantly support victims. However, women's advancement into leadership roles remains limited, with few female officers occupying high managerial positions across the region, ranging from 18.6 % in Serbia to the absence of woman in top managerial positions in Montenegro (Zvekic et al., 2024).

In prosecution services, gender inequality persists despite women being generally better represented than in law enforcement. Montenegro, for example, boasts high female representation in prosecution, with 62 % of state prosecutors being women, significantly surpassing the EU average of 54 % (Zvekic et al., 2024). North Macedonia also shows promising figures, where 55 % of prosecutors are women, and women occupy 43 % of leadership positions, a notable increase from 15 % in 2012 (Zvekic et al., 2024). However, countries like Kosovo, Albania and Bosnia and Herzegovina lag behind, with female representation in prosecution ranging from 47.2 % to 42.6 % (Zvekic et al., 2024). Despite these numbers, women remain markedly underrepresented in senior and leadership roles across the region, limiting their influence on decision-making processes and perpetuating a predominantly male-dominated prosecutorial culture.

The underrepresentation of women in leadership positions within prosecution services has tangible implications for institutional integrity and effectiveness. Diverse perspectives brought by female prosecutors enhance decision-making, foster inclusive prosecutorial strategies and improve community trust. However, the persistent glass ceiling in many Western Balkan countries restricts women's career advancement, undermining the potential benefits of gender diversity. To address these disparities, it is essential to implement specific recruitment targets for women, especially in leadership roles, and to develop comprehensive mentorship and leadership development programmes. Additionally,

reducing political interference in prosecutorial appointments and promotions is crucial to establishing a merit-based system that genuinely reflects the capabilities and contributions of female prosecutors (Zvekic et al., 2024).

For example, in Serbia, prosecutor B.S., who maintained a 100 % success rate in her cases within the specialised anti-corruption department, was abruptly transferred to the General Prosecution Department in February 2022, just days before conducting major interrogations arising from arrest warrants she had issued against individuals charged with serious abuses of power in a large case. Later, in May 2024, she was moved again to the Juvenile Delinquency Prosecutor's Office without explanation. These transfers suggest political interference aimed at removing a highly effective female prosecutor from sensitive cases, highlighting the absence of a merit-based promotion system and the challenges women face in advancing within prosecutorial ranks (Zvekic et al., 2024).

Conclusion

Despite extensive reform efforts and formal alignment with EU and international standards, police and prosecution services across the Western Balkans continue to face persistent challenges that undermine their integrity and operational independence. These challenges are not confined to isolated incidents or individual misconduct but are rooted in structural vulnerabilities that affect governance, accountability and professional autonomy. Political interference, which is often exercised indirectly through appointments, case allocation and managerial discretion, remains a defining constraint, shaping institutional behaviour and limiting the capacity of criminal justice institutions to address high-level corruption and organised crime effectively.

The findings presented in this article highlight a recurring gap between formal legal frameworks and institutional practice. While legislative reforms have strengthened guarantees of independence on paper, their implementation has been uneven and vulnerable to informal influence. Weak oversight mechanisms, fragmented accountability arrangements and insufficient coordination between police, prosecution and other relevant authorities continue to impede effective enforcement. These deficits are compounded by operational constraints, including limited resources, outdated digital infrastructure and skills gaps in specialised areas such as financial investigations and cross-border cooperation. Together, these factors contribute to selective enforcement, procedural delays and diminished public trust in the criminal justice system.

Gender inequality emerges as both a symptom and a driver of these institutional weaknesses. The underrepresentation of women, particularly in leadership positions within police and prosecution services, reflects broader governance challenges, including politicised appointments and non-merit-based career progression. Beyond questions of representation, gender imbalance has tangible implications for institutional integrity, decision-making quality and, importantly, community engagement. Efforts to strengthen independence and accountability must therefore incorporate gender-sensitive reforms, not as a secondary objective but as an integral component of institutional resilience.

At the same time, the analysis underscores the limits of technocratic reform approaches that prioritise formal compliance over substantive change. Measures such as integrity strategies, training programmes and specialised units are necessary but insufficient in the absence of sustained political commitment and credible enforcement. Reforms aimed at strengthening oversight, protecting operational autonomy and improving cooperation across

institutions inevitably confront entrenched interests and resistance from those who benefit from existing arrangements. In this context, implementation challenges that include reform fatigue, limited administrative capacity and political contestation must be explicitly acknowledged rather than treated as peripheral considerations.

Strengthening the integrity and independence of criminal justice institutions in the Western Balkans therefore requires a shift from *ad hoc* reforms towards a more holistic and sustained approach. This includes reinforcing merit-based appointments and career advancement, clarifying mandates and chains of responsibility, investing in professional capacity and digital infrastructure and ensuring meaningful external oversight by parliaments, independent bodies, the media and civil society. International and regional cooperation through frameworks such as Europol and Interpol remains essential but needs to be complemented by domestic reforms that enable institutions to absorb and act on shared intelligence effectively.

Ultimately, progress in this area will depend less on the adoption of new laws than on the political will to enforce existing ones consistently and impartially. Without credible safeguards against interference and stronger accountability for institutional leadership, efforts to combat corruption and organised crime risk remaining symbolic. Conversely, sustained investment in integrity, independence and professional capacity offers a pathway toward rebuilding public trust, strengthening the rule of law and supporting the region's broader democratic and European integration objectives.

References

A2 CNN (2023), 'Dhuna në Borizanë, ndryshime në Komisariatin e Krujës', 17 July, https://a2news.com/dhuna-ne-borizane-ndryshime-ne-komisariatin-e-krujes.

Civil Rights Defenders (2023), 'CoE report urges Montenegro to investigate cases of police brutality', 7 July, Civil Rights Defenders website, https://crd.org/2023/07/07/coe-report-urges-montenegro-to-investigate-cases-of-police-brutality/.

Doci, A. (2023), 'Përparim Rraja pjesë e dosjes Viluni me Bardhok Pllanajn, mister si u përjashtua nga hetimi, kompaninë e gurores e bleu për 100 mijë euro, nuk zbatoi kushtet, nënkontraktor i Gener 2 për Thumanë-Kashar, krimet dhe bizneset', Prapaskena, 8 July, https://prapaskena.com/2023/07/08/perparim-rraja-pjese-e-dosjes-viluni-me-bardhok-pllanajn-mister-si-u-perjashtua-nga-hetimi-kompanine-e-gurores-e-bleu-per-100-mije-euro-nuk-zbatoi-kushtet-nenkontraktor-i-gener-2-per-thumane-kasha/.

Đorđević, S. (2023), 'Uncertain future of Sky ECC coms in criminal proceedings', LinkedIn, 9 October, https://www.linkedin.com/pulse/uncertain-future-sky-ecc-coms-criminal-proceedings-sasa-djordjevic/.

Erebara, G. (2023), 'Prokuroria dhe policia i dërgojnë letra njëra-tjetrës në lidhje me skandalin e gurores së Borizanës', Reporter.al, 10 July, https://www.reporter.al/2023/07/10/prokuroria-dhe-policia-i-dergojne-letra-njera-tjetres-ne-lidhje-me-skandalin-e-gurores-se-borizanes/.

Euronews Albania (2023), 'Bledi Çuçi dismissed as Interior Minister, PM Rama proposes Taulant Balla', 9 July, https://euronews.al/en/cuci-dismissed-as-interior-minister-pm-rama-proposes-taulant-balla/.

Kajosevic, S. (2023), 'Robbers dig tunnel to stage break-in at Montenegro court', *Balkan Insight*, 12 September, https://balkaninsight.com/2023/09/12/robbers-dig-tunnelto-stage-break-in-at-montenegro-court/.

Kosovo Constitutional Court (2023), Cases Nos KO 100/22 and KO 101/22, Judgment, 5 April, https://gjk-ks.org/decisions/details/5615.

Magleshov, V. and Marusic, S. J. (2023), 'North Macedonia's president urged to block sudden criminal law changes', Balkan Insight, 7 September, https://balkaninsight.com/2023/09/07/north-macedonias-president-urged-to-block-sudden-criminal-law-changes/.

Official Gazette of the Republic of Kosovo (2019), Law No 06/L-056 on Kosovo Prosecutorial Council, No 10/2019, Article 12.1, 3 April.

Politiko (2024), 'The Mayans were barbarically raped, three members of the Rraja tribe are released from prison', Politiko, 19 January, https://politiko.al/english/e-tjera/dhunuan-barbarisht-majat-lirohen-nga-qelia-tre-anetare-te-fisit-rraja-i500235.

Magleshov, V. (2023), 'North Macedonia Court confirms ex-PM Gruevski's sentence', Balkan Insight, 20 December, https://balkaninsight.com/2023/12/20/north-macedonia-court-confirms-ex-pm-gruevskis-sentence/.

Venice Commission (European Commission for Democracy through Law) (2023), 'Kosovo – Follow-up Opinion No 1149/2023 to the previous opinions concerning amendments to the Law on the Kosovo Prosecutorial Council', I 326 CDL-AD(2023)043, 18 December, https://www.coe.int/en/web/venice-commission/-/opinion-1149.

Vojinović, M. (2021), 'Inspektor osumnjičen da je sarađivao sa Belivukom pušten iz pritvora', Krik, 19 August, https://www.krik.rs/inspektor-osumnjicen-da-je-saradjivao-sa-belivukom-pusten-iz-pritvora/.

Vojinović, M. (2024), 'Bivši inspektor SBPOK-a ponovo osuđen za odavanje informacija Belivukovom klanu', *Krik*, 23 July, https://www.krik.rs/bivsi-inspektor-sbpok-a-ponovo-osudjen-za-odavanje-informacija-belivukovom-klanu/.

Zúñiga, N. (2020), *Examining State Capture: Undue influence on law-making and the judiciary in the Western Balkans and Turkey*, Transparency International, https://images.transparencycdn.org/images/2020_Report_ExaminingStateCapture_English.pdf.

Zvekic, U. and Vlassis, I. (eds) (2024), *Integrity and independence of criminal justice institutions in the Western Balkans: Police and prosecution*, Global Initiative Against Transnational Organized Crime, Geneva, https://globalinitiative.net/wp-content/uploads/2024/11/Ugljesa-Ugi-Zvekic-Ioannis-Vlassis-Integrity-and-independence-of-criminal-justice-institutions-in-the-Western-Balkans-Police-and-prosecution-GI-TOC-November-2024.v2.pdf.

High-risk cybercriminal networks: Strategies for combating them in cyberspace

Alp Cenk Arslan

https://doi.org/10.3013/g3vn9q76

Abstract

As cybercriminal networks grow increasingly complex and globalised, traditional cybersecurity measures struggle to address these sophisticated threats. This study examines the structures and strategies of high-risk cybercriminal networks, focusing on their technological, geopolitical and operational dynamics. Methodologically, the study employs a qualitative comparative analysis framework, utilising a 'most different systems design' to evaluate the strategic divergence between the United States and the European Union. The research contributes to the literature by establishing a theoretical nexus between 'state–cybercrime alignment' and current geopolitical security doctrines. Drawing on the US national cybersecurity strategy and the EU cybersecurity strategy, the research analyses their approaches to combating such networks and fostering international cooperation. Case studies of cyberattacks originating from China, North Korea and Russia highlight the global connections and state-sponsored elements of these networks. The study proposes an integrated framework combining advanced technologies and international collaboration to disrupt, predict and mitigate cybercriminal activities. Additionally, it underscores the importance of harmonised global laws and inter-agency partnerships to address jurisdictional and technological challenges. By comparing the US and EU strategies, this research provides policymakers and cybersecurity professionals with actionable insights and recommendations to navigate the evolving threat landscape and promote a secure digital ecosystem.

Keywords: high-risk cybercriminal networks, international cooperation, US cyber strategy, EU cyber strategy, cybersecurity, security strategies.

Introduction

High-risk cybercriminal networks represent one of the most formidable challenges to global cybersecurity in the digital age. These networks, often characterised by their sophistication, international reach and adaptability, pose significant threats to critical infrastructure, economic stability and national security. As technological advancements continue to evolve, so do the methods and tools employed by cybercriminals, making traditional cybersecurity measures increasingly inadequate. The nexus between cybercrime, geopolitical ambitions and state sponsorship further complicates the landscape, blurring the lines between criminal and strategic motives. Nations such as China, North Korea and Russia have been implicated in fostering or tolerating such activities, leveraging cybercrime for both financial gain and strategic advantage.

This study aims to explore the complex dynamics of high-risk cybercriminal networks and examine the strategic responses outlined in the cybersecurity frameworks of the United States and the European Union. By analysing the US national cybersecurity strategy (2023) and the EU cybersecurity strategy for the Digital Decade (2020), the study seeks to understand the underlying intentions, mechanisms and collaborative approaches adopted by these actors to combat cyber threats. Particular attention is paid to international cooperation, given the transnational nature of cybercrime and the challenges posed by jurisdictional boundaries.

This article makes three concrete contributions. First, it proposes a typology of the state–cybercrime nexus (state-operated, state-enabled and state-tolerated) tailored to high-risk cybercriminal networks. Second, it operationalises this typology through a qualitative comparative analysis and structured documentary coding to compare the United States' and the EU's strategic responses across three analytic nodes: operational disruption, regulatory resilience and diplomatic attribution. Third, it distils these findings into actionable implications for European law enforcement, particularly for cross-border investigations, evidence production and disruption coordination with the European Union Agency for Law Enforcement Cooperation (Europol) European Cybercrime Centre (EC3) and national cybercrime units.

The research also evaluates the operational and strategic advancements in cybersecurity, focusing on emerging technologies such as AI and quantum computing, and the frameworks designed to counteract their exploitation by cybercriminals. Additionally, the study highlights the importance of harmonising legal frameworks, strengthening public–private partnerships and fostering international collaboration to mitigate the risks posed by these networks. Despite the abundance of policy reports, scholarly literature lacks a systematic comparison of how transatlantic security architectures adapt to the industrialisation of cybercrime. This study addresses this gap by answering three core research questions (RQs). RQ1: How do the United States and the EU conceptualise the state–cybercrime nexus within their national security priorities? RQ2: To what extent do offensive strategies (United States) versus regulatory harmonisation (EU) provide more effective deterrence against high-risk networks? RQ3: What are the structural barriers to achieving a unified transatlantic response to state-sponsored cybercriminal activities? To address these questions, the study moves beyond a narrative comparison by specifying conditions and outcomes, thereby enabling a replicable assessment of strategic divergence. The practical focus is on how EU law enforcement can reduce jurisdictional 'grey zones' exploited by state-aligned networks. This work aims to provide policymakers, cybersecurity professionals and academics with actionable insights and strategies to address the evolving threat landscape effectively, while promoting a secure and resilient digital ecosystem.

Methodology

This research utilises a qualitative comparative analysis and documentary research methodology. Three primary archetypes of high-risk networks (China, North Korea and Russia) were selected based on the 'most similar' and 'most different' case criteria. These cases represent the full spectrum of the state–cybercrime nexus, from direct state-operated units (Lazarus) to state-tolerated syndicates (Russian ransomware). The study analyses the US national cybersecurity strategy (2023) and the EU cybersecurity strategy (2020) using three thematic coding nodes: (1) operational disruption; (2) regulatory resilience; and (3) diplomatic attribution. Analysis is derived from primary legal documents, threat intelligence reports (2020–2024) and peer-reviewed security studies. The study acknowledges the limitations of using open-source intelligence, mitigating this by triangulating government reports with academic security discourse.

Theoretical framework: the industrialisation of cybercrime

High-risk cybercriminal networks are deeply intertwined with technological innovation, geopolitical motivations and criminal enterprise, creating a complex challenge for cybersecurity and law enforcement. These networks operate with industrialised processes that mirror corporate structures, characterised by specialisation, scalability and coordination (Luo, 2024). For instance, specialised teams handle malware development and phishing, while ransomware as a service enables global scalability (Meland et al., 2020). Collaboration through Dark Web forums further enhances their adaptability and resilience.

To understand high-risk networks, this study applies 'network governance theory' and 'routine activity theory' (RAT) adapted for digital spaces. These frameworks suggest that the convergence of 'motivated offenders' (cybercriminals), 'suitable targets' (critical infrastructure) and the 'absence of capable guardians' (jurisdictional gaps) creates the current techno-political threat environment. This lens directs attention to network chokepoints (infrastructure, financing and coordination layers) as the most disruptive intervention targets (Jones et al., 1997). Complementarily, RAT (Cohen et al., 1979) informs the comparative reading of US and EU strategies by mapping policy instruments onto the 'capable guardianship' function, such as mandatory reporting, public–private operational integration, certification regimes and financial disruption measures. Together, these frameworks explain why state-aligned networks exploit jurisdictional gaps and why a strategic divergence between disruption-oriented and regulation-oriented approaches produces persistent transatlantic grey zones.

State sponsorship significantly amplifies the threat posed by these networks. Countries like China, North Korea and Russia use cybercriminals for both financial gain and geopolitical strategy. North Korea's Lazarus Group exemplifies this dual purpose, conducting operations such as the USD 625 million Axie Infinity heist to finance nuclear ambitions. These actors also use cryptocurrency mixers to launder stolen funds, leveraging anonymity-enhancing technologies to obscure their tracks (O'Neill, 2024; Tidy, 2024).

Chinese networks, like the Vigorish Viper syndicate, operate at both the organisational and individual levels, targeting industries such as gambling and intellectual property theft (Lakshmanan, 2024). Innovative methods, such as Domain Name System (DNS) Canonical Name (CNAME) traffic distribution, and the use of underregulated regions like Zambian call centres, highlight the industrialisation of Chinese cybercrime (Muia, 2024).

Russian cybercriminals benefit from state protection, integrating ransomware operations into geopolitical strategies. Investigations like Operation Destabilise have exposed money-laundering networks linked to drug trafficking, ransomware and espionage (National Crime Agency, 2024). Russian actors have also targeted critical infrastructure and political systems, exemplified by interference in Ukrainian military systems and in US elections (Klepper, 2024; Euronews, 2024).

Technological advancements further complicate the landscape. Tools like AI and encrypted communication enhance operational capacity, while cryptocurrencies facilitate financial transactions. These dynamics underline the urgent need for international cooperation and robust strategies to combat the global nature of high-risk cybercrime (Leukfeldt et al., 2017).

Analysis of the United States and European Union cybersecurity strategies

From a network governance perspective, high-risk cybercriminal activity is best understood not as a series of isolated operations but as a coordinated ecosystem of interdependent actors, including malware developers, access brokers, hosting providers, money launderers and state-linked facilitators. This lens highlights why strategies that focus solely on individual threat actors often fail to generate sustained disruption. Instead, effective intervention depends on identifying and targeting network-level chokepoints, particularly those enabling coordination, financing and scalability. This perspective provides an analytical foundation for assessing how the US and EU strategies conceptualise and intervene in cybercriminal ecosystems rather than in discrete incidents.

The United States national cybersecurity strategy

The US national cybersecurity strategy released in March 2023 outlines a multifaceted approach to addressing high-risk cybercriminal networks. Its intentions and strategies in this domain aim to strengthen national security by protecting critical infrastructure and sensitive data from increasingly sophisticated and damaging cybercriminal activities. High-risk cybercriminal networks, such as those engaging in ransomware, are recognised as threats to national security and economic stability. The United States seeks to lead globally in establishing norms of responsible state behaviours in cyberspace while holding states and actors accountable for cyber misconduct. By disrupting cybercriminal networks, the United States aims to safeguard not only its interests but also those of its allies, projecting global leadership. A key goal is to leverage public–private partnerships for intelligence sharing and operational collaboration to effectively dismantle threat actors. Building resilience into the digital ecosystem is a foundational objective, ensuring systems are defensible and that attacks have limited impact (The White House, 2023, p. 23).

The strategy emphasises disrupting and dismantling threat actors through integrated federal efforts. Federal agencies, led by the Department of Justice and supported by entities like the Cybersecurity Infrastructure Security Agency and the National Security Agency, coordinate campaigns targeting cybercriminal infrastructure such as botnets and ransomware servers (The White House, 2023, p. 14). The Department of Defense employs a 'defend forward' strategy to neutralise threats before they materialise (The White House, 2023, p. 14). Recognising that private companies often have better visibility into cybercriminal activities, the strategy calls for closer collaboration with private entities for threat intelligence. Rapid response cells, such as those within the National Cyber-Forensics and Training Alliance, are tasked with responding to active threats in real time.

Interpreted through a network governance lens, the United States' emphasis on persistent engagement and defend-forward operations reflects an effort to destabilise the coordination mechanisms of cybercriminal networks rather than merely neutralising individual nodes. By targeting infrastructure, financial intermediaries and communication channels, the US strategy seeks to increase systemic friction across the network, thereby raising operational costs and reducing regenerative capacity. This approach aligns with governance-based disruption logic, where weakening connective tissue is prioritised over episodic actor removal.

Specific actions against ransomware include applying economic pressure by targeting cryptocurrency platforms used for laundering funds. The Counter Ransomware Initiative, an international coalition of over 30 countries, shares intelligence and disrupts ransomware campaigns globally. Legal and regulatory measures, such as enhancing the security of cloud services and mandating critical infrastructure entities to report cyber incidents, strengthen the broader cybersecurity framework. The strategy also prioritises intelligence sharing through automated, real-time data exchange and enhanced declassification policies to facilitate actionable intelligence sharing with private entities (The White House, 2023, p. 30).

Global partnerships are a central element of the strategy, with alliances such as the North Atlantic Treaty Organization (NATO) and the Quadrilateral Security Dialogue (the Quad) playing critical roles in addressing transnational cyber threats. Collaborative efforts with organisations like Europol's EC3 strengthen cross-border law enforcement. These international coalitions are designed to address shared cybersecurity challenges and hold malicious actors accountable (The White House, 2023, p. 1).

The strategy reflects a proactive, deterrent and collaborative approach to cybersecurity. It emphasises shifting the burden of cybersecurity from individual end users and small organisations to more capable actors, such as infrastructure operators and technology providers, promoting long-term resilience and equitable risk distribution (The White House, 2023, p. 30). The multilayered defence mechanism combines technological innovation, such as zero trust architecture, with operational coordination. The focus on sustained disruption campaigns signifies a shift from reactive to persistent offensive actions against cybercriminals, aiming to make cybercrime economically unviable (The White House, 2023, p. 14). The integration of international law, sanctions and diplomatic tools to isolate and penalise states that harbour cybercriminals highlights a comprehensive geopolitical strategy.

However, the strategy also faces challenges, including overcoming implementation barriers such as bureaucratic inertia, the complexity of public–private collaboration and the evolving tactics of cybercriminals. Balancing national security measures with civil liberties will be critical in maintaining public trust (The White House, 2023, p. 26). Despite these challenges, the 2023 US national cybersecurity strategy represents a robust framework for combating high-risk cybercriminal networks. By integrating technical innovation, policy reforms and international cooperation, the strategy seeks to create a digital ecosystem where cyberattacks are both costly and less impactful.

The European Union cybersecurity strategy for the Digital Decade

The EU cybersecurity strategy for the Digital Decade, dating from December 2020, addresses high-risk cybercriminal networks through an integrated framework encompassing resilience-building, operational capacity, international cooperation and technological leadership. The strategy aims to enhance cyber resilience by building robust defences

for critical infrastructures and digital services, ensuring they are secure by design (European Commission, 2020, p. 5). The revised directive on the security of network and information systems (NIS2 Directive) plays a crucial role in harmonising regulatory frameworks to strengthen the cyber resilience of key sectors such as energy, healthcare and finance. It also emphasises operational preparedness by establishing mechanisms like the Joint Cyber Unit to detect, prevent and respond to large-scale cyber incidents through cross-border and cross-sector collaboration.

From a RAT perspective, the EU strategy primarily seeks to strengthen the 'capable guardianship' component of the cybercrime equation. Regulatory harmonisation, mandatory incident reporting, certification frameworks and sectoral resilience measures are designed to reduce target suitability and increase guardianship density across critical infrastructures. Rather than directly confronting motivated offenders, the EU approach aims to structurally constrain opportunity spaces by embedding security obligations throughout the digital ecosystem.

The strategy seeks to deter malicious cyber activities and hold perpetrators accountable by integrating law enforcement, judicial cooperation and diplomatic tools. This includes improving digital investigations, evidence gathering and partnerships with Europol and the European Union Agency for Cybersecurity (ENISA). International cooperation is a key element in recognising the global nature of cyber threats and promoting responsible state behaviours and global norms. The strategy prioritises technological sovereignty to reduce dependency on non-EU suppliers, emphasising investment in cybersecurity technologies like AI, quantum computing and 5G infrastructure (European Commission, 2020, p. 8).

The strategy employs regulatory frameworks, including the NIS2 Directive, to enforce strict security requirements on critical sectors and strengthen incident reporting obligations. The Cybersecurity Act introduces a European cybersecurity certification framework to ensure stringent security standards for digital products and services. To build operational capacity, initiatives like the Joint Cyber Unit promote real-time information sharing among national computer security incident response teams, law enforcement and private stakeholders. AI-enabled security operations centres enhance threat detection and response capabilities (European Commission, 2020, pp. 6–13).

Cooperation between Europol and ENISA enhances law enforcement's ability to investigate cybercrime, including Dark Web marketplaces and ransomware attacks (European Commission, 2020, p. 10). The e-evidence framework facilitates cross-border access to electronic evidence, critical for prosecuting cybercriminal networks. Financial and technological investment through programmes like Horizon Europe and digital Europe fund research and development for advanced cybersecurity solutions and capacity building, particularly for small and medium-sized enterprises, which are often targeted by cybercriminals. The strategy also addresses supply chain vulnerabilities and ensures the resilience of emerging technologies like 5G and quantum communication (European Commission, 2020, p. 7).

Global cyber diplomacy plays a significant role in the strategy, with the EU promoting frameworks like the Budapest Convention on Cybercrime and using the Cyber Diplomacy Toolbox to impose sanctions against entities responsible for cyberattacks. The EU advocates for its values in international standardisation processes to prevent the proliferation of insecure technologies. Public–private partnerships are encouraged, with information sharing and analysis centres facilitating intelligence sharing and collaboration. Small and medium-sized enterprises receive tools and training to strengthen their cyber defences (European Commission, 2020, p. 7).

Despite its comprehensive approach, the strategy faces challenges. Fragmented implementation across EU Member States could hinder a unified response to high-risk cybercriminal networks. The effective attribution of cyberattacks remains difficult, particularly with respect to state-sponsored actors. Rapid technological advancements like deepfakes and AI-generated cyber tools necessitate constant adaptation of strategies. Additionally, the shortage of skilled cybersecurity professionals poses a barrier to effective implementation.

The EU cybersecurity strategy for the Digital Decade demonstrates a thorough approach to combating high-risk cybercriminal networks by integrating regulatory measures, operational frameworks, international cooperation and technological investment. Its success will depend on consistent implementation across Member States, effective public–private collaboration, and the ability to address emerging threats. This strategy positions the EU as a global leader in cybercrime prevention while ensuring economic, social and political stability.

Findings and comparative analysis: the European Union cybersecurity strategy versus the United States national cybersecurity strategy

The comparative analysis reveals a clear divergence in the strategic orientation underpinning the US and EU cybersecurity frameworks when confronting high-risk cybercriminal networks. The US national cybersecurity strategy is fundamentally oriented toward operational disruption and cost imposition, reflecting a security logic that treats cybercriminal infrastructures as active battlefields. Within this approach, cybercrime is framed not merely as a law enforcement issue but as a national security threat requiring persistent engagement. As a result, the US strategy normalises proactive interventions against adversary infrastructure, including pre-emptive actions designed to degrade capabilities before attacks materialise. By contrast, the EU cybersecurity strategy prioritises regulatory resilience and harmonised governance mechanisms, positioning cybersecurity as a systemic risk management challenge. The EU approach focuses on ensuring that critical sectors, digital services and supply chains are resilient by design, emphasising uniform standards, compliance obligations and coordinated preparedness across Member States. This divergence reflects deeper differences in strategic culture: the US privileges deterrence through disruption, while the EU privileges stability through institutional harmonisation.

When read jointly through network governance theory and RAT, the strategic divergence between the US and EU becomes analytically clearer. The US model prioritises network disruption by targeting coordination and enablement layers, whereas the EU model prioritises guardianship by reducing systemic vulnerability and opportunity structures. This divergence explains why both strategies generate partial effectiveness while simultaneously leaving jurisdictional and operational grey zones that high-risk networks continue to exploit.

These contrasting orientations are further reflected in the instruments each of them deploys to counter high-risk cybercriminal activity. The US strategy explicitly institutionalises persistent operational campaigns against adversarial networks, integrating intelligence, law enforcement and military capabilities to dismantle botnets, ransomware infrastructure and financial enablers. Offensive cyber operations, economic sanctions and coordinated takedowns are treated as complementary tools within a single disruption ecosystem. In the EU framework, however, the emphasis shifts toward coordinated preparedness, incident response and post-incident management. Mechanisms such as certification schemes, sector-specific security requirements and cross-border incident handling are designed to reduce systemic vulnerability rather than to actively pursue adversaries in cyberspace. While these measures

significantly enhance resilience, they tend to operate reactively, engaging once an incident has occurred rather than shaping the threat environment upstream.

Attribution practices constitute another area of convergence in principle but are divergent in execution. Both the United States and the EU recognise attribution as essential for accountability and deterrence, yet they embed it within different consequence structures. The US strategy more directly links attribution to operational and economic consequences, including sanctions, indictments, asset seizures and follow-on cyber operations. Attribution thus functions as a trigger for action, enabling rapid escalation across legal, financial and cyber domains. In contrast, the EU embeds attribution within a broader framework of diplomatic coordination and collective response, most notably through the Cyber Diplomacy Toolbox. Here, attribution serves to build consensus among Member States and partners before sanctions or diplomatic measures are applied. While this approach enhances legitimacy and unity, it can also introduce delays that reduce the immediacy of deterrent effects, particularly against agile and state-aligned cybercriminal networks.

A critical structural finding concerns the persistent exploitation of jurisdictional grey zones by high-risk cybercriminal networks. These actors consistently leverage the asymmetry between their rapid operational tempos and the comparatively slower legal, evidentiary and diplomatic processes governing transatlantic cooperation. Differences in legal thresholds, evidence standards and procedural timelines create enforcement gaps that criminal networks exploit to relocate infrastructure, launder proceeds and reconstitute operations before coordinated responses can be executed. This challenge is especially pronounced in cases involving state-aligned actors, where political sensitivities further complicate attribution and enforcement. The analysis suggests that these grey zones are not incidental but structural, arising from the misalignment between cyber operational speed and institutional response mechanisms. In RAT terms, these grey zones represent persistent gaps in capable guardianship across jurisdictions, enabling motivated offenders to operate transnationally with minimal disruption.

Finally, the comparative coding indicates that financial disruption tools, such as anti-money-laundering measures, cryptocurrency tracing and sanctions, are now widely adopted across both the US and EU strategies. However, their presence alone does not appear sufficient to achieve sustained disruption of high-risk networks. Instead, effective and durable disruption correlates with the conjunction of three conditions: a clearly articulated operational disruption doctrine, coordinated and credible attribution mechanisms and structured public–private operational integration. Where these elements reinforce one another, disruption efforts impose higher costs on adversaries and reduce their capacity to regenerate. Where they are absent or weakly coupled, enforcement efforts tend to remain episodic, allowing cybercriminal ecosystems to adapt and persist. This finding underscores the importance of integrated strategic design rather than isolated policy instruments in confronting industrialised, state-aligned cybercrime.

The EU cybersecurity strategy for the Digital Decade and the US national cybersecurity strategy of 2023 offer distinct approaches to addressing cybersecurity challenges, including high-risk cybercriminal networks. The EU strategy emphasises a comprehensive regulatory framework, digital sovereignty, resilience-building, cyber diplomacy and capacity building for Member States. Its advantages include the strong cybersecurity and data protection standards provided by the General Data Protection Regulation and the NIS2 Directive, a focus on reducing reliance on foreign technologies through initiatives like Gaia-X, and the promotion of responsible state behaviours via international norms. The strategy also prioritises resilience across critical infrastructures and digital services, emphasising

cybersecurity-by-design principles. However, it faces challenges such as implementation complexity due to disparities in Member State capabilities, a limited focus on offensive cyber capabilities and potential dependency risks associated with strict regulatory measures.

The US strategy takes a proactive and forward-looking approach, emphasising the need to prepare for emerging threats like quantum computing and AI vulnerabilities while employing offensive cyber operations to dismantle high-risk networks. It introduces a shared responsibility model, shifting the burden from individuals to large corporations and technology providers, and incentivises secure-by-design practices through liability measures. The strategy is supported by broad regulatory frameworks for critical infrastructure protection. Nevertheless, its reliance on the private sector may encounter resistance due to increased regulation, and fragmentation risks arise from the diversity of stakeholders across the federal, state and private sectors. Additionally, the strategy's occasional prioritisation of unilateral actions may alienate international partners.

In terms of targeting threat actors, the EU strategy focuses on state-sponsored threats, ransomware operators and transnational criminal networks, relying on defensive measures such as harmonised frameworks and the EU Cyber Diplomacy Toolbox for imposing sanctions and attributing attacks. The US strategy targets both state and non-state actors, leveraging offensive capabilities like the 'defend-forward' approach to neutralise threats proactively and employing economic and legal tools to impose consequences on cybercriminals.

International collaboration is a cornerstone of both strategies, but their approaches differ significantly. The EU strategy emphasises global cooperation through legal frameworks like the Budapest Convention on Cybercrime, which facilitates international coordination. It also prioritises norm-setting through partnerships with organisations like the United Nations and the Organization for Security and Cooperation in Europe while advocating for cybersecurity certification standards and regional cybersecurity hubs. Collaboration with NATO and capacity-building initiatives in developing countries are key components of its global approach. The US strategy, on the other hand, leverages multilateral initiatives like the Counter Ransomware Initiative and builds regional alliances through frameworks such as the Quad, Aukus (a trilateral security partnership between Australia, the United Kingdom and the United States) and the EU–US Trade and Technology Council. It focuses on countering the abuse of cryptocurrencies by cybercriminals through anti-money laundering and countering the financing of terrorism standards and fosters bilateral collaboration with allies like the United Kingdom and Israel for joint cyberdefence exercises.

The EU strategy employs legal instruments such as the NIS2 Directive to enforce uniform cybersecurity measures across Member States and uses cyber diplomacy tools like sanctions to coordinate EU-wide responses to cyberattacks. Public–private partnerships are encouraged through platforms like ENISA. The US strategy emphasises public–private operational models for disrupting adversaries, such as the Joint Cyber Defence Collaborative, and promotes real-time intelligence sharing between private entities and federal agencies. Offensive cyber operations are also integrated into its international collaboration efforts to dismantle high-risk networks.

Both strategies address emerging challenges in their own ways. The EU strategy focuses on building resilience by addressing supply chain vulnerabilities and promoting digital sovereignty while prioritising ethical AI and data privacy. Long-term capacity-building efforts aim to harmonise cybersecurity capabilities across Member States. The US strategy takes a forward-looking approach by preparing for quantum computing risks with quantum-resistant cryptography

and targeting ransomware ecosystems by addressing financial enablers and supply chains. It also places significant emphasis on securing critical infrastructure and emerging technologies like the internet of things (IoT) and AI.

While both strategies aim to strengthen cybersecurity and combat high-risk cybercriminal networks, their approaches reflect their respective political, economic and technological contexts. The EU strategy leans heavily on regulatory measures and harmonisation, focusing on resilience and sovereignty, whereas the US strategy adopts a proactive stance with offensive capabilities, public–private collaboration and a focus on emerging threats. Both face challenges in implementation, but their combined efforts contribute significantly to global cybersecurity advancements.

The analysis reveals a fundamental strategic divergence. While the US strategy is rooted in 'realist deterrence' (utilising offensive 'defend-forward' operations to raise costs for adversaries), the EU strategy leans towards 'institutional liberalism' (emphasising norm-setting and regulatory sovereignty). However, the findings suggest that the US model faces challenges in legitimacy and private sector compliance, whereas the EU model is hampered by the 'capability-expectations gap' among its Member States. This divergence explains why high-risk networks continue to exploit the jurisdictional 'grey zones' between these two major powers.

Table 21.1. Comparison of EU cybersecurity strategy and US national cybersecurity strategy

Aspect	EU cyber strategy	US cyber strategy
Advantages	Strong regulatory frameworks, emphasis on digital sovereignty, harmonised standards and proactive cyber diplomacy.	Forward-looking, offensive capabilities, shared responsibility, strong focus on market incentives and resilience.
Disadvantages	Implementation challenges, limited offensive measures and risk of innovation slowdown.	Over-reliance on the private sector, complex implementation and potential unilateralism.
International collaboration	Emphasises legal frameworks, norm-setting and capacity building through multilateral institutions.	Focuses on multilateral disruption campaigns, offensive collaboration and real-time intelligence sharing.
Emerging threats	Addresses supply chain risks, promotes digital sovereignty and focuses on AI ethics and resilience.	Prepares for quantum threats, targets ransomware ecosystems and emphasises IoT and AI security.

Source: Created by the author.

Conclusion

This study highlights the evolving complexities of high-risk cybercriminal networks and the critical need for comprehensive strategies to combat their growing threat. The comparison between the US National Cybersecurity Strategy (2023) and the EU cybersecurity strategy for the Digital Decade (2020) reveals distinct approaches shaped by differing political, technological and economic priorities. By combining network governance and routine activity perspectives, the study demonstrates that the sustainable disruption of high-risk cybercriminal networks requires both ecosystem-level intervention and the systematic strengthening of capable guardianship across jurisdictions.

The US strategy demonstrates a proactive stance, emphasising offensive cyber operations, public–private collaboration and the integration of emerging technologies to disrupt cybercriminal networks. By shifting the responsibility of cybersecurity from individuals to large corporations and infrastructure providers, the US promotes resilience while leveraging its global alliances to counter transnational threats. However, the strategy's reliance on private-sector cooperation and occasional unilateral actions could limit its global efficacy.

Conversely, the EU strategy focuses on building a robust regulatory framework, harmonising cybersecurity capabilities across Member States and advancing digital sovereignty. Its emphasis on defensive measures, norm-setting and international cooperation through legal frameworks like the Budapest Convention highlights a more collaborative and resilience-oriented approach. Nonetheless, challenges such as fragmented implementation and limited offensive capabilities may hinder its effectiveness against sophisticated and state-sponsored cybercriminal networks.

Both strategies underscore the importance of international collaboration, leveraging alliances such as NATO and multilateral initiatives like the Counter Ransomware Initiative to address global cybercrime. The study also identifies emerging technologies, such as AI, quantum computing and IoT, as both threats and opportunities in the fight against cybercrime, emphasising the need for continuous adaptation and innovation.

While the US and EU approaches differ in focus, their complementary strengths – offensive measures from the United States and robust regulation from the EU – offer valuable insights for a global framework to combat high-risk cybercriminal networks. A unified, cooperative effort combining offensive capabilities, regulatory harmonisation and technological innovation will be essential to navigating the increasingly complex landscape of cybercrime. This study provides a foundation for further research and policy development aimed at fostering a secure and resilient digital ecosystem worldwide.

Future research should focus on the impact of large language models on the automation of the cybercriminal life cycle. A significant limitation of this study is the rapid evolution of crypto-mixer technologies, which may bypass the current US and EU financial sanctions. Policymakers must move beyond static strategies towards a 'dynamic defence' model that integrates AI-driven attribution with real-time transatlantic intelligence sharing.

References

Cohen, L. E. and Felson, M. (1979), 'Social change and crime rate trends: A routine activity approach', *American Sociological Review*, Vol. 44, No 4, August, pp. 588–608, https://doi.org/10.2307/2094589.

Euronews (2024), 'Russia increasingly using cybercriminals to target adversaries, Microsoft says', Euronews, 16 October, https://www.euronews.com/next/2024/10/16/russia-increasingly-using-cybercriminals-to-target-adversaries-microsoft-says.

European Commission (2020), Joint Communication to the European Parliament and the Council – The EU's cybersecurity strategy for the Digital Decade, JOIN(2020) 18 final of 16 December, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018.

Felbab-Brown, V., Paz García, D. and Bajji, V. (2024), 'Chinese crime and geopolitics in 2024', Brookings, 29 January, https://www.brookings.edu/articles/chinese-crime-and-geopolitics-in-2024/.

Jones, C., Hesterly, W. S. and Borgatti, S. P. (1997), 'A general theory of network governance: Exchange conditions and social mechanisms', Academy of Management Review, Vol. 22, No 4, October, pp. 911–945, https://doi.org/10.2307/259249.

Klepper, D. (2024), 'Cyber criminals are increasingly helping Russia and China target the US and allies, Microsoft says', AP News, 15 October, https://apnews.com/article/microsoft-russia-china-iran-israel-cyberespionage-cyber-d3a22dd2dcea32615ac15ed4fb951541.

Lakshmanan, R. (2024), 'Experts uncover Chinese cybercrime network behind gambling and human trafficking', The Hacker News, 22 July, https://thehackernews.com/2024/07/experts-uncover-chinese-cybercrime.html.

Leukfeldt, E. R., de Poot, C. J., Verhoeven, M. A., Kleemans, E. R. and Lavorgna, A. (2017), 'Cybercriminal networks', in: Leukfeldt, E. R. (ed.), The Human Factor in Cybercrime and Cybersecurity: Research agenda, Eleven International Publishing, The Hague, pp. 33–42.

Luo, Q. (2024), 'Cybercrime as an industry: Examining the organisational structure of Chinese cybercrime', *Humanities and Social Sciences Communications*, Vol. 11, p. 1554. https://doi.org/10.1057/s41599-024-04042-w.

Meland, P. H., Bayoumy, Y. F. F. and Sindre, G. (2020), 'The ransomware-as-a-service economy within the darknet', *Computers and Security*, Vol. 92, February, 101762, https://doi.org/10.1016/j.cose.2020.101762.

Muia, W. (2024), 'Zambia uncovers "sophisticated" Chinese cybercrime syndicate', *BBC News*, 10 April, https://www.bbc.com/news/world-africa-68777137.

National Crime Agency (2024), 'Operation Destabilise: NCA disrupts multi-billion Russian money laundering networks with links to drugs, ransomware and espionage, resulting in 84 arrests', National Crime Agency, https://www.nationalcrimeagency.gov.uk/news/operation-destabilise-nca-disrupts-multi-billion-russian-money-laundering-networks-with-links-to-drugs-ransomware-and-espionage-resulting-in-84-arrests.

O'Neill, A. (2024), 'Countering North Korean cybercrime and its enablers', *Lawfare Media*, 2 May, https://www.lawfaremedia.org/article/countering-north-korean-cybercrime-and-its-enablers.

The White House (2023), *National Cybersecurity Strategy*, March, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Tidy, J. (2024), 'Firm hacked after accidentally hiring North Korean cyber criminal' *BBC News*, 16 October, https://www.bbc.com/news/articles/ce8vedz4yk7o.

The challenge of organised agricultural criminality: The psychological and wider societal impacts

Kreseda Smith

https://doi.org/10.3013/33zkqa09

Abstract

Globally, farmers are increasingly threatened by organised criminal networks, leading to a rise in agricultural crime. This shift from traditional opportunistic offences to more organised crime is severely impacting the psychological well-being of farmers. It is also causing broader societal issues, including farmers' departure from the sector, diminished trust in law enforcement and threats to food chain security.

Farmers encounter various stressors – negative events that affect their well-being – and hinder successful business management. Existing research has identified stressors such as weather, finance, regulation, staffing and time pressures. However, the impact of organised agricultural criminality (OAC) on farmers' mental health and its broader implications have not been explored.

This pioneering research investigates whether agricultural crime should be recognised as a stressor for farmers. It compares the impact of agricultural crime with other well-documented stressors on farm management in Great Britain. Additionally, this study examines the wider repercussions of OAC, considering the secondary and tertiary impacts of these events.

While this research was conducted in Great Britain, its findings have international relevance, given the global reach of these criminal networks. The results indicate that OAC is a significant stressor for farmers, surpassed only by weather, finance and time pressures. Moreover, acts of criminality have extensive societal consequences often overlooked by those involved in crime prevention and law enforcement.

The study argues that without serious international law enforcement consideration of OAC, the psychological and societal effects of these crimes could jeopardise global food security in unforeseen ways.

Keywords: organised agricultural crime, farmers' mental health, farming.

Introduction

Rural and agricultural crime has become a small but emerging area of research in the last 30 years (Barclay et al., 2002; Bunei et al., 2013; DeKeseredy et al., 2013; Saltielet, 1992; Smith et al., 2019). Criminological literature has discussed the increasingly organised nature of rural and agricultural crime since the mid 2010s (Smith et al., 2017; Smith, 2018; Smith et al., 2016). Recent work supported by the United Kingdom's newly established National Rural Crime Unit has identified a clear link between the theft of agricultural machinery and organised crime group (OCG) networks (Tudor, 2024). Despite this slowly developing academic evidence, there remain issues in the practical policing of organised agricultural criminality (OAC) in Great Britain due to not only a lack of a national working definition of rural and agricultural crime despite the recent establishment and best efforts of the National Rural Crime Unit, but also a dearth of official data relating to rural and agricultural crime incidents. As a result of the inability to show the true extent of agricultural crime incidents, it remains a challenge to get regional organised crime policing units to accept that much of the agricultural criminality that is experienced is organised in nature. It is often the case that organised criminality in rural communities is seen as directly related to urban crime, such as organised drug trafficking, and as such organised criminality is seen as negligible in the rural space (Fraser et al., 2018; Clark et al., 2021). Despite increasing evidence of OAC and the impact it can have on farmers, farming communities and global food security (Smith, 2024), the impact of OAC is often overlooked by strategic policing decision-makers and as such fails to attract the resources that city-based organised criminality does (Clark et al., 2021).

Academic literature has long recognised that farmers worldwide are working under levels of immense stress (Booth et al., 2000; Kearney et al., 2014; Olson et al., 1986; Walker et al.,1986). Indeed, farming is one of the industries where workers are most likely to become a victim of suicide (Booth et al., 2000). The tenuous balance of competing stressors such as finances, weather and regulations are recognised in the literature and could be considered chronic stressors that farmers learn to deal with in the daily running of their farms. However, the introduction of an acute stressor such as a criminal incident can lead to this delicate stressor balance being disrupted, leading to short- and long-term financial and business continuity pressures, in addition to affecting the confidence farmers have in the police, which can lead to ongoing extensive social, psychological and physical health effects (Smith, 2024; Smith et al., 2024). Farmers have reported anxiety, depression and suicidal tendencies as a direct result of agricultural crime (Smith, 2020, 2022). This original article extends the author's previous work (Smith, 2020, 2022, 2024) by examining new data to provide an in-depth understanding of the extensive impact that crime has on farming communities and the wide-reaching second- and third-order effects to which this leads. Additionally, this work identifies the need for policing strategists to recognise the increasingly organised nature of these types of crimes, and the ability of OCGs to pivot their business plans to respond very quickly to local, national and global demands.

This exploratory research aims to address the following issues: (1) How does OAC compare with other stressors? (2) Do farmers feel that agricultural criminality is organised? (3) How is OAC affecting farmer mental health? This research explores the key research question: To what extent is OAC impacting farmers' mental health?

Methodology

This research extends the previous work of the author through the collection of new data leading to practical policy recommendations based on the quantitative analyses undertaken. The target population for this work was British farmers who had been victims of crime within the previous 12 months, with non-probability purposive snowball sampling being employed via an online questionnaire delivered using JISC online surveys (https://www.jisc.ac.uk/online-surveys). While it is recognised that online surveys pose methodological issues through the reduced equality in availability, particularly in rural areas due to poor internet stability, this method does allow research requests to be sent to a widely dispersed target population quickly, easily and at a low cost to the researcher, particularly where communities might be hard to reach, remote or isolated (Smith, 2021).

The questions are partly based on the work carried out by Smith (2020; 2022) exploring the impact of agricultural crime on farmers' psychological well-being and experiences of victimisation. Additional questions were added to explore the issue of who farmers thought were committing such offences. This was done with the intention of exploring the extent to which farmers believed these crimes to be committed by OCGs or other potential offenders.

The questionnaire comprised 27 questions divided into four sections: crime victimisation; the impact of agricultural crime on farmers' psychological well-being; do the farmers think agricultural crime is organised; and general information about the farmers. The questionnaire was completely anonymous, and no identifying information was collected. The research was conducted with ethical approval via the Harper Adams Research Ethics Committee.

The questionnaire was piloted by six colleagues who have knowledge of farming but who do not fit the target population to ensure avoidance of sample contamination. Feedback from the pilot members was reviewed and actioned where necessary to ensure that the questionnaire was workable and contained no confusing or leading questions. Once adapted as required, the questionnaire was made live on the online software. The link and QR code were promulgated via various social media platforms including X, Facebook, Instagram and LinkedIn. Further, a press release was drafted and released by the Harper Adams Press Office, and the link and QR code were sent to staff at the university to share with their own networks, with the aim of reaching as many potential respondents as possible. The survey was open for four weeks to allow as many responses as possible to be collected. In total, 239 responses were received in that period. The demographic data of respondents are included in Table 22.1.

Table 22.1. Demographic data of respondents

		N
Age	18–34	39
	35–44	74
	45–54	60
	55–64	64
	65+	2
Role	Farmer	87
	Full-time farm worker	20
	Part-time farm worker	108
	Farmer family	24

		N
Gender	Male	76
	Female	163
Production	Arable	54
	Beef finishing	8
	Dairy	35
	Fruit	97
	Sheep	45
Ownership	Owner occupier	89
	Tenant	148
	Share farming agreement	2

Results were exported from JISC online surveys into Statistical Product and Service Solutions software for cleaning and analysis. Descriptive statistics were collated and analysed with the aim of addressing the key objectives as presented in the next section. Inferential statistical analysis was undertaken with non-parametric tests being employed due to the non-random sampling strategy, the non-normal distribution of the data and the scales of measurement of the individual variables tested.

Results

How does organised agricultural criminality compare with other stressors?

Figures 22.1 to 22.7 provide an overview of OAC victimisation experiences and how respondents feel crime ranks as a stressor when considered alongside other stressors. Figure 22.1 shows that almost two thirds (61 %) of respondents have been victims of crime at least four times in the proceeding 12-month period, with Figure 22.2 presenting the type of crimes experienced.

When considering the impact of repeat victimisation on experiencing crime-related mental health issues, there are several statistically significant positively correlated results, as shown in Appendix 22.1. One key exception is the reporting of worrying about their own safety, which indicated a negative correlation. This suggests that the issue of 'defence othering' (Stough-Hunter, 2015) may play a key part in the minds of farmers by deflecting any of their concerns for their own safety either in an attempt to remain stoic or because they must in order to continue with the business of farming.

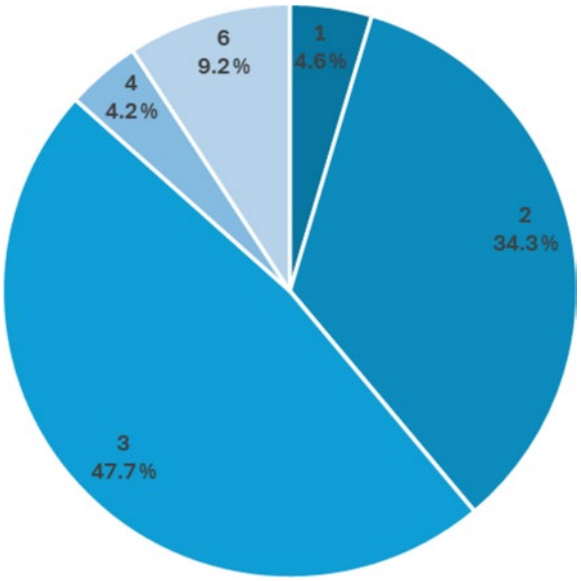


Figure 22.1. Number of criminal incidents experienced by respondents in the previous 12 months, showing a majority reporting more than four criminal events

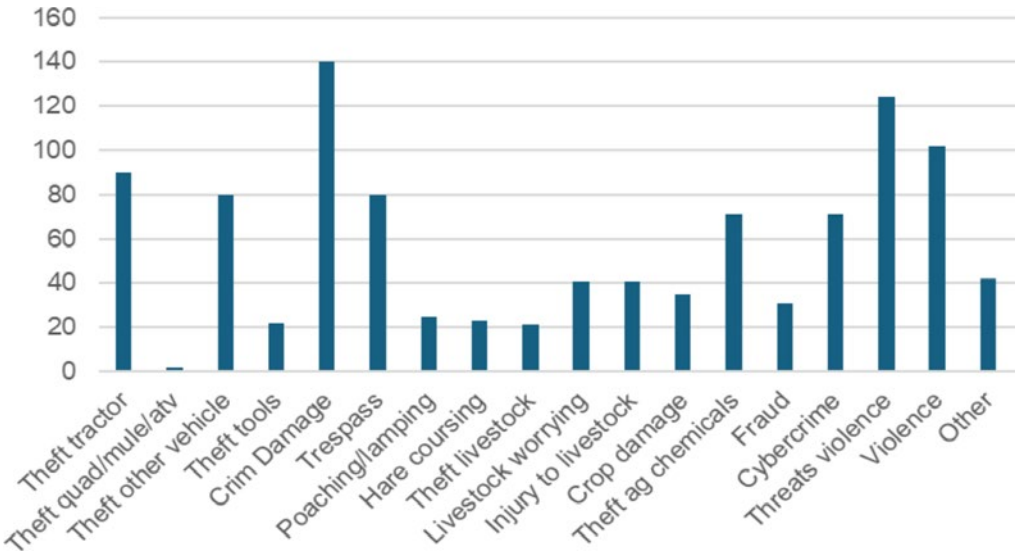


Figure 22.2. Types of crimes experienced by farmers, showing that criminal damage, violence and threats of violence are the crimes most experienced

When considering the reporting of crimes to the police (Figure 22.3), it is interesting to note that three quarters of respondents did report the crime to the police (75.7 %); however, over half of respondents (54.2 %) felt that the police response was either 'fairly unhelpful' or 'very unhelpful' (Figure 22.4).

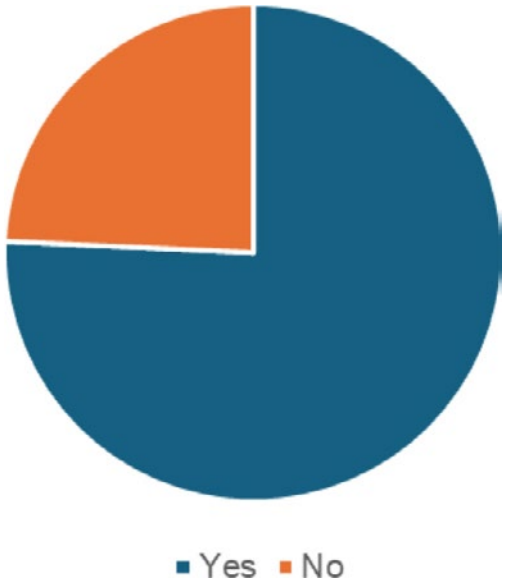


Figure 22.3. Level of reporting crimes to police, showing that over three quarters of crimes were reported to the police by respondents

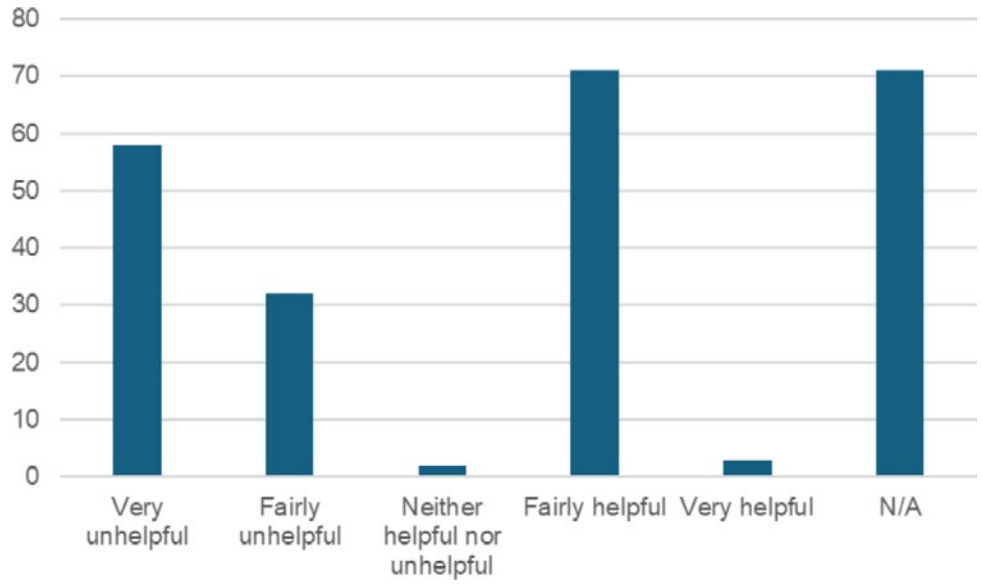


Figure 22.4. Over half of respondents felt the police were either fairly or very unhelpful when they reported the crime

Figure 22.5 provides a word cloud representing the most mentioned words by respondents when asked about the top three impacts of being a victim of crime. Keywords identified include 'financial', 'costs', 'vulnerable' and 'suspicious'. This seems to indicate a more equal weighting between financial and emotional impacts than previously thought. Figure 22.6 further provides a word cloud representing the most mentioned words by respondents when asked about the top three day-to-day stressors when running a farm. Keywords identified here include 'finance', 'weather', 'lone', and 'machinery', which reflects the existing literature. However, it is notable that 'crime' does feature quite prominently on this word cloud, despite most respondents (64 %) ranking crime as at least 10th on their stressor list (Figure 22.7).

Figure 22.5. This word cloud highlights that the most reported impacts of crime were 'financial', 'costs', 'vulnerable' and 'suspicious'

Figure 22.6. Key stressors are highlighted as 'finance', 'weather', 'productivity' and 'lone', and that 'crime' remains prominent on this list despite this

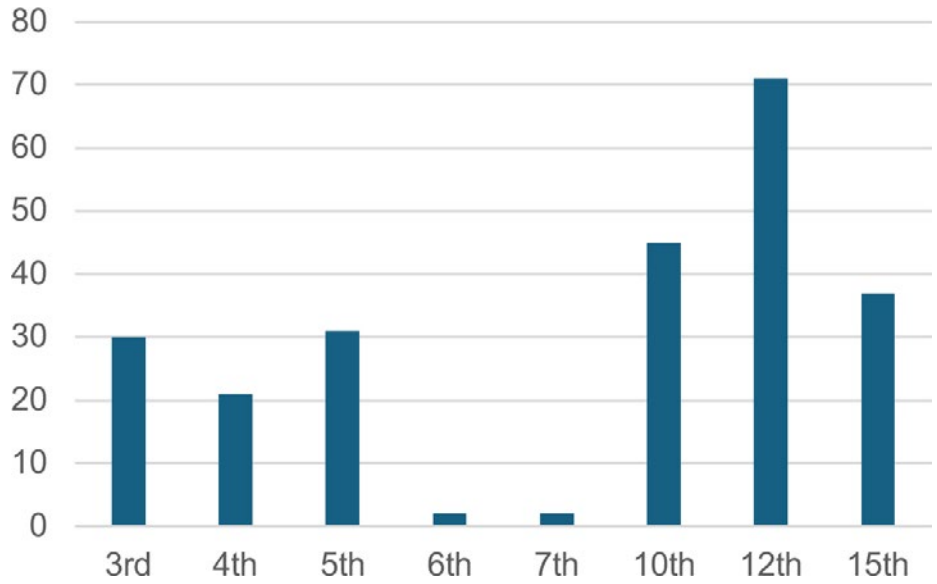


Figure 22.7. A majority of respondents felt that crime ranked at least 10th on this list of stressors despite the prominent appearance of crime in the above word cloud

Despite crime seemingly being quite low down in the stressor ranking, inferential correlational analysis found that in several cases rank is positively correlated with crime-related mental health indicators (Appendix 22.2). The exceptions are isolation ($R = -0.14$, $p = 0.03$), worry about my safety ($R = -0.33$, $p < 0.001$) and worry about securing firearms ($R = -0.17$, $p = 0.01$). This suggests that despite not considering crime to be a key stressor, farmers often experience crime-related mental health indicators, suggesting that this may be more stressful than initially considered by respondents.

Do farmers feel agricultural crime is organised?

Figures 22.8 to 22.11 provide results relating to respondents' thoughts about the level of organisation of agricultural crime. While there is an indication that respondents feel that each offender type is always represented (Figure 22.8), there seems to be a strong indication that respondents feel that OAC is very much driven by three key cohorts: OCGs (66.5 % 'very often' or 'always'); urban residents (71.9 % 'very often' or 'always'); and travelling communities (83.7 % 'very often' or 'always'). It is arguable that each of these three cohorts in some way suggest some level of organisation, even if not overtly stated as such due to the nature of the historic links of urban residents and elements of the travelling community being involved in agricultural crime (McElwee et al., 2012; Mawby et al., 2016).

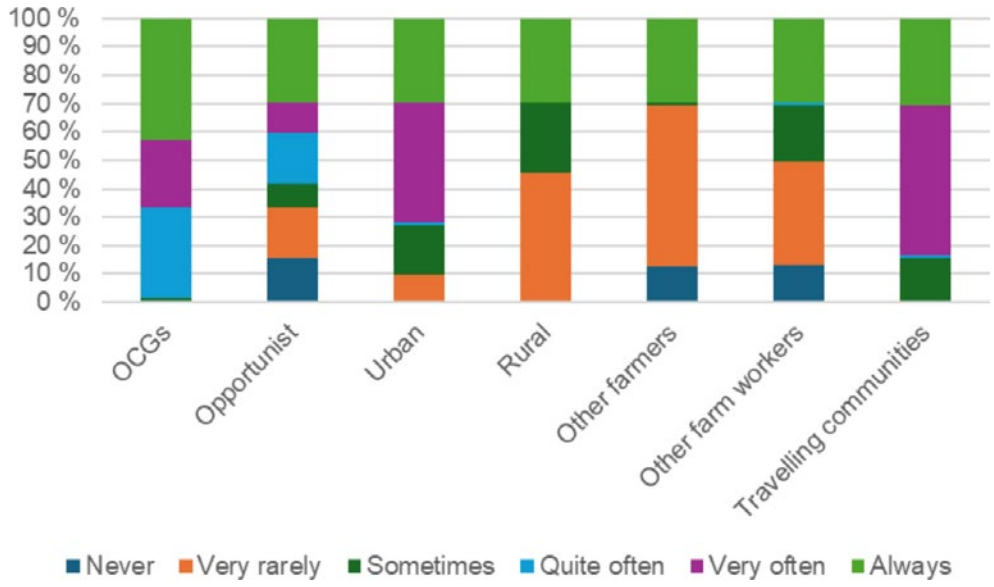


Figure 22.8. Despite a belief that agricultural crime is most often committed by travelling communities, most respondents felt that OCGs committed agricultural crime at least quite often

To underpin the responses indicating OCG involvement, Figure 22.9 shows that almost all respondents (*n* = 237) either 'agree' or 'strongly agree' that agricultural crime is committed by OCGs, and Figure 22.10 shows that all respondents believe that the level of OCGs targeting farms has either 'increased a little' or 'increased a lot' over the last five years. Most interestingly, Figure 22.11 shows that 76 % of respondents believe that the police do not see agricultural crime as organised crime. This suggests a perceived increase in OCG activity that is clearly recognised by the farmer respondents, but they equally feel that the police do not recognise this effect.

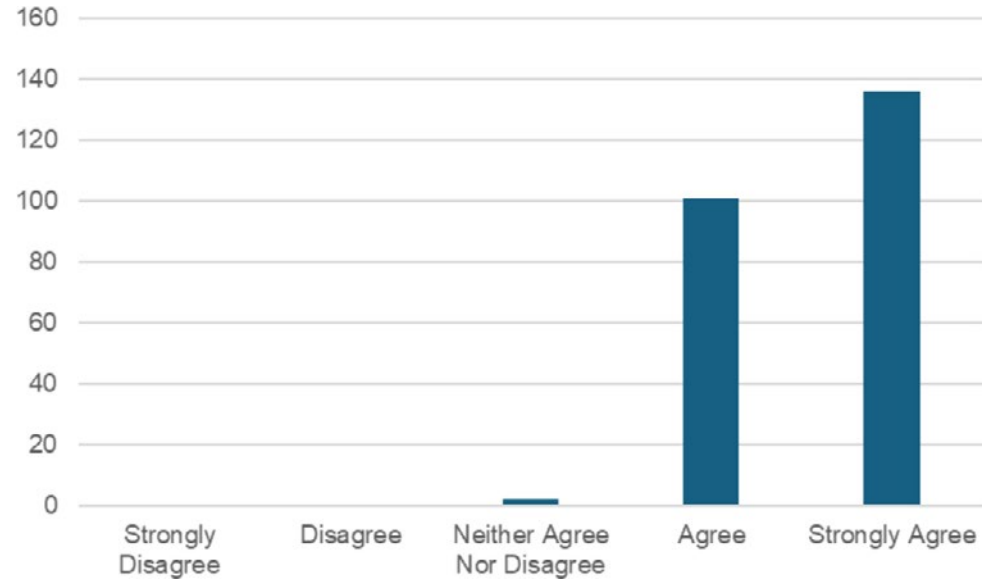


Figure 22.9. Almost all respondents felt that OCGs were key offenders in agricultural crime

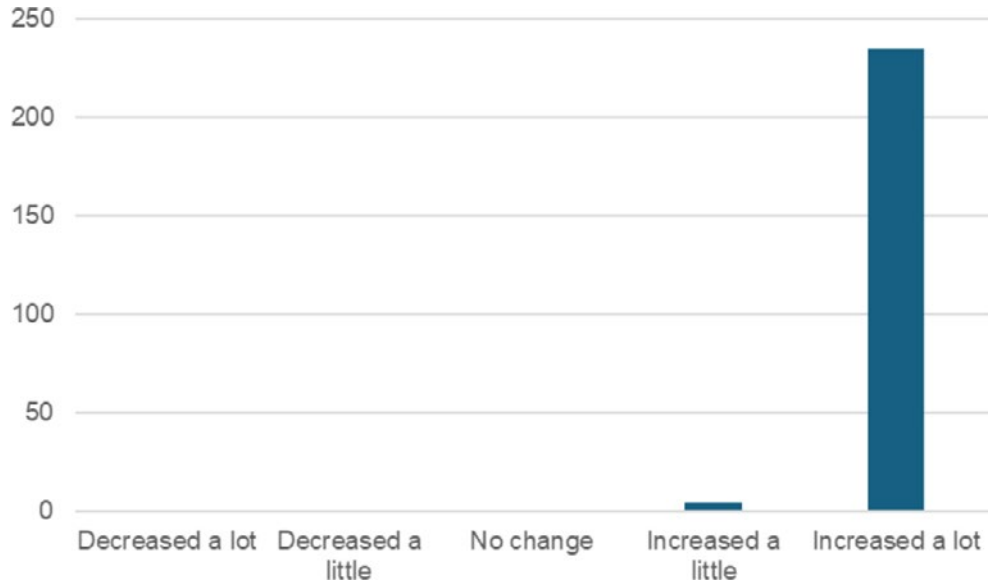


Figure 22.10. Almost all respondents felt that OCGs targeting farms has increased in the last five years

Table 22.2 shows the statistically significant positive associations between perceptions of OCG increase and reported crime-related mental health indicators experienced. This shows a clear relationship between feeling that OCGs are increasingly targeting farms and leading to farmers experiencing anxiety, inability to prevent victimisation, feeling vulnerable, lack of sleep, loss of confidence and control, suicidal thoughts and worries about family safety.

Table 22.2. Spearman's rho associations between crime-related mental health indicators and recognition of increased targeting of farms by OCGs

Mental health indicator	*N*	*R*	*P*
Feeling anxious	239	0.13	0.04
Cannot prevent being victim	239	0.15	0.02
Feeling vulnerable	239	0.21	0.001
Lack of sleep	239	0.15	0.02
Loss of confidence	239	0.13	0.04
Loss of control	239	0.15	0.02
Suicidal thoughts	239	0.15	0.03
Worry about family safety	221	0.19	0.006

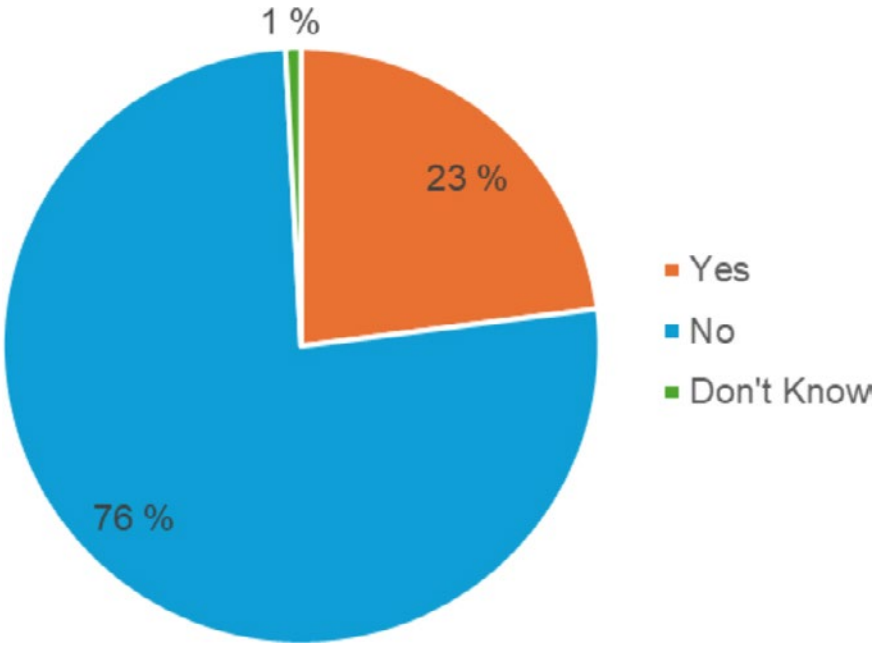


Figure 22.11. Most respondents felt that the police do not see agricultural crime as organised

Appendix 22.3 presents the inferential results when exploring statistically significant differences of crime-related mental health indicators across whether respondents feel that the police recognise agricultural crime as organised. In all but two cases, those who felt the police did not recognise agricultural crime as organised were statistically more likely to report experiencing crime-related mental health issues. The exceptions were not being able to prevent being a victim (organised $\bar{x}R = 135.88$; not organised $\bar{x}R = 115.94$; do not know $\bar{x}R = 52.5$), ($H = 7.08$ (2, 239), $p = 0.03$), and feeling vulnerable (organised $\bar{x}R = 139.89$; not organised $\bar{x}R = 115.07$; do not know $\bar{x}R = 21.5$), ($H = 11.95$ (2, 239), $p = 0.003$).

How is organised agricultural criminality affecting farmers' mental health?

Multiple indicators were used to assess the impact of OAC on farmers' mental health. These were grouped into five categories: victimisation (Figure 22.12); simple worries (Figure 22.13); losses (Figure 22.14); worries (Figure 22.15); and personal (Figure 22.16). It can be seen from these figures that each indicator is experienced by all respondents to varying degrees, with no responses showing that indicators are wholly either 'never' or 'very rarely' experienced. Key highlights include farmers feeling 'always abandoned by the police' (38.5 %), 'always feeling vulnerable' (55.6 %) (Figure 22.12), 'always feeling anxious' (46.4 %) (Figure 22.13), and a feeling 'loss of trust' (42.7 %) (Figure 22.14). Key worries for respondents centred around the safety of their family (38.9 % 'always'), which may suggest an element of 'defence othering' (Stough-Hunter, 2015) and worry about lone working (46.4 % 'always') (Figure 22.15). From the 'personal' category, while all indicators showed a response of between 40 % and 50 % reporting they never experience these indicators, it is particularly notable that 38.4 % of respondents 'always' thought about giving up farming and the same number reported 'always' having suicidal thoughts, and while no respondents reported 'always' exhibiting suicidal behaviour, 30.1 % did report experiencing this behaviour very often as a direct result of OAC (Figure 22.16).

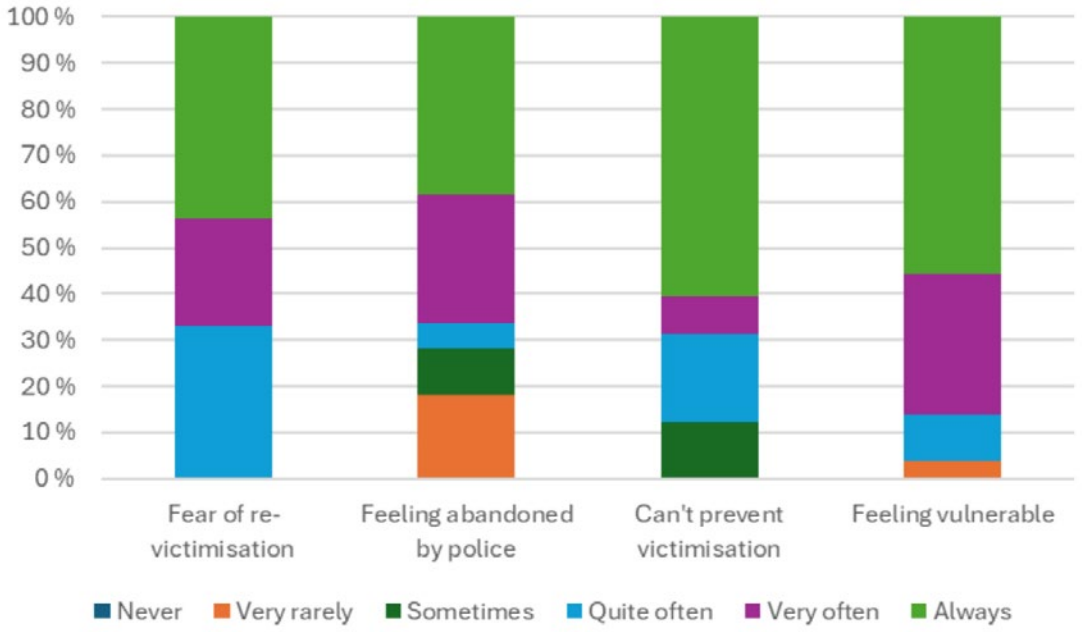


Figure 22.12. Victimisation shows the greatest impact on worries around repeat victimisation and inability to prevent victimisation

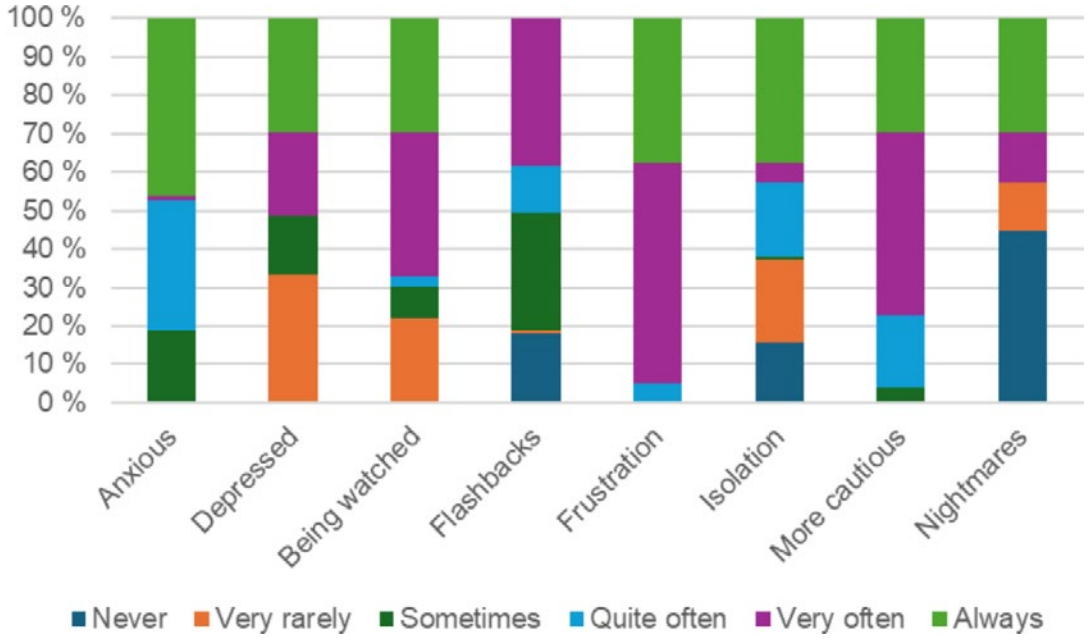


Figure 22.13. Simple worries affected by victimisation are primarily presented through feelings of frustration and anxiety

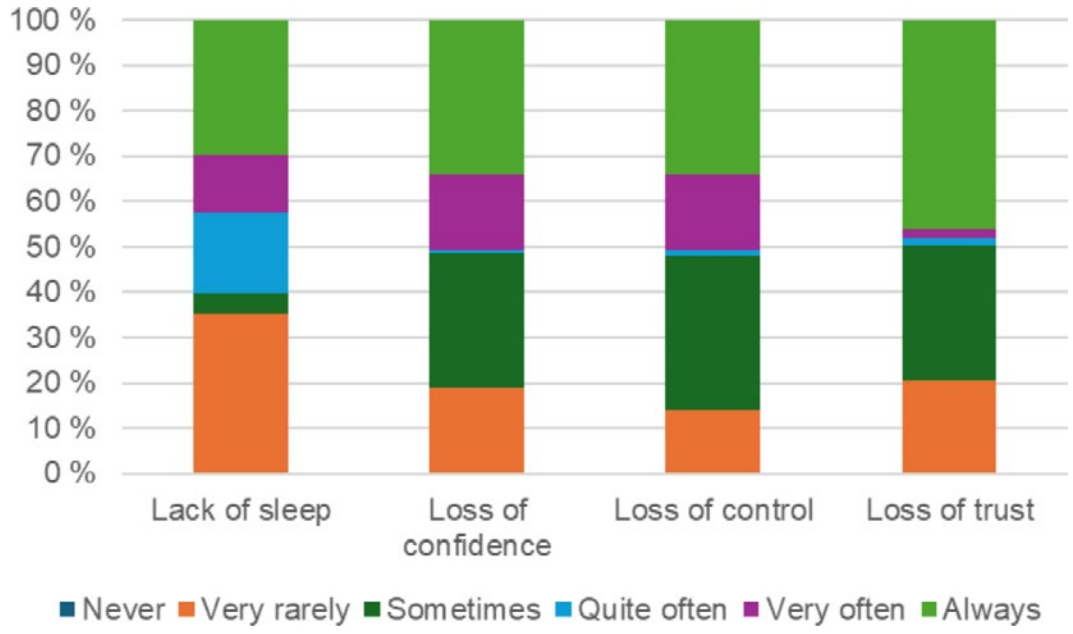


Figure 22.14. Losses affected by victimisation are seen at least 'quite often' in a minimum of 50 % of respondents

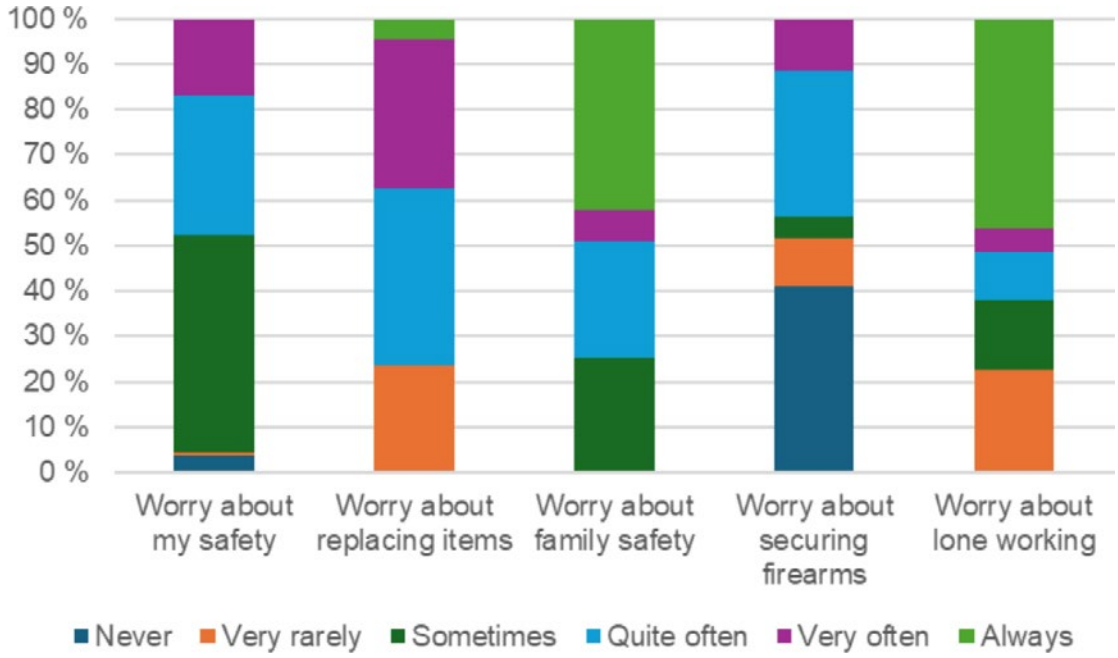


Figure 22.15. Worries about replacing items are most common, but worries about family safety and lone working are seen at a higher level in the 'always' category

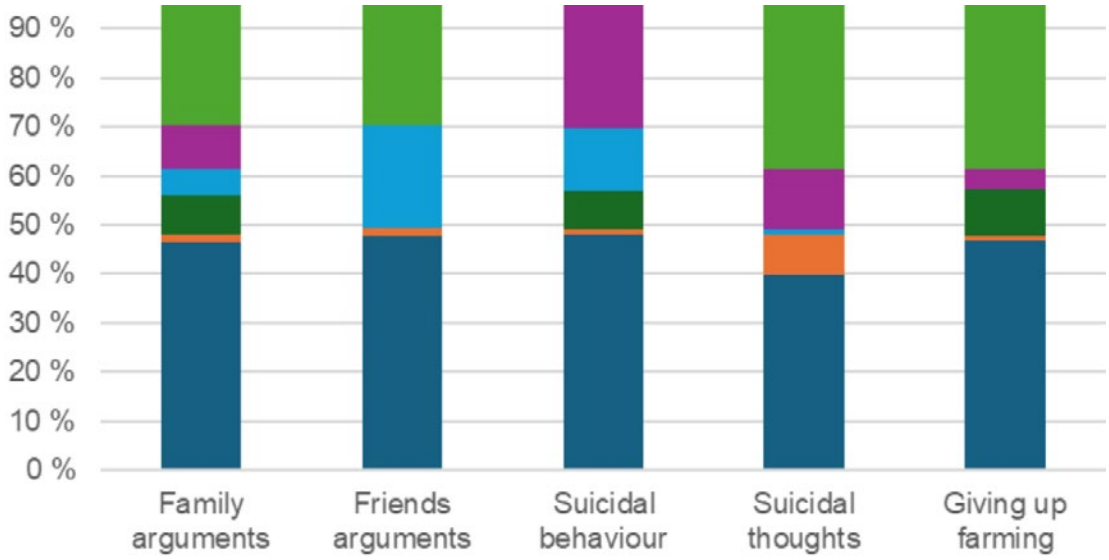


Figure 22.16. Suicidal thoughts and thoughts of giving up farming are 'always' seen in around 40 % of respondents

When considering the inferential analysis of the effect of OAC on farmers' mental health, gender and age were seen as being particularly relevant. When analysing the effect of gender on crime-related mental health, a Mann–Whitney *U* test found that, across all measures seen in Figures 22.12–22.16, female respondents were significantly more likely to experience these effects (Appendix 22.4). When considering age as the independent variable, a Spearman's rho test found a significant correlation across all mental health indicators except feelings of isolation ($p = 0.43$), worry about safety ($p = 0.34$) and worry about securing firearms ($p = 0.41$). As can be seen in Appendix 22.5, all except two significant results suggest that older respondents are less likely to experience crime-related mental health issues.

Conclusion

Interpretation of results

This novel research found that all respondents report worrying about re-victimisation at least 'quite often', which suggests that the face of agricultural crime is changing, and that fear is increasing. This may be due to the clear link that farmers are seeing between agricultural crime and OCGs as shown by this research. There is the potential to focus on women working within agriculture, those who have been repeat victims and younger people in this sector, as this analysis indicates that they are more likely to feel the effects on their mental health from OAC victimisation. Regardless of this, these findings show that the perception of the rural space as idyllic and crime-free is very quickly being eroded by the in-roads that OCGs are making in the farming community. These findings build on the work done by Tudor (2024) but go further by suggesting that the role of OCGs in agricultural crime is moving beyond tractor and machinery theft to cover a much wider range of criminality, whether acquisitive, criminal damage or violence. This research has identified that, while agricultural crimes and repeat victimisation are increasingly being reported to the police, respondents remain sceptical about the police's recognition of the organised nature of agricultural crimes. This seems to be reinforced, in part, by the fact that the response farmers received when reporting such crimes remains well below par.

Worries as a direct result of victimisation cover initial financial worries through to indicators of traumatic events such as suspicion and feelings of vulnerability. While recognised stressors were most reported, crime did feature prominently in the responses despite being ranked fairly low when asked directly. Whether this is due to the cohort who completed the questionnaire having been a victim of crime should be questioned; however, it is indicative of the impact that crime is having on the farming community.

While this research has shown that OAC is having a detrimental effect on farmers' mental health, the fact that varying numbers of respondents report experiencing all of the mental health indicators at least 'very often' should be a cause for serious concern. The wider implications of the impact of OAC on farmers' mental health, that is, the second- and third-order impacts, present a real challenge for farmers. Although Smith (2024) explores these downstream consequences, this does not consider the wider social implications of OAC that can have a direct effect on farmers, including a loss of trust, and health and safety issues due to a lack of sleep, anxiety and depression. Furthermore, the potential for victimisation to trigger suicidal ideation or lead to a decision for farmers to leave the sector should be seen as extremely problematic due to the wider food security implications this may have.

Implications for law enforcement practices

This research has taken a step forward in highlighting the fears and experiences of the British farming community in relation to the increased nature of OAC. While more research is needed to expand on these findings, this work clearly shows that there is a need for a better understanding of OAC among police forces internationally, so that they are better able to support victims in a more effective way. Despite the UK's *Rural and Wildlife Crime Strategy 2022–2025* (National Wildlife Crime Unit, n.d.) stating that there is a need to 'relentlessly pursue' organised criminals targeting rural environments, there remains little capacity or will within police regional organised crime units to highlight OAC as a strategic priority. This lack of consideration of crime in the rural space is further illustrated by the introduction of the 'Neighbourhood policing guarantee' by the UK government (UK government: Home Office, 2025), which proposes a minimum standard of policing across all communities (UK government, 2025); however, nowhere in the framework is there any mention of rural policing or resourcing. There is a need to include some level of rural awareness training for law enforcement as standard to enable better understanding of rural life and how crime can affect those living and working in the rural space. This may form part of the initial training that new recruits undertake or part of a programme of continued professional development. Police training in England and Wales is conducted via an apprenticeship degree; however, none of the educational providers include any content on rural criminality across the three-year course. Without this understanding of rural life, how will police officers be able to undertake appropriate and effective response and investigation? It is argued that there is a need for a clear understanding among law enforcement officers, and those training them, as to the real impact that OAC is having on the farming community to enable effective communication between the police and the victims and encourage information sharing to effect a true understanding among police resource allocators of the implications that crime in the rural space can have on wider society. Finally, there is an opportunity for the police at all levels to work in liaison with academic researchers and local communities to co-create collaborative preventative and protective approaches to addressing the effects at a local level that recognise the individual nature of rural communities and their needs and experiences.

Recommendations for future research

This piece of work was exploratory in nature to gain a broad understanding of who farmers believe are the offenders targeting their farms. More importantly, this work goes some way to build on what is already known about the effects that OAC has on farmer mental health and adds new perspectives across the fields of rural criminology and mental health scholarship by extending the previous work conducted by the author (in particular Smith, 2020, 2022) to consider the growing issue of OAC and its wider effects. Key recommendations for researchers going forward firstly centre around obtaining much broader quantitative data to add to these findings, focusing on a much larger sample than that obtained with this work. This may be extended to countries outside the United Kingdom to allow for an international comparison on how OAC is affecting farmers globally. Furthermore, additional research should be undertaken from a qualitative perspective to enable a more in-depth exploration of the issues raised by this research, how OAC is affecting farmers and their mental health. The possibility of co-developing appropriate and effective police responses to OAC with farmers and academics should be explored to ensure such practices take into account what farmers consider such a response should look like. In addition, there is a need to identify key research to underpin new and innovative practices – or indeed adapt existing practices – to work through a rural lens.

References

Barclay, E. and Donnermeyer, J. F. (2002), 'Property crime and crime prevention on farms in Australia', *Crime Prevention and Community Safety: An International Journal*, Vol. 4, No 4, pp. 47–61, https://doi.org/10.1057/palgrave.cpcs.8140169.

Booth, N., Briscoe, M. and Powell, R. (2000), 'Suicide in the farming community: Methods used and contact with health services', *Occupational Environmental Medicine*, Vol. 57, No 9, pp. 642–644, https://doi.org/10.1136/oem.57.9.642.

Booth, N. J. and Lloyd, K. (2000), 'Stress in farmers', *International Journal of Social Psychiatry*, Vol. 46, No 1, pp. 67–73, https://doi.org/10.1177/002076400004600108.

Bunei, E. K., Rono, J. K. and Chessa, S. R. (2013), 'Factors influencing farm crime in Kenya: Opinions and experiences of farmers', *International Journal of Rural Criminology*, Vol. 2, No 1, December, pp. 75–100, https://doi.org/10.18061/1811/58846.

Clark, A., Fraser, A. and Hamilton-Smith, N. (2021), 'Networked territorialism: The routes and roots of organised crime', *Trends in Organized Crime*, Vol. 24, October, pp. 246–262, https://doi.org/10.1007/s12117-020-09393-9.

DeKeseredy, W. S. and Donnermeyer, J. F. (2013), 'Thinking critically about rural crime: Toward the development of a new left realist perspective', in: Winlow, S. and Atkinson, R. (eds), *New Directions in Crime and Deviancy*, Routledge, Abingdon, pp. 206–222.

Fraser, A., Hamilton-Smith, N., Clark, A., Atkinson, C., Graham, W. et al. (2018), *Community Experiences of Serious Organised Crime in Scotland*, Scottish government, Edinburgh, https://www.gov.scot/publications/community-experiences-serious-organised-crime-scotland/.

Kearney, G. D., Rafferty, A. P., Hendricks, L. R., Allen, D. L. and Tutor-Marcom, R. (2014), 'A cross-sectional study of stressors among farmers in eastern North Carolina', *North Carolina Medical Journal*, Vol. 75, No 6, November, pp. 384–392, https://doi.org/10.18043/ncm.75.6.384.

Mawby, R. and Yarwood, R. (eds) (2016), *Rural Policing and Policing the Rural: A constable countryside?*, Routledge, London.

Smith, R., McElwee, G. and Somerville, P. (2017), 'Illegal diversification strategies in the farming community from a UK perspective', Journal of Rural Studies, Vol. 53, No 2, July, pp. 122-131, https://doi.org/10.1016/j.jrurstud.2017.05.011.

Smith, R. and McElwee, G. (2016), 'Criminal farmers and organized rural crime groups: A UK case study', in: Donnermeyer, J. F. (ed.), The Routledge International Handbook of Rural Criminology, Routledge, London, pp. 127–136.

National Wildlife Crime Unit (n.d.), *Wildlife and Rural Crime Strategy 2022–2025*, https://www.nwcu.police.uk/wp-content/uploads/2022/09/NPCC-Wildlife-Rural-Crime-Strategy-2022-2025.pdf.

Olson, K. R. and Schellenberg, R. P. (1986), 'Farm stressors', *American Journal of Community Psychology*, Vol. 14, No 5, October, pp. 555–569, https://doi.org/10.1007/BF00935358.

Saltiel, J., Gilchrist, J. and Harvie, R. (1992), 'Concern about crime among Montana farmers and ranchers', *Rural Sociology*, Vol. 57, No 4, pp. 535–545, https://doi.org/10.1111/j.1549-0831.1992.tb00478.x.

Smith, K. (2018), *Behavioural science and farm crime prevention decision-making: Understanding the behavioural culture of farmers in England and Wales*, PhD thesis, Harper Adams University, https://hau.repository.guildhe.ac.uk/17339/.

Smith, K. (2020), 'Desolation in the countryside: How agricultural crime impacts the mental health of British farmers', *Journal of Rural Studies*, Vol. 80, December, pp. 522–531, https://doi.org/10.1016/j.jrurstud.2020.10.037.

Smith, K. (2021), 'Conducting online crime and safety surveys with British farmers', *International Criminal Justice Review*, Vol. 31, No 4, December, pp. 369–383, http://doi.org/10.1177/10575677211042262.

Smith, K. (2022), 'Piling on the pressure: Crime and stress in British farming', *International Journal of Rural Criminology*, Vol. 6, No 2, pp. 197–222, https://doi.org/10.18061/ijrc.v6i2.8754.

Smith, K. (2024), 'The intersection of rural criminology and food security: The impact of organised criminal groups in the rural space', in: Meško, G., Ivković, S. K. and Hacin, R. (eds), *The UN sustainable development goals and provision of security, responses to crime and security threats, and fair criminal justice systems*, University of Maribor Press, Ljubljana, pp. 185–208, https://press.um.si/index.php/ump/catalog/book/894.

Smith, K. and Byrne, R. (2017), 'Farm crime in England and Wales: A preliminary scoping study examining farmer attitudes', *International Journal of Rural Criminology*, Vol. 3, No 2, pp. 191–223, http://doi.org/10.18061/1811/81047.

Smith, K. and Byrne, R. (2019), 'Horizon scanning rural crime in England', *Journal of Crime Prevention and Community Safety*, Vol. 21, pp. 231–245, http://doi.org/10.1057/s41300-019-00073-7.

Smith, K. and Byrne, R. (2024), 'The darker side of rural masculinity: Second and third order impacts of low help-seeking behaviour following the trauma of victimisation', *International Journal of Rural Criminology*, Vol. 8, No 4, pp. 642–670, https://doi.org/10.18061/ijrc.v8i4.9971.

Stough-Hunter, A. N. (2015), 'Negotiating masculinity, class, and health in a rural context', *International Journal of Men's Health*, Vol. 14, No 2, pp. 129–145, https://www.ivysci.com/en/articles/4730369__Negotiating_Masculinity_Class_and_Health_in_a_Rural_Context.

Tudor, K. (2024), *Rural Crime: Serious, organised and international – Who victimises rural communities?*, National Rural Crime Network, https://nationalruralcrimenetwork.net/rural-crime-report-2024/.

UK government (2025), 'New measures to put neighbourhood bobbies back on beat', gov.uk website, https://www.gov.uk/government/news/new-measures-to-put-neighbourhood-bobbies-back-on-beat.

UK government: Home Office (2025), 'Neighbourhood policing guarantee performance framework', gov.uk website, https://www.gov.uk/government/publications/neighbourhood-policing-guarantee-performance-framework/neighbourhood-policing-guarantee-performance-framework-accessible.

Walker, J. L., Walker, L. S. and MacLennan, P. M. (1986), 'An informal look at farm stress', *Psychological Reports*, Vol. 59, No 2, pp. 427–430, https://doi.org/10.2466/pr0.1986.59.2.427.

Appendices

Appendix 22.1. Spearman's rho analysis of statistical correlation between repeat victimisation and experience of crime-related mental health indicators

	Fear of revic-timisa-tion	Feeling aban-doned by police	Feeling anxious	Feeling depressed	Can't prevent being victim	Feeling vulner-able	Feeling being watched	Flash-backs	Frustra-tion
R	0.024	0.068	–0.159*	0.212**	0.280**	0.201**	0.018	–0.022	0.210**
p (2-tailed)	0.710	0.293	0.014	0.001	0.000	0.002	0.785	0.739	0.001
N	239	239	239	239	239	239	239	239	239

	Isolation	Lack of sleep	Loss of confi-dence	Loss of control	Loss of trust	Family argu-ments	Friends argu-ments	More cautious	Night-mares
R	0.320**	0.289**	0.115	0.133*	0.002	0.131*	0.148*	0.287**	0.104
p (2-tailed)	0.000	0.000	0.076	0.041	0.971	0.044	0.023	0.000	0.109
N	239	239	239	239	221	239	239	239	239

	Suicidal behaviour	Suicidal thoughts	Thought of giving up farm-ing	Worry about my safety	Worry about replacing items	Worry about family safety	Worry about secure firearms	Worry about lone working
R	0.182**	0.200**	0.318**	–0.293**	0.266**	0.030	0.146*	0.052
p (2-tailed)	0.005	0.002	0.000	0.000	0.000	0.656	0.030	0.422
N	239	239	239	239	221	221	221	239

* Significant at the 0.05 level.

** Significant at the 0.001 level.

Appendix 22.2. Spearman's rho analysis of statistical correlation between how respondents ranked agricultural crime as a stressor and crime-related mental health indicators

	Fear of revic-timisa-tion	Feeling aban-doned by police	Feeling anxious	Feeling depressed	Can't prevent being victim	Feeling vulner-able	Feeling being watched	Flash-backs	Frustra-tion
R	0.258**	0.255**	0.096	–0.001	0.084	0.332**	0.470**	0.107	0.322**
p (2-tailed)	0.000	0.000	0.138	0.983	0.196	0.000	0.000	0.099	0.000
N	239	239	239	239	239	239	239	239	239

	Isolation	Lack of sleep	Loss of confi-dence	Loss of control	Loss of trust	Family argu-ments	Friends argu-ments	More cautious	Night-mares
R	–0.141*	–0.023	0.138*	0.245**	0.079	0.142*	0.159*	0.644**	0.121
p (2-tailed)	0.029	0.725	0.033	0.000	0.240	0.029	0.014	0.000	0.062
N	239	239	239	239	221	239	239	239	239

	Suicidal behaviour	Suicidal thoughts	Thought of giving up farm-ing	Worry about my safety	Worry about replacing items	Worry about family safety	Worry about secure firearms	Worry about lone working
R	0.154*	–0.050	–0.020	–0.325**	0.222**	0.181**	–0.172*	–0.004
p (2-tailed)	0.017	0.444	0.758	0.000	0.001	0.007	0.010	0.947
N	239	239	239	239	221	221	221	239

* Significant at the 0.05 level.

** Significant at the 0.001 level.

Appendix 22.3. Kruskal–Wallis *H* test analysis of statistical difference between whether respondents feel that the police recognise agricultural crime as organised and crime-related mental health indicators

Do police think crime is organised?		Yes	No	Don't know	Kruskal–Wallis *H*	df	*p*-value
Fear of re-victimisation	*N*	55	182	2	111.042	2	0.000
	Mean rank	40.00	143.43	187.50			
Feeling abandoned by police	*N*	55	182	2	129.478	2	0.000
	Mean rank	32.34	147.20	55.50			
Feeling anxious	*N*	55	182	2	128.627	2	0.000
	Mean rank	36.75	146.23	23.00			
Feeling depressed	*N*	55	182	2	73.175	2	0.000
	Mean rank	53.15	140.44	98.50			
Can't prevent being victim	*N*	55	182	2	7.084	2	0.029
	Mean rank	135.88	115.94	52.50			
Feeling vulnerable	*N*	55	182	2	11.949	2	0.003
	Mean rank	139.89	115.07	21.50			
Feeling being watched	*N*	55	182	2	137.572	2	0.000
	Mean rank	29.20	147.92	76.00			
Flashbacks	*N*	55	182	2	123.564	2	0.000
	Mean rank	35.09	146.49	44.50			
Frustration	*N*	55	182	2	61.907	2	0.000
	Mean rank	64.75	137.13	81.00			
Isolation	*N*	55	182	2	46.819	2	0.000
	Mean rank	66.28	136.29	114.50			
Lack of sleep	*N*	55	182	2	74.225	2	0.000
	Mean rank	54.31	140.70	42.50			
Loss of confidence	*N*	55	182	2	121.974	2	0.000
	Mean rank	35.65	146.55	23.00			
Loss of control	*N*	55	182	2	51.784	2	0.000
	Mean rank	67.41	137.02	17.00			
Loss of trust	*N*	55	164	2	119.669	2	0.000
	Mean rank	37.24	136.81	23.00			

Do police think crime is organised?		Yes	No	Don't know	Kruskal–Wallis *H*	df	*p*-value
Family arguments	*N*	55	182	2	63.622	2	0.000
	Mean rank	60.64	138.64	56.00			
Friends arguments	*N*	55	182	2	71.450	2	0.000
	Mean rank	57.50	139.57	57.50			
More cautious	*N*	55	182	2	11.832	2	0.003
	Mean rank	94.07	127.93	111.50			
Nightmares	*N*	55	182	2	54.254	2	0.000
	Mean rank	65.21	137.28	54.00			
Suicidal behaviour	*N*	55	182	2	64.458	2	0.000
	Mean rank	60.65	138.62	58.00			
Suicidal thoughts	*N*	55	182	2	88.730	2	0.000
	Mean rank	49.54	142.09	48.00			
Thoughts of giving up farming	*N*	55	182	2	66.837	2	0.000
	Mean rank	60.29	138.74	56.50			
Worry about my safety	*N*	55	182	2	56.509	2	0.000
	Mean rank	63.24	136.69	162.50			
Worry about replacing items	*N*	55	164	2	131.876	2	0.000
	Mean rank	30.26	138.27	95.50			
Worry about family safety	*N*	55	164	2	126.980	2	0.000
	Mean rank	33.55	137.98	28.50			
Worry about secure firearms	*N*	55	164	2	80.031	2	0.000
	Mean rank	49.11	130.56	209.00			
Worry about lone working	*N*	55	182	2	132.277	2	0.000
	Mean rank	31.67	146.66	122.50			

Appendix 22.4. Mann–Whitney *U* test analysis of statistical difference between gender and experience of crime-related mental health indicators

Gender		Male	Female	Mann–Whitney *U*	*Z*	*p*-value
Fear of re-victimisation	*N*	76	163	409.000	–12.470	0.000
	Mean rank	43.88	155.49			
Feeling abandoned by police	*N*	76	163	1 225.000	–10.442	0.000
	Mean rank	54.62	150.48			
Feeling anxious	*N*	76	163	775.000	–11.779	0.000
	Mean rank	48.70	153.25			
Feeling depressed	*N*	76	163	2 066.000	–8.634	0.000
	Mean rank	65.68	145.33			
Can't prevent being victim	*N*	76	163	4 900.000	–2.968	0.003
	Mean rank	102.97	127.94			
Feeling vulnerable	*N*	76	163	5 074.000	–2.519	0.012
	Mean rank	105.26	126.87			
Feeling being watched	*N*	76	163	102.000	–12.821	0.000
	Mean rank	39.84	157.37			
Flashbacks	*N*	76	163	651.000	–11.694	0.000
	Mean rank	47.07	154.01			
Frustration	*N*	76	163	2 559.500	–8.386	0.000
	Mean rank	72.18	142.30			
Isolation	*N*	76	163	3 076.000	–6.512	0.000
	Mean rank	78.97	139.13			
Lack of sleep	*N*	76	163	2 211.500	–8.329	0.000
	Mean rank	67.60	144.43			
Loss of confidence	*N*	76	163	620.000	–11.653	0.000
	Mean rank	46.66	154.20			
Loss of control	*N*	76	163	953.500	–11.016	0.000
	Mean rank	51.05	152.15			
Loss of trust	*N*	76	145	612.500	–11.652	0.000
	Mean rank	46.56	144.78			

Gender		Male	Female	Mann–Whitney *U*	*Z*	*p*-value
Family arguments	*N*	76	163	1 445.000	–10.216	0.000
	Mean rank	57.51	149.13			
Friends arguments	*N*	76	163	1 562.000	–10.057	0.000
	Mean rank	59.05	148.42			
More cautious	*N*	76	163	2 840.500	–7.271	0.000
	Mean rank	75.88	140.57			
Nightmares	*N*	76	163	1 931.500	–9.129	0.000
	Mean rank	63.91	146.15			
Suicidal behaviour	*N*	76	163	1 627.500	–9.901	0.000
	Mean rank	59.91	148.02			
Suicidal thoughts	*N*	76	163	1 956.500	–9.087	0.000
	Mean rank	64.24	146.00			
Thoughts of giving up farming	*N*	76	163	2 872.000	–7.286	0.000
	Mean rank	76.29	140.38			
Worry about my safety	*N*	76	163	3 660.500	–5.498	0.000
	Mean rank	86.66	135.54			
Worry about replacing items	*N*	76	145	903.000	–10.804	0.000
	Mean rank	50.38	142.77			
Worry about family safety	*N*	76	145	370.000	–12.055	0.000
	Mean rank	43.37	146.45			
Worry about secure firearms	*N*	76	145	2 036.000	–8.136	0.000
	Mean rank	65.29	134.96			
Worry about lone working	*N*	76	163	884.000	–11.351	0.000
	Mean rank	50.13	152.58			

Appendix 22.5. Spearman's rho analysis of statistical correlation between age and experiencing crime-related mental health indicators

	Fear of revicti-misation	Feeling aban-doned by police	Feeling anxious	Feeling depressed	Can't prevent being victim	Feeling vulnera-ble	Feeling being watched	Flash-backs	Frustra-tion
R	–0.443**	–0.622**	–0.330**	–0.202**	0.185**	0.193**	–0.638**	–0.406**	–0.180**
p (2-tailed)	0.000	0.000	0.000	0.002	0.004	0.003	0.000	0.000	0.005
N	239	239	239	239	239	239	239	239	239

	Isolation	Lack of sleep	Loss of confi-dence	Loss of control	Loss of trust	Family argu-ments	Friends argu-ments	More cautious	Night-mares
R	0.052	–0.242**	–0.413**	–0.274**	–0.434**	–0.280**	–0.248**	–0.376**	–0.271**
p (2-tailed)	0.427	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
N	239	239	239	239	221	239	239	239	239

	Suicidal behaviour	Suicidal thoughts	Thought of giving up farm-ing	Worry about my safety	Worry about replacing items	Worry about family safety	Worry about secure firearms	Worry about lone working
R	–0.242**	–0.170**	–0.321**	0.062	–0.542**	–0.444**	–0.055	–0.229**
p (2-tailed)	0.000	0.009	0.000	0.343	0.000	0.000	0.413	0.000
N	239	239	239	239	221	221	221	239

* Significant at the 0.05 level.

** Significant at the 0.001 level.

Authors, editors and reviewers

Authors

Patricia Faraldo Cabana: Universidade da Coruña, Spain

Country: Spain

Expertise area: criminal law

Patricia Faraldo Cabana	Biographical introduction
	**Patricia Faraldo** is full professor of criminal law at the Universidade da Coruña, Spain. She has been a Marie Skłodowska-Curie researcher at the Max Planck Institute for Foreign and International Criminal Law and an Eurias senior researcher at the Freiburg Institute for Advanced Studies. She has also been adjunct professor at the Queensland University of Technology, Australia. She has published 8 monographs and more than 200 papers and book chapters in different countries and languages. **ORCID**: https://orcid.org/0000-0001-7420-3749 **Contact**: patricia.faraldo@udc.es

Gabriela Boneva: CENTRIC

Country: England, United Kingdom

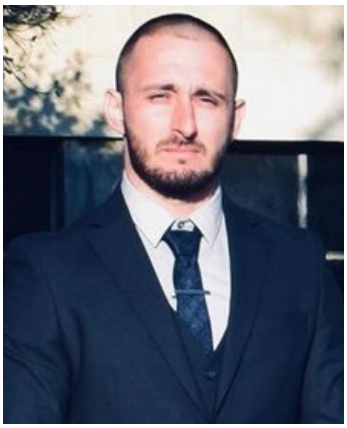
Expertise area: organised and serious crime, forensics, ballistics, illicit drugs

Gabriela Boneva	Biographical introduction
	**Gabriela Boneva** (BSc (Hons), MSc, ACSFS, IBSM, BAFS) is a research fellow at CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research), United Kingdom. Gabriela holds an MSc Forensic Ballistics degree from Cranfield University, with part of her training conducted at the Defence Academy of the United Kingdom, and a BSc (Hons) Forensic Science with Criminology degree from the University of Greenwich. Main research areas include serious and organised crime, forensics, ballistics, illicit drugs, and more. **ORCID**: https://orcid.org/0009-0004-6303-5507 **Contact**: G.Boneva@shu.ac.uk
Co-author: Luke Bates **Country**: United Kingdom	CENTRIC, Sheffield Hallam University **Expertise area**: organised crime, societal perspectives **ORCID**: https://orcid.org/0009-0005-6247-3908 **Contact**: L.Bates@shu.ac.uk
Co-author: Babak Akhgar **Country**: United Kingdom	CENTRIC, Sheffield Hallam University **Expertise area**: informatics, knowledge management **ORCID**: https://orcid.org/0000-0003-3684-6481 **Contact**: B.Akhgar@shu.ac.uk

Aleksandar Atanasov: Academy of the Ministry of Internal Affairs of the Republic of Bulgaria

Country: Bulgaria

Expertise area: criminal intelligence, special tactics, criminal psychology

Aleksandar Atanasov	Biographical introduction
	**Aleksandar Atanasov** is a doctoral candidate at the Academy of the Ministry of Internal Affairs of the Republic of Bulgaria and an intelligence officer with a tactical unit background and over 10 years of operational experience countering illegal immigration, human trafficking and terrorism. His fieldwork directly grounds his academic research. He authored Bulgaria's first field manual for detecting high-risk individuals with traits of radicalisation or terrorist group affiliation among illegal migrants and developed officially adopted counterterrorism protocols for active shooter response. A certified firearm, combat and tactical instructor, he serves as visiting lecturer at the Academy of the Ministry of Interior and as an active law enforcement officer. **ORCID**: https://orcid.org/0009-0005-4447-558X **Contact**: AlVaAtanasow@mvr.bg

Hanna-Mari Lahtinen: University of Eastern Finland

Country: Finland

Expertise area: crimes against children, forensic psychology

Hanna-Mari Lahtinen	Biographical introduction
	**Hanna-Mari Lahtinen, PhD**, is a forensic psychology expert and lecturer at the University of Eastern Finland. Her research focuses on child sexual abuse victims and offenders. She has also published several book chapters on crimes against children and collaborates with the police in child investigative interviewer training in Finland. **ORCID**: https://orcid.org/0000-0002-8275-0811 **Contact**: hanna.lahtinen@uef.fi
Co-author: Kirsi Honkalampi **Country**: Finland	University of Eastern Finland **Expertise area**: clinical psychology **ORCID**: https://orcid.org/0000-0002-4328-5291 **Contact**: kirsi.honkalampi@uef.fi
Co-author: Tegan Insoll **Country**: Finland	Protect Children ry **Expertise area**: sexual violence, child protection, law **ORCID**: https://orcid.org/0009-0006-2403-4477 **Contact**: tegan.insoll@suojellaanlapsia.fi

Hanna-Mari Lahtinen	Biographical introduction
Co-author: Juha Nurmi **Country**: Finland	Tampere University **Expertise area**: cyber intelligence, Dark Web **ORCID**: https://orcid.org/0000-0003-3071-9027 **Contact**: juha.nurmi@tuni.fi
Co-author: Anna Ovaska **Country**: Finland	Protect Children ry **Expertise area**: sexual violence, child protection, law **ORCID**: https://orcid.org/0009-0002-6288-019X **Contact**: anna.ovaska@suojellaanlapsia.fi
Co-author: Nina Vaaranen-Valkonen **Country**: Finland	Protect Children ry **Expertise area**: sexual violence, child protection, psychotherapy **ORCID**: https://orcid.org/0009-0002-8577-4373 **Contact**: nina.vaaranen-valkonen@suojellaanlapsia.fi

Victoria Koutsoupia: Legal Council of the State of Greece

Country: Greece

Expertise area: criminal economic law, money laundering, criminal procedure

Victoria Koutsoupia	Biographical introduction
	**Victoria Koutsoupia** is a judicial attorney at the Legal Council of the State of Greece and a postdoctoral researcher in criminal procedure, specialising in criminal evidence, digital proof, asset recovery, anti-money laundering and European criminal law. She holds a PhD (Juris Doctor) with distinction and an LLM in transnational and European commercial law. Her professional profile combines senior-level public sector legal practice with advanced academic research, including a published monograph, international peer-reviewed publications and regular participation in European research projects and international scientific conferences, bridging legal theory with applied institutional practice. **ORCID**: https://orcid.org/0009-0002-1559-2857 **Contact**: v.koutsoupia@nsk.gr; victoriakouts@hotmail.com

Mari-Liis Tohvelmann: Tallinn University

Country: Estonia

Expertise area: investigative interviewing, eyewitness testimony, witnesses

Mari-Liis Tohvelmann	Biographical introduction
	**Mari-Liis Tohvelmann** is a doctoral student at Tallinn University, Estonia. She works as a psychology counsellor, and her field of research is investigative interviewing and eyewitness testimony. **ORCID**: https://orcid.org/0009-0008-2764-9850 **Contact**: mari-liis.tohvelmann@tlu.ee
Co-author: Kristjan Kask **Country**: Estonia	School of Natural Sciences and Health, Tallinn University, Tallinn, Estonia **ORCID**: https://orcid.org/0000-0002-9396-6941 **Contact**: kask@tlu.ee
Co-author: Shumpei Haginoya **Country**: Japan	Faculty of Psychology, Meiji Gakuin University, Tokyo, Japan **ORCID**: https://orcid.org/0000-0001-6909-674X **Contact**: haginoya@psy.meijigakuin.ac.jp
Co-author: Pekka Santtila **Country**: China	Faculty of Arts and Sciences, New York University Shanghai, Shanghai, China **ORCID**: https://orcid.org/0000-0002-0459-1309 **Contact**: pekka.santtila@nyu.edu

Denis Solodov: University of Warmia and Mazury in Olsztyn

Country: Poland

Expertise area: criminal justice, human rights, interviewing and interrogation models, criminal defence and forensic science, digital forensics

Denis Solodov	Biographical introduction
	**Dr habil. Denis Solodov** is an associate professor at the Faculty of Law and Administration of the University of Warmia and Mazury in Olsztyn. He previously combined academic work with legal practice as a defence attorney. Author of more than 120 scientific publications in Polish, English and Russian, his research includes criminalistics, criminal defence, forensic evidence evaluation, and interviewing and interrogation models, among other topics. Habilitation was completed in 2013 at the Faculty of Law of the University of Białystok. Solodov is a member of the Polish Forensic Science Society and serves as President of its Warmian-Masurian Branch. **ORCID**: https://orcid.org/0000-0003-2884-9420 **Contact**: denis.solodov@uwm.edu.pl

Zaur Gouliev: University College Dublin

Country: Ireland

Expertise area: cybercrime networks, foreign interference, cyber threat intelligence, hybrid threats

Zaur Gouliev	Biographical introduction
	**Zaur Gouliev** is a PhD candidate at University College Dublin researching foreign information manipulation and interference. His interests span cyber intelligence, AI and disinformation, with a research focus on data and the measurement of state-sponsored influence operations. He has held roles as a machine learning engineer, open-source intelligence analyst and law enforcement agency analyst. He recently contributed a chapter to the EU-funded Athena Project book that presents the first detailed examination of foreign information manipulation and interference and examines tactics, techniques and procedures that malign actors employ to deceive populations and undermine democracy. **ORCID**: https://orcid.org/0009-0008-6588-6945 **Contact**: zaur.gouliev@ucdconnect.ie

Luna Filipović: University of California, Davis

Country: United States of America

Expertise area: forensic linguistics, forensic psychology, investigative interviewing, multilingual and multicultural criminal investigations

Luna Filipović	Biographical introduction
	**Luna Filipović** is affiliated professor in the Department of Linguistics, University of California, Davis. Her doctorate in linguistics is from the University of Cambridge, and her research in psychology and language has been funded by the Newton Trust, the Leverhulme Trust, the Leventis Foundation, the Cambridge Overseas Trust, the Economic and Social Research Council, the Arts and Humanities Research Council and the Spanish Ministry of Economy and Competitiveness. She leads the TACIT Lab (Translation and Communication in Training: www.tacit.org.uk), which integrates the latest research findings on bilingualism, witness memory, evidence elicitation and interpersonal communication into training programmes for law enforcement and fraud investigators in Europe and the United States. **ORCID**: https://orcid.org/0000-0001-9460-9797 **Contact**: lfilipovic@ucdavis.edu; lf214@cantab.net

Pasquale Danese: Italian Guardia di Finanza

Country: Italy

Expertise area: economic and financial crime

Pasquale Danese	Biographical introduction
	**Lieutenant Colonel Pasquale Danese** (Italian Guardia di Finanza) is Commander of the Public Expenditure Protection Group of the Economic and Financial Police Unit of Milan, a specialised unit combating offences related to public spending and crimes against public administration. He graduated with honours in economic and financial security sciences from the Guardia di Finanza Academy after completing secondary education at the Francesco Morosini Naval Military School in Venice. He has held operational and staff assignments across Italy, coordinating investigations into transnational money laundering, corruption and organised crime. He holds a law degree and a second-level master's degree in criminology. **Contact**: danese.pasquale@gdf.it

Murat Tinas: Turkish National Police Academy

Country: Türkiye

Expertise area: radicalisation, terrorism and intelligence studies

Murat Tinas	Biographical introduction
	**Dr Murat Tinas** is a lecturer at the Turkish National Police Academy. He holds a PhD in area studies from Middle East Technical University and conducted advanced Arabic studies in Jordan, in addition to his research affiliation at the American University of Beirut. Since 2018, he has served as an academic adviser to NATO- and EU-sponsored projects. **ORCID**: https://orcid.org/0000-0001-5844-0808 **Contact**: muratinas@gmail.com

Wendy Schreurs: Dutch Police Academy; University of Twente

Country: The Netherlands

Expertise area: data-driven policing, intelligence, social psychology, public administration

Wendy Schreurs	Biographical introduction
	**Dr Wendy Schreurs** is a senior scientific researcher at the Dutch Police Academy and a guest researcher at the University of Twente. She earned her PhD studying citizen participation in policing, and her current research focuses on intelligence-led and data-driven approaches to law enforcement. **ORCID**: https://orcid.org/0000-0001-5508-5169 **Contact**: wendy.schreurs@politieacademie.nl

Wendy Schreurs	Biographical introduction
Co-author: Jessica Cozzi **Country**: The Netherlands	Dutch Police Academy **Expertise area**: intelligence **ORCID**: https://orcid.org/0009-0003-4748-3468 **Contact**: jessica.cozzi@politieacademie.nl
Co-author: Jurjen Jansen **Country**: The Netherlands	Dutch Police Academy and NHL Stenden University of Applied Sciences **Expertise area**: online resilience in policing, human-centred cybersecurity **ORCID**: https://orcid.org/0000-0001-8607-5326 **Contact**: jurjen.jansen@politieacademie.nl

Jasmin Saarijärvi: Researcher, Ecorys

Country: The Netherlands

Expertise area: organised crime, anti-corruption, trafficking of illicit goods

Jasmin Saarijärvi	Biographical introduction
	**Jasmin Saarijärvi** is a researcher in the security and justice team at Ecorys. She has an academic background in international relations and conflict studies and in crisis and security management. Her expertise lies within organised crime and terrorism, which includes projects on illicit financial flows, corruption and firearms and drug trafficking. **Contact**: jasmin.saarijarvi@ecorys.com
Co-author: Gabriëlle op 't Hoog **Country**: The Netherlands	Ecorys **Expertise area**: organised crime, corruption, international police cooperation **Contact**: Gabrielle.optHoog@ecorys.com
Co-author: Sabine Hellemons **Country**: The Netherlands	Ecorys **Expertise area**: organised crime, corporate crime, environmental crime **Contact**: sabine.hellemons@ecorys.com
Co-author: Federica Genna **Country**: Italy	Senior associate, Fondazione SAFE, Italy **Expertise area**: corruption, organised crime, security **ORCID**: https://orcid.org/0009-0001-6127-1774 **Contact**: federica@safe-europe.eu
Co-author: Victoria Tokatzian **Country**: Italy	Junior associate, Fondazione SAFE, Italy **Expertise area**: security, corruption, environmental crime **Contact**: victoria.tokatzian@safe-europe.eu
Co-author: Halima Guelai	Please read Halima Guelai's biographical introduction in the Article 14 section below.

Jasmin Saarijärvi	Biographical introduction
Co-author: Margarita Gasparinatou **Country**: Greece	Assistant professor in criminology and crime policy, Department of Social Policy, Democritus University of Thrace, Greece **Expertise area**: criminology, crime policy, youth delinquency, corruption, financial crime and organised crime **Contact**: mgaspari@sp.duth.gr
Co-author: Eirini Stamouli **Country**: Greece	Assistant professor in critical criminology and crime policy, Department of Social Anthropology, Panteion University of Social and Political Sciences, Greece **Expertise area**: organised crime, corruption, anti-crime policy **ORCID**: https://orcid.org/0000-0002-3173-5478 **Contact**: i.stamouli@panteion.gr
Co-author: Júlia Miralles-de-Imperial **Country**: Spain	Postdoctoral researcher, Department of Political Science, Social Anthropology and Public Finance, Universidad de Murcia, Spain **Expertise area**: public integrity, public policy, public administration **ORCID**: https://orcid.org/0000-0003-1977-2310 **Contact**: julia.mirallesdeimperial@um.es
Co-author: Fernando Jiménez-Sánchez **Country**: Spain	PhD in political science / Full professor of political science, Department of Political Science, University of Murcia, Spain **Expertise area**: corruption analysis, good governance, institutional reforms **ORCID**: https://orcid.org/0000-0002-7273-4332 **Contact**: fjimesan@um.es

Halima Guelai: Scientific researcher, Ghent University – Institute for International Research on Criminal Policy, Belgium

Country: Belgium

Expertise area: corruption, radicalisation (femosphere)

Halima Guelai	Biographical introduction
	**Halima Guelai** holds a master's degree in criminology (Ghent University, 2021, summa cum laude) and a Master of Education in Social Sciences (Ghent University, 2023, magna cum laude). From 2023 to 2025, she worked on the EU-funded project POSEIDON (Ports United Against Corruption). Since May 2025, she has been an academic assistant and doctoral researcher at the Institute for International Research on Criminal Policy, within the Department of Criminology, Criminal Law and Social Law at Ghent University. **ORCID**: https://orcid.org/0009-0009-4804-4276 **Contact**: halimaguelai@outlook.be; halima.guelai@ugent.be

Kristin Weber: Centre for Criminological Research Saxony

Country: Germany

Expertise area: radicalisation, extremism, terrorism, salafism, jihadism, right-wing extremism, social network analysis, content analysis

Kristin Weber	Biographical introduction
	**Dr phil. Kristin Weber** is a criminologist and sociologist. She currently works as a postdoctoral researcher at the Centre for Criminological Research Saxony. She leads the projects 'Prejudice crime and the recording system of politically motivated crime' and 'Closing protection gaps: Improving the protection of women against violence'. Her research focuses on extremism, (online) radicalisation, terrorism, Islamism, jihadism, foreign terrorist fighters, right-wing extremism, extremist social media ecosystems and extremist/terrorist networks. She has key experiences in court file analysis, content analysis, social network analysis, manifest analysis, social media analysis and much more. Between 2015 and 2023, she was affiliated with the German Police University. **ORCID**: https://orcid.org/0009-0001-1077-8284 **Contact**: Kristin.Weber@zkfs.de

Marco Garofalo: Colonel of Polizia di Stato

Country: Italy

Expertise area: mafia-style organised crime networks

Marco Garofalo	Biographical introduction
	The **Colonel of Polizia di Stato Dr Marco Garofalo** was born in Avellino on 3 February 1971. A graduate in law, he joined the ranks of the State Police in 2000, attending the '91st training course for deputy commissioners' and later the second-level master's degree 'Inter-force coordination for security and international cooperation', and then successfully passed the 'XXXIV advanced course' at the Police Force Training School. Since April 2010, he has been serving in the Central Operations Service of the Central Anti-Crime Directorate, where he currently serves as director of Division I, which specialises in combating mafia-style organised crime. **ORCID**: https://orcid.org/0009-0007-9735-2238 **Contact**: marco.garofalo@poliziadistato.it
Co-author: Cristian Maffongelli **Country**: Italy	Head of National Unit Combating 'Ndrangheta, Division I, Polizia di Stato (SCO) **Expertise area**: mafia-style organised criminal groups **Contact**: cristian.maffongelli@poliziadistato.it
Co-author: Fabrizio Sbicca **Country**: Italy	SBICCA, Senior Manager, Italian National Anti-Corruption Authority (ANAC) **Expertise area:** economics and statistics **ORCID**: https://orcid.org/0009-0000-9372-2325 **Contact**: f.sbicca@anticorruzione.it

Marco Garofalo	Biographical introduction
Co-author: Luca Turchi **Country**: Italy	Manager, Gaming Controls Office, Gaming Directorate (ADM) **Expertise area**: illegal gaming **Contact**: luca.turchi@adm.gov.it
Co-author: Giovanni Nicolazzo **Country**: Italy	Postdoctoral researcher, Università Cattolica del Sacro Cuore and Senior Researcher, Transcrime **Expertise area**: Organized crime and illicit markets **ORCID**: https://orcid.org/0000-0002-5551-2682 **Contact**: giovanni.nicolazzo@unicatt.it
Co-author: Marco Dugato **Country**: Italy	Associate Professor, Università Cattolica del Sacro Cuore and Senior Researcher, Transcrime **Expertise area**: Organized crime and illicit markets **ORCID**: https://orcid.org/0000-0003-4611-6183 **Contact**: marco.dugato@unicatt.it
Co-author: Alessandra Porcu **Country**: Italy	Officer, Division I, SCO **Expertise area**: National unit combating illegal gambling **Contact**: alessandra.porcu@poliziadistato.it
Co-author: Francesca Basso **Country**: Italy	Researcher, Transcrime **Expertise area**: Organised crime infiltration in the legal economy **ORCID**: https://orcid.org/0009-0008-7158-1304 **Contact**: francesca.basso@unicatt.it

Ana Isabel Barros: Netherlands Police Academy; Tilburg University, Jheronimus Academy of Data Science; TNO Defence, Safety and Security

Country: The Netherlands

Expertise area: intelligence-led policing, intelligence analysis, organised crime, subversive crime, complex system analysis, artificial intelligence

Ana Isabel Barros	Biographical introduction
	**Ana Isabel Barros** is applied research professor at the Netherlands Police Academy, professor of AI and data science in organised and subversive crime at the Tilburg University, Jheronimus Academy of Data Science, and Principal scientist at TNO Defence, Safety and Security. With over 30 years of experience in defence and security, her work centres on intelligence-led policing, intelligence and operational analysis, complex systems modelling and the application of AI to counter organised and subversive crime. She advises the National Police Intelligence organisation, contributes to EU projects and serves as associate editor of the *NATO Journal of Science and Technology*. Her awards include the NATO Service Award (2024), NATO STO Honour (2020) and INFORMS Best Dissertation Award (1995). **ORCID**: https://orcid.org/0000-0003-1632-4723 **Contact**: Ana.barros@politieacademie.nl

Ana Isabel Barros	Biographical introduction
Co-author: Koen Van Der Zwet **Country**: The Netherlands	TNO Defence, Safety and Security **Expertise area**: complex systems modelling, criminal analysis, artificial intelligence **ORCID**: https://orcid.org/0000-0001-6395-7393 **Contact**: Koen.vanderzwet@tno.nl
Co-author: Eldine Verweij **Country**: The Netherlands	TNO Vector **Expertise area**: cost analysis, criminal business modelling **Contact**: Eldine.Verweij@tno.nl
Co-author: Louis Weyland **Country**: The Netherlands	TNO Defence, Safety and Security **Expertise area**: computational modelling, artificial intelligence **ORCID**: https://orcid.org/0000-0002-0085-4239 **Contact**: Louis.weyland@tno.nl

Sónia Maria Aniceto Morgado: Higher Institute of Police Sciences and Internal Security, Department of Economic Sciences

Country: Portugal

Expertise area: economics, management, technology

Sónia Maria Aniceto Morgado	Biographical introduction
	**Sónia Maria Aniceto Morgado** is an economist and associate professor at the Higher Institute of Police Sciences and Internal Security, where she directs the Department of Economic Sciences and contributes to the ICPOL–ISCPSI Research Centre. She also lectures at the Santarém Polytechnic University and Atlantic University. With a PhD in business economics and management, she has extensive experience in higher education, EU-funded security and domestic violence projects, and consultancy in health economics, internal security and public policy. She has also held roles in public sector auditing, economic advisory and hospital administration, and she has served on recruitment panels for public administration. **ORCID**: https://orcid.org/0000-0002-7036-5174 **Contact**: smmorgado@iscpsi.pt
Co-author: Sérgio Felgueiras **Country**: Portugal	**Expertise area**: police sciences, digital transition **ORCID**: https://orcid.org/0000-0001-6885-7439 **Contact**: srfelgueiras@iscpsi.pt

Jasmin Saarijärvi: Security and Justice team, Ecorys

Country: The Netherlands

Expertise area: organised crime, anti-corruption, trafficking of illicit goods

Jasmin Saarijärvi	Biographical introduction
	Please read Jasmin Saarijärvi's biographical introduction in the Article 13 section above.
Co-author: Mark Worth **Country**: Germany	Ecorys **Expertise area**: anti-corruption policy and practice, EU policy and enlargement, corruption investigations, whistleblower protection, access to information **ORCID**: https://orcid.org/0009-0008-5954-7074 **Contact**: mark.worth@ecorys.com

Ioannis Vlassis: Global Initiative Against Transnational Organized Crime

Country: Greece

Expertise area: anti-corruption, organised crime, gender and youth expertise

Ioannis Vlassis	Biographical introduction
	**Ioannis Vlassis** is an analyst and monitoring, evaluation and learning (MEL) officer at the Global Initiative Against Transnational Organized Crime. His work focuses on organised crime and corruption, with regional experience in the Western Balkans and South-East Asia. He has contributed to analytical studies on organised corruption, corruption and state–crime interactions, and to strategic foresight exercises examining the future evolution of organised crime. He currently supports the Mekong Network to Counter Transnational Crime, leading MEL processes and contributing to regional analysis. Vlassis holds an LLB from the University of Warwick and an Advanced LLM cum laude in international criminal law from Leiden University. **ORCID**: https://orcid.org/0009-0006-1551-8218 **Contact**: ioannis.vlassis@globalinitiative.net

Alp Cenk Arslan: Turkish National Police Academy

Country: Türkiye

Expertise area: intelligence studies, techno-political studies

Alp Cenk Arslan	Biographical introduction
	**Alp Cenk Arslan** is an early-career scholar (assistant professor) at the Turkish National Police Academy and a researcher working at the intersection of intelligence studies, techno-politics, AI governance and cybersecurity. His work focuses on state–industry relations under techno-politics, digital sovereignty and security policy. He contributes to international projects through research, training and publication, offering a policy-oriented, interdisciplinary perspective on how emerging technologies reshape governance and security. **ORCID**: https://orcid.org/0000-0002-5526-2089 **Contact email**: alpcenk.arslan@pa.edu.tr

Kreseda Smith: Harper Adams University

Country: United Kingdom

Expertise area: rural criminology, organised agricultural crime

Kreseda Smith	Biographical introduction
	**Dr Kreseda Smith** is a senior lecturer in rural criminology and social science at Harper Adams University (HAU). Her research includes agricultural crime, farmer mental health, impacts of rural crime and crime prevention decision-making. She is the Chair of the European Rural Criminology Working Group and Director of HAU's Rural Resilience Research Group (3RG). **ORCID**: https://orcid.org/0000-0002-3683-6550 **Contact**: kresedasmith@harper-adams.ac.uk

Maria João Guia, Editor-in-Chief: European Union Agency for Law Enforcement Training (CEPOL)

Country: Portugal, Hungary

Expertise area: strategic border management, migration, human trafficking, migration and crime, rights of victims of crimes

Maria João Guia	Biographical introduction
	**Maria João Guia** is the Research and Knowledge Management Officer at CEPOL. She holds a PhD in law and sociology ('Law, justice and citizenship in the 21st century'), and four master's degrees (in law, sociology, translation and strategic border management). She is professionalised in pedagogy and invited assistant professor of criminology at Universidade Autónoma de Lisboa. She is the author of several scientific books and articles, with the most recent book being published by Springer in 2024, co-edited with Professor Anabela Miranda Rodrigues, entitled *New Forms of Human Trafficking: Global South highlights and local contexts on sexual and labor exploitation*. **ORCID**: https://orcid.org/0000-0003-1876-8694 **Contact**: maria.guia@cepol.europa.eu; mjguiaual@gmail.com

Matteo Arru, co-editor assistant of this conference volume: European Union Agency for Law Enforcement Training (CEPOL)

Country: Italy, Hungary

Expertise area: information systems, artificial intelligence, operational excellence

Matteo Arru	Biographical introduction
	**Matteo Arru**'s research specialises in applying AI, natural language processing and business process management to improve organisational efficiency. His work, particularly in law enforcement training, focuses on enhancing security and operational capabilities through digital transformation and advanced AI tools. He has significant expertise in knowledge management systems, cybersecurity and AI-driven innovation. **ORCID**: https://orcid.org/0000-0003-2756-9582 **Contact**: matteo.arru@cepol.europa.eu; matteo@arru.it

Giacomo Florio, editor assistant: European Union Agency for Law Enforcement Training (CEPOL)

Country: Italy, Hungary

Expertise area: criminology, political science, terrorism

Giacomo Florio	Biographical introduction
	**Giacomo Florio** is a multilingual junior professional currently serving as an administrative assistant at CEPOL in Budapest. He holds a master's of law in criminology and security from the University of Lausanne and a bachelor's degree in political science from the University of Trieste, enriched by academic exchanges in Paris and Montreal. **ORCID**: https://orcid.org/0009-0003-0539-5953 **Contact**: Giacomo.florio.ext@cepol.europa.eu

André Pires da Silva, trainee/editor assistant: European Union Agency for Law Enforcement Training (CEPOL)

Country: Portugal

Expertise area: Portuguese law, European law

André Pires da Silva	Biographical introduction
	**André Pires da Silva** is currently a trainee at CEPOL. He holds a bachelor's of law (LL.B.) from the Faculty of Law of the University of Lisbon (where he also had an exchange experience at the Comenius University, Bratislava) and a master's of law (LL.M.) in European public law from the European Law School – Maastricht University. **ORCID**: https://orcid.org/0009-0004-1857-8916 **Contact**: andre.pires-da-silva@cepol.europa.eu

Aurelija Pūraitė: Mykolas Romeris University, Lithuania

Country: Lithuania

Expertise area: geopolitical security, human rights, hybrid threats

Aurelija Pūraitė	Biographical introduction
	**Dr Aurelija Pūraitė** is the Vice-Dean for Science and Project Activities at the Academy of Public Security, Mykolas Romeris University, and Head of the Sustainable Security Research Centre. A distinguished scholar, she has authored over 50 scientific articles and book chapters, and leads numerous scientific and educational projects aimed at advancing sustainable security initiatives. **ORCID**: https://orcid.org/0000-0001-9228-1396 **Contact**: aurelija.puraite@mruni.eu

Bernd Bürger: Institute for Further Education of the Bavarian Police

Country: Germany

Expertise area: leadership, public order policing, shift work

Bernd Bürger	Biographical introduction
	**Colonel Dr Bernd Bürger** has served with the Bavarian State Police since 1997 and brings extensive practical experience in both leadership and incident management. He holds a master's degree in criminology and police science from the Ruhr University Bochum (ECTS A), a master's degree in public administration – police management (ECTS A) and a PhD in public administration from the German Police University and is a certified Positive Leadership PERMA-Lead® consultant. **ORCID**: https://orcid.org/0009-0002-0386-3613 **Contact**: bernd.buerger@polizei.bayern.de

Eugenio Zaniboni: University of Foggia

Country: Italy

Expertise area: international cooperation against transnational organised crime

Eugenio Zaniboni	Biographical introduction
	**Eugenio Zaniboni** has a PhD in European public law and is a CEPOL expert trainer and an Italian Ministry of Interior expert trainer and advisor. He was appointed as Italian member of the Board of Editors of the CEPOL *European Law Enforcement Research Bulletin*. **ORCID**: https://orcid.org/0000-0001-7645-076X **Contact**: eugenio.zaniboni@unifg.it

Mihaela Pop: Bihor County Police

Country: Romania

Expertise area: international relations, European affairs, data protection

Mihaela Pop	Biographical introduction
	Since 2003, **Mihaela Pop** has been a police officer with Bihor County Police in Romania, focusing on international relations, especially after Romania's 2007 EU accession, and on increasing international police cooperation, after Romania's 2025 Schengen accession. She holds an economics degree from the University of Oradea, a specialisation in international relations from the Alexandru Ioan Cuza Police Academy, and a master's degree in freedom of movement for persons in Europe. Currently, she oversees international cooperation and acts as a data protection officer, ensuring compliance and coordinating crime prevention efforts. **Contact**: mihaela.pop@bh.politiaromana.ro

Nada Milisavljević: Unit "Innovation and Security Research" of the Directorate-General Migration and Home Affairs (DG HOME)

Country: Belgium

Expertise area: fighting crime and terrorism, including resilient infrastructure (FCT/INFRA)

Nada Milisavljević	Biographical introduction
	**Dr Ir. Nada Milisavljević** works in the 'Innovation and security research' unit of the Directorate-General for Migration and Home Affairs, where she is the EU security research coordinator and the team leader for the area of 'Fighting crime and terrorism, including resilient infrastructure'. Before joining the European Commission, Milisavljević was a researcher at the Signal and Image Processing Centre of the Royal Military Academy of Belgium, and she is (co-)author of around 100 scientific publications, mainly in the areas of image processing and data fusion. Milisavljević holds bachelor's and master's degrees in electrical engineering, and a PhD degree in applied sciences.

Paulo Machado: ICPOL – PSP Research Unit, Portugal

Country: Portugal

Expertise area: sociology, statistics applied to crime research, ecology of crime

Paulo Machado	Biographical introduction
	**Paulo Machado** has a PhD in sociology of development and social change at the Universidade Nova de Lisboa and a postgraduate qualification in social demography. He is scientific coordinator of the ICPOL – PSP Research Unit and professor of sociology and cultural studies at the Higher Institute for Police Sciences and Internal Affairs (Lisbon). He is a consultant for the Council of Europe Committee on Safety and Security at Sports Events and is a former consultant at the European Forum for Urban Security (EuroSocial programme in Latin America). He is President of the Portuguese Association of Demography. **ORCID**: https://orcid.org/0000-0003-1555-3620 **Contact**: pfsmachado@psp.pt

Roberto Fernandes: Portuguese Public Security Police; Higher Institute of Police Sciences and Internal Security

Country: Portugal

Expertise area: international relations, policing, internal security

Roberto Fernandes	Biographical introduction
	**Dr Roberto Fernandes** is a police colonel in the Portuguese Public Security Police and holds a PhD in international relations, specialising in geopolitics and geoeconomics. He serves as innovation adviser, researcher and lecturer at the Higher Institute of Police Sciences and Internal Security. Dr Fernandes is also an appointed external expert for the European Union Agency for Law Enforcement Training and the European cooperation in science and technology (COST), and a member of the Editorial Board of the *European Law Enforcement Research Bulletin*. His research interests focus on security governance, innovation in policing and the geopolitical dimensions of internal security. **ORCID**: https://orcid.org/0000-0002-3649-8694 **Contact**: rnfernandes@psp.pt

Ruža Karlović: Ministry of the Interior of the Republic of Croatia; University of Applied Science of Criminal Investigation and Public Security

Country: Croatia

Expertise area: police and society, crime, crime prevention

Ruža Karlović	Biographical introduction
	**Dr Ruža Karlović** is an assistant professor at the University of Applied Sciences for Criminal Investigation and Public Security, which is affiliated with the Ministry of the Interior. She holds a master's degree in criminal investigation and earned her doctorate in sociology from the University of Zagreb. Her research primarily focuses on crime prevention and the sociology of crime. Dr Karlović has contributed to numerous international security projects as part of the Horizon 2020 programme. Currently, she serves as the president of the Ethics Committee at her institution. In addition to her teaching and research, she has authored several scientific papers, conference summaries and books. Dr Karlović is also a member of the European Society of Criminology. **ORCID**: https://orcid.org/0000-0002-6810-0062 **Contact**: rkarlovic@fkz.hr

Alexander Resch: Bavarian State Police, European Union Agency for Law Enforcement Cooperation (Europol)

Country: Germany

Expertise area: corruption, financial crime, money laundering, sanctions

Alexander Resch	Biographical introduction
	**Alexander Resch** is a senior officer of the Bavarian State Police (Germany) and has been Head of Unit of Financial Crime at Europol's European Financial and Economic Crime Centre since September 2023. He leads a multidisciplinary team tackling money laundering, corruption, sanctions enforcement and asset tracing and recovery. He also drives strategic cooperation with financial intelligence units, asset recovery offices, customs authorities and the financial sector. Previously, he served at the International Criminal Police Organization (Interpol) General Secretariat in Lyon in the Financial Crime Unit. **Contact**: alexander.resch@europol.europa.eu

Ana Guerreiro: University of Maia (UMaia) and Faculty of Law, University of Porto (FDUP)

Country: Portugal

Expertise area: gender studies, female crime, organised and violent crime, criminal networks, sentencing studies, prevention policies

Ana Guerreiro	Biographical introduction
	**Ana Guerreiro** has a PhD in Criminology with a Foundation for Science and Technology fellowship at FDUP through the Interdisciplinary Research Centre on Crime, Justice and Security. She is an assistant professor at UMaia and an invited assistant professor at FDUP – School of Criminology. Guerreiro also collaborated with the Military Polytechnic Unit (2021/2022 academic year). She was the Director of the Research Unit in Criminology and Behavioural Sciences of the UMaia between 2022 and 2024 and is currently a full member at the Interdisciplinary Centre for Gender Studies of the Institute of Social and Political Sciences, University of Lisbon, and a collaborator researcher at the Centre for Interdisciplinary Research on Justice. **ORCID**: https://orcid.org/0000-0003-2312-6266 **Contact**: aguerreiro@umaia.pt; aguerreiro@direito.up.pt

Ana Isabel Barros: Netherlands Police Academy; Tilburg University, Jheronimus Academy of Data Science (JADS); Netherlands Organisation for Applied Scientific Research (TNO).

Country: The Netherlands

Expertise area: intelligence-led policing, intelligence analysis, organised crime, subversive crime, complex system analysis

Ana Isabel Barros	Biographical introduction
	Please read Ana Isabel Barros's biographical introduction in the Article 17 section above.

Anastasios-Nikolaos Kanellopoulos: International Association for Intelligence Education Europe; Counterterrorism Travel Pool of Experts at the UN Office of Counterterrorism; the International Propeller Club of the United States; the Hellenic Institute for Strategic Studies

Country: Greece

Expertise area: counterintelligence, counterterrorism, organised crime

Anastasios-Nikolaos Kanellopoulos	Biographical introduction
	**Dr Anastasios-Nikolaos Kanellopoulos** is a senior intelligence executive with 13+ years of experience in counterintelligence, counterterrorism and business intelligence. He combines operational law enforcement expertise with advanced academic training, holding a PhD in competitive intelligence and counterintelligence an MSc in intelligence, security, international relations and strategy; a BA in business administration and management; and a BSc in homeland security and policing. He also serves as a board member of the International Association for Intelligence Education Europe, and is a member of the Counterterrorism Travel Pool of Experts at the UN Office of Counterterrorism, the International Propeller Club of the United States and the Hellenic Institute for Strategic Studies. **ORCID**: https://orcid.org/0009-0001-1875-9264 **Contact**: ankanell@aueb.gr

André Malick: Hamburg Police

Country: Germany

Expertise area: police research, conflict research, protest research

André Malick	Biographical introduction
	**Dr André Malick** is a police director with the Hamburg Police. He is currently deputy director of the Hamburg Police Academy. Previously, he held various positions, including at the State Criminal Police Office, and taught criminal strategy and analysis at the Münster Police University. He holds master's degrees in police management, criminology, and political science, as well as a doctorate in public administration. **ORCID**: https://orcid.org/0009-0009-4604-2875 **Contact**: andre.malick@polizei.hamburg.de

Clara Cotroneo: Capgemini Invent, University of Leiden, College of Europe

Country: Italy, The Netherlands

Expertise area: EU internal security, defence innovation, critical infrastructure resilience

Clara Cotroneo	Biographical introduction
	**Clara Cotroneo** is a consultant in EU security, cybersecurity, defence policy and the protection of critical infrastructures. She has over a decade of experience supporting EU institutions, agencies and bodies, she has led high-impact evaluations. Currently working full-time at Capgemini Invent, Cotroneo manages complex EU studies and coordinates multidisciplinary research teams. She serves as service manager for the EU cybersecurity professional services framework contract, overseeing cybersecurity-related project delivery and contributing to capability development across the EU cybersecurity ecosystem. Beyond consultancy, she lectures at the University of Leiden and at the College of Europe on EU's approaches to hybrid threats, which is her academic and policy research focus. **ORCID**: https://orcid.org/0009-0003-9577-0242 **Contact**: Clara.cotroneo@capgemini.com; C.cotroneo@fgga.leidenuniv.nl

Daniel Camara: French Gendarmerie

Country: France

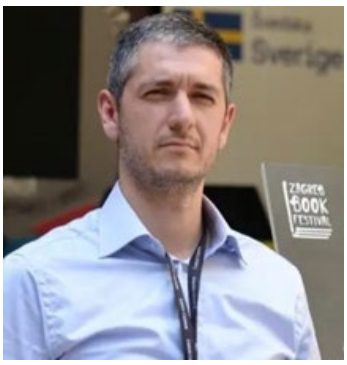
Expertise area: computer science, artificial intelligence, law enforcement data treatment, criminality forecast

Daniel Camara	Biographical introduction
	**Daniel Camara** specialises in forensic artificial intelligence within the National Unit of Judiciary Police of the French Gendarmerie. He holds an Habilitation to Direct Research as well as two PhDs, one in computer science and the other in telecommunications. His work involves developing tools and methods aimed at helping law enforcement agencies process their data, better understand crime, and improve their efficiency in the investigative process. His main research areas are related to the use of artificial intelligence methods for data processing in general, and more specifically, data related to crime. **ORCID**: https://orcid.org/0000-0001-9837-952X **Contact**: daniel.camara@gendarmerie.interieur.gouv.fr

Dean Savić: Ministry of the Interior of the Republic of Croatia

Country: Croatia

Expertise area: organised crime, terrorism, crime investigation

Dean Savić	Biographical introduction
	**Dean Savić** has been an employee of the Ministry of the Interior of the Republic of Croatia since 1991. He received his PhD degree at the Faculty of Political Sciences in Zagreb. He is the author of several scientific and professional papers. He has completed several courses in the field of criminal investigations at the University of Applied Sciences in criminal investigation and public security in Zagreb. **Contact**: dsavic@mup.hr

Eugenio Zaniboni: University of Foggia

Country: Italy

Expertise area: international cooperation against transnational organised crime

Eugenio Zaniboni	Biographical introduction
	Please read Eugenio Zaniboni's biographical introduction in Editor's section above.

Filippo Vanni: Carabinieri

Country: Italy

Expertise area: human resources management

Filippo Vanni	Biographical introduction
	**Filippo Vanni** is a senior law enforcement executive with 25+ years of command experience and a proven record in international security cooperation, operational leadership and EU-level strategic policy work. Former Justice and Home Affairs Expert at the Permanent Representation of Italy to the EU and Member of the eu-LISA Management Board, with direct involvement in the governance of EU large-scale IT systems. Vanni has expertise in cross-border information exchange, data governance, criminal intelligence analysis and the operationalisation of EU security policies. **ORCID**: https://orcid.org/0009-0007-6198-6132 **Contact**: filippo.vanni@carabinieri.it

Gábor Kemény: European Union Agency for Law Enforcement Training (CEPOL)

Country: Hungary

Expertise area: information exchange, cross-border cooperation, law enforcement organisational environment

Gábor Kemény	Biographical introduction
	**Gábor Kemény** is an experienced senior police officer and education professional with a demonstrated history of working for law enforcement authorities at the national and international levels. He is skilled in law enforcement, cross-border cooperation, leadership, capacity building, training and project management. He has a strong education background, with various postgraduate qualifications in the fields of the special jurisprudence of the law of the EU and strategic border management. **ORCID**: https://orcid.org/0000-0003-0062-2160 **Contact**: Gabor.kemeny@cepol.europa.eu

Gianluigi Me: Italian Ministry of Defence, European Union Agency for Law Enforcement Training (CEPOL) expert and trainer; Tor Vergata, Libera Università degli Studi Maria Ss. Assunta di Roma (LUMSA) and Libera Università Internazionale degli Studi Sociali Guido Carli (LUISS)

Country: Italy

Expertise area: open-source intelligence (OSINT), crime data science, cybercrime, security economics, digital forensics

Gianluigi Me	Biographical introduction
	**Gianluigi Me** is a computer engineer with a PhD in business management engineering and OF5 officer in the Carabinieri, currently serving as IT Program Director at the Italian Ministry of Defence, after leading national digital investigations, ICT security and IT operations at Carabinieri headquarters. He has extensive academic experience as adjunct professor at Tor Vergata, LUMSA and, since 2011, at LUISS. He also serves CEPOL and other international organisations as an expert and trainer in advanced cybersecurity master courses. His expertise spans OSINT, crime data science, cybercrime, security economics and digital forensics, supported by patents, co-editing the *Handbook of Electronic Security and Digital Forensics*, and the book *OSINT in the Intelligence Era*. **ORCID**: https://orcid.org/0000-0002-8805-2547 **Contact**: gme@luiss.it

Heiko M. Edlinger

Country: Germany

Expertise area: security governance and cyber strategy

Heiko M. Edlinger	Biographical introduction
	Expert in security governance and cyber strategy, strategic advisory at the intersection of cybersecurity, national resilience, and proactive crisis management, data protection in security contexts, analysing the tension between data protection (privacy) and security interests (security), ensuring the identification of criminal networks within hybrid scenarios remains operationally effective and legally sound. **ORCID**: https://orcid.org/0009-0004-6343-636X **Contact**: heiko.edlinger@polizei.bayern.de

Henrique Britto de Mello: University of Pernambuco

Country: Brazil

Expertise area: criminalistics, crime scene interpretation, criminology

Henrique Britto de Mello	Biographical introduction
	**Henrique Britto de Mello** is a PhD candidate in forensic sciences at the University of Pernambuco. He holds a master's degree in forensic sciences, with research focused on investigative reasoning, homicide investigations and violent crime. Britto de Mello has professional experience as a forensic consultant in homicide cases and in training police officers in investigative interviewing methodologies. He has served as a field researcher in the 'crime in Latin America' project, an international research collaboration between the University of Oslo and the Universidad Nacional Autónoma de México. **ORCID**: https://orcid.org/0000-0001-8330-4867 **Contact**: henriquebrittodemelo@gmail.com

Inês Simões Farinha: Inspector at the General Inspection of Home Affairs and Assistant Professor at Autónoma University in Lisbon

Country: Portugal

Expertise area: penal law, procedural penal law, prison

Inês Simões Farinha	Biographical introduction
	Currently I'm an inspector at the General Inspection of Home Affairs and also an assistant professor at Autónoma University in Lisbon (Penal Law and Procedural Penal Law). I'm a PhD candidate in the field of penal law. I've also been a jurist working on matters of racial discrimination at the Portuguese public entity that focuses directly on racial discrimination. In my current role, my work focuses on matters of auditing, inspection, control and oversight of police forces. Also, as my master's degree and PhD thesis are also focused on prison matters, I also hold experience in this field of academic research. **ORCID**: https://orcid.org/0000-0002-4117-5216 **Contact**: inesimoesf@gmail.com

Irina Slabu: Seconded National Expert, CEPOL

Country: Romania

Expertise area: cybercrime, human resources, training, gender policies

Irina Slabu	Biographical introduction
	**Chief-Commissioner Irina Slabu** has over 20 years of professional experience within the Romanian Ministry of Home Affairs, where she has held several key positions, including human resources officer, training officer, gender adviser and Head of Selection for the International Missions, Schengen and CEPOL Unit. She is currently serving as a Seconded National Expert at CEPOL, contributing to European law enforcement training and cooperation initiatives. **Contact**: irina.slabu@cepol.europa.eu

Ivana Glavina Jelaš: University professor and external associate at the Department of Psychology; Deescalate

Country: Croatia

Expertise area: crisis communication, mental health

Ivana Glavina Jelaš	Biographical introduction
	**Associate Professor Ivana Glavina Jelaš, PhD**, was a police psychologist for 18 years. From 2008 to 2026, she taught at the University of Applied Sciences in Criminal Investigation and Public Security, where she also founded and led the Psychological Counseling Center. Between 2022 and 2026, she served as the psychologist for Croatian police negotiators. She has conducted extensive research, and published numerous scientific and professional publications in these fields. Since 2019, she has worked as a university professor and an external associate at the Department of Psychology. In 2026, she founded Deescalate, a business for science, research, and counselling. **ORCID**: https://orcid.org/0009-0001-6518-9444 **Contact**: info@deescalate.hr

Joachim Faßbender: German Police University (DHPol)

Country: Germany

Expertise area: politically motivated crime, police state security, organised crime, money laundering, hybrid threats

Joachim Faßbender	Biographical introduction
	**Criminal Director Joachim Faßbender** holds a degree in public administration and has been teaching at the German Police University (DHPol) since 2018 in the master's programmes 'Public administration – police management' and 'Public governance and democratic resilience'. Since 2021, he has headed the department of 'Criminalistics – Phenomenon-based criminal strategy'. His work there focuses on politically motivated crime and organised crime. Previously, he worked in various positions at the Federal Criminal Police Office. At the DHPol, he was involved in the joint project 'Organised crime 3.0' as a sub-project manager, among other things. **ORCID**: https://orcid.org/0009-0009-8888-2952 **Contact**: joachim.fassbender@dhpol.de

Jozef Medelský: Academy of the Police Force in Bratislava, Slovakia

Country: Slovakia

Expertise area: criminal law, international security

Jozef Medelský	Biographical introduction
	**Jozef Medelský** is associate professor at the Academy of the Police Force in Bratislava, Slovakia. He currently serves as Vice-Rector for Education and lectures in criminal law, international security, international public law and international police cooperation. He is the author of numerous publications in the fields of criminal law, international security and international police cooperation. At the same time, he serves as a CEPOL research and science correspondent. **ORCID**: https://orcid.org/0000-0003-3062-4167 **Contact**: jozef.medelsky@akademiapz.sk

Kari Laitinen: Adjunct Professor of University of Tampere & National Defence School

Country: Finland

Expertise area: international relations, security studies, situation awareness function and strategic foresight, terrorism and national security

Kari Laitinen	Biographical introduction
	Kari Laitinen (Dr. Soc. Sc., adjunct professor of University of Tampere & National Defence School) works currently as senior advisor at the Finnish security and intelligence service. Between 1995 and 2005, Laitinen held various positions at the Universities of Tampere and Helsinki. Since then, he has worked in the Prime Minister's Office, in the National Police Board and in the Ministry of Defence. His areas of expertise are international relations, security studies, situation awareness function and strategic foresight, terrorism and national security. He has worked extensively in various working groups and committees in the governmental level. **Contact**: kari.laitinen@supo.fi

Khalil Hariss: École Supérieure d'Ingénieurs de Beyrouth (ESIB), Université Saint-Joseph de Beyrouth (USJ), Lebanon

Country: Lebanon

Expertise area: applied cryptography, cybersecurity, homomorphic encryption

Khalil Hariss	Biographical introduction
	**Dr Khalil Hariss** is an assistant professor in the Department of Computer and Communication Engineering at the École Supérieure d'Ingénieurs de Beyrouth (ESIB), Université Saint-Joseph de Beyrouth (USJ), Lebanon. His research focuses on applied cryptography, homomorphic encryption and authentication, and post-quantum cryptography. **ORCID**: https://orcid.org/0009-0006-7408-7032

Linhares dos Reis: Judiciary Police

Country: Portugal

Expertise area: criminal investigation, organisational and personal leadership, forensic psychology

Linhares dos Reis	Biographical introduction
	**Linhares dos Reis** has served as a police officer since 1994. From 1998 to the present day, he has been part of the Judiciary Police in the category of inspector, criminal investigation career, specialising in the areas of falsification or counterfeiting of documents, determination and investigation of the causes of fires and crimes against persons, such as homicide, crimes against freedom and sexual self-determination, and robbery. As for his academic qualifications, dos Reis holds a degree in security studies from Lusófona University and a master's degree in leadership, people and organisations from the Military Academy. He also has a postgraduate degree in forensic psychology from Faculty of Law of the University of Lisbon / Institute for Interdisciplinary Legal Research. **ORCID**: https://orcid.org/0000-0003-2843-9114 **Contact**: +351 211967284

Maria Brás: University of Algarve; ICPOL Research Centre

Country: Portugal

Expertise area: psychology, risk perception and safety, health psychology, clinical psychology, anthropology, management and economics, human resources

Maria Brás	Biographical introduction
	**Maria Brás** holds a PhD in psychology, with her doctoral research focused on risk perception and safety. She also earned a master's degree in health psychology and undergraduate degrees in clinical psychology and anthropology. She is currently pursuing a PhD in management and economics. Brás is a faculty member at the University of Algarve, where she teaches in several programmes and serves as director of the master's degree in human resources management. Her research and academic supervision focus primarily on psychology and human resources, safety and related fields. She is a researcher at the ICPOL Research Centre. **ORCID**: https://orcid.org/0000-0002-1817-7694 **Contact**: mfbras@ualg.pt

Marzena Kordaczuk-Wąs: European Union Agency for Law Enforcement Training (CEPOL)

Country: Poland

Expertise area: Prevention of radicalisation, community policing and crime prevention, evidence-based evaluation, policy and practice, designing of preventive measures

Marzena Kordaczuk-Wąs	Biographical introduction
	**Marzena Kordaczuk-Wąs**, PhD in social sciences, specialises in crime prevention and the sociology of security. She served for 18 years in the Polish police, focusing on social prevention. Currently, she is a senior training officer at the European Union Agency for Law Enforcement Training, coordinating the law enforcement cooperation portfolio. Kordaczuk-Wąs is also an expert in radicalisation prevention and collaborates with the Polish Platform for Homeland Security and Collegium Civitas. She has worked with the Radicalisation Awareness Network as co-chair of the Police and Law Enforcement Working Group under the European Union's Radicalisation Awareness Network (RAN). **ORCID**: https://orcid.org/0000-0001-5479-7455 **Contact**: marzena.kordaczuk-was@cepol.europa.eu

Michal Cikhart: Department of Investigation, Academy of the Police Force in Bratislava

Country: Slovakia

Expertise area: environmental crime; chemical, biological, radiological and nuclear (CBRN) threats; law enforcement

Michal Cikhart	Biographical introduction
	**Michal Cikhart** is an assistant professor at the Department of Investigation, Academy of the Police Force in Bratislava, Slovakia, with over 24 years of experience in law enforcement. His expertise spans environmental crime and CBRN threats, where he has established himself as a leading authority. As a former investigator, he played a crucial role in combating these issues, significantly contributing to efforts against both environmental and hazardous materials-related crimes. **ORCID**: https://orcid.org/0009-0000-3870-364X **Contact**: michal.cikhart@akademiapz.sk

Noemi Alexa: European Union Agency for Law Enforcement Training (CEPOL)

Country: Hungary

Expertise area: training needs analysis, integrity, corruption

	Biographical introduction
	**Noemi Alexa** is an economist and holds a Ph.D. in Multidisciplinary Social Sciences. She has broad experience in conducting applied research. She is responsible for the coordination of training needs analyses at CEPOL. Prior to joining CEPOL she worked in academia teaching integrity in business and leadership at the Business School of Central European University. Before that, she worked as the Executive Director of Transparency International Hungary. **ORCID**: https://orcid.org/0009-0008-8814-9307 **Contact**: noemi.alexa@cepol.europa.eu

Pasquale Danese: Italian Guardia di Finanza

Country: Italy

Expertise area: economic and financial crime

Pasquale Danese	Biographical introduction
	Please read Pasquale Danese's biographical introduction in the Article 10 section above.

Rashid Minhas: University of West London, School of Human and Social Sciences

Country: United Kingdom

Expertise area: investigative interviewing; cognitive and implicit bias in decision-making; ethical, evidence-based interrogation practices within criminal justice and organisational contexts

Rashid Minhas	Biographical introduction
	**Dr Rashid Minhas** is an associate professor of criminology and psychology at the University of West London. His research examines investigative interviewing, prejudicial stereotyping and bias mitigation in criminal justice contexts. He has led and contributed to nationally and internationally funded projects and works closely with policing organisations, policymakers and industry partners. His current research explores the ethical application of artificial intelligence to support information gathering, fairness and decision-making in investigative and interviewing practices. **ORCID**: https://orcid.org/0000-0002-1479-0985 **Contact**: Rashid.minhas@uwl.ac.uk

Rui Sousa-Silva: Faculty of Arts and Humanities of the University of Porto

Country: Portugal

Expertise area: forensic linguistics

Rui Sousa-Silva	Biographical introduction
	**Rui Sousa-Silva** holds a PhD in applied linguistics / forensic linguistics from Aston University. He is currently an assistant professor and researcher at the Faculty of Arts and Humanities of the University of Porto, where he is also coordinator of the specialisation course in forensic linguistics. He has published widely on these topics. He is co-editor of the international bilingual journal *Language and Law / Linguagem e Direito* and of the 2nd edition of *The Routledge Handbook of Forensic Linguistics*. He is the principal investigator of the project NORTE IA+, 'Transparent and secure artificial intelligence for a more human and competitive future'. **ORCID**: https://orcid.org/0000-0002-5249-0617 **Contact**: rssilva@letras.up.pt

Silvia Smadova: European Union Agency for Law Enforcement Training (CEPOL)

Country: Slovakia

Expertise area: capacity building in area of combating child sexual abuse / child sexual exploitation

Silvia Smadova	Biographical introduction
	Silvia Smadova graduated from the Faculty of Political Science and International Relations (FPV MV) at Matej Bel University in Slovakia, where she also earned a master's degree in political science. After spending several years in the private sector in Ireland, Silvia joined Europol's European Cybercrime Centre (EC3), contributing to strategic and development initiatives supporting EU-level operational and capacity-building priorities. She subsequently joined CEPOL as the Cybercrime Portfolio Manager. In this role, she is responsible for developing and coordinating the EU-wide law enforcement training portfolio in the area of combating child sexual exploitation (CSE).

Silvia Tabusca: Romanian-American University; Director of the Centre for Human Rights and Migration

Country: Romania

Expertise area: law

Silvia Tabusca	Biographical introduction
	**Silvia Tabusca** is a law lecturer at the Romanian-American University and Director of the Centre for Human Rights and Migration, with over 20 years of experience as a human rights lawyer, international consultant and trainer. She has served as personal advisor to the Romanian Minister of Justice, and collaborates extensively with UN agencies, Organization for Security and Cooperation in Europe, Interpol, the Council of Europe and EU institutions. She is a member of Council of Europe's Network of Anti-Trafficking Lawyers, the Global Initiative Against Transnational Organized Crime and Interpol's Human Trafficking Expert Group. Tabusca is also an external evaluator for the European Commission and national research agencies, and she holds a PhD and a post-doctorate in law. **ORCID**: https://orcid.org/0000-0002-07630959 **Contact**: silvia.tabusca@rau.ro

Sónia Maria Aniceto Morgado: Higher Institute of Police Sciences and Internal Security, Department of Economic Sciences

Country: Portugal

Expertise area: economics, management, technology

Sónia Maria Aniceto Morgado	Biographical introduction
	Please read Sónia Maria Aniceto Morgado's biographical introduction in the Article 18 section above.

Vesa Muttilainen: Police University College of Finland (Polamk)

Country: Finland

Expertise area: research in the field of policing and security, research projects, publishing and leadership

Vesa Muttilainen	Biographical introduction
	**Dr Vesa Muttilainen** holds a PhD in social sciences and is a senior researcher at the Police University College of Finland (Polamk). He has several decades of experience in research and has worked as a director of research for about 12 years. His research interests cover themes such as corruption, organised crime and financial crime. Dr Muttilainen has been involved in numerous projects funded by the European Union (Horizon Europe, Internal Security Fund, Twinning) and by national and Nordic organisations. He has edited several extensive collections of articles on the police's operating environment. He is the former editor-in-chief of the *Nordic Journal of Studies in Policing*. **Contact**: vesa.muttilainen@polamk.fi

Zágon Csaba: Law Enforcement Faculty at Ludovika University

Country: Hungary

Expertise area: law enforcement risk management and international police cooperation

Zágon Csaba	Biographical introduction
	**Zágon Csaba, PhD**, is committed to strengthening the academic performance and international visibility of the Law Enforcement Faculty at Ludovika University. He contributes to European Commission higher-education programmes and was a member of CEPOL's Research and Science Correspondents' Network between 2024 and 2025. A former customs officer with over 30 years of experience, he has led risk management and border security capacity-building initiatives across EU and accession states. He has taught for more than a decade in BA, MA and PhD programmes. His research focuses on law enforcement risk management, crime analysis, international criminal cooperation and infrastructure networks. **ORCID**: https://orcid.org/0000-0001-6615-8466 **Contact**: csaba.zagon@uni-nke.hu

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls);
— at the following standard number: +32 22999696;
— via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

CEPOL
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

European Union Agency for Law Enforcement Training

Office address: European Union Agency for Law Enforcement Training, 1101 Budapest, Üllői út 114-116, Hungary

Correspondence: H-1903 Budapest, Pf. 314, Hungary

Telephone: +36 1 803 8030 • Email: info@cepol.europa.eu

www.cepol.europa.eu

Publications Office of the European Union

Law | Data | Publications