Special Conference Edition Nr. 4

EUROPEAN LAW ENFORCEMENT RESEARCH BULLETIN

Innovations in Law Enforcement –

Implications for practice, education and civil society

Editors:
Detlef Nogala
Thomas Görgen
Justyna Jurczak
Bence Mészáros
Peter Neyroud
Lucia G. País
Barbora Vegrichtová

EUROPEAN LAW ENFORCEMENT RESEARCH BULLETIN

Special Conference Edition Nr. 4

Also published online:
Current issues and the archive of previous Bulletins are available from the journal's homepage https://bulletin.cepol.europa.eu.
(Continues from the previous title European Police Research and Science Bulletin)

Published by:
European Union Agency for Law Enforcement Training (CEPOL) (Acting Executive Director: Dr. h.c Detlef Schröder)

Readers are invited to send any comments to the journal's editorial mailbox:
research.bulletin@cepol.europa.eu

For guidance on how to publish in the European Police Science and Research Bulletin:
https://bulletin.cepol.europa.eu/index.php/bulletin/information/authors

Luxembourg: Publications Office of the European Union, 2019

Print	ISSN 2599-5855	QR-AG-18-002-EN-C
PDF	ISSN 2599-5863	QR-AG-18-002-EN-N

Publications Office

SPECIAL CONFERENCE
EDITION Nr. 4

Innovations in Law Enforcement – Implications for practice, education and civil society

2017 CEPOL European Police Science and Research Conference
Budapest, Hungary 28-30 November 2017

Editors:
Detlef Nogala
Thomas Görgen
Justyna Jurczak
Bence Mészáros
Peter Neyroud
Lucia G. País
Barbora Vegrichtová

Content

H2020 Research Projects

Learning Innovation(s)

Applied Innovation

Editorial Introduction

Innovations in Law Enforcement – Introduction to the Special Conference Edition

Detlef Nogala
Detlef Schröder
European Agency for Law Enforcement Training, Budapest

Being no exception to any other walk of modern life, institutions established to enforce the law (the police, customs, judiciary and others), often find themselves subject to calls for more efficiency, efficacy and better performance, in particular, when misgivings about their capability for keeping public order or ensuring citizens' safety are entering the public and political agenda. Looking at Europe alone and focusing on the period after the collapse of the Sowjet empire, police organisations in many countries have witnessed several waves of reform – some fundamental, some fractional. For an observer it would look like that over the last three decades, at any moment, some kind of profound police reorganization is happening in at least one European country[1] - police reform as a permanent practice. When "police reform" can be understood as dealing with the rearrangement of organizational (or institutional) structures and often implies turning bigger political wheels, "innovation" in law enforcement comes across as the "little brother": more piecemeal, subtle, less orchestrated or steered politically, but by no means less fraught with consequences for law enforcement institutions, the officers on the ground, or for the citizens they are serving.

Within law enforcement, it is most likely the police owning the most vivid history of innovations – when considering the developments and novelties in terms of strategy, tactics and equipment since the modest beginnings of modern formats of policing in the mid 19th century and onwards. However, in the academic and professional literature, the combination of the terms police/policing and "innovation" has caught attention comparatively sparsely, and only in the last two decades, most likely driven by the rise of new managerial mindsets and even more impactful, by technological progress, this has changed.

With this conceptual background in mind, the conference organisers[2] had put forward "Innovations in Law Enforcement" as the leitmotif for the 14th edition of the CEPOL Research and Science Conference. As is the tradition of this convention, practitioners in policing and other areas of law enforcement, trainers, educators and scientific scholars from Europe and beyond[3], where invited to discuss and reflect on the implications for practice, education and civil society, innovations in law enforcement might yield in general terms as well as specifically: How would novel ideas, technologies,

1 For a recent comparative examination of developments in Europe see Fyfe et al. (2013), Mesko et al. (2013), Caparini & Marenin (2004).

2 The 2017 CEPOL Research and Science Conference was jointly organised by the European Union Agency for Law Enforcement Training and the Hungarian National University of Public Service, hosted at the university' premises in Budapest.

3 Over 200 participants, mainly from Europe, but also from Canada, Hong Kong, Thailand, Ukraine and the United States, attended more than 80 presentations, including poster sessions and practical demonstrations of advanced training hard- and software.

concepts – as reaction to new forms of crime and deviance - form and shape law enforcement institutions, like police, customs, border guards, prosecution and courts, and their demands for training and education today and in the future?

In the open Call for Papers, contributors were invited to submit papers and presentations, preferably based on recent empirical research or academic study, addressing the following areas and aspects:

1. Which are the emerging innovations in society that are prompting a response from the law enforcement community, both in terms of adapting strategies and tactics, as well as the law enforcement educational requirements?
2. What are the expectable implications, benefits, risks or potential ramifications of introducing certain new technologies (gadgets or systems), organisational or operational concepts for doing law enforcement work in a new, innovative manner? Is it different for innovations that are driven or imposed by the outside environment as opposed to those that are emerging from "inside"? Where and when have law enforcement innovations failed and what lessons have been learned so far?
3. Which educational innovations will have significant impact on the training and education of law enforcement officials on the various levels of the organisations – and why?
4. Some innovations in law enforcement are received with great sympathy and endorsement, some with lesser enthusiasm by members of the civil society. What has to be considered in the management of the innovation process so a particular innovation is not perceived as ineffective, undue, unfair or even illegal? Are there innovative ways to manage potential disputes between "innovators" and "preservers"?

In order to cover all the relevant aspects and angles, the presenters where encouraged to examine particular innovations by taking the perspective of police or law enforcement officers, teachers, trainers, educators in the law enforcement education systems as well as those of the citizens, who will be subject to and beneficiaries of innovative law enforcement practices.

Innovation: notion and meaning of

„There are words and concepts – many words and concepts – that we use with no knowledge of their past. Such concepts are taken for granted and their meaning is rarely questioned. Innovation is such an anonymous concept", (Godin 2015: 5).

All discussions about "innovation(s)" need to be aware from the start about the semantical risk the term carries inherently, almost becoming a potential "false friend"[4] when used without caution or further specification in the dialogue between different professions and professional cultures. "Innovation" can signify a variety of entities and processes, and all depends if the term is used in a *descriptive*, *ascriptive* or even *prescriptive* manner:

Its original Latin root – "innovare" – literally means "to remake" or to "renew something" – and is purely descriptive, without implying any positive or negative connotation or statement about the outcome of this action. In this sense "to innovate" or "innovation" delineates little more than that something has changed or has been transformed. However, over the course of time, and specifically in contemporary public discourse, "innovation" is frequently used in an ascriptive way, that is becoming "loaded" with (predominantly positive) value and meaning: it implies that how something is changed is progressive and desirable.

Outside critical academic discourse, "innovation" can come across in its prescriptive guise, when it conveys a message or demand that something has to change in a certain way and towards a certain outcome.

All this is to say, that "innovation" is not a simple and neutral notion – it has changed its meaning over time and professional boundaries – and thus deserves reflection and qualification, in respect to context and intention. For example, to "invent" – to design or create something, that has not existed before - is not exactly the same as to innovate (although often mixed up); or, to do something different, even in a new way, does not necessarily and automatically imply that this way is the better one, or that the outcome is superior. But this is exactly the association most often evoked in unguarded casual talk: new is (always) better! Maybe it is not, or only under specific circumstances and in reference to specific objectives.

4 See Wikipedia entry "False friend".

In the modern classics of business and management sciences, the introduction of "innovation" as a theoretical notion and concept is often attributed to the Austrian economist and later Harvard-Professor Joseph Alois Schumpeter:

"*By innovations I understand (...) changes of the combinations of the factors of production. (...) They consist primarily in changes in methods of production and transportation, or in changes in industrial organization, or in the production of a new article, or in the opening up of new markets or of new sources of material*" (Schumpeter 1927 - cited in Disch 2016).

Schumpeter's approach has been quite influential in forming and shaping the notion of innovation among economists and the managerial classes. Still relevant for the proper grasp of innovation in our contemporary discussion is his emphasis that innovation is a rather complex social complex and its success full of preconditions. There is a burgeoning specialized literature about innovation in the business and social sciences[5], for which is no room to elaborate on in this introductory chapter. It should suffice to underline that "innovation" is a complex (social) concept, which deserves to be studied in detail and to being made use of in context and with proper caution.

Innovation as a topic for law enforcement

The history of law enforcement in modern times[6] – that is from the mid 19th century onwards – could easily be written as an ongoing progression of innovations: either in organizational, technological or tactical terms – finding new organizational forms, adapting to and adopting new technologies and gadgets (in line with the major developments of modern civilization), differentiating, diversifying and finetuning its working methods:

- From the early metropolitan police offices to national and globally interlinked institutional networks;
- From telegraph to telephone to radio (Brown 2011) to social media as means for internal and external communication
- From the proverbial "Bobby-on-the-beat" to centrally dispatched fleets of patrol cars to Internet-squads;
- From an almost exclusive male workforce to mirroring the diversities of modern society;
- From military-style units to "Community" and "Intelligence-Led" Policing (Carter 2013);
- From Bertillonage to fingerprints, DNA and other biometric identification methods
- From Sherlock Holmes' notebook and his power of combination to ubiquitous databases covering almost every aspect of (social) life to Compstat (Moore 2003) towards Artificial Intelligence-based applications (Interpol & UNICRI 2019).

This is of course only a incomplete selection of relevant developments - the full history of innovations in law enforcement is of course a long, uneven and multifaceted one, with im- and exports of new ideas, concepts, technologies and practices happening all over, shaping and forming the various police forces in specific

5 For a discussion of Schumpeter's original approach, see for example Borbély (2008) and a study of his concept's reception in academic and business literature since its inception by Lazzarotti et al. (2011). Influential in managerial circles has been the now classical article by Peter F. Drucker (2002). Only recently innovation has become subject to a critical challenge by historians and social scientists, stressing the century long evolution of the term and morphing of its social public connotation to something diametrical meaning: "The "spirit" of innovation, what we would call today the culture of innovation, acquired new meaning and changed to become essentially positive in the last century and a half (…). A totally new representation of innovation developed, far different from the previous centuries. Innovation is no longer seen as subversive to the social order, but simply as opposed to traditional ways of doing things. The innovator is not a heretic. He is simply different from the masses or from his fellows. He may be a deviant, but in a sociological sense: an original, a marginal, a nonconformist, an unorthodox. He is also ingenious and creative. He is an experimenter, an entrepreneur, a leader; he is the agent of change" (Godin 2018: 5). For a thorough and detailed historical review see Godin & Vinck (2017) and, with a linguistic focus, Weber (2018).

6 Such an assertion is grounded on two premises: read "law enforcement" as (state-organised) policing/police and look at the process from an overarching international perspective. There are strong scholarly arguments to analyze and understand police forces and their development as country-specific entities, as the modern notion of police is inextricably jointed to the rise of the modern nation state. Such a claim can be uphold even against the early emergence of cross-border police cooperation networks like Interpol, or later Europol (see e.g Deflem 2002).

ways and resulting in the kind of institutions, we are familiar with today.[7]

More often than not, police organisations have been under pressure to cope with increasing workloads and heightened expectations, as societies have become more complex and opportunities to commit offenses multiplied – modernisation becoming a constant imperative (Senior et al. 2007). Deploying scarce resources efficiently and effectively – this has always been a major occupation for police leadership and intensified in the 1990's along the rise of the notion of "New Public Management" - at least in Western countries (see Kennedy 1993; Cope et al. 1997; McLaughlin et al. 2002).

Police managers, urged to find new solutions to old and familiar policing problems, directed their attention inadvertently to attainable innovations – which also sparked a rise of interest in the study of police innovation since the turn of the millennium. When King (2000) made a study of various innovations in American policing, differentiating and looking at radical management (COP, POP), radical technical (e.g. AFIS, DNA, mobile phones), line technical (e.g. pepper spray, unmarked cars), administrative (e.g. hiring women, decentralisation) and programmatic (e.g asset forfeiture, crime analysis and others), his main conclusion was that *"(…) it is apparent that police organizational innovation is certainly not a unidimensional construct. Future studies of police innovation should address this finding by exploring their measures of innovation for multi-dimensionality concluded*" (King 2000: 314).

While King can be taken as supportive of the position that innovation is a genuine social process, subsequent studies stressed out that *"(…) improving police performance through innovation is often not straightforward. Police departments are highly resistant to change and police officers often experience difficulty in implementing new programs (…)*" (Weisburd & Braga 2006: 339) and content that *"…it is misleading to speak of innovations as though they are all identical. In the three case studies, we saw that each innovation took its own trajectory and involved various ingredients for its success*" (Allen & Karanasios 2011: 96). Underlining what has stated before – that the term innovation shall be implemented with care and caution in particular in the context of policing and other law enforcement, Willis & Mastrofski find: *"(…) that one of the major challenges confronting police scholars is conceptualization. Not only must the term innovation be defined clearly and appropriately according to the context in which it is being used, but the multifaceted nature of many innovations requires that they be defined according to their relevant dimensions or attributes. Failure to do so hinders meaningful cross-study comparisons and the development of the field as a whole. Moreover, researchers should query rather than accept the popular view that innovations are socially desirable and superior to current practices. Doing so will contribute to more comprehensive and considered assessments of the identification, diffusion, adoption, and implementation of innovations"* (2011: 43f). An interesting implementation of this recommendation is delivered by Okabe (2014), who, when comparing police innovation patterns in Japan and the United States, discovered significant differences between those countries. It is more likely than not, that any comparison between national systems will discover peculiarities and genuine patterns of which organisational or technical innovations have been taken up and successfully implemented full, to a certain degree or not at all[8].

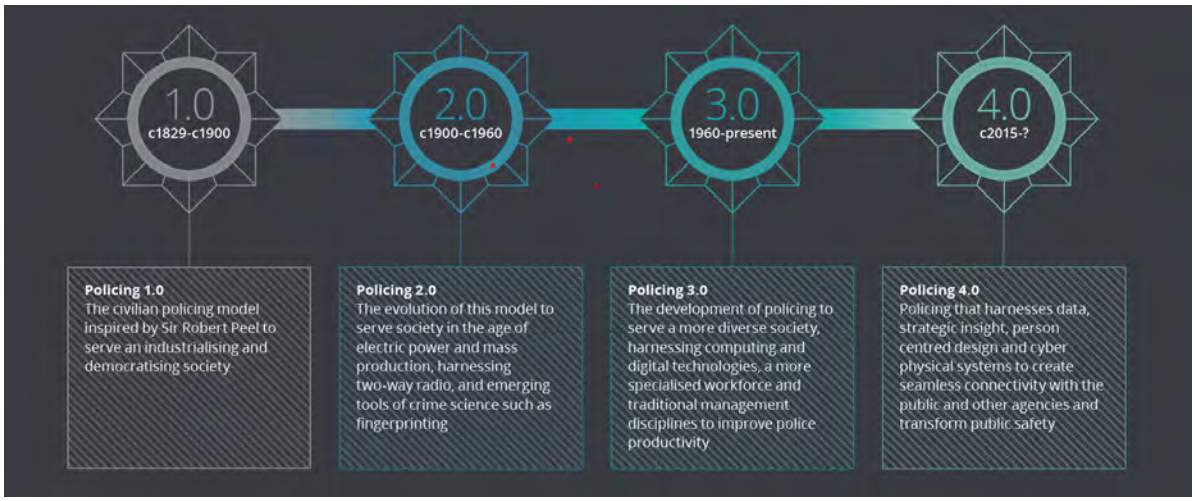
Innovations in law enforcement have a sell-by day – that is, their novelty can fade fast and yesterday's sensational new tool or organisational strategic change, is adopted and turned into today's normal way of doing things: the innovation no longer an innovation.[9]

It seems that it is rather the cumulative effect of various, mostly independent and asynchronous innovate initiatives taken in a range of dispersed offices, departments and leadership chairs, which have created a dynamic of change, that had, is about and will change the structure and appearance of the institutions law enforcement (in particular the police). While those innovations can take time to appear before the public eye, when seen under a historical perspective, the occasional short-time disruptive effect, morphs into a more evolutionary perspective, as suggested in publication considering the future of policing in the UK: moving towards a data-

7 In regard to the inventiveness of organising law enforcement structures in the particular European context, see the recently published authoritative work by Fijnaut (2019).

8 The diffusion of Community Policing in its various formats in Europe would be a case in point (EUCPN/CEPOL 2019, another the introduction of body-worn cameras or Tasers into the police forces of European countries another (internal CEPOL Survey 2019). For a theoretical reflection on the diffusion of innovations into law enforcement practice in the U.S., see DeGarmo 2012).

9 Sarre & Prenzler (2018) have provided their top-ten list of key developments in Australian policing, which at one point all had been innovations.



Source: Gash *& Hobbs (2018: 3)*

and technology driven vision[10] for law enforcement – Policing version 4.0 (Gash & Hobbs 2018).

Conference Contributions

It is in the aforementioned context that the editors are proud to present in this fourth Special Conference Edition of the European Law Enforcement Research Bulletin[11] twenty-nine articles, which are based on original contributions made at the CEPOL Research and Science Conference in late 2017, covering a wide spectrum of law enforcement innovations and considering their various aspects[12]. As being demonstrated, "innovation" is not a trivial, straightforward topic – nor is it a simple task for the editors to sort and cluster the contributions in this collection for the reader – there are various ways to do it. In order to provide some structure and guidance through for the readers, we have divided the sections by bundling those papers:

- reflecting the wider institutional context of innovation processes aimed at law enforcement and security (in the EU);
- tackling innovations that are driven by new technology, including critical perspectives
- reporting about the outcomes and findings of projects funded by the H2020 research programme;
- presenting innovation in regard to learning, training and education
- informing about innovation projects in national and regional contexts.

Innovation: The Institutional Context

In her ***Welcome Address*** to the participants, *Anabela Gago* sat the stage of the conference as Head of Unit "Innovation and Industry for Security" at the EU Commission, by pointing out the key role education and research have in providing law enforcement officers with the competencies, they urgently need for successfully tackling the security threads, the Union's citizens are faced with. In reference to the investments made in security research within the Horizon 2020 funding programme, she provides various examples of research projects, where academic scientists worked closely together with industry and law enforcement practitioners, delivering innovate and useful tools for doing law enforcement.

Crime in the age of technology is the topic of the contribution presented by *Oldrich Martinu and Gary McE-*

10 It shall come to no surprise that the occasional enthusiasm for new technology options for the purposes of policing and law enforcement, have been met with scholarly scepticism and put under analytical scrutiny (see e.g. Nogala (1995), Byrne & Marx 2011, Lum et al. 2017).

11 Earlier Special Conference Editions were published under the previous title of the publication as "European Police Science and Research Bulletin".

12 A handful of other conference contributions have already been published in regular issues of the European Law Enforcement Research Bulletin, available at https://bulletin.cepol.europa.eu. Files of presentations given at the conference can be retrieved from the section of CEPOL's website (https://www.cepol.europa.eu/science-research/conferences).

wen from Europol[13], delivering a real-life perspective of emerging crime-threat scenarios, fostered by new technologies and already used by criminal elements. Various cyber-enabled and cyber-facilitated crimes are on top of their list of concerns, but also 3D-printing and drone technology. In the second part, they discuss aspects of the necessary law enforcement's response to those developments.

Illustrating an innovative approach to tackling new challenges from another Justice and Home Affairs Agency's point of view, *Piotr Malinowski* (Frontex) describes an ***Application of modern technology for migration management***, stressing the crucial relevance of customer-orientation in development and service of such complex systems.

As it has been demonstrated in earlier paragraphs of this introduction, "innovation" is often framed in the academic literature as an organizational challenge or issue. The ***Reflections on the triple helix as a vehicle to stimulate innovation in technology and security*** brought down to paper by *Marleen Easton* from Ghent University, could be read as a supporting comment to Mrs. Gago's conference address: what would an optimised model for stimulating innovation in the field of internal security look like? Her answer in a nutshell is, for yielding better results out of the cooperation between the state, industry and academia, one have to move away from a state-centered towards a trilateral approach. How this works in practice is exemplified for the Belgian Innovation Centre for Security.

Innovation driven by technology

The invention, introduction and implementation of new technologies has always had a decisive impact on how societies are organized and how people go on with their lives – our hypermodern times are inconceivable without looking at the key technologies which "changed the game". This is for sure the case for law enforcement, in particular for policing: technologies on various level of scale and scope of application have changed and transformed police work in general and the tools and instrument used by law enforcement officers in particular.

A good example of how even a small gadget can alter the way the "look and feel" of everyday-policing can change, is the recent wide-scale introduction of body-worn cameras for police officers on the ground – a new kind of "eye of the law". In his paper ***Opening up the black box: Understanding the impact of bodycams on policing,*** *Sander Flight* wonders if these gadgets actually work – and his empirically informed answer is not a simplistic one, as this apparently depends immensely on the circumstances of how the device is implemented and what the actually invested expectations were.

While also innovating on the visual aspects of law enforcement work, the article ***Automatic Weapon Detection in Social Media Image Data using a Two-Pass Convolutional Neural Network*** by a group of authors from the *Munich Innovations Lab* ventures into the technologically advanced area of artificial intelligence- driven automated support for police analysts to find and identify objects like weapons in images distributed on social media.

The next two papers examine in more general terms, how advanced technology alters the ecology of police intelligence work: imposing new conditions, but opening new possibilities as well. The contribution by *Akghar & Wells* discusses the *Critical Success Factors for OSINT Driven Situational Awareness* - where OSINT stands for open-source intelligence - and how the material delivered via social media is creating completely new challenges – and chances – for investigative techniques. How advanced new technology – the "***T-factor***", as they call it – is affecting the so-called "intelligence cycle", in particular new requirements in regard to skills and learning settings for the analysists. is the subject of the paper submitted by *Blanco, Cohen, Rubio & Brezo*. They also examine the issue of "identity management" as a matter of professional protection for the analysts.

The internet is producing torrents of new data on a daily basis, literally creating gigantic hay-stacks, in which menacing "moving" needles have to be located and tracked by law enforcement bodies. According to *Liberatore, Quijano-Sanchez & Camacho-Collados*, technology is carrying its own innovative solution for policing in the form of applied data science. They exemplify their claim in presenting a study on ***VeriPol, an Investigation Support Tool***, designed to help investigators to sort out false reports on violent robberies from the actual ones, in order to cope with the raising number of cases and efficient investment of scarce resources.

13 See also, as an update, "Do criminals dream of electronic sheep?" (Europol 2019).

The risk of being at some point being overwhelmed by the flood of data generated by police organisations internally and by the internet-juggernaut externally, is the point of concern in the paper by *Casey, Burrell & Sumner* on ***Decision Support Systems in Policing***. With reference to the body of research on decision making, they wonder if the technology under the label of "artificial intelligence" has actually advanced to the point, where these systems are now moving beyond the point of "just" supporting the decisions to be made by analysts and police officers. Their case in point argued for is the swiftly rising notion of *predictive policing*, one of the recent law enforcement innovations, which has attracted a lot of professional, scholarly and media attention. While predictive policing is seen by some with high anticipation as becoming a timely problem solver for law enforcement, others are less enthusiastic, of not outright skeptical. Two contributions explore this controversially discussed innovation from the empirical side: *Cyril Piotrowicz* has examined the ***Perceptions of its Risks and Benefits by Police Trainees and Citizens*** in France in a small survey study. He finds that his sample of French citizens want their police make use of it, even if they do not really grasp what is means and think it could be potentially dangerous. In contrast, the police trainees believe the understand the concept, but have doubts about its success and demand specific training for it. Results from an evaluation study on a pilot project in the German land of Baden- Württemberg about ***Using Predictive Policing to Prevent Residential Burglary*** is reported by *Dominik Gerstner*. A specific predictive policing market product was used and tested in urban and rural pilot areas. More remarkable than concluding than that there were no clear conclusions to be made about the effectiveness of the software, is maybe his finding that the assessment and acceptance of the new innovative tool among police officers as either system users, management or first line officers was obviously heterogeneous, if not divisive.

The two articles rounding up the cluster of contributions looking at the technology driven aspects of innovations in law enforcement, are pouring cold water on the optimism and enthusiasm about the potential bright future of predictive policing from an academically informed theoretical observation point. *Lucia G. Pais* headlines her contribution as ***Predictive Policing: Is it really an Innovation?*** - and her finding is apparently trending towards the negative, based on three objections: suspicion about the epistemological roots of the mindset the concept of predictive policing is built on, a lack of aptness of many police forces to adopt to methods based on scientific research, the reduction of (potential) offenders to mere data objects, missing out on their human agency and potential. A fundamentally critical position if also taken by Canadian Professor James Sheptycki, in his essay ***Technology and Policing Practice***, which concludes this group of papers focusing on technology-driven innovations in law enforcement. Empirically intimately familiar with the history, structure and principles of operation of police forces internationally, he states his serious reservations against promised future technology-focused scenarios of almost total information awareness, better cost effectiveness or sustainable forms of automated policing. He suspects that such a model of future policing is drifting away from ideas of citizen centered philosophies of policing by consent, in line with democratic principles and being guided by values of social justice as well.

H2020 Research Projects

A major stimulus for triggering innovation is research – in particular the type of applied research, which is intended to solve a specific, practical problem that has been identified. As explicated in the ***Welcome Address***, the Commission's Horizon 2020-programme is a research fund, which identifies an array of urgent research tasks, of which some are very relevant for internal security and law enforcement. Those H2020 research programme projects deserve special attention, as they regularly bring together distinct cutting-edge knowledge of academic scientists with the hands-on experience and comprehension of strategic requirements of law enforcement practitioners. A selection of security-related H2020 research projects presented final or interim findings at the conference and provided a paper for this Bulletin. Their common nominator is that they are all seeking innovation effects by applying a combination of capabilities enabled by new technologies and fresh approaches[14].

The ***RAMSES*** project addresses the rise of ransomware attacks on public and private computers, and intends to create countermeasures by building an internet-based forensic support platform for tracking the money flow

14 More detailed information about the projects is available from their dedicated websites:
RAMSES: https://ramses2020.eu/
UNITY: https://www.unity-project.eu/
INSPEC2T: http://site.inspec2t-project.eu/en/
LAW-TRAIN: http://www.law-train.eu/index.html
TARGET: http://www.target-h2020.eu/

behind the dissemination and exploitation of mal- and ransomware by malicious hacker groups. Gaining better forensic evidence faster for criminal prosecution is the ultimate goal of this undertaking.

The ***UNITY*** and ***INSPEC²T*** projects are two consortiums striving to render new technologies useful for fostering connections between the police and the citizens in the spirit of Community Policing. Both projects emphasize the innovative role of internet-based social media for law enforcement in building mutually beneficial relationships with their communities and various community-cultures. Network platforms, mobile apps, even games and specific training tools are the deliverables to achieve these objectives.

Two other projects, ***LAW-TRAIN*** and ***TARGET*** are exploring the new possibilities of training law enforcement officers in innovative, ambitious ways, making use of cutting-edge augmented and virtual reality equipment and software. The consortium of LAW-TRAIN aims at building a "virtual platform" which will allow to train law enforcement officers in cross-border investigation cases in jointly interviewing suspects in a multilingual context. It also builds on artificial intelligence elements, by introducing a "virtual trainer" as an intelligent pedagogical agent, in order to ensure that all trainees are following the same methodology of interviewing. The ultimate goal is to foster cross-border law enforcement by facilitating innovative interview scenarios. Even more aspiring is the TARGET project consortium, which strives to bring serious gaming technology for law enforcement officers to a new level, developing it finally into a commercial tool, available at the market and offering flexibility to design a wide variety of training narratives and scenarios. Testing of six pilot scenarios are described in the paper.

Exploring and testing innovative approaches for training and educating law enforcement personnel or for new ways of how-to police and enforce the law, is by no means a prerogative of EU-funded research projects – similar intensive efforts are pursued also in the Member States of the EU, albeit with less emphasis and use of advanced technology.

Learning Innovation(s)

Two papers are in this chapter are dealing with innovative training projects from Finland. *Sirpa Virta & Harri Gustafsberg* take the International Performance Resilience and Efficiency Programme as an example, to describe how ***Innovation Management in Police Organisations*** can be succesful, when innovations resulting from research are properly transformed into new training formats. As a point of note, the iPREP training programme, developed and tested as an international research project, obviously took its initial course from a CEPOL seminar in 2013. The introduction, implementation and evaluating reception of a new ***Executive Master of Business Administration in Policing*** as a training programme in police leadership in the Finnish police is delineated in detail in *Tiina Koivuniemi's* paper.

Innovation in training is not happening just at the top level of law enforcement organisations. *Andrea Beinicke & Albin Muff* present findings of their study on the ***Effectiveness of simulation-based learning in basic police training*** in Bavaria, Germany – the introduction of unassuming role-play scenarios has yielded measurable positive effects on learning satisfaction of trainers and learners alike.

How improvement in qualifications for law enforcement training instructors can be achieved through EU-funded twinning projects – here between Lithuania and Croatia - is reported by Žaneta *Navickienė & Vidmantas Vadeikis* in their paper ***Integrated concept for the training of trainers within police cooperation of the EU member states.***

Applied Innovation

In this final cluster of conference contributions, the reader will find studies and reports on innovative projects, which are located in the specific national context of law enforcement institutions and processes, which nevertheless can serve though as potential examples and blueprints for triggering initiatives, aiming for innovation elsewhere in Europe.

Erna Uricska & Katalin Molnár inform about the format of ***The Police Café*** (an import from Belgium), and its introduction to Hungary, aimed at becoming an efficient method to facilitate and foster community policing-style dialogue between the police and citizens.

The issue of ***Recording Hate Crime***, an offense which seems to rise in parallel with the increasing use of social media, has come lately under scientific scrutiny in Ireland. *Amanda Haynes & Jennifer Schweppe's* paper gives an account of the development, as they point out the

limited gain of technical innovation, when agreed definitions and proper training are neglected.

How even rather trivial innovative changes of internal formal procedures can have a significant positive effect on the workplace and speeding up of case-work is exemplified by *Damir Osterman & Damir Maracic* when they present the ***Croatian Model of Telecommunication Information Requests Management (TIRM).***

Evidence, that the introduction of new IT-technology and the accompanying European legislation into a law enforcement environment of candidate countries can be a real challenge, can be taken from the account *Kristina Doda & Aleksandar Vanchoski* are giving in their ***Situational Analyis in Northern Macedonia, Montenegro and Serbia***.

Directions towards future desirable innovations in the law enforcement context are outlined and discussed in two contributions from Portugal. ***Interoperability*** for first responders to incidents is the subject of concern for *Felgueiras, Pais & Morgado* and their sketch of a research scenario for developing a new assessment tool. More than a research project is the ambition of *Nelson Macedo da Cruz* – his vision of the ***MOLECULA*** project aims to bring the investigation of tax, financial, and economic transnational organised crime in the European Union to a new level by taking advantage of new information flow architectures.

In Conclusion

Reflecting academically on the origin, history and semantic meaning of the term "innovation" can open new perspectives and unsuspected insights, but innovation is happening constantly in all occupations of life – it is the fuel feeding modernization in general, and is driving forward developments in the policy area of law enforcement as well. As pointed out earlier: looking back at how ways, instruments and tools of modern policing have changed and advanced only in the last few decades, the strong innovation dynamic in this field becomes more than evident. The presentations given at the CEPOL conference and the articles are helping to grasp the wide variety of promising initiatives, which are ongoing.

However, one can expect that innovation in law enforcement will be forced to speed up to a higher pace in the years to come - with technical innovations likely to have a decisive role again.

Law enforcement communities need to adjust to the challenges that will come with e.g. 5G, 6G telecommunication, "Internet of Things", driverless cars, AI and drone technologies. Apart from other change-driving factors (e.g. ageing societies in Europe), these technologies are expected to transform significantly the daily life in our societies - the citizens have the rightful expectation that law enforcement is prepared to protect them even in such dynamic changing environments. There is little doubt, that indispensable innovations in law enforcement communities can and will only be successful in a very close cooperation of law enforcement communities, academics, industry and civil society across Europe.

We trust that this compilation of articles, originating in contributions made to the CEPOL Research and Science Conference in late 2017 in Budapest, is not just a documentation of the inspirational presentations on contemporary innovations in law enforcement given at this particular event, but that this publication itself might serve as a catalyst for fostering and facilitating a much needed further multi-disciplinary and multi-professional discussion on how to innovate law enforcement in Europe: not to do things just differently, but better, and with a better result.

The European Union Agency for Law Enforcement Training is committed to facilitate such much needed close cross-professional dialogue and cooperation with similar conference events like this in the future.

References

- Allen, D. and Karanasios, S. (2011) 'Critical Factors and Patterns in the Innovation Process', *Policing*, 5(1), pp. 87–97. doi: 10.1093/police/paq058.
- Borbély, E. (2008) 'J. A. Schumpeter und die Innovationsforschung', in Kadocsa, G. (ed.) *Proceedings-6th International Conference on Management, Enterprise and Benchmarking (MEB 2008)*. Óbuda University, Keleti Faculty of Business and Management, pp. 401–410.
  Available at: https://ideas.repec.org/h/pkk/meb008/401-410.html.
- Brown, T. J. (2011) 'Police Radio History and Innovation: What Have We Learned?', *Journal of Law Enforcement*, 3(6).
  Available at: https://jghcs.info/index.php/l/article/view/306.
- Byrne, J. and Marx, G. (2011) 'Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact', *Cahiers Politiestudies*. (Journal of police studies), Nr.20, pp. 17–40.
- Caparini, M. and Marenin, O. (eds) (2004) *Transforming Police in Central And Eastern Europe: Process And Progress*. Münster, Germany : New Brunswick, N.J: LIT Verlag.
- Carter, J. G. (2013) *Intelligence-Led Policing: A Policing Innovation*. Lfb Scholarly Pub Llc (Criminal Justice: Recent Scholarship).
- Cope, S., Leishman, F. and Starie, P. (1997) 'Globalization, new public management and the enabling State', *International Journal of Public Sector Management*, 10(6), pp. 444–460. doi: 10.1108/09513559710190816.
- Deflem, M. (2002) *Policing World Society: Historical Foundations of International Police Cooperation*. New. Oxford ; New York: Oxford University Press.
- DeGarmo, M. J. (2012) 'The Diffusion of Innovation among United States Policing Jurisdictions: A Cautionary Tale for Theorists and Researchers', *International Journal of Criminal Justice Sciences*, 7(1), pp. 450–465.
- Disch, W. K. A. (2016) *Innovation neu denken – Von Schumpeter lernen*. Studie zur Vorbereitung auf den Beitrag „Von Schumpeter lernen" in Block II »Innovationen als „neue Kombinationen" zur Verfügung stehender Ressourcen« beim 20. G·E·M Markendialog »Innovation neu denken – Energie für die Marke« am 25. Februar 2016 in Berlin. Berlin: Gesellschaft zur Erforschung des Markenwesens e.V.
  Available at: https://www.gem-online.de/pdf/forschung/Studie_Von_Schumpeter_lernen.pdf (Accessed: 1 August 2019).
- Drucker, P. F. (2002) 'The Discipline of Innovation', *Harvard Business Review*, 80(August), pp. 95–104.
  Available at: https://hbr.org/2002/08/the-discipline-of-innovation.
- EUCPN and CEPOL (2019) *Toolbox 14 - Community-Oriented Policing in the European Union Today*. Brussels: European Crime Prevention Network.
  Available at: https://eucpn.org/toolboxcop (Accessed: 3 November 2019).
- Europol (2019) 'Do Criminals Dream of Electric Sheep? How Technology Shapes the Future of Crime and Law Enforcement'. Europol.
- Fijnaut, C. (2019) *A Peaceful Revolution: The Development of Police and Judicial Cooperation in the European Union*. First. Cambridge; Antwerp; Chicago: Intersentia.
- Fyfe, N. R., Terpstra, J. and Tops, P. (2013) *Centralizing forces?: comparative perspectives on contemporary police reform in Northern and Western Europe*. The Hague: Eleven International Publishing.
  Available at: https://discovery.dundee.ac.uk/en/publications/centralizing-forces-comparative-perspectives-on-contemporary-poli (Accessed: 3 November 2019).
- Gash, T. and Hobbs, R. (2018) *Policing 4.0 - Deciding the future of policing in the UK*. Deloitte.
  Available at: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/PublicSector/deloitte-uk-future-of-policing.pdf.
- Godin, B. (2015) *Innovation: A Conceptual History of an Anonymous Concept*. Working Paper No. 21.
  Available at: http://www.csiic.ca/PDF/WorkingPaper21.pdf.
- Godin, B. (2018) 'The Spirit of Innovation': INRS.
  Available at: http://www.csiic.ca/wp-content/uploads/2018/06/Spirit.pdf.
- Godin, B. and Vinck, D. (eds) (2017) *Critical Studies of Innovation - Alternative Approaches to the Pro-Innovation Bias*. Cheltenham, UK & Northampton, MA, USA: Edward Elgar.
- INTERPOL and UNICRI (2019) *Artificial Intelligence and Robotics for Law Enforcement*. Torino: Unicri.
  Available at: http://www.unicri.it/news/article/Artificial_Intelligence_Robotics_Report.
- Kennedy, D. M. (1993) *The Strategic Management of Police Resources*. No. 14. U.S. Department of Justice.

- King, W. R. (2000) 'Measuring police innovation: issues and measurement', *Policing: An International Journal of Police Strategies & Management*, 23(3), pp. 303–317. doi: 10.1108/13639510010342994.
- Lazzarotti, F., Samir Dalfovo, M. and Emil Hoffmann, V. (2011) 'A Bibliometric Study of Innovation Based on Schumpeter', *Journal of technology management & innovation*, 6(4), pp. 121–135. doi: 10.4067/S0718-27242011000400010.
- Lum, C., Koper, C. S. and Willis, J. (2017) 'Understanding the Limits of Technology's Impact on Police Effectiveness', *Police Quarterly*, 20(2), pp. 135–163. doi: 10.1177/1098611116667279.
- McLaughlin, K., Osborne, S. P. and Ferlie, E. (eds) (2002a) *New Public Management: Current Trends and Future Prospects*. 1st edn. London and New York: Routledge. doi: 10.4324/9780203996362.
- McLaughlin, K., Osborne, S. P. and Ferlie, E. (eds) (2002b) *New Public Management: Current Trends and Future Prospects*. 1st edn. London and New York: Routledge. doi: 10.4324/9780203996362.
- Mesko, G. *et al.* (eds) (2013) *Handbook on Policing in Central and Eastern Europe*. New York: Springer-Verlag. doi: 10.1007/978-1-4614-6720-5.
- Moore, M. H. (2003) 'Sizing up Compstat: an important administrative innovation in policing', *Criminology & Public Policy*, 2(3), pp. 469–494.
- Nogala, D. (1995) 'The future role of technology in policing', in Brodeur, J.-P. (ed.) *Comparison in policing: an international perspective*. Avebury, pp. 191–210.
- Okabe, R. (2014) 'Police innovation paradigm in the United States and Japan', *Police Practice and Research*, 15(3), pp. 192–206. doi: 10.1080/15614263.2012.754125.
- Sarre, R. and Prenzler, T. (2018) 'Ten key developments in modern policing: an Australian perspective', *Police Practice and Research*, 19(1), pp. 3–16. doi: 10.1080/15614263.2016.1242424.
- Senior, P., Crowther-Dowey, C. and Long, M. (2007) 'Modernisation and the police', in *Understanding the Modernisation in Criminal Justice*. McGraw-Hill Education, pp. 159–181.
- Weber, S. (2018) *Innovation: Begriffsgeschichte eines modernen Fahnenworts*. Tectum Wissenschaftsverlag (kommunikation & kultur).
- Weisburd, D. and Braga, A. A. (2006) *Police innovation: Contrasting perspectives*. Cambridge University Press.
- Willis, J. J. and Mastrofski, S. D. (2011) 'Innovations in Policing: Meanings, Structures, and Processes', *Annual Review of Law and Social Science*, 7(1), pp. 309–334. doi: 10.1146/annurev-lawsocsci-102209-152835.

INNOVATION: The Institutional Context

Welcome Address

CEPOL 2017 Research and Science Conference, Budapest 28 November 2017

Anabela Gago
Head of Unit – "Innovation and Industry for Security", European Commission

Dear Ladies and Gentlemen,

I would like to thank the Organisers, and especially Dr Detlef Nogala, for the invitation to participate to the CEPOL 2017 Research and Science Conference "Innovations in Law Enforcement – Implications for practice, education and civil society". It is a pleasure for me to give a keynote speech at this Conference in Budapest. I will give you an overview, including on the added-value of EU funded security research, WP2018-2020, key features, examples, FP9.
Nowadays, criminals and terrorists exploit technological developments and find more and more sophisticated ways to act and elude investigations. Moreover, we are facing new challenges through cyber-crime attacks on infrastructures, companies, public administrations.

As stated in Tallinn two weeks ago, at the Security Research, Innovation and Education Event, co-organized by DG HOME with the Estonian Academy of Security Sciences and EE Ministry of Interior (Panel "What can research and education do for police"?), we need police officers with the right competences to face these challenges. To this end, research and education are the keys, and not only on a national level. Building an EU capacity is vital.
We can only find solutions to safeguard the security of our citizens through cross-border cooperation. If crime does not know borders, responses shouldn't either. Also Member States do not have the necessary capacity to face certain challenges. We need to tailor our actions consequently and provide practitioners with the support they need in their daily work.

In a recent Special Eurobarometer on Europeans' attitudes towards security, the importance of cross-border co-operation for the European citizens has been underlined: 69% think national law enforcement authorities should share info with other EU countries on a systematic basis. Also in Spring 2017 Eurobarometers, for the first time, terrorism comes as number one challenge facing the EU.

There is thus a clear mandate of the citizens for the Member States to work together on security matters and that they benefit from EU support. And EU support includes support through research funding. Research can help identify new security threats, better understand their real causes and their impacts on societies. Security research also plays an important role in the development of innovative security solutions that help to mitigate security risks more effectively. It can be new technologies, or new systems or processes.

We have invested nearly 2 billion euro in over 400 projects since the "EU security research programme" started ten years ago, in the seventh Framework Programme, and continued in Horizon 2020. Under the Programme for 2014-2020 1.7 billion are foreseen for "Secure Societies". EU Security Research accounts for 50% of all public funding for research in security in the EU. Only 7 MS have their own national security research programmes. The EU and its citizens rightfully expect to see a return for this investment. We do have quite a number of results. Some of these will be presented here. I will also mention some a bit later.

Let me underline: we face a major challenge: market uptake that is to ensure that research results are effectively translated into tools and services that police, customs, etc. can use in their daily work. For that to happen, we need practitioners, trainers, educators, civil society, to be involved in our projects and also industry, if we want the EU security research to have a real added-value for European citizens.

The current framework programme, Horizon 2020, has a central role in ensuring that the EU's research effort is well targeted, factoring in the needs of law enforcement authorities by involving end-users at all stages of the process. To this end, the participation of practitioners in research projects is now mandatory. Eligibility criteria have been made stricter in this respect. Furthermore, under the current work programme, we fund pan-European practitioners' networks.

The reasoning behind funding networks of practitioners lies in the following:
1) Practitioners (LE) police, customs have little means to free workforces from daily operations, and to dedicate time and resources to monitor innovation and research that could be useful to them and to be thinking about long-term threats and what tools they would need to tackle those threats.
2) Practitioners have little opportunities to interact with academia or with industry on research and innovation.
The newly created networks include two on law enforcement (I-LEAD, ILEA-net), one on firefighters, one on CBRN testing sites (forensics) and one on the Danube River Basin. They aim at helping practitioners identify their future needs, make those needs known to research and industry and be able to monitor what research has brought and what innovative solutions could be of use for their work on the ground. Role of Agencies: Frontex / European Boarder and Coast Guard Agency, Europol, eu-LISA should play an important role in research leading to the tools their relevant practitioners need.

Using the outcomes of research in police practice is very important and should cover a whole range: technology-related research as well as cultural, social and human sciences. And this is why an event like this one organised by CEPOL is so important and so much welcome, convening practitioners in policing and other areas of law enforcement, trainers, educators and scientific scholars from Europe and beyond around the topic of Innovation. I recognise in particular from the programme a number of projects funded by EU Security Research's familiar names such as TENSOR, ASGARD, UNITY, AUGMED, TARGET and I am particularly pleased and grateful that they are presented here in this forum.

On 27 October the Commission adopted the WP2018-2020 of H2020. The overall funding for the 2018-2020 Work Programme will exceed 30 billion euro, 700 million of which dedicated solely to security research. It will focus efforts on fewer topics with bigger budgets, directly supporting the Commission's political priorities:

- preventing and fighting serious crime including terrorism;
- improving border security; and
- protecting infrastructure against threats, including cyberattacks.

In this context, a key feature is the creation of 'Focus areas', cut across several parts of the overall Work Programme and expected to create an exceptional impact, addressing 'big ticket' challenges. These focus areas have been designed around four political priorities: a low-carbon, climate resilient future; circular economy; digitising and transforming European industry and services; and 'Boosting the effectiveness of the Security Union'.

The Focus Area 'Boosting the effectiveness of the Security Union' will have an overall budget of one billion euro. It will bring together a wide array of security relevant topics from different parts of Horizon 2020, including ICT, Space, Health and Energy.
I would like to give some examples on how we try to:

- on the one hand, use security research as a tool to implement security policies; and
- on the other hand, use security research to feed into the policy development cycle.

The most recent example is the comprehensive Counterterrorism Package which was adopted on 18 October. It comprises a number of practical and operational EU measures to support Member States in fighting terrorism, such as two Action Plans: one on CBRN preparedness and one on EU support to protect public spaces. The Package also entails Recommendations on

- the better application of the Regulation on explosives precursors; i.e. better control of supply chain
- as well as actions to counter radicalisation;
- to counter terrorist financing; and
- to strengthen the external dimension of counter-terrorism.

Let me bring an example related to technology-oriented research on home-made explosives. Most bombs used by terrorists or criminals actually benefit from commercially available products. Innovative solutions to neutralise and detect these explosives have been a constant theme in both EU security policy and EU security research. Our research projects PREVAIL and EXPEDIA have found a way to alter the composition of commercially available chemicals, to make them unusable for bomb makers. These findings will now be used in the revision of the new regulation on explosives. But short-term relevant recommendation to MS is already proposed. Through this, research is providing scientific advice to the policy development process and contributes to the shaping of legislation.

Another example is the Action Plan to protect public spaces – H2020 2018-2020 funding, ISF Police – 18.5M in 2018, plus 100 M in 2018 Urban Innovation Act.

Our work on violent radicalisation is another, [less technology and more socially oriented example, but by no means less important.] Since 2007, research on violent radicalisation has been a recurrent topic in our Work Programmes. Under FP7, four such projects were funded with 14 million euro in EU contribution. Research projects on violent radicalisation are producing scientific tools, and providing policy suggestions for direct use by law enforcement agencies and security policy-makers, including by the experts of the Radicalisation Awareness Network.

As an illustration of their usefulness, let me just mention one of these projects, called SAFIRE, which developed, for the first time, a model of the radicalisation process in its full complexity. This model is already actioned by services in some Member States to address individual cases of radicalisation. Within Horizon 2020, TENSOR and DANTE, two projects related to the detection of online terrorist content, started last year. Four more projects, worth 12 million euro in EU contribution, were launched for funding this year, through the 2016 call for proposals under the H2020 Secure Societies Challenge. They propose among others to develop policy recommendations and improved communication tools for law enforcement and security agencies. Violent radicalisation and explosives will remain research priorities for the 2018-2020 Work Programmes of the Secure Societies Challenge. These are some examples of how the circle between research and policy is closed.

Some of you are already engaged in our projects. I would encourage all of you to look into our Work Programme, into our projects. Our ultimate goal, from a European security research perspective, is to be useful to policy makers and to law enforcement. Let's join forces to be effective in the fight against crime and terrorism.

I wish you all three very successful days of discussions, mutual learning and networking.

Thank you for your attention.

Crime in the Age of Technology

Oldrich Martinu
Gary McEwen
Europol, The Hague, Netherlands

Abstract
The serious and organised crime landscape in the EU has changed drastically in the past years - in large part due to advancements in technology. Criminals quickly adopt and integrate new technologies into their modi operandi or build brand-new business models around them. The use of new technologies by organised crime groups (OCGs) has an impact on criminal activities across the spectrum of serious and organised crime. This includes developments online, such as the expansion of online trade and widespread availability of encrypted communication channels, as well as other aspects of technological innovation such as more accessible and cheaper drone technology, and advanced printing technologies. Technology has become a key component of most, if not all, criminal activities carried out by OCGs in the EU and has afforded organised crime with an unprecedented degree of flexibility.

Keywords: card fraud, child sexual exploitation, crime-as-a-service, cybercrime, darknet, data, drones, drugs, encryption, Europol, firearms, human trafficking, illegal immigration, intellectual property, internet, malware, money laundering, online trade, organised crime, prevention, public-private partnerships, ransomware, technology.

1. Introduction

Serious and organised crime is a key threat to the security of the EU. Criminal groups and individual criminals continue to generate multi-billion euro profits from their activities in the EU each year. Some parts of the serious and organised crime landscape in the EU have changed drastically in recent years — in large part due to advancements in technology that have had a profound impact on the wider society and economy. While these advances have provided great benefit to society in general, they are often used, abused, or exploited for criminal intent. Technology is therefore now a key component of most, if not all, criminal activities carried out by criminal groups in the EU and has afforded organised crime with an unprecedented degree of flexibility. This flexibility is particularly apparent in the ease with which criminals adapt to changes in society. The vital role of technology for organised crime is clearly reflected in both the SOCTA 2017 (Europol 2017a) and IOCTA 2017 (Europol 2017b). The range and variety of technological advances that can be exploited by criminals is extensive, this article will therefore focus on some of the more noteworthy.

2. Crime and the internet

While many technological advances play an important role in a wide range of criminal activities, none has likely had greater impact or influence than the internet. Just as internet can be used to enhance and augment the daily lives of everyday citizens, and the functioning of businesses and services, it has not only given rise to a completely new form of crime, but can facilitate or assist criminality across almost all other crime areas.

The internet is of course fundamentally a source of information, and an environment where communities of like-minded individuals can meet. The list of information that could be used to assist criminals is essentially endless, but key examples include access to detailed map data, including satellite and street-views for reconnaissance, shipping routes and schedules, tutorials, guides and recipes for drugs or explosives, and tips on operational security.

Cybercrime

Cybercrime is a global phenomenon, and is as borderless as the internet itself. The attack surface continues to grow as society becomes increasingly digitised, with more citizens, businesses, public services and devices connecting to the internet. Moreover, the potential for one attacker to affect many victims is scaling exponentially. The term 'cybercrime' encompasses a broad range of different criminal threats however. The most threatening aspects of cybercrime involve crimes such as the distribution of **ransomware** and other **malware**, **fraud involving non-cash payments** and the **online trade in child sexual exploitation material**.

Cyber-dependent crime

Cyber-dependent crime can be defined as any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT). In essence, without the internet these crimes could not be committed. It includes such activity as the creation and spread of malware, hacking to steal sensitive personal or industry data and denial of service attacks to cause reputational damage.

A mature Crime-as-a-Service business model underpins cybercrime and provides easy access to tools and services across the entire spectrum of cyber-criminality, from entry-level to top-tier actors, or any other party, including those with other motivations such as hacktivists or even terrorists. The development and distribution of malware continues to be the cornerstone for the majority of cybercrime. Information-stealing malware, such as banking Trojans, represent a significant threat, although ransomware has become the leading malware in terms of threat and impact, as demonstrated by with the scale of the WannaCry and NotPetya attacks of mid-2017. Network intrusions that result in unlawful access to or disclosure of private data (data breaches) or intellectual property are growing in frequency and scale, with hundreds of millions of records compromised globally each year.

Cybercrime continues to expand in scope and impact. Digital economies and societies are an attractive target for cybercriminals. Technological innovation holds exciting prospects for businesses and citizens alike, but also creates new attack vectors for those criminals seeking to capitalise on these developments. Increasing internet connectivity by citizens, businesses and the public sector, along with the exponentially growing number of connected devices and sensors as part of the Internet of Things is creating new opportunities for cybercriminals.

Cyber-facilitated crime

Cyber-facilitated crimes are crimes which can be conducted either online or offline. The role played by the internet is to increase the scale, geographic scope, and speed of these crimes. **Online child sexual exploitation** epitomises the worst aspects of cyber-facilitated crime. The hands-on abuse of vulnerable minors occurs very much in the real world, but it is captured, shared, distributed, encouraged and even directed over the internet. The internet provides offenders and potential offenders with an environment in which they can operate with an enhanced level of safety and anonymity; where they can research, target, and groom minors for abuse. Moreover, the Darknet hosts a growing number of forums dedicated specifically to the production, sharing and distribution of child sexual exploitation material. The internet additionally offers a wide range of internet-based applications, such as Peer-to-peer file sharing, and secure data storage, which facilitate this crime.

Fraud involving non-cash payments is an ever-present threat. Many aspects of this crime area are highly organised, highly specialised, and constantly evolving to adapt to both industry measures to combat it, and new payment technologies. This crime priority is divided into two, relatively distinct crime areas: card-

not-present (CNP) fraud, which occurs largely online and card-present fraud, which typically occurs at retail outlets and ATMs.

Fuelled by the availability of compromised card data stemming from data breaches, phishing, and malware, the fraudulent use of compromised card data to make purchases online continues to plague the e-commerce industry. The retail sector is predictably one of the hardest sectors hit; however, airline ticket fraud continues to have a high impact and priority across Europe. Fraud relating to accommodation (e.g. hotels booked using compromised cards) is on the increase. Both individuals and OCGs are involved in this type of activity. Where OCGs are involved, this crime is often linked to other crimes such as trafficking in human beings (THB) or drugs, and illegal immigration – crimes where transport and temporary accommodation is required to facilitate the criminal activity.

Technology is also providing criminals with new methods of intrusion into ATMs and similar systems. By drilling or burning small holes into an ATM case, attackers can reach the ATM's computer hardware components. The attackers use this access to control the ATM's operating system and force it to dispense cash.

Criminal groups involved in the theft of motor vehicles increasingly rely on high tech tools to gain access to vehicles and to overcome security measures. Information on how to overcome car security systems can be easily accessed via online messaging boards and websites. As vehicles increasingly rely on keyless entry systems and other new technologies to aid navigation, driving and entertainment, this trend is set to intensify over the coming years.

The online trade in illicit goods

Online platforms operating in the legal economy have had a profound impact on business models, shopping experiences and customer expectations. The multiplication of sales platforms makes online trade easier, more accessible and cheaper. This development has been mirrored in the online trade in **illicit goods and services** as criminals, like legitimate traders, seek opportunities to grow their businesses. Illicit online markets, both on the surface web and Darknet, provide criminal vendors the opportunity to purvey all manner of illicit commodities. Many of these illicit goods, such as cybercrime toolkits or fake documents, are key enablers for further criminality.

The **drugs market** is undoubtedly the largest criminal market on the Darknet, offering almost every class of drug for worldwide dispatch. Earlier this year, the now defunct AlphaBay, one of the largest Darknet markets, had over 250 000 separate listings for drugs, accounting for almost 68% of all listings. 30% of the drugs listings related to Class A drugs. Prior to this year's law enforcement action, some studies suggest that the total monthly drugs revenue of the top eight Darknet markets ranged between EUR 10.6 million and EUR 18.7 million, when prescription drugs, alcohol and tobacco were excluded.

Infringements of **intellectual property rights (IPR)** are a widespread and ever-increasing worldwide phenomenon, exacerbated by online markets. The impact of counterfeiting is high in the European Union, with counterfeit and pirated products amounting to up to 5% of imports. Most counterfeit products can be sold on the surface web, being presented as (or mixed with) genuine products. Sale of counterfeit products on the Darknet tends to relate to those commodities that are explicitly illegal, such as counterfeit bank notes and fake ID documents.

Compromised **data** is another key commodity commonly traded online, and subsequently used for the furtherance of fraud. Typically, this is financial data such as compromised payment card data or bank account logins. However, any data that could be exploited to commit fraud or other crimes is also readily available for sale. This includes everything from lists of full personal details and scanned documents to email lists and online account logins.

Firearms are increasingly traded on online platforms including Darknet marketplaces. Both individual criminals and OCGs can obtain illegal firearms via these markets. This online trade allows individuals with no or limited connections to organised crime to procure firearms. Given the number of terrorist attacks throughout 2016/2017, the potential easy availability of firearms and explosives is a worrying trend.

3. Communications technology

There have been many developments in communications technology in the last few decades - innovations that have vastly improved the availability, speed, range, and security of channels of communication.

In parallel with this are developments in the devices through which these channels operate. As an example, the modern mobile phone is not simply a telephone, but a fully functional, internet-enabled computer. The internet, coupled with almost ubiquitous access via smart devices has spawned a myriad of communication applications and options, from text-based instant messaging to Voice-over-internet protocols (VoIP) and live video streaming.

Criminals make use of all and every communication channel available, not just for their own internal communication, but also to contact potential victims, which modern technology allows them to do in unprecedented numbers. For example, email can be used for phishing campaigns or to distribute malware, and social media can be used to find and groom victims for online child abuse.

Law enforcement is witnessing a transition into the use of secure apps and other services by criminals across all crime areas. The majority of the apps used are the everyday brand names popular with the general populace. As not only these applications, but also the devices they operate on, become increasingly secure, incorporating end-to-end encryption for example, they are readily adopted by criminals seeking reliable, secure communications. This creates additional challenges for law enforcement as it renders many traditional investigative techniques, such as wire-tapping, ineffective.

Encryption

While the use of encryption is increasingly important to private citizens and industry for protecting their data, thereby denying it to criminals who desire it for criminal purposes, the growing use of legitimate anonymity and encryption services by criminals and other malicious actors poses a serious impediment to the detection, investigation and prosecution of crime. This is pertinent across all crime areas, including terrorism.

4. Criminal finances and money laundering

Criminal finance has benefitted greatly from technological innovation such as the shift to online solutions for most financial services provided for the legitimate economy. The emergence of new forms of payment such as cryptocurrencies and the appearance of a plethora of highly diverse and often difficult to regulate online payment and banking platforms has afforded criminals with new ways of financing and expanding their criminal businesses. The rapid processing of transactions across multiple jurisdictions and the proliferation of encryption and anonymisation tools represent some of the most significant obstacles encountered in increasingly complex and technically demanding financial investigations.

Sitting largely outside the regulated financial sector, cryptocurrencies are increasingly exploited by criminals. For the past few years, this has almost universally meant Bitcoin, the criminal abuse of which has grown in parallel with its general adoption and legitimate use. It is the most commonly used currency for criminal-to-criminal payments within cybercrime, for example when purchasing or renting cybercrime tools or services on the digital underground. It is the *only* currency accepted on most Darknet marketplaces and automated card shops, and is the currency required by almost all of today's ransomware and DDoS extortion demands. There are also a growing number of cases where it is used for crimes outside of cyberspace, as payment for ransom in kidnappings for example.

5. Industrialisation and manufacturing

Many crime areas have benefitted from developments in, or the increased availability of technology associated with manufacturing and the industrialisation of processes. One such area is the drugs market. The market for drugs remains the largest criminal market in the EU. 45% of the criminal groups active in the EU are involved in the production, trafficking or distribution of various types of drugs across Member States, generating multi-billion euro profits for the groups involved in this activity. Technical innovation and the accessibility of sophisticated equipment has allowed criminal groups to maximise production output. Large-scale cannabis cultivation sites are often maintained using professional growing equipment such as climate control systems, CO2 and ozone generators. Similarly, laboratories manufacturing synthetic drugs feature advanced equipment and production lines capable of producing synthetic drugs on an industrial scale. The production, trafficking and distribution of illicit drugs remains a key threat to the EU that is only enhanced by the availability of advanced production equipment and the shift to online platforms used to trade these illicit drugs.

Other crimes that have benefited from advances in manufacturing technology are those that concern the production of other illicit commodities, such as counterfeit products, including counterfeit banknotes. Industrialisation, automating and miniaturisation have all contributed to faster and greater production of higher quality (in terms of apparent authenticity) counterfeit goods.

3D-printing

One particular manufacturing technology that has demonstrated its potential for criminal abuse is that of 3D printing. Already readily available, 3D printers can print in a wide variety of materials including ceramics, plastic and metals. Moreover, assuming that the appropriate files can be obtained, almost any object can be printed with those materials. It is already possible to print handguns, and magazines, and as bigger printers become available, it will be possible to print larger objects. Such technology is already used by ATM skimmers to produce skimming devices and equipment (such as ATM panels). Developments in 3D printing technology have seen many consumer 3D printers hit the markets making it easier for criminals to acquire the technology they need to make the custom components required for any illicit purpose.

Drone technology

Advances in drone technology are expected to have an impact on a number of areas of criminality - essentially any crime that could exploit a low profile mechanism of transporting or delivering illicit goods. The trafficking and distribution of drugs or other contraband are obvious examples. As drones develop greater travel distance and the ability of carrying heavier loads, as well as becoming more affordable, criminal groups involved in drug trafficking will likely invest in drone technology in order to avoid checks at border crossing points, ports and airports.

The availability of drones will open up a number of opportunities for criminals and other malicious actors. Drones will allow for reconnaissance and counter surveillance, and it has already been demonstrated that civilian drones can be mounted with firearms, including automatic weapons, or potentially even explosives.

6. The law enforcement response

It is clear that that any developments in the use of technology by criminals must be matched and countered by an appropriate and effective law enforcement response. There is an obvious challenge here for law enforcement to not only keep pace with new technological developments, but with emerging crimes and a continually changing threat landscape.

Cybercrime, as a relatively new crime area, is a good example of this, and poses many challenges peculiar to that crime area. Attribution – determining who is behind an attack, and where they globally are located, is especially challenging, particularly in an environment where cybercriminals share tactics and tools with malicious actors with other motivations, such as hacktivist or nation state actors. Furthermore, many aspects of cybercrime are developing rapidly, requiring specific expert knowledge and the use of cutting-edge investigative techniques and advanced digital forensic tools.

In order for law enforcement to effectively fight technology-enabled crime, it must of course embrace technology itself. Technology can also be a significant aid to law enforcement authorities in the fight against serious and organised crime, often using the very same technology abused by criminals. For example, mapping and geo-location tools have proved to be invaluable for planning and co-ordination during large events such as public protests, especially if combined with other technologies such as drones and social media monitoring on the internet. Developments in artificial intelligence and machine learning could have significant benefits when considering predictive policing software, or the processing of the increasing volumes of (big) data that potentially arise from modern police investigations.

Naturally, the use of such technology by law enforcement has considerable resource implications, not just in gaining access to or ownership of the technology in question, but in ensuring that adequate training is available to capitalise on the technology. A harmonised and co-ordinated approach towards training and capacity building across the EU is therefore essential.

Many aspects of the criminal abuse of technology are out-with the implicit remit of law enforcement, and instead lie with regulators and policy makers. This applies to issues such as encryption, or the commercial availability and use of drones. Emerging technology fields such the Internet of Things (IoT) for example, have resulted in the creation of new legal, policy and regulatory challenges, and demand cooperation between different sectors as well as different stakeholders. In such discussions, it is essential for law enforcement to

have a voice, and to provide guidance and recommendations regarding the needs and requirements of law enforcement in order to be able to continue effectively combatting crime where these technologies are involved.

Combatting crime however is not something law enforcement can or should shoulder alone. A critical factor for success is therefore to develop working relationships with private industry and academia. Industry and academia often have access to data, resources, technology and expertise that is simply unavailable to law enforcement. Moreover, they are often willing partners, particularly when a threat affects their industry. An excellent example of this are Europol's Global Airport Action Days that target fraudsters travelling on tickets bought using compromised payment cards. Such events bring together law enforcement, airline companies, travel agents, banks, and payment card companies from over 60 countries round the world, and have had a significant impact on this threat area.

This level of joint working and engagement with the private sector represents a significant change in the mind-set for many law enforcement agencies, whereas previously they may only have 'engaged' with companies through court orders and warrants. This formation of successful and mutually beneficial collaborative partnerships with non-law enforcement bodies demonstrates how law enforcement has had to adapt to factors other than emerging technologies, and has changed the way it interacts with other facets of society.

Another such development is the growing involvement of law enforcement in prevention measures. While the *prevention and detection* of crime has long been the mission of law enforcement, the focus has typically been on the detection. However, prevention has proved to be a key non-investigative measure for many crime areas, and another with which law enforcement can work closely with the private sector. Prevention measures aim to address the lack of knowledge or information about potential threats from various technologies that often leaves potential victims vulnerable to more tech-savvy criminals, or attempts to dissuade would-be criminals from following the wrong path. Simply raising awareness of these threats, and educating potential victims, can have significant impact on the success of malicious actors. This is again, particularly pertinent in cyberspace where a little knowledge can protect victims from attacks such as phishing, malware or sexual extortion.

Technology will continue to adapt and develop, often at a pace greater than either law enforcement or potential victims can maintain their knowledge or perhaps even awareness of it. New and developing technology will also continue to create new attack vectors, and further expand existing ones. While criminals continue to abuse and exploit new and existing technologies - in order to enhance their criminal activities, or perhaps as a key component of their criminality - it is essential that law enforcement continues to use all the resources, tools, and opportunities at its disposal. Public-private partnerships, the development of innovative technical solutions, prevention measures, and training and capacity building are all required in order for law enforcement to remain an effective countermeasure to crime in the age of technology.

References

- Europol (2015) Guidance and recommendations regarding logical attacks on ATMs.
  Retrieved from https://www.ncr.com/sites/default/files/brochures/EuroPol_Guidance-Recommendations-ATM-logical-attacks.pdf
- Europol (2017a) Serious and Organised Crime Threat Assessment.
  Retrieved from https://www.europol.europa.eu/socta/2017/resources/socta-2017.pdf
- Europol (2017b) 2017 Internet Organised Crime Threat Assessment.
  Retrieved from https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf
- RAND Europe (2016) Internet-facilitated drugs trade – An analysis of the size, scope and the role of the Netherlands, p41.
  Retrieved from https://www.rand.org/pubs/research_reports/RR1607.html

Application of Modern Technology for Migration Management

Piotr Malinowski
Eurosur/Copernicus Fusion Services Sector, Frontex[1]

Abstract
The traditional methods of migratory management alone cannot withstand the challenges the migration authorities are facing today, therefore the state-of-art solutions have become indispensable for situation monitoring. This paper gives a brief overview of the surveillance tools – Eurosur Fusion Services (EFS) applied by Frontex under the EUROSUR framework. Special attention was paid to optical and radar imagery, airborne aerial surveillance technologies, maritime surveillance tools enabling detection and tracking of the vessels of interest, geographical information system (GIS) technology for data integration and dissemination. The paper provides valuable insights into the full EFS lifecycle – from service design integration to transition and implementation, and stresses the importance of the customer-oriented approach and continuous service improvement to better respond to the situation monitoring needs of Member States.

Keywords: migration management, border surveillance, surveillance tools, aerial surveillance, state-of-the-art technology

Introduction

The migratory pressure that Europe has been experiencing for couple of years now is a hot topic in the public and social media. It is however even hotter topic for actors who are directly engaged in dealing with migration management on a day-to-day basis. The traditional methods of migratory management alone cannot withstand the wide scope of issues the migration authorities are facing today. Thus the use of modern technology has been one of the viable solutions used by most of the notable actors on the stage of the European migration management.

One of the actors that highly values and makes the best use of the state-of-art technologies is Frontex, the European Border and Coast Guard Agency. As per the Council Regulation (EC) 2007/2004 of 26 October 2004 the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex) was established and repealed by Regulation (EU) 2016/1624 of 14 September 2016, as Frontex, the European Border and Coast Guard Agency. The core mission of Frontex is to promote, coordinate and develop European border management in line with the Charter of Fundamental

1 Corresponding author's email: Piotr.Malinowski@frontex.europa.eu

Rights of the European Union and the concept of Integrated Border Management[2].

Frontex takes an active role in variety of migratory matters, helping to identify migratory patterns, as well as trends in cross-border criminal activities by monitoring the situation at the borders and supporting border authorities in sharing information. The Agency also carries out vulnerability assessments, coordinates and organises joint operations and rapid border interventions, as well as assists EU Member States in forced returns of people and organises return operations.

In addition, Frontex supports the cooperation between law enforcement authorities, EU agencies and customs and works closely with European Fisheries Control Agency (EFCA) and European Maritime Safety Agency (EMSA) to implement multipurpose operations. In these operations, vessels and aircraft deployed for border surveillance can also be used for fishing and environmental monitoring.

In all of the aforementioned activities Frontex focuses on preventing smuggling, human trafficking and terrorism as well as many other cross-border crimes, sharing gathered intelligence with relevant entities. In doing so, the Agency acts as the centre of expertise in the area of border control by developing training curricula and specialised courses in a variety of areas. In all of these matters, Frontex encourages the use to the newest technologies available to match the latest challenges that the wide scope of migratory issues entails. In particular, the state-of-art solutions available have been indispensable and crucial for the situation monitoring purposes.

The Agency strives to become the leading source of balanced assistance to the European Commission and Member States in relation to the long-term EU Research Framework Programmes, which are relevant to border security. The Agency plays a key role in analysing existing and future capacity needs and feeding them into the planning and implementation of the EU Research Programmes. The Agency also serves as a technical advisor and support to Member States and the European Commission as well as other stakeholders. It facilitates information exchange by organising demonstrations, pilot projects, workshops and conferences.

Common application of surveillance tools - the legislative framework

The situation monitoring assignment stems largely from the Agency's tasks entrusted by the Eurosur Regulation No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur). Under Eurosur, Frontex maintains a European situational picture and common pre-frontier intelligence picture that contain information on the situation at European borders and the pre-frontier area.

Frontex is also responsible for coordinating the so-called common application of surveillance tools, i.e. Eurosur Fusion Services. At the strategic level, the EFS implementation relies on the legislative framework for the provision of the high quality Eurosur Fusion Services (EFS) – the common application of surveillance tools as per Art. 12 of Eurosur regulation (EU) No 1052/2013, the Regulation (EU) 2016/1624 on the European Border and Coast Guard and the Copernicus Regulation (EU) No 377/2014.

In addition, the EFS provision in 2018 will also be based on the Copernicus Delegation Agreement, signed on November 11, 2015 between the European Commission and Frontex, which provides for the implementation of the border surveillance component of the Copernicus Security Service. This allows Frontex to access resources both financial and technical provided by this Programme, including privileged use of Copernicus Space Component Data Access (Copernicus Data Warehouse).

State-of-the-art technology in the field of border surveillance

The vision of the Eurosur Fusion Services is to support and add value to operational activities, as well as to provide essential components to compile the European Situational Picture (ESP) and the Common Pre-frontier Intelligence Picture (CPIP) from a variety of sources, including platforms deployed under the Common Application of Surveillance Tools. In practice this means that a number of information services and data

2 See Article 77 TFEU (ex-Article 62 TEC), Article 4 of Regulation (EU) No 2016/1624, Council Conclusions of 4-5 December 2006 on Integrated Border Management (2768th Justice and Home Affairs Council meeting in Brussels).

sources (external: institutional, commercial providers; internal: Frontex systems) are bundled together into customised and integrated services. These customised services are delivered to EU Member States authorities and other partners via different communication channels, including the Eurosur network. These services are defined based on user needs in Member States and Frontex, and contribute to achieving the strategic and operational objectives of border surveillance. Frontex Fusion Services currently include 13 services with three new services still in pipeline.

The EFS makes extensive use of the satellite data with optical and radar imagery. Radar imagery is mostly used for the Vessel Detection Service where it helps to detect objects at sea. The service can be correlated with the collaborative ship reporting systems such as Automatic Identification System (AIS) and Long Range Identification and Tracking (LRIT) to identify uncooperative vessels or small boats not required to have such a transmitter. This allows operational planners to effectively allocate seaborne and airborne assets to investigate these detections and intercept vessels.

Optical data is mainly used over land to perform tasks such as verifying intelligence reports and applying change detections. This is useful to establish the man-made built ups and changes in the terrain potentially indicating departures. Both imageries data is best used complimentary to benefit from the advantages of both technologies. Over the course of last years the resolution of optical imagery has significantly increased from a few meters to 30-50 centimetres, allowing for the identification of even the smallest objects of interest. This is mainly due to military technology becoming available for civilian use and an increased number of satellite constellations becoming available to Frontex, helping further improve service capabilities.

Another area of activity where state of the art technology applies is anomaly detection. Special algorithms are applied to identify general patterns of behaviour of vessels. This allows operators to identify potentially suspicious behaviour for further analytical and decision making purposes.

The Maritime Simulation Module provides operators with a tool to compute and simulate the likely positions of vessels in distress and possible routes, taking into consideration the meteorological and oceanographic information such as wave high, current, wind speed and water temperature.

The use of modern technology would not be complete without the use of real-time data. The incorporation of the real-time data is achieved by using airborne aerial surveillance technologies through the extended use of Fixed Wing Aircrafts (FASS) and Remotely Piloted Aircraft Systems (RPAS) under the Multipurpose Aerial surveillance (MAS) service. The streamed real-time data is received from the airplane to the European Monitoring Room at Frontex premises and other dedicated coordination centres. In case of a detection, EMT experts analyse the information and alert the responsible authorities or the responsible international coordination centre - who also have parallel access to the live video stream – to take over and coordinate the proper follow-up activity. The gathered information is inserted real-time into different information exchange platforms between the Frontex, Member States and other entities (e.g. EU Agencies) concerned (to create a real-time awareness picture). It is also combined with other available data sources.

To manage and process the variety of data collected (ship data, geospatial data, reporting data etc.), Frontex requires cutting edge geographical information system (GIS) technology for data integration, visualisation and dissemination[3].

The Eurosur Fusion Services are delivered through the Frontex web-based information exchange systems adapted to fit the customer needs and reflect the user-friendly approach to service delivery. These systems are also continuously upgraded with features such as new search functionalities and more intuitive user interface.

The Eurosur Fusion Services (EFS) - service design and implementation

The Frontex Situation Centre (FSC), a unit within the Situational Awareness and Monitoring Division of Frontex, manages the design and delivery of these services. It is important to highlight that the services undergo a complete service lifecycle from service design inte-

3 Geographic Information Systems is a computer-based tool that allows to analyse and integrate geospatial data from a variety of sources and display multiple layers of information on a single map.

gration to transition and implementation. In all of these aspects continuous service improvement is the key process that ensures that the modern technologies are applied directly to the services delivered to customers.

The customer-oriented approached is achieved through the daily support of the Service Desk - Single point of contact for situational monitoring and information exchange services and products, and also through numerous user uptake activities, involving workshops, awareness sessions and other forms where valuable feedback stimulates the improvement of services.

In order to ensure that the technologies are applied in the best way to fit the operational environment the EFS Service Managers who are dealing with the direct service implementation in the Member States provide detailed hands-on trainings to the users. In order to make the best use of technologies for training purposes, Frontex also benefits from remote training options via video-conferences, video tutorials and e-Learning platform.

Services and their newest capabilities are tested and tried in the real operational environment during the EFS exercise campaigns to ascertain the service quality and possibilities of use cases through combination of different service combinations. During the recent years the exercises were organised and services tried in all major sea regions from Atlantic, through Mediterranean, Black and Baltic Sea, as well as in the external land border sections most affected by migration. All of these efforts demonstrate the intent to ensure that the technologies used are up-to-date and reflect the best use of services for purposes of the situational monitoring.

Conclusions

Frontex's vast experience demonstrates that the use of modern technology is indispensable for ensuring that migratory management is efficient and addresses contemporary challenges.

The Eurosur Fusion Services (EFS) are all about continuous expansion and enhancement of the existing capabilities with the state-of-the-art technology and widening the range of information and data fused and provided to Frontex customers. In that respect, Frontex closely cooperates with other Agencies, making use of service contracts and products already available to avoid duplication and receive best value for money.

The continuous service improvement lifecycle is key to ensure that the modern technologies applied in the migratory management field are still valid and reflect the current technological achievements. The crucial part of this is the availability of information on the latest technology progress in the field.

Frontex plays an active role in exploring the newest innovations and tools offered and is a regular participant in the technology expositions and conferences related to its potential use for the border management purposes.

Ever since its launch in 2014, and full operationalisation in 2015, the EFS have facilitated situational awareness of Member States and other Frontex stakeholders. Over the last 4 years, the number of EFS service users has significantly increased.

The services offered to the Frontex stakeholders via EFS are dynamically evolving in response to users' needs, feedback and latest available technical solutions. For Frontex, the service evolution stands for the improvement of the existing service capabilities, e.g. infrastructure upgrade and decreased time of service delivery. Few years ago it was unimaginable to have a high resolution imagery detecting object of less than 1m, and now such imagery is delivered on a day-to-day basis.

Following the increased demand for higher resolution and better quality, Frontex motivates and drives commercial suppliers to strive for success in the field of research and innovation. In doing so, Frontex serves as a linkage between research (and development) community, end users and policy makers involved in border management issues to ensure that the challenges faced at the EU borders are duly tackled. Therefore, the Agency not only stays abreast of the latest border surveillance technology, but also constantly looks into the future to identify opportunities for further development.

References

Official documents

- Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur) [2013] OJ L295/11
- Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC [2016] OJ L251/1
- Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010 Text with EEA relevance [2014] OJ L122/44
- Treaty on the Functioning of the European Union (Consolidated version 2016), [2016] OJ C 202.

Reflections on the Triple-Helix as a Vehicle to Stimulate Innovation in Technology and Security – a Belgian case study

Marleen Easton
Department Public Governance & Management, Faculty of Economics and Business Administration, Ghent University, Belgium[1]

Abstract
In this contribution the main argument is that a triple helix collaboration between industry, government and knowledge institutes can be a vehicle to stimulate innovation and technology in the field of safety and security. To underpin this argument the significance of the evolution from a state model to a triple-helix model is described as well as the paradigm of open innovation that is a necessary condition for the triple-helix model. Relying on experiences since 2014 with the Belgian Innovation Centre for Security reflections are made on the dynamics of the triple-helix collaboration taking into account its creation, objectives, ambition, methodology, partners and funding. Some of the (perceived) barriers encountered and logics used by government, as one of the 'hesitating' participants in the triple-helix collaboration, are further discussed.

Key Words: triple-helix, innovation, technology, security, safety, Belgium

Introduction

In Europe and indeed around the world, the security sector is seen as one of the sectors with the most potential for growth in employment and turnover (BVBO, 2012; CoESS, 2013). Over the past decade, safety and security issues have undergone a fundamental change. Supervisory and surveillance tasks are ever more rapidly evolving towards traditional on-site surveillance by deploying security staff with mobile security, which are backed up by technological and electronic equipment (CoESS, 2013). The traditional 'system and technology solutions' consisted of cable laying, camera positioning and routine surveillance service planning. Nowadays, when it comes to supporting businesses with their security challenges, there are high expectations with regard to securing the cloud and handling Big Data and smart solutions (mobile and integrated) (Marti, 2011). In a large-scale survey of 28 EU Member States, Bosnia-Herzegovina, Macedonia, Norway, Serbia, Switzerland and Turkey, conducted by the Confederation of European Security Services (CoESS), 92.31% of respondents said they expected to see positive growth in technological applications in the safety and security markets. According to 92.31% of the respondents, there will be solid growth in pooled technology, ICT and security staff services, whereas according to 53.85%, the traditional security and surveillance market will shrink, thus appearing to be in decline.

1 Director of the research group 'Governing & Policing Security'. In 2014 she took up the presidency of the Innovation Center for Security to pursue a nexus in the field of innovation, technology and security. Since 2017 she is also Adjunct Professor at the Griffith Criminology Institute at Griffith University in Brisbane, Australia.

In recent years, the field of security in Belgium has seen a great many technological initiatives and innovative developments. For example, several local police forces have taken the initiative to deploy new technologies such as ANPR (Automatic Number Plate Recognition), drones and/or unmanned cameras. These initiatives typically begin as a local initiative, which results in a much broader spread. On the one hand, this is positive, because it reveals the flexibility of local police forces when it comes to technology and innovation. On the other hand, however, it is a drawback, because the initiatives' local character does little in the way of encouraging the technological and innovation learning process among other police forces. Fire services are embracing innovation too, turning to 'smart' clothing, which integrates sensors and communication devices into the protective clothing, or experimenting with the potential to deploy drone technology during fire-fighting events. The opportunity to stimulate cross-sector innovation is not being fully exploited. In other words, too little knowledge is being exchanged within and between organisations (Easton & Dormaels, 2016).

It is worth noting that a great many of these security-related initiatives take shape through bilateral partnerships. These are largely local security actors from the public sector who partner with private sector actors, businesses which generate new products and services in the fields of technology and innovation. One example would be the police zone of MidLim (As, Genk, Houthalen-Helchteren, Opglabbeek, Zutendaal) which partnered with a drone company and became the first zone to deploy drone technology. Rarely in Belgium do partnerships arise involving the state, industry and academia when it comes to innovation and technological development in the field of security (Dormaels & Easton, 2016).

One exception to this is the Innovation Centre for Security, the non-profit organisation INNOS[2], which was established in 2014 and acts as a Belgian intermediate organisation that stimulates innovation and technology partnerships between industry, government and knowledge institutes in the field of security. The interaction among these three actors forms the foundation of the triple-helix model. Below, we explain the significance of the evolution from a state model to a triple-helix model (2). Then, we go on to outline the paradigm of open innovation as a necessary condition for the triple-helix model coming to full fruition (3). We also take a close look at the complex workings of the triple-helix model (4). After that, we describe the creation, objectives, ambition, methodology, partners and funding of the Innovation Centre for Security in Belgium. Finally, based upon our experiences[3] at the innovation centre, we reflect on the triple-helix as a vehicle for spurring on innovation and technology in the field of security.

The evolution from a State Model to a Triple-helix Model

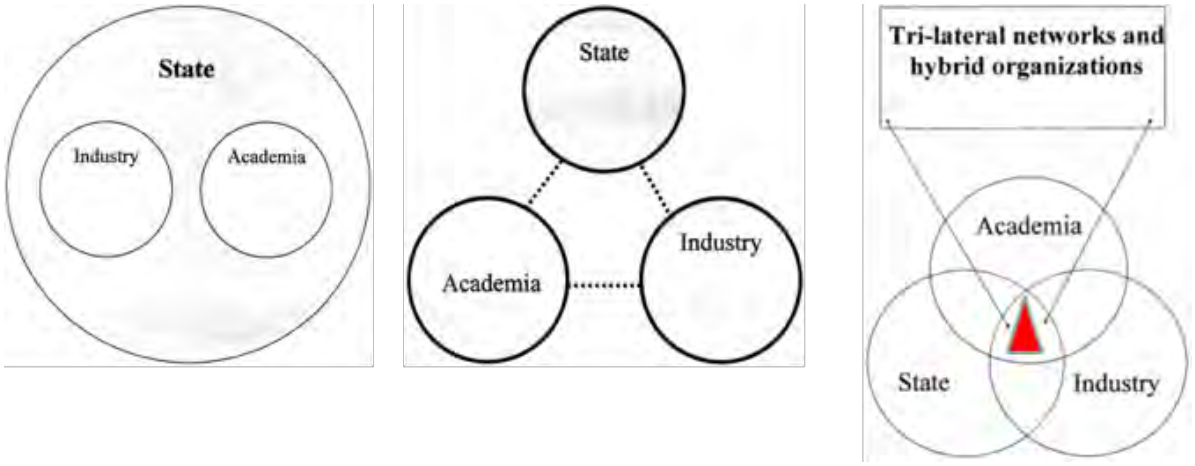
When we consider the models available to us on the creation of technological innovation, we come across the triple-helix concept, which made its debut in the 1990s and was introduced by Etzkowitz and Leydesdorff (Etzkowitz, 1993; Etzkowitz & Leydesdorff, 1995). The concept has been described as: 'The interaction among university, industry and government.' (Etzkowitz, 2008: 1) and can be situated on the evolutionary line from *state model* to *laissez-faire model* to *triple-helix* model, which is depicted in Figure 1 below and briefly explained thereafter.

The most significant institutional pillar of the so-called state model is government, to which industry and knowledge institutes are subordinate. The government governs relations between these actors and takes the lead in any projects or new initiatives. These institutional spheres are a fair distance apart. The downside to this model is the lack of bottom-up initiatives, which stifles innovation. In the laissez-faire model (middle of the illustration above), the government, industry and knowledge institutes operate autonomously and independently of each other. In other words, there are clear boundaries, as a result of which interaction, and therefore innovation, is limited. The triple-helix model (to the far right in the illustration above), implies cooperation and interaction between knowledge institutes, industry and government. The purpose of this intensive cooperation is to promote innovation and, through a mutual exchange of knowledge and experience, bring about economic growth. As a consequence of this, the model provides a means by which to analyse innovation in a knowledge economy. In addition, it can also be seen as a workable model for steering processes of innovation (Etzkowitz & Ranga, 2013).

2 www.innos-center.be

3 This experience consists of four years of participation in the functioning of the Innovation Center for Security (vzw INNOS) as president (Marleen Easton) of this non-profit organization.

Figure 1: Evolution from a state model to a laissez-faire model to a triple-helix model (compilation of models from Etzkowitz, H., 2008).



At the heart of the triple helix lies the issue of constructing an entrepreneurial state in which knowledge institutes, industry and government can jointly innovate in response to current economic challenges in any number of policy areas. The triple-helix concept is underpinned by the thesis that in a knowledge economy the potential for innovation and economic development resides in the interaction between knowledge institutes, government and industry. That very interaction, the model's Achilles' heel, is seen as the source of new, innovative organisational forms and social interactions, which stimulate the production, transfer and application of knowledge (Ranga and Etzkowitz, 2013:239).

The triple-helix partnership is also thought to have the potential to resolve the so-called 'innovation paradox'. The paradox exists in the sense that knowledge institutes' research activities do not align with private sector innovation needs (SERV, 2011; Flemish Government, 2014:13). Indeed, the same paradox exists in respect of public sector needs for innovation. The paradigm of open innovation is thus essential for spurring on interaction between the three institutional spheres (government, industry and knowledge institutes).

The Paradigm of Open Innovation

A precondition to a full appreciation of the triple helix is the paradigm of open innovation. '*By open innovation we mean close collaboration by all stakeholders (businesses, citizens, universities, financial institutions and other intermediate organizations) in addressing a business and social opportunity or challenge. Engaging with each other through multiple channels and pooling their internal resources; including knowledge, finance, people, markets and data.... It is about co-innovating and co-creating.*' (Anderson & Hutton, 2013:4). Chesbrough[4] (2006:15) argues that 'open innovation' deserves its status as a new paradigm because external knowledge is employed; because there is a new perspective on successful innovation (not merely organisation-specific) and because intermediate organisations have emerged and other measurement tools have been developed to monitor an organisation's innovation.

In other words, open innovation is about sharing knowledge (= power) in partnership and in interaction with others. It is about open interaction between disciplines, sectors, organisations and professions. The 'boundaries' are, as it were, deliberately exceeded. A process is put in place which is at once practically oriented and theoretically based, and this brings us to what is known as 'evidence-based co-created public policy'. The ability to develop this rests on active commitment of the stakeholders and partners involved, a commitment of resources (personnel, money, equipment and infrastructure) and high-quality employees and leaders/managers, who are able to set up the networks[5].

4 Chesbrough Henry is executive director Center for Open Innovation, Walter A. Haas School of Business, University of California, Berkeley, USA.

5 www.biginnovationcentre.com

Mutual confidence is crucial to bringing all of this about in practice. Given that the parties in the triple helix (government, industry and knowledge institutes) each have their own structural and cultural identity, it is important that they get to know one another, demonstrate mutual understanding and communicate clearly. Moreover, a shared interest is needed to create and maintain a 'balanced' triple helix at the very least (Smits, 2011).

Europe also encourages the concept of 'open innovation', and even takes it a step further with its 'open innovation 2.0', which rests on a Quadruple Helix Innovation Model. In addition to government, industry and knowledge institutes, the quadruple helix involves citizens. The end users are involved at the start of the innovation process to create a stronger impact (including societal impact), or this is the idea at any rate. In other words, it is not just about open innovation, but about participative innovation. This sort of participation takes shape in the so-called Living Labs, in which a *public-private-people* partnership (PPPP) is created and social innovation is considered alongside technological innovation[6]. But whether and how the impact will be felt in practice is very much a matter of wait and see. Keeping a healthy critical eye on the process seems absolutely appropriate here. After all, the triple helix's workings are complex. In the following section we consider a few of the model's core dynamics.

The Workings of the Triple-helix Model

Figure 2 below introduces the complex workings of the triple helix. We introduce a few of the main dynamics, but the list is by no means exhaustive. Etzkowitz makes a distinction between circulation at the macro level (between actors) and at the micro level (within each institutional sphere). The first form leads to partnership, projects and networking between the actors involved, whereas the second consists of output from each individual actor (Etzkowitz, 2007: 8). In other words, it requires circulation of flows *within* and a circulation of flows *between* universities/knowledge institutes, industry and government. Below, we focus on circulation of flows between the actors involved, in that our contribution is about the stimulation of interaction between these actors.

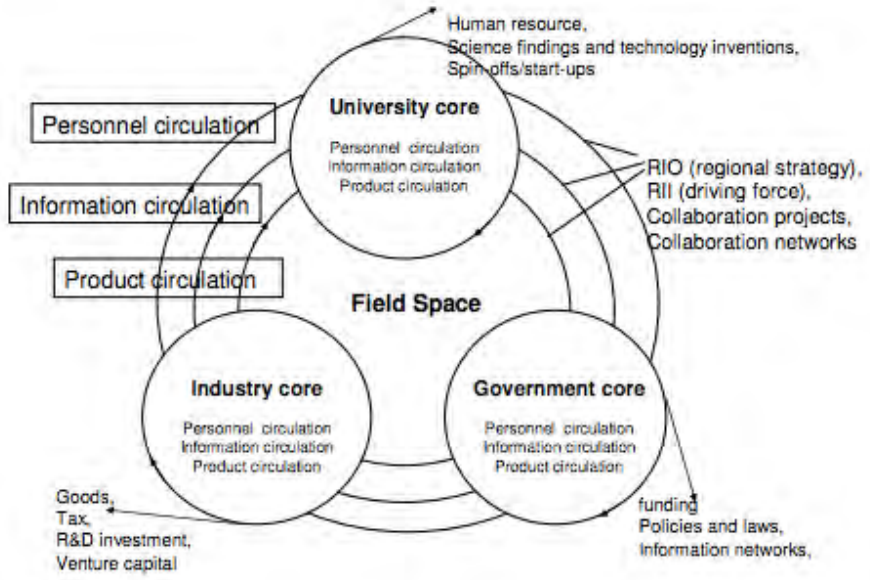
6 https://ec.europa.eu/digital-agenda/en/open-and-participative-innovation

If we zoom in on the workings of the triple helix, Figure 2 tells us that the circulation of people, information and output is a crucial factor in generating interaction between the actors (Etzkowitz, 2007).

The triple-helix model recognises the importance of people (academics, policy-makers, students, entrepreneurs and business angels) as individual innovators. Within this model Ranga and Etzkowitz draw a distinction between the innovative organiser and the enterprising academic, among others. The innovative organiser takes a key position in one of the institutional spheres and exerts the influence needed to bring government, industry and knowledge institutes together. He or she takes the initiative to coordinate top-down and bottom-up processes, initiatives and stakeholders, with a view to developing new ideas, promoting economic and social development and winning support for accomplishing innovations (Ranga and Etzkowitz, 2013:242). The enterprising academic seeks to harmonise the research activities with the needs of the market and government. This results, among other things, in the establishment of spin-off organisations and sale of patents, but also includes the accumulation of knowledge about how technology impacts organisational processes (Ranga and Etzkowitz, 2013:243). In other words, the enterprising academic offers a response to the aforementioned innovation paradox.

It is clear that individual innovators (innovative organisers and enterprising academics) step outside of their traditional roles, which are linked to their institutional context, whether it be industry, government or knowledge institutes. This is precisely why the boundaries between the actors involved become blurred in this sort of triple-helix partnership. In any event it facilitates better circulation of people, ideas, knowledge and capital. This openness stimulates flexibility, creativity and innovation (Ranga and Etzkowitz, 2013). Specifically, the circulation of people can be achieved in several ways. It can be done through a permanent shift from one sphere to another. A professor, for example, can become a full-time business entrepreneur. What's more, there is also the potential to combine two positions, for example to have a part-time or full-time appointment at a university, along with a part-time position in industry or government. For example, a practitioner might be appointed part-time to a university to conduct research or prepare his or her doctoral dissertation. It could also happen that a person transfers to another sphere where he or she enjoys relative success before returning to his or her

Figure 2: Triple helix circulation (Etzkowitz, 2007:9).



previous position. According to Ranga & Etzkowitz this dynamic can break down 'parochial thinking' and generates empathy within the triple-helix model.

At the same time, this blurring of the boundaries can be a source of conflict, particularly from the demands which stem from a traditional perspective on roles within an institution's own context. At universities, for example, professors are judged on their publications and funded research projects, and not so much on the relationships they develop with other disciplines, businesses and government based on their expertise. On the other hand, it is about the traditional government view of partnership with industry, and the limitations that government experiences in this form of partnership as a result of the public procurement legislation. Finally, seeing the direct added value and return on investment through partnership with government and knowledge institutes is a challenge for many businesses.

Figure 2 also clearly illustrates the need to actively stimulate information flows between the actors in the triple helix. This is because partnership relies on communication and information. Nowadays information and communication technologies provide a wealth of opportunities to share information and stay up-to-date on potential new developments. These information networks must be actively set up in the triple helix (Etzkowitz, 2007: 10). An organisation's traditional seminars, workshops and newsletters are a valuable start, but more intensive forms of exchange based on specific software, Dropbox, WeTransfer or email are sorely needed. It is essential that these flows be organised and maintained. After all, they do not appear of their own volition.

Finally, the exchange of output is important. This deals with the outcome of a partnership. Output must, by necessity, create a win-win situation for every actor involved. Moreover, equivalent contribution to the outcome is fundamental: '*If there is a negative imbalance in contributions; a gap might appear in innovation: conversely a positive imbalance might stimulate other actors to increase their efforts.*' (Etzkowitz, 2007:10). In light of the preceding information it is vital that freerider behaviour in these partnerships be avoided at all times. It is, in and of itself, a challenge to find ways of preventing this behaviour.

To facilitate the circulation of people, information and output, Ranga & Etzkowitz tell us that space is required for knowledge development, innovation and consensus (Ranga & Etzkowitz, 2013). *Space for knowledge* is created when knowledge institutes and resources are in adequate supply. These can throw up technological ideas and fuel regional development. *Space for innovation* implies that knowledge institutes, governments and businesses exchange skills and knowledge on a regular basis,

which can result in innovative new ideas. Specifically, this could be set up in a science park, a cooperative research group or a centre for excellence in a particular field. H-STAR, at Stanford University, is a specific example of this (http://hstar.stanford.edu). As an interdisciplinary research institute it aims to serve as a crossroad for people, expertise, projects and programmes that blends human sciences with research and innovation in information technology. In this innovation space the development of a separate Triple Helix organisation has a major role to play in bringing knowledge institutes, governments and businesses together. This institute can set up, manage and encourage subsequent cooperation between the three actors. *Space for consensus* implies that each party involved is assured of the partnership's benefits and added value. This is because the actors must have an interest in common if a balanced triple helix is to be created. The outcome must be a win-win situation for everyone. In addition, the presence of a sense of urgency is a prerequisite to achieving a productive partnership.

These 'spaces' are not formed the same way in every policy domain, region or country and are often triggered by the local or regional needs specific to the relevant actors partnering in the triple-helix model. These needs reveal the actors, relationships, resources and new institutional forms required. The creation of a triple-helix partnership thus depends to a considerable degree on the actors' motivation to participate in joint projects, which is easier said than done. It calls for a seismic shift in an organisation's way of thinking. '*This is not an easy process, as setting joint agendas often involves a major change of vision, crossing organizational silos, thinking beyond the boundaries of a single institutional sphere, harmonizing institutional and individual objectives, resources and cultures, etc.*' (Ranga & Etzkowitz, 2013).

The Innovation Centre for Security in Belgium (INNOS vzw)

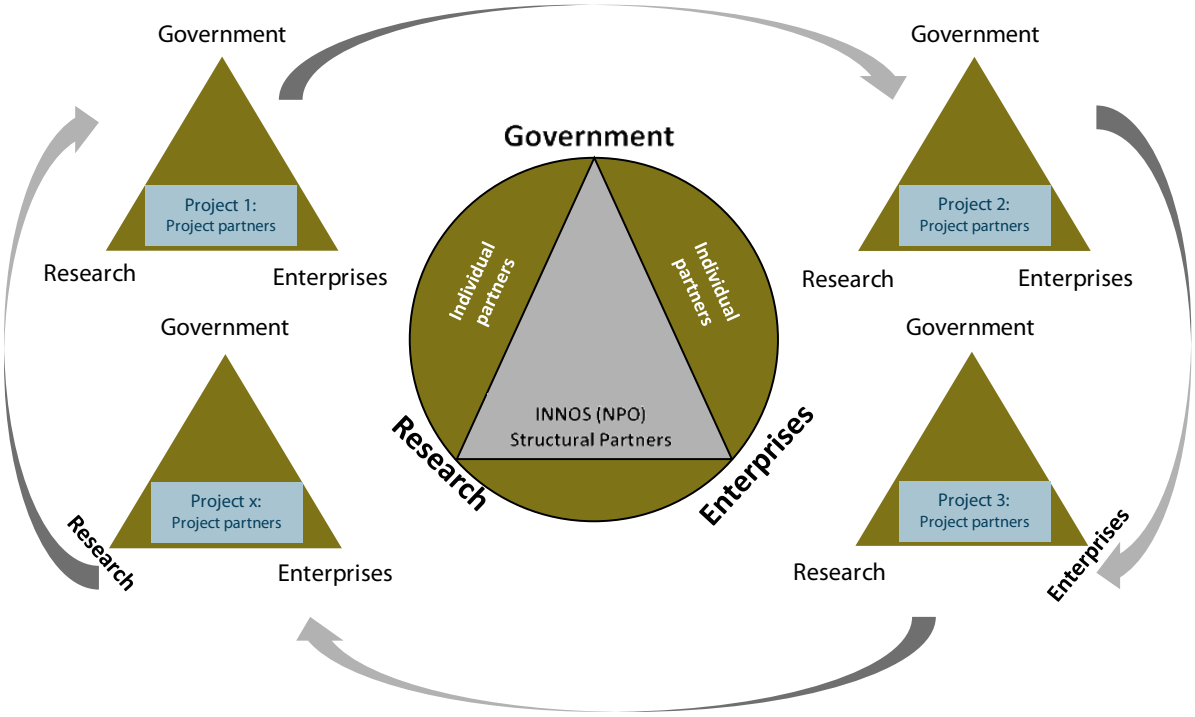
INNOS was set up as a non-profit organisation on 28 July 2014, by individuals from the private sector, the public sector and knowledge institutes, i.e., the so-called partners in the triple-helix model. In practice, Securitas and Betafence joined forces with the support of the West Flanders Development Agency, the Provincial Security Services Training Centre (POV, Zedelgem) and local police, represented by the chiefs of police in the local Westkust and Ypres police zones. The initiative also received support from knowledge institutes from Prof. Dr. Paul Ponsaers of the Centre for Police Studies (CPS), Evelien De Pauw (VIVES) and Prof. Dr. Marleen Easton (Ugent).

These partners came together through a desire to help find an answer to three obstacles to technology, innovation and security in Belgium (Dormaels & Easton, 2015a, Dormaels, Moons, Easton, 2016). The first of these obstacles being the observation that, irrespective of the field, society is reluctant to accept new approaches, products and technologies. In other words, an effort has to be made to get innovations established, a point against which the field of security is not immune. A second sticking point is the observation that Belgian businesses (including the security sector, with a few exceptions) tend to be very conservative, so that innovation is fairly scarce and no (national) strategy has been developed to book progress in this area (Haïd, 2014). A third difficulty is the observation that the actors in the field of security are often short on market insight, with the result that current technologies are under-exploited, as are opportunities for innovation. Public sector actors, for example, are not always aware of how recently developed technologies from the private sector can optimise their work processes, in managing information flows, for example.

INNOS has set itself the goal of responding to the fundamental security challenges in the area of new technologies, social innovation and integrated security. The Innovation Centre runs projects to simplify the introduction of innovative products, services and applications. In this way a contribution to the development of knowledge and a contribution to the development of the economy take place simultaneously. Finally, INNOS contributes to the social and economic clout of the public/private security sector, while at the same time bringing greater efficiency to the security actors' collective pursuit of a safer society (Dormaels & Easton, 2015a). INNOS vzw was not however set up for commercial purposes, nor does it broker contracts between government and industry. INNOS occupies an explicitly intermediate role in the heart of a triple-helix model, which is geared towards interaction between governments, businesses and knowledge institutes. The diagram below illustrates the network structure which arises as a result.

Based on this interaction, the innovation centre unites knowledge and needs in the field of safety and security, and multidisciplinary knowledge and innovation projects are produced in the fields of new technologies, social innovation and integrated security. In this

Figure 3: INNOS as a triple helix network organisation



manner, INNOS combines the expertise of each of its partners and generates a win-win situation for all those involved (Dormaels & Easton, 2015b). In its first two years of operation, INNOS has shown that triple-helix projects can yield good, innovative solutions. For example, INNOS created an ad hoc command post during the administration of the First World War commemorations in Nieuwpoort (Dormaels & Easton, 2015 and 2016)[7]. The method was found useful not only for the commemorations, but also for security in relation to other events, such as the Tomorrowland festival (Barco, 2016) and E3 Harelbeke cycling race (Noppe, Dormaels & Easton 2016). Additionally, INNOS deals with the exchange of knowledge and identification of needs. For example, it organised a seminar on critical infrastructure security and a seminar involving workshops designed to stimulate interaction between industry, government and knowledge institutes in the areas of technology, innovation and security (Dormaels & Easton, 2015a). In other words, INNOS has a very wide range of activities.

The *'Triple-helix DNA'* is crucial in the work of INNOS. This means that partners are drawn from each of the institutional spheres (industry, government and universities) for every activity. For example, in the aforementioned ad hoc command post, multiple sources of information (mobile camera images, helicopter images, radio communication, social media data) were exchanged in real-time between the Westkust and Ypres police zones, the Federal Crisis Centre and several emergency services, such as the fire service and emergency medical services. At the same time, the knowledge institutes went on to study how this exchange of information affected the information flow, Dormaels & Easton (2015c). If an activity does not meet the 'Triple-helix DNA' criteria it is passed over and will undoubtedly go to another organisation within the field of security.[8] In other words, the triple helix is the common thread uniting the INNOS network. The am-

7 VIPs from 83 countries were invited to this international ceremony. The project resulted in the creation of an ad hoc command post, which was set up on a piece of land in the ceremony's vicinity. The expertise and partnership between Barco, Securitas and the police services led to an innovative solution. Several sources of information (mobile camera images, helicopter images, radio communication, social media data) were exchanged in real time between the Westkust and Ypres police zones, the Federal Crisis Centre and between various emergency services, such as the fire service and emergency medical services.

8 The members of the INNOS Board of Directors decided that the 'Commemoration of the Battle of Waterloo' did not qualify as an innovation project because it did not satisfy the conditions for a triple-helix partnership. The management role lay squarely with a private organiser, government participation had not been finalised and the project involved no added value from knowledge institutes' input.

bition is to become the point of reference for technology, innovation and integrated security by 2020.

At start up, INNOS vzw was unable to rely on government funding with the exception of individual membership by the West Flanders Development Agency. The first two years of operation were funded almost exclusively by the private sector. Through structural funding, Securitas, Betafence and Barco made it possible to set the organisation up in the first place. Although these companies conceived the idea of the innovation centre alongside representatives from government and the knowledge institutes, they also bankrolled the staff in order to make the centre a reality. Thus, the non-profit organisation INNOS was created from the bottom up, without state support.

Below, we reflect on the specific workings of the triple helix and the questions it generates, with reference to our experience at the Innovation Centre for Security over the last two years. We devote the greater share of our attention to the government point of view, because this partner is often 'hesitating' and 'holding back' from participating in this initiative.

Reflections on the Belgian triple-helix cooperation

A major reason for the government to withhold support from the INNOS non-profit is partially due to the complex structure of the Belgian state, which gives a great many government authorities the potential to play a role in the realm of technology, innovation and security. The federalisation of Belgium has turned innovation policy (to name but one of many factors) into a patchwork of programmes and initiatives. Added to this is the complexity involved in the process of actually steering security policy, with powers delegated to the federal state, the regions, communities and local authorities. This is because federal, regional, subregional and local authorities are saddled with the responsibility of security in Belgium, in which they are confronted with the future challenges of technology and innovation. There are a number of federal public services (FPS) involved, such as the FPS for Information and Communication Technology, the FPS Interior, FPS Justice, FPS Mobility and Transport and the Ministry of Defence. Moreover, each of the local mayors is responsible for the administration of his or her local police service and emergency relief zone (fire service) and has special powers when it comes to the enforcement of public order. The Flemish Government also has powers in the area of innovation, exercised by a minister who is also responsible for employment, economy and sport.

A partnership between industry, government and knowledge institutes also touches on the relationship between market and government. A so-called 'entrepreneurial state' is needed to enable innovation and entrepreneurial spirit and to keep it going in the long term. This also applies to the policy domain of security and to the various authorities with security powers in that domain within the Belgian state structure. At first sight there is no easily identifiable entity to take up the gauntlet. Belgium has a need for an entrepreneurial and, perhaps more importantly, networking government, one that can make itself felt at the central and decentralised levels alike. Moreover, it fits in seamlessly with the network structure which is central to the current activities of INNOS.

Given that Belgium currently does not have an entrepreneurial, networking government (read: combination of different administrative levels), which profiles itself in the domain of technology and innovation in the field of security, bottom-up initiatives such as INNOS vzw, which is primarily funded by the private sector, are viewed with a certain degree of suspicion. The question is often raised, and rightly so, as to whether INNOS is supply-driven or demand-driven. To put it another way, the question is one of whether INNOS facilitates the placement of new services and technology on the market for business by creating needs among end users, or whether innovation arises from needs among end users, which then translate into innovation projects. In order to answer to this question it is often speedily assumed that because INNOS is largely privately funded it must surely exclusively pursue economic profit on the basis of supply-driven operations. However, this assumption overlooks a number of elements.

Although INNOS does not receive structural funding from the government, the Board of Directors does reflect the 'triple-helix DNA'. This means that the Board of Directors is composed of private partners and representatives from the local police, fire service and knowledge institutes. The nature of this composition is crucial in answering any question in relation to supply-driven or demand-driven innovation. This is because the composition of the Board of Directors

ensures that innovation is demand-driven, on the basis of societal challenges in the field of security, and not 'merely' supply-driven to create a sales market for existing technology. The 'triple-helix DNA' indeed means that a balance is sought between the two, and it is found in the pursuit of win-win scenarios for industry, government and knowledge institutes. If a business is uncomfortable with this, it is asked to refrain from participating in the triple helix. As are governments and knowledge institutes that are uncomfortable with the idea of bringing to the market the results of innovation projects with which they are involved.

One specific example of a demand-driven innovation project is the INNOS pilot project. INNOS brought government, industry and knowledge institutes together in response to the specific needs expressed by the Westkust and Ypres police zones. Barco and Securitas were responsible for setting up an ad hoc command post by employing 'open' technology applications, in which various ICT platforms and CCTV systems were integrated. This project was accomplished in a period of six weeks. This type of result is only possible when businesses are given a clear understanding of the needs of government and are prepared to incorporate existing applications and services into a single final project. In this manner a balance was found between demand-driven and product-driven innovation.

The significance of these demand-driven projects should not be underestimated. In such cases the success of an innovation project cannot only be measured in terms of the pure economic return for the private partners alone. Indeed, it also includes improved service (e.g. decisions taken and communicated more rapidly) or a justification in terms of personnel or resources. An evaluation of the pilot project, for example, shows that the use of technology brings personnel savings of about 25%. In other words, the pursuit of innovation not only requires an investment by the party requesting it, it can also pay that party back. In this case, police capacity can be freed up for other tasks and redirected towards service (or better service) for the population. It also immediately justifies government investment in innovative solutions and offers a clear return on investment.

This is why it is so important for government to come to the table and help identify the challenges that face the field of security, for which innovative solutions must be sought. When government participates in the innovation process, often as an end user, it becomes a co-owner of the innovation process. This means that innovations can be set up and tested more rapidly through projects, and that the effect of the technology on the regulatory framework can be more readily identified. It leads to a quicker implementation of technology and innovation in response to security issues. As a result, services are more extensive, come to market sooner and contribute towards security solutions. The mission to simulate better security in society through a triple-helix organisation will then contribute indirectly to economic growth.

The operation of INNOS shows that co-investment is needed from government and industry, and that a return on investment is needed by both parties if the initiative is to create and retain its credibility over the long term. Our experience at INNOS puts into perspective the notion that in Europe (Mazzucato, 2013) there is too much 'state', not enough market and a lack of entrepreneurial culture. The Innovation Centre for Security was created from the bottom up by the entrepreneurial culture of the actors involved and with the majority of its financial support derived from a few businesses. It is now up to the government to show its entrepreneurial spirit at various levels of the Belgian state structure, and to take up the gauntlet too, to give the triple helix a better chance in the long term. This implies funding, but it also implies involvement and open dialogue with all partners. After all, it is a way of shaping the current and future challenges in technology, innovation and security.

Our experience in the setting up of specific projects through INNOS has taught us that action on specific challenges and issues can only be taken if a certain degree of harmonisation is reached in the awareness, motivation, methodology and rewards available for each of the actors involved. This piece of the puzzle must fit if we are to generate real impact in technology and innovation in the field of security. There is also no single actor that should take up the gauntlet alone to face this challenge. Our experience has shown us that where there is a will, there is a way that will lead to innovation.

Where budget is concerned, the triple-helix logic faces a serious challenge in the future. It is not so much to do with the available amount of budgetary room for manoeuvre, it is more to do with a recurrent budget being obtained that covers basic funding: a budget

with a balanced composition, based on the membership of the triple-helix partners (government, knowledge institutes and private businesses), which are seen as its founding partners. From this platform, additional funding can be sought in relation to specific issues, for which projects will be set up.

To conclude we are aware of the fact that there is a need for more comparative international research to get insights on the true added value of the triple-helix model for stimulating innovation and technology in the field of security. The study of the rise, the goals, the ambitions, the work processes, the partners and the funding of different initiatives in different nations can teach us something about the impact of politics and socio-economic conditions on the development of triple-helix collaborations around the world. Possible initiatives to be studied are the Dutch Institute for Technology, Safety and Security; the Safety Lab in the West Cape in South Africa and the Australian Research Council Centre of Excellence in Policing and Security to name a few. This kind of research can generate a more solid answer to the question whether the triple-helix can be a vehicle for stimulating innovation and technology in the field of security and what the necessary conditions and possible dynamics are.

References

- Barco (2016) *Mobile, networked visualization system helps keep festival-goers safe.* Available from: https://www.barco.com/en/References/2016-02-08---International-music-festival-Belgium.aspx BVBO vzw (2012). Figures and information 2010/2011.
- Chesbrough, H. (2006) *Open Innovation: Researching a New Paradigm*. Oxford: Oxford University Press.
- CoESS General Secretariat (2013) *Private Security services in Europe. CoESS Facts and Figures 2013*.
- CoESS General Secretariat (2015) *The new security Company: integration of services and technology responding to changes in customer demand, demography and technology*.
- Dormaels, A. & Easton, M. (2015a) Innovation Center for Security (vzw INNOS). (Inter)nationaal referentiepunt (Innovation Center for Security: an international point of reference). *West-Vlaanderen Werkt. Themanummer de veiligheidsindustrie*, 2 (57), 7-8.
- Dormaels, A. & Easton, M. (2015b) Triple helix netwerken (Triple helix networks). *Lead@Pol*, 11(1), 4-7.
- Dormaels, A. & Easton, M. (2015,c) *Rapport Pilootproject INNOS: Installatie Commandopost ad hoc. Herdenkingsplechtigheid 28/10 - politiezone Westkust (Final report pilot project: ad hoc command room to secure the commemoration of WOI)*.
- Dormaels, A., Moons, S. & Easton, M. (2016) *Projectaanvraag Flanders Innovation Safety Security Network (Flanders.ISSN). Aanvraagtemplate innovatieve bedrijfsnetwerken (fase 2) ingediend bij het Vlaams Agentschap Innoveren en Ondernemen (VLAIO)* (Project application Flanders Innovation Safety Security Network (Flanders.ISSN). Application Template for innovative business networks (phase 2) submitted to the Flemish Agency for Innovation and Entrepreneurship (VLAIO)).
- Dormaels, A. & Easton, M. (2016) Het Innovatiecentrum voor Veiligheid (vzw INNOS) bestaat 2 jaar: enkele reflecties. In: M. Easton, A. Dormaels & E. De Pauw (Eds.) (2016). Innovatie, veiligheid en technologie. Partnerschap als katalysator? Special Issue No.75, *Orde van de Dag*, september 2016, Mechelen: Kluwer.
- Easton, M. (2013) Managing Innovation in Public Policing. In Bruinsma, G., Weisburd, D. (Eds.), *Encyclopedia of Criminology and Criminal Justice* (ECCJ), New York: Springer.
- Easton, M. (2015) Het managen van innovatie door een netwerkende publieke politie: de triple-helix als vehikel. In: Ponsaers, P., Bruggeman, W., Easton, M., Lemaître, A. (Eds.) De Toekomstpolitie. Triggers voor een voldragen debat. Antwerpen: Maklu.
- Easton, M., Dormaels, A. & De Pauw, E. (eds.) (2016) Innovatie, veiligheid en technologie. Partnerschap als katalysator? Special Issue No.75, *Orde van de Dag*, september 2016, Mechelen: Kluwer.
- Easton, M. & Van den Borre, A. (2016) Interacties tussen technologie, innovatie en veiligheid: in de greep van diverse krachten. In: M. Easton, A. Dormaels & E. De Pauw (Eds.) Innovatie, veiligheid en technologie. Partnerschap als katalysator? Special Issue No.75, *Orde van de Dag*, september 2016, Mechelen: Kluwer.
- Etzkowitz, H. & Leydesdorff, L. (2000) The dynamics of innovation: from National Systems and "Mode 2" to a Triple Helix of university – industry – government relations. Research Policy 29 (2), p. 109-123. Accessed at http://www.chss.uqam.ca/Portals/0/docs/sts8020/(20)Etzk-Leides.Triple.Helix.pdf

- Etkozwitz, H. (2007) University-Industry-Government: The Triple Helix Model of Innovation. Asia-Pacific Tech Monitor 24 (1), p. 14-23.
  Accessed at http://www.eoq.org/fileadmin/user_upload/Documents/Congress_proceedings/Prague_2007/P roceedings/007_EOQ_FP_-_Etzkowitz_Henry_-_A1.pdf
- Etzkowitz, H. (2008) The Triple Helix: university – industry – government. Innovation in action. New York: Routledge
- Etzkowitz, H. & Ranga, M. (2013) Triple Helix systems: an analytical framework for innovation policy and practice in the Knowledge Society. Industry and Higher Education 27 (4), p. 237-262.
  Accessed at https://www.academia.edu/4807351/Ranga_M._and_H._Etzkowitz_2013_Triple_Helix_Systems_An_Analytical_Framework_for_Innovation_Policy_and_Practice_in_the_Knowledge_So ciety_Industry_and_Higher_Education_27_4_237-262
- Haid, M. (2014) VBO-analyse. Focus Conjunctuur: Te veel onzekerheden verhullen een veelbelovende toekomst.
  Accessed at http://www.vbo-feb.be/globalassets/actiedomeinen/europa/europa/europa-aan-de-jongeren/focus-conjunctuur-november-2014.pdf
- Marti, C. (2011) *A survey of the European security market. Economics of Security Working Paper 43*, Berlin: Economics of Security.
- Mazzucato, M. (2013) *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*. London: Anthem Press.
- Noppe, P.J., Dormaels, A. & Easton, M. (2016) *Evaluatie commandopost ad hoc Record Bank E3 Harelbeke (Evaluation Command Post ad hoc Record Bank E3 Harelbeke)*.
- Vlaamse Regering (2014) Regeerakkoord Vlaamse Regering 2014-2019.
  Accessed at http://www.vlaanderen.be/nl/overheid/vlaamse-regering/regeerakkoord- van-de-vlaamse-regering-2014-2019

INNOVATION:
Driven By Technology

Opening Up the Black Box: Understanding the Impact of Bodycams on Policing

Sander Flight
Consultant, The Netherlands[1]

Abstract
Police forces in countries all over the world are using body cameras or considering the introduction of these small wearable devices. Most impact assessments are based on projects within one geographical area or jurisdiction. Yet, the results are sometimes seen as an answer to the general question: 'Do bodycams work: yes or no?' In the first part of this article, I present a meta-analysis aggregating nine impact assessments from three different countries. The average results are positive prompting the conclusion that bodycams work. However, the overwhelming majority of research on bodycams comes from the United States or the United Kingdom. As police forces in other countries try to copy projects from abroad, they quickly discover that bodycams are about much more than just acquiring the devices. Any bodycam program needs careful preparation and attention to implementation to enable the devices to work as intended. By looking at effectiveness from this perspective, a different question appears from underneath the average results: 'How do bodycams work, under what conditions and for whom?' In the second part of the article, I sketch a framework to help science and practice to answer this much more relevant and realistic question. Central tenets within this framework are mechanisms, context and implementation. The final part of the article focuses on two topics that are often overlooked, but might prove essential in the quest for transferable lessons on bodycams: the visibility of the bodycam and the guidelines regulating the use of the bodycams.

Keywords: bodycams, police, evaluation, meta-analysis, implementation

The rise of the body camera

Bodycams are small cameras that are worn on the person, that have at least one microphone and an internal data storage that allows audio and video footage to be recorded.[2] The cameras are typically located on the officer's chest, shoulder or head. In 2015, according to a trend analysis of the global market for bodycams, 135,000 bodycams were sold to police and other law enforcers, mainly in the North Americas and Western Europe. Markets in countries such as France, Germany and Benelux were predicted to grow rapidly at least until 2020 (IHS, 2016). Police forces in many other countries are also either using these wearable cameras or testing the technology. At the annual technology conference of the International Association of Chiefs of Police in 2016, the number of workshops about bodycams outnumbered all other topics, including cyber security, big data, predictive analytics and forensic science.[3]

1 Correspondence email: info@sanderflight.nl. I wish to thank Rylan Simpson for detailed comments on an earlier version of this article and the anonymous reviewers for their feedback.

2 The technology is known under different names in different countries: body-worn cameras or BWC (mostly in the United States and Australia) or body worn video or BWV (popular in the United Kingdom and Canada). In this article, I call them bodycams or body cameras.

3 An overview of all presentations is available here: http://www.iacp.org/2016LEIMPresentations.

In 2012, in a market review by the U.S. Department of Justice, eight different bodycams were compared (National Institute of Justice, 2012). Four years later, in 2016, a similar market review included 38 different vendors producing 66 different types of bodycams (Hung & Babin, 2016). Bodycams are becoming 'the new normal' inside the world of policing at an unprecedented speed, even when we compare them to other types of video technology that were very popular from the start, such as closed-circuit television or automated license plate readers (Lum et al., 2015).

Bodycams in The Netherlands

In The Netherlands, the police has experimented with wearable cameras for quite some time. The first small-scale experiments were done as early as 1997 when portable video cameras were attached to helmets of officers (Flight, 2017). A second, more centrally co-ordinated, test was organised in 2009 when bodycams were introduced in four of the 25 regional units. The aim was to reduce aggressive behaviour from citizens towards police officers. Although the evaluation documented some encouraging results and showed there was considerable support for the bodycams among the officers, the body cameras did not reduce the number of assaults on police officers[4] (Ham, Kuppens & Ferwerda, 2011). Based on the report, the leadership of the police decided not to roll-out bodycams on the national level. This decision created the space for local and regional forces to start their own experiments, which they did on a large scale.[5] A third wave of nationally co-ordinated experiments was recently announced by the Dutch National Police and is taking place in 2017 and 2018. A total of 32 experiments are conducted to answer the question whether bodycams can be added to the standard equipment of police officers.

Since 2011, no independent academic impact assessment of bodycams has been done in The Netherlands. There have been several high-quality studies in other countries. To make optimal use of these evaluations, a review of the available international literature was commissioned in 2016 by Police and Science. The aim was to better inform the Dutch National Police about the effects bodycams have on policing (Flight, 2017).[6] In this article, I first present a summary of the meta-evaluation that formed the starting point of that literature review. The second part of the article is about the challenges facing practitioners and policy-makers who hope to copy postive outcomes that were reached in other countries into their own social and legal context. The third part of the article highlights two specific issues that have not received the attention I believe they need: the visibility of bodycams and the policies regulating bodycams. But first, I describe the reasons why body cameras are almost universally regarded as 'inevitable', making it one of the very few types of surveillance that are embraced by nearly all stakeholders.

Everybody happy?

One of the main drivers behind the widespread introduction of bodycams within the world of policing, is the fact that support for the technology comes from a rainbow-coalition of politicians, civil rights activists and police officers. Political leaders embrace bodycams because they will 'build and sustain trust' between the police and the community (White House, 2014) and because they will increase police accountability and legitimacy (Mateescu, Rosenblat & Boyd, 2016). Civil rights advocates in many countries also support the introduction of bodycams, because they believe they will increase police accountability. If interactions between citizens and police officers are recorded, officers are expected to act in a professional manner and in accordance with official guidelines. And even if cameras don't prevent incidents, the recordings can still be used for internal sanctions or criminal investigations.

The police also like body cameras, even though it is popular to think that the main purpose of the bodycams is to expose police misconduct and correct it. Police leadership organizations publicly support bodycams and the cameras are rapidly adopted by them. Research into police officers' perceptions shows strong support for bodycams and that support becomes even stronger post-deployment (White & Coldren, 2017). Re-

4 One of the reasons might have been that the number of assaults against the police was small to begin with, making it unlikely that bodycams (or anything else, for that matter) could bring it down any further.

5 In 2011, one year after the decision was made not to roll out bodycams at the national level, 17 of the 25 regional units had started bodycam programs (Flight, 2017).

6 Police and Science is an independent research program funded by the Dutch Ministry of Justice and Security. Its aim is to build bridges between academic research and police practice. As a follow-up to the literature review of 2016-2017, Police and Science has commissioned me to evaluate two of the 32 experiments that are currently being done. The results are scheduled for publication at the end of 2018.

Table 1
Meta-evaluation bodycams

Indicator	Effect	Number of studies
Complaints against the police	decrease	5
	no effect	2
	increase	-
	(unknown	2)
Use-of-force by the police	decrease	3
	no effect	1
	increase	-
	(unknown	5)
Use of recordings as evidence	positive	2
	no effect	2
	negative	-
	(unknown	5)

searchers in Florida, for instance, concluded that police officers are supportive of body-worn cameras because they perceive a potential for the body cameras 'in improving citizen behaviour, their own behaviour, and the behaviour of their fellow officers' (Jennings, Fridell & Lynch, 2014). This finding has since been confirmed by several studies that measured officer 'buy-in' of the technology (Gaub et al., 2016). The goals police officers and their organisations hope to achieve with bodycams are often a little more down-to-earth than the ideals of politicians. Typical benefits police officers and their organisations hope to achieve with bodycams, are to cut down on paperwork and help prosecute criminals (NBC, 2007), decrease offending, increase prosecution and guilty pleas (Palmer, 2016) or to improve operational effectiveness of policing by using the recordings as evidence (Edmonton Police Services, 2015).

A final powerful driver behind the technology is the idea that body cameras are in some way 'inevitable' for any modern police organisation. This seems to have been an important reason for the former mayor of London, when he described the acquisition of 23,000 bodycams for the Metropolitan Police Service as 'a huge step forward in bringing London's police force into the 21st century' (Mayor of London, 2015). His colleague, the mayor of New York City, agreed when he announced the full rollout of body cameras to all 30,000+ police officers of the NYPD, without waiting for the results of a 12-month trial: 'This is the shape of things to come' (Southall, 2017).

Meta-analyses

Several times a year, we can find articles in the media that claim to have the answer to the million dollar question: "Do bodycams work: yes or no?" Sometimes, the answer is yes, sometimes no. Typically, the weight attached to these pieces of 'evidence' from impact assessments depends less on how thoroughly the research was done, than on how recently it was published. A meta-analysis or research synthesis is often quite helpful in such an environment because they are based only on studies that meet rigorous scientific criteria for internal validity and because they aggregate findings from several studies.

The first meta-evaluation of bodycams was published in 2014 and included all high-quality evaluations that were available at that time (White, 2014). Another meta-analysis adding another five high-quality evaluations, was published three years later (Flight, 2017). The raw material for the 2017 analysis was gathered using an internet query aimed at finding all publications in either English or Dutch that reported on the effects of bodycameras and that were based on independent academic research. This resulted in a longlist of a little under 150 publications, which were all studied and included in the literature review. Of these, 36 publica-

tions were labelled evaluations, but 18 were technical evaluations containing no information about the impact bodycams have on policing. For the remaining 18 studies, the quality of the research design was assessed and nine studies were eliminated because they were based on anecdotal evidence or on pre-post outcome measures for a treatment group (officers with bodycams) without a control group (officers with no bodycams). The nine studies that were included in the meta-evaluation were either pre-post measurements for both a control group and a treatment group (5 studies) or RCT's in which the bodycams were randomly assigned to either different groups of officers or different shifts (4 studies).[7]

The results are discussed in detail in the literature review, including some promising findings from the less rigorous studies. For the purposes of this article, I have selected three indicators that were presented in at least four of the nine studies: i) complaints against the police, ii) use-of-force by the police and iii) the use of recordings as evidence.

The number of complaints against the police decreased according to five of the nine studies. The effect size ranged from a 14% decrease to an 87% decrease. Two other studies reported that the number of complaints had not changed. The two other studies did not contain information on the number of complaints.

Use of force by the police decreased in three of the nine evaluations, with an effect size ranging from a decrease of 28% up to a decrease of 75%. One study reported no change in use of force by the police. The other five evaluations did not contain information on use of force.

Finally, the use of bodycam recordings as evidence for investigations was reported on by four of the nine evaluations: two studies reported a positive contribution, two reported there was no change in either the quality or the speed of investigations.

Yes, they work! No, they don't!

Based on the results of this meta-analysis, police forces that hope to reduce the number of complaints against police officers or to reduce the use of force by the police, would be tempted to start using bodycams. But before buying the equipment, it may be wise to take a closer look at what lies hidden beneath the aggregated results. All major reductions in the number of complaints and the use of force were found in bodycam projects in the United States; the studies that were done in the United Kingdom or Canada reported either much smaller decreases or no difference at all.

This could be a coincidence, but it could also show that there is something about policing in the United States that influences the way bodycams work; something that is not present in the United Kingdom or Canada. Furthermore, there are differences between the studies from the United States as well that might contain useful information about the factors that impact the effects bodycams have. But what type of factors should we start looking for? How can we find relevant patterns within what at first appears to be random? To help us find the right direction, we can turn back the clock one or two decades and look at another form of visual surveillance: CCTV. A systematic review of 41 evaluations from five different countries (Welsh & Farrington, 2007; Welsh & Farrington, 2009) concluded that CCTV on average reduced crime by 16 percent. But underneath that average result, some remarkable patterns were visible. First of all, there seemed to be a 'country' effect, just as with bodycams. Only this time, all the positive results came from the United Kingdom, whereas all non-UK studies, mostly from the United States, found no significant effects.[8] And there were other, more informative, ways to disaggregate the results, for instance by location. In car parks, crime went down by 51%, but in city centres, public transportation and public housing, CCTV did not decrease crime significantly. A third meaningful way to split up the aggregate results was by crime type: significant reductions were found for vehicle crime and property crime but there was no evidence of an effect of CCTV on violent crimes. In short: country, location and crime-type mattered. But how can we be certain that these are the only important

7 The cut-off point for the analysis was June 2016, which means all studies published after that date have not been included. The nine studies included were from Edmonton in Canada (Edmonton Police Services 2015), from Plymouth (Goodall 2007), Essex (Owens et al. 2014) and London (Grossmith et al. 2015) in the United Kingdom, and from Rialto (Ariel et al. 2015), Mesa (Mesa Police Department 2013 and Ready & Young 2015), Phoenix (Katz et al. 2014), and Orlando (Jennings et al. 2015) in the United States.

8 This is a summary of the text on the website of the Crime Reduction Toolkit for CCTV, published by the What Works Centre for Crime Reduction: http://whatworks.college.police.uk/toolkit/Pages/Intervention.aspx?InterventionID=1.

variables? And how should this knowledge be applied to specific crime problems in specific settings?

One way of approaching this very problem, had already been written fifteen years before the meta-analysis was published (Tilley, 1993). In this article, Tilley approached the problem from the theoretical starting point and tried to think of all the ways in which CCTV might have an impact on crime in car parks. He then went on to describe the contexts within which these mechanism could be triggered leading to measurable outcomes. He called these 'context-mechanism-outcome configurations' and concluded these would have to be described and understood if our aim is to be able to successfully transfer positive results from one CCTV-scheme to the next.

It depends

Returning to the subject of bodycams, we can see that history is starting to repeat itself. The first meta-evaluations suggest that on average bodycams 'work', but that they are more successful in some places than in others. If we limit ourselves to individual studies, we will never be able to explain why this is the case. We need to start looking at patterns across different studies from different settings. The first meta-analysis of bodycams already contained this conclusion. The author of that study wrote that even though we know from the positive results that were discovered that bodycams can have a civilizing effect, we cannot really generalise the information because the 'dynamics of police-citizen encounters are complex, and there are numerous potential explanations for the decline in citizen complaints and use of force' (White, 2014). Three years later, this has not improved. One of the most influential teams of researchers in the area of bodycams concluded: 'The evidence on [bodycams] is substantially long on evidence but rather short on theory. Why should [bodycams] 'work' and under what conditions or on whom?' (Ariel, Sutherland, Henstock, Young & Sosinski, 2017).

We have no clear idea on how the mechanisms of deterrence and increased self-awareness work, nor do we know who is influenced by the bodycam: the police officer, the citizen or both. To remain relevant to practitioners, academics should no longer ask baldly stated questions about whether bodycams do or do not work, because it depends. A more interesting question would be: 'On what?' Academics need to start aiming at making ever better informed judgments about the potential of bodycameras to fire specific mechanisms in specific contexts.

In the remainder of this article, I try to take some steps in the right direction by looking at two issues that have not received a lot of academic attention even though both are essential to unpack why different evaluations can lead to seemingly contradictory findings. The first is the visibility of the bodycam: 'Can people see it?' The second issue is the policy that regulates the use of the bodycam and the footage: 'The rules of the game'.

Can people see the bodycam?

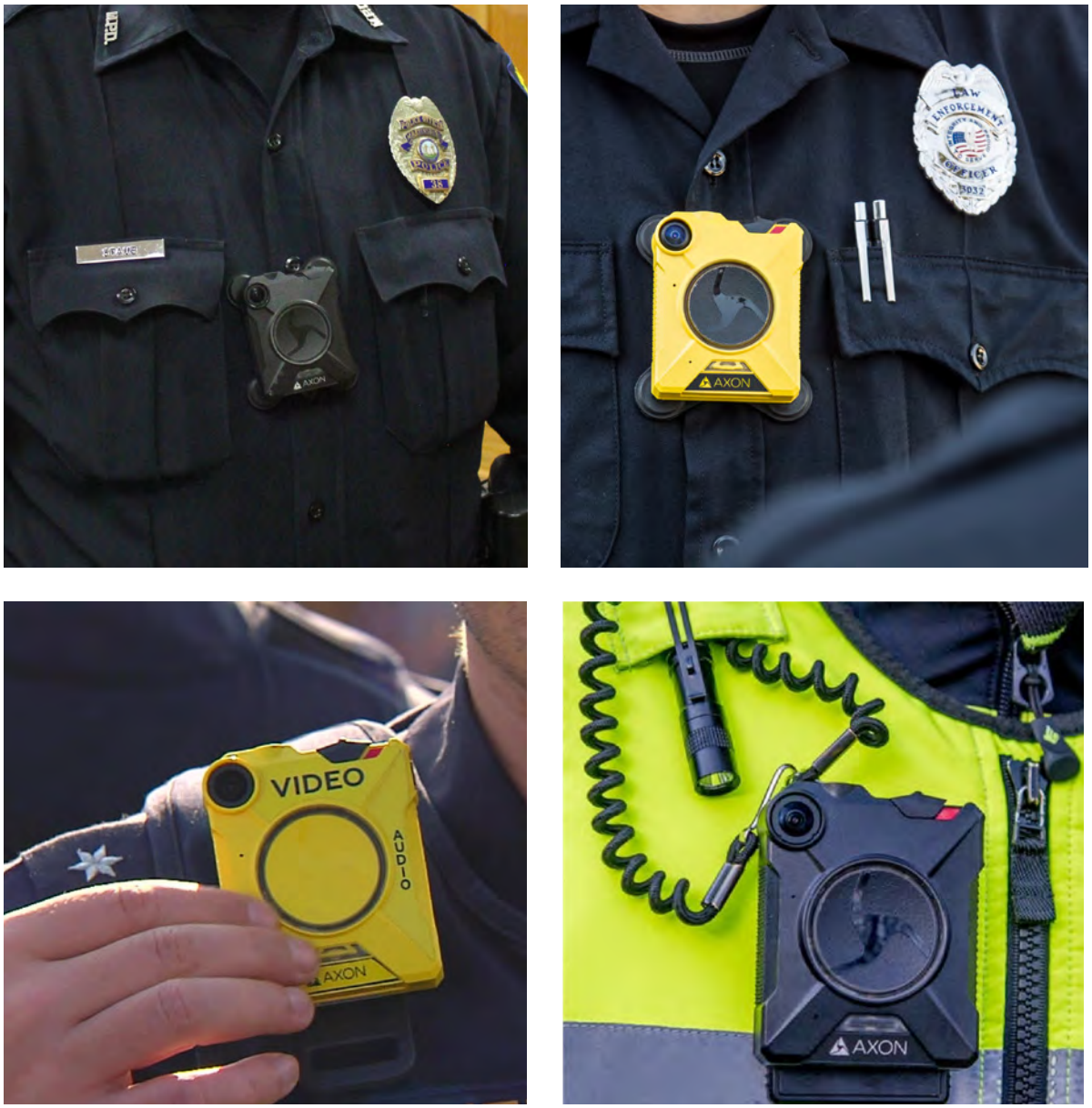
There are over fifty types of bodycams, each with their own design. Because one of the main objectives of all bodycam programs is to influence the behaviour of citizens in the desired direction, it would make sense to choose a bodycam that people can easily see. It would also make sense to include information on the visibility of the bodycam in academic publications that report on the (absence of a) civilizing effect of bodycams, yet this information is hardly ever included in reports.[9] To give an impression of the wide range in the visibility of bodycams, some examples of devices, colours, mounts and signs are shown below.

9 Some researchers have tried to find out whether it makes a difference if an officer gives a verbal warning that a recording is in progress. But the question whether different physical appearances of the device itself can lead to different outcomes has not received considerable scientific attention yet. The only exception I could find is Timan (2013) who describes the way in which the design of one type of bodycam, Zepcam, was partially based on demands from policymakers, partially on technical and practical considerations and partially on legal requirements. Timan concludes that the design that was settled on in the end, had intended and unintended consequences for both police officers and citizens. Unfortunately, no empirical studies have been done yet to measure the size of these effects.

Figure 1 – The device

Some of the early bodycams were quite literally a 'black box' which effectively rendered them invisible to citizens. In order to trigger the civilizing effect, to activate the mechanism of deterrence, or to comply with legal requirements, vendors have started to design bodycams that can be made visible by the officer using the device. One option is a red flashing light around the record-button once it has been activated (top left). Another option is to start the recording by pushing down a slide, which reveals a green circle around the camera lens (top right and bottom left). A third option is a camera lens on top of the device that can pan and tilt, combined with a small screen that displays what the camera sees (bottom right). All three bodycams are visible after activation, but the level of 'noticeability' will probably still differ considerably between these three options and between being switched on and off. But there is more than just the device that influences visibility of the bodycam.

Figure 2 – Colour of the uniform



A black box on a black uniform (top-left) is less visible than a yellow box (top-right and bottom-left). But not if the uniform itself is yellow, in which case the black bodycam is easy to see (bottom-right). The point here is not whether more visibility is necessarily better: that depends on the mechanisms the police hope to activate. The point is that in any project, the colour of the bodycam in combination with the colour of the uniform should be considered carefully, because a highly visible bodycam can become an invisible one, or vice versa.

Figure 3 – Mounting of the device

Where the bodycam is positioned on the body of the officer will impact visibility and, therefore, whether a civilizing effect can be expected or not. A body camera on the chest will probably not be noticed as easily as a camera on the shoulder or collar (top-left). The most visible bodycam is probably the one attached to a pair of glasses, because it positions the camera directly next to the eyes of the officer.[10] Other, less visible, options are available as well. Consider for instance the bodycam that is integrated with the radio microphone (bottom left), or a camera that can be hidden from view (bottom-right).

10 These choices have other important consequences as well. An advantage of attaching the camera to the head instead of the shoulder or chest, could be that the camera 'sees' what the officer sees when she turns her head. The advantage of attaching the camera to the torso of the officer is a more stable image.

Figure 4 – Signs

Research on CCTV in Cincinnati has shown that signs that inform the public of the presence of CCTV cameras, sometimes have more impact on behaviour than the actual cameras (Mazerolle, Hurley & Chamlin, 2002). There is no reason to expect this will be completely different for bodycams. This means that signs informing the public about the bodycam, either on the camera itself or on the officer, may influence behaviour more than the actual bodycam itself. Signs can be handmade (top-left) or provided by the manufacturer (top-right and middle-left). An interesting option is to place an extra sign on the police officer wearing the camera; either on the front of the officer (middle-right and bottom-left), or on the back (bottom-right). Again, there is no one design that is best for all purposes; this depends on the mechanisms that should be triggered.[11]

11 The pictures of officers with signs on their body and on the camera, are from Germany and Austria. The reason for this may not even be a conscious attempt to maximise the civilizing effect of the bodycam, but instead may be necessary to comply to the stricter legal framework regulating surveillance in these countries compared to others.

Does design matter?

We cannot assume that citizens will be aware of the fact that their interactions with police are being recorded. In a study in the United States, researchers interviewed 250 citizens who had encounters with police officers that were recorded with a bodycam. Only 29% was aware they had been recorded (White, Todak & Gaub 2017). Another survey among 400 citizens in a city in southwestern United States showed that 38% of all people who had a recent documented interaction with a police officer with a bodycam, correctly remembered there was a bodycam present. An even more striking finding was, that when the officer was *not* wearing a bodycam, 27% of citizens still said they remembered seeing a bodycam (McClure et al., 2017). This type of research is not without its methodological difficulties,[12] but the findings do suggest that a majority of these citizens did not notice if the officer they are talking with is wearing a bodycam or not. The interesting thing about the study, however, is that the authors do not describe the type of bodycam the officers were wearing. Given the fact that some bodycams are nearly invisible, it would be useful if researchers would include information on the design to enable others to compare their situation to the one that was studied.

The point here is not to find a design which is best: there may not be one single design that is best for all applications. Sometimes maximum visibility will be desirable, for instance if the aim is to deter aggressive citizens from assaulting police officers through the mechanism of deterrence. But sometimes a less visible or even a completely hidden camera could work much better, for instance in an under-cover operation or if the bodycam would escalate an already tense situation. The point is that these choices need to be considered before acquiring a specific bodycam and that these decision should not be made on the basis of technical considerations only.

12 In the second case (the n = 400 study), surveys were administered within one to two weeks of the actual interaction between community members and officers. An experimental methodology could eliminate this time-problem, by creating an artificial setting in which different images of police officers can be shown to participants, immediately followed by a questionnaire. For a recent example of this methodology to gauge perceptions of police officers with different attire or on different patrol strategies (see Simpson, 2017). An experimental setting could create its own problems, however, for instance by making the 'encounter' less stressful than an actual encounter with a police officer. This could result in an overestimation of people's ability to accurately remember information compared to actual street encounters with the police (Wells, 1978).

The rules of the game

Anyone who has witnessed the introduction of bodycams in a police force will have discovered that many police officers worry about the policy or guidelines that dictate the use of the device and the handling of the recordings. Often, these three questions are central to the debate:

- Is the use of a bodycam voluntary or mandatory?
- Who decides what has to be recorded: the individual officer or will there be rules?
- Who has access to the footage?

Deciding on these questions and documenting them in written guidelines is not a task that should be taken lightly. The Dutch National Police, for instance, has been improving the national framework for bodycams for four years before the first version was published in November 2017. The New York Police Department based their guidelines on input from thousands of citizens and police officers and went through sixteen different versions of the document before the 'BWC Operations Order Final Draft' was published.[13]

The reason these policies are so important is that they influence officer buy-in of the bodycam technology.[14] Police officers unfamiliar with the bodycams will have concerns, especially about the policy that dictates how often and in what way their supervisors can review the footage. If access is restricted to specific incidents, such as complaints, use of force or random quality checks, this concern can be alleviated (White & Coldren, 2017). But in many cases, bodycams are supposed to (also) increase accountability of the police, which could lead to policies that are the exact opposite of what police officers would choose themselves.

Guidelines have received academic attention recently. One recent study that was already mentioned above, compared use of force by police officers in nine differ-

13 The Dutch policy ('Voorlopig inzetkader Bodycams bij operationeel gebruik') can be downloaded here: https://www.politie.nl/binaries/content/assets/politie/algemeen/algemeen/inzetkader-bodycams.pdf.
The NYPD ('BWC Operations Order') can be downloaded here: https://www1.nyc.gov/assets/ccrb/downloads/pdf/investigations_pdf/oo_16_17.pdf.

14 For a discussion of officer buy-in of bodycams within three police forces in the United States, see Gaub et al., 2016.

ent sites in various countries. The conclusion was that on average bodycams had no effect on use of force by the police. But beneath this average there were different results. Use of force depended on how well officers complied with protocol. Where officers followed the protocol (turn on the camera throughout every interaction and give a verbal warning of the camera/recording that is going on), use of force decreased by nearly 40%. Where officers did not comply with protocol guidelines (they decided during the shift when they turned the cameras on or off), the use of force increased dramatically – more than 70% (Ariel, Sutherland, Henstock, Young & Sosinski 2017). So: policies make all the difference.

Another interesting thing is that the three questions mentioned above are intricately linked together. If the decision is made that use of bodycams will be mandatory and if all interactions with citizens have to be recorded ('always on'), the pressure will be on the policy-makers to prevent the recordings from being a public record. This happened for instance in the state of South Carolina where all officers had to start wearing bodycams (Williams, 2015). If, on the other hand, all recordings will be published online without redacting them first, police officers will probably not immediately embrace a policy that includes mandatory use of bodycams, or that is based on the 'always on' principle.

Just as there is no general rule that determines which design of the bodycam itself is best, there is no single policy that will work best in all settings. The political, policy and policing context is different from one police force to the next. If the reason for the bodycams is external, for instance a legal ruling or a consent decree that forces the police to start using bodycams, the police will probably prefer a policy with as much room for officer discretion as possible. If, on the other hand, the police opt to use bodycams as a proactive step to demonstrate transparency, the policy may leave less room for choice on the level of the individual officer.

A final point that needs to be stressed is that guidelines are only meaningful when introduced together with mechanisms to enforce compliance. Without a system of, for instance, random pulls of recordings and internal sanctions for officers who do not comply with the protocol, the policy will remain ineffectual.

Conclusions

Police forces around the globe will continue to invest millions in bodycams over the coming years. Yet, many of them – especially outside of the United States and the United Kingdom – are quickly discovering that bodycams are about much more than just the technology. Buying a set of body cameras and distributing them among all front-line police officers does not provide enough focus to fundamentally influence the way these officers do their job, let alone for a coordinated attempt to improve the relationships between the police and the community as a whole. Police forces that aim to emulate 'success' from elsewhere, will need to start looking beneath the surface to find out what it was that made the bodycams 'work'. We need to understand *how* and *where* and *for whom* they work.

In this article, two aspects of any bodycam program that are very influential are discussed: the visibility of the bodycam and the policies that regulate the use of the device and of the recordings. These issues have not received a lot of systematic academic attention yet. Practitioners that look to science in the hope of receiving useful information can feel overwhelmed by the number of variables that have to be considered. This article adds another two items to their desktop that was probably already overflowing with 'evidence' and 'lessons learned'. But if the number of high-quality empirical studies keeps increasing and academics start paying more and more attention to mechanisms, contexts and implementation issues, we may end up with a relatively small number of variables that are the most relevant. Furthermore, academics need to broaden their view to include not only validity of the findings within a specific context, but to include more descriptive methodologies and theoretical explorations. This will be the only way in which we will be able to make sense as the number of superficially contradictory findings will inevitably increase. This task can only be achieved by increasing the number of projects where academics and practitioners collaborate.

References

- Ariel, B., Farrar, W. A., & Sutherland, A. (2015) The effect of police body-worn cameras on use of force and citizens' complaints against the police: A randomized controlled trial. *Journal of Quantitative Criminology*. 31(3), 509-535.
- Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., Megicks, S., & Henderson, R. (2016) Wearing body cameras increases assaults against officers and does not reduce police use of force: Results from a global multi-site experiment. *European Journal of Criminology*, 13(6), 744-755.
- Ariel, B., Sutherland, A., Henstock, D., Young J., Drover, P., Sykes, J., Megicks, S., & Henderson, R. (2017) "Contagious Accountability" A Global Multisite Randomized Controlled Trial on the Effect of Police Body-Worn Cameras on Citizens' Complaints Against the Police. *Criminal Justice and Behavior*, 44(2), 293-316.
- Ariel, B., Sutherland, A., Henstock, D., Young J. & Sosinski, G. (2017) The Deterrence Spectrum: Explaining Why Police Body-Worn Cameras 'Work' or 'Backfire' in Aggressive Police–Public Encounters. Policing: A Journal of Policy and Practice,Vol 12 (1), 6-26.
- Edmonton Police Services. (2015) Body Worn Video: Considering the Evidence; Final Report of the Edmonton Police Service Body Worn Video Pilot Project.
- Flight, S. (2017). De mogelijke meerwaarde van bodycams voor politiewerk; Een internationaal literatuuronderzoek. Amsterdam: Reed Business.
  Available from: http://www.politieenwetenschap.nl/cache/files/5a5f34348576cPW93.pdf [Accessed 17th January 2018]
- Gaub, J. E., Choate, D. E., Todak, N., Katz, C. M., & White, M. D. (2016) Officer perceptions of body-worn cameras before and after deployment: A study of three departments. *Police Quarterly*, 19(3), 275-302.
- Goodall, M. (2007) Guidance for the police use of body-worn video devices. London: Home Office.
- Grossmith, L., Owens, C., Finn, W., Mann, D., Davies, T., & Baika, L. (2015) Police, Camera, Evidence: London's cluster randomised controlled trial of Body Worn Video. London: College of Policing.
- Ham, T. van, J. Kuppens & H. Ferwerda (2011) Mobiel cameratoezicht op scherp; Effecten op geweld tegen de politie en het politieproces in beeld. Arnhem: Bureau Beke.
- Hung, V. & Babin, S. (2016) A Market Survey on Body Worn Camera Technologies. Laurel, Maryland: Johns Hopkins University Applied Physics Laboratory.
  Available from: https://www.ncjrs.gov/pdffiles1/nij/grants/250381.pdf [Accessed 17th January 2018].
- IHS (2016) Top Video Surveillance Trends for 2016.
  Available from: https://technology.ihs.com/api/binary/572252 [Accessed 17th January 2018].
- Jennings, W., M. Lynch & L. Fridell (2015) Evaluating the impact of police officer body-worn cameras (BWCs) on response-to-resistance and serious external complaints: Evidence from the Orlando police department (OPD) experience utilizing a randomized controlled experiment. Journal of Criminal Justice. 43, 480-486.
- Katz, C. M., Choate, D. E., Ready, J. R., & Nuño, L. (2014) Evaluating the impact of officer worn body cameras in the Phoenix police department. Phoenix, AZ: Center for Violence Prevention and Community Safety, Arizona State University.
- Lum, C. M., Koper, C. S., Merola, L. M., Scherer, A., & Reioux, A. (2015) Existing and ongoing body worn camera research: Knowledge gaps and opportunities. George Mason University.
- Mateescu, A., Rosenblat, A., & Boyd, D. (2016) Dreams of accountability, guaranteed surveillance: The promises and costs of body-worn cameras. *Surveillance and Society*, 14(1), 122.
- Mayor of London (2015) Mayor on track to roll-out body cameras across the Met. Press release London Assembly; Mayor of London.
  Available from: https://www.london.gov.uk/press-releases/mayoral/mayor-on-track-to-roll-out-police-body-cameras [Accessed 17th April 2018].
- Mazerolle, L., Hurley, D., & Chamlin, M. (2002) Social behavior in public space: An analysis of behavioral adaptations to CCTV. *Security Journal*, 15(3), 59-75.
- McClure, D., La Vigne, N., Lynch, M. & Golian, L. (2017) How Body Cameras Affect Community Members' Perceptions of Police; Results from a Randomized Controlled Trial of One Agency's Pilot. Washington: Urban Institute.
- Mesa Police Department (2013) On-officer Body Camera System; Program Evaluation and Recommendations. Presentation Mesa Police Department: Mesa, United States.
- National Institute of Justice U.S. Department of Justice (2012) A Primer on Body Worn Cameras for Law Enforcement.
  Available from: https://www.justnet.org/pdf/00-Body-Worn-Cameras-508.pdf [Accessed 17th January 2018].

- NBC (2007) Britain straps video cameras to police helmets. 13 July 2007.
- Owens, C., Mann, D., & Mckenna, R. (2014) The Essex body worn video trial: The impact of body worn video on criminal justice outcomes of domestic abuse incidents. College of Policing, UK.
- Palmer, D. (2016) The mythical properties of police body-worn cameras: A solution in the search of a problem. *Surveillance and Society*, 14(1), 138.
- Ready, J. T., & Young, J. T. (2015) The impact of on-officer video cameras on police–citizen contacts: findings from a controlled experiment in Mesa, AZ. *Journal of Experimental Criminology*, 11(3), 445-458.
- Simpson, R. (2017) The Police Officer Perception Project (POPP): An experimental evaluation of factors that impact perceptions of the police. *Journal of Experimental Criminology*, 13(3), 393-415.
- Southall, A. (2017) Do Body-Cameras Help Policing? 1,200 New York Officers Aim To Find Out. *New York Times*, *26 April 2017*.
- Tilley, N. (1993) Understanding car parks, crime and CCTV; evaluation lessons from safer cities. Police Research Group/ Home Office Police Department.
- Timan, T. (2013) Changing landscapes of surveillance: emerging technologies and participatory surveillance in Dutch nightscapes (No. 13-276). Universiteit Twente.
- Wells, G. L. (1978) Applied eyewitness-testimony research: System variables and estimator variables. *Journal of Personality and Social Psychology*, 36(12), 1546-1557.
- Welsh, B., & Farrington, D. P. (2007) Closed-circuit television surveillance and crime prevention: A systematic review. Swedish National Council for Crime Prevention.
- Welsh, B. C., & Farrington, D. P. (2009) Public area CCTV and crime prevention: an updated systematic review and meta-analysis. *Justice Quarterly*, 26(4), 716-745.
- White, M. (2014) Police Officer Body-Worn Cameras; Assessing the Evidence. Washington DC: Office of Community Oriented Policing Services.
- White, M. & Coldren, J. (2017) The Impact of Body-Worn Cameras: Perceptions and Reality. Washington DC: Office of Justice Programs.
- White, M. D., Todak, N., & Gaub, J. E. (2017) Assessing citizen perceptions of body-worn cameras after encounters with police. *Policing: An International Journal of Police Strategies and Management* 40(4), 689-703.
- White House (2014) Factsheet: Strengthening Community Policing. Washington DC: Office of the Press Secretary.
- Williams, R. (2015) South Carolina First State to Require Body-Worn Police Cameras. Denver/Washington: National Conference of State Legislatures.

Automatic Weapon Detection in Social Media Image Data Using a Two-Pass Convolutional Neural Network

Jens Elsner
Thomas Fritz
Laura Henke
Oussama Jarrousse
Mathias Uhlenbrock
Stefan Taing
Munich Innovation Labs, Germany[1]

Abstract
Police analysts are faced with a deluge of data when monitoring the activities in specific areas of social networks and other internet data sources. Image recognition can help to prioritize the reading and subsequent analysis. The paper presents a case study for weapon detection in image data that has the potential to reduce the workload of the analyst by a factor of 200.

Keywords: Image Classification, Weapon Detection, TensorFlow, Social Network Analysis

1. Introduction

Police analysts are faced with a deluge of data when monitoring the activities in specific areas of social networks and other internet data sources. Image recognition can help to prioritize the reading and subsequent analysis. For example, when monitoring online resources of potential radicals, any posting of a weapon is of interest as it might indicate a possible threat. In recent years, image object classification using deep learning techniques has made significant progress with the advent of powerful computational architectures such as Graphical Processing Units (GPUs). The purpose of this paper is to study the performance of the application of the publicly available and open source TensorFlow framework (Abadi et al., 2015) to the problem of weapon recognition in images.

A classification approach that allows to incorporate and learn from analyst feedback using supervised learning while keeping the total retraining time of the classifier at a minimum is presented.

1 Corresponding author's email: je@munich-innovation.com

2. Methods

2.1. 2-Pass Image Object Detector

The presented 2-pass image object detector consists of two modules: First, the Search-Net, a region-based fully convolutional network (R-FCN) (Dai et al., 2016) with a ResNet-101 feature extractor (He et al. 2016) for

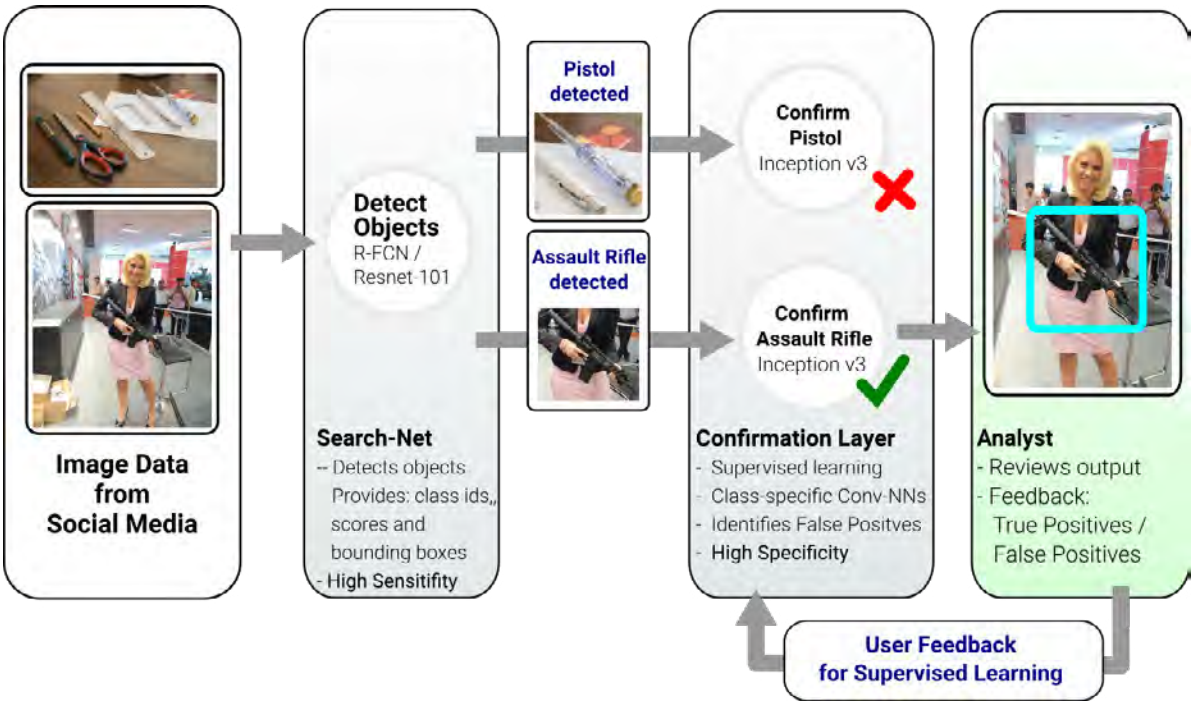
object detection and second, the Confirmation-Layer network which is used to revise the output of the first network and consists of multiple Inception v3 networks (Szegedy et al., 2015), one for each respective class of the Search-Net. The Search-Net analyzes the input data and returns class ids, scores and bounding boxes for the detected objects. The extracted objects are provided to the Confirmation Layer which evaluates whether a detection is correct (true positive) or incorrect (false positive) (see Fig. 1). The classifiers of the Confirmation Layer are continuously trained on the user feedback and thereby learn to detect systematic misclassifications of the Search-Net. The system was implemented using Python and the machine learning framework Google TensorFlow (Abadi et al., 2015), in particular its object detection functionality (Huang et al., 2017). All computations are conducted on an Intel i7 workstation equipped with a Nvidia Geforce GTX 1080 for GPU processing.

For all detected objects, the Search-Net and the classifiers of the Confirmation Layer calculate confidence scores based on the extracted features. By setting thresholds for both modules, the sensitivity and specificity of the whole system can be optimized for the specific use case.

2.2. Training Data

The Search-Net was trained on pictures collected from the ***Internet Movie Firearms Database*** (IMFD, 2017) for two classes (1162 pistols and 387 assault rifles) which were annotated manually. The classifier of the Confirmation Layer were trained on true and false positive samples for both classes. To generate the true positive data, the Search-Net was run on the training data and the image sections which contained the detected objects were extracted and validated manually (pistols: 1391 / assault-rifles: 734). Moreover, 5703 random images collected from ***Flickr*** (Flickr, 2017), which contained no weapons, were classified by the Search-Net. Here, 738 assault-rifles and 1211 pistols were mistakenly detected and were used to generate the false positive data. With this data, the Confirmation Net was trained to detect false positives of the Search-Net for both pistols and assault rifles separately.

Figure 1: 2-Pass Object Detector. The Search-Net provides class ids, scores and bounding boxes of detected objects. The Confirmation Layer checks the output for misclassifications. The analyst gives feedback regarding correct and incorrect classifications which is used for refinement of the Confirmation Layer network.



3. Results

The performance of the 2-Pass Object Detector was evaluated using a test data set with images collected from ***Flickr*** (Flickr, 2017) and ***Wikimedia Commons*** (Wikimedia, 2017), which consisted of 80 images depicting weapons (40 pistols / 40 assault rifles) and 734 random images with no weapons. The Search-Net was configured to classify an object as weapon if the confidence score exceeded 0.90. With this threshold, it identified 75 of the 80 images depicting weapons correctly, which corresponds to a true positive rate (sensitivity) of 93 %. However, 117 images were mistakenly classified to either show at least one pistol or assault rifle which corresponds to a true negative rate (specificity) of 85%. The output of Search-Net was then re-evaluated by the Confirmation Layer. Here, the threshold for the confidence score was set to 0.50. The Confirmation Layer was able to correct 75 false positive detections, but also reclassified 5 correctly identified weapons as false detection. Consequently, the specificity of the whole framework increased to 95% while the sensitivity was decreased to 87% (see Tab. 1). Some of the results are shown in Fig. 2.

Table 1: Results before and after reclassification by the Confirmation Layer

	True Positive	False Positives	Sensitivity	Specificity
Search-Net	75 of 80	117 of 734	93 %	85%
Confirmation Layer	70 (-5)	42 (-75)	87 %	95%

Figure 2: Results obtained from the test image data set. Top: All weapons have been correctly detected and annotated by the 2-pass object detector. Bottom left: All but one assault rifle have been correctly detected and annotated. Button right: Combination of two objects mistakenly classified as pistol.

4. Discussion

The 2-pass approach allows for a direct refinement of the object detector based on the user feedback. A common mistake of the Search-Net was for example to misinterpret a cell phone, which is held in a hand, as a gun due to shared geometrical features. After providing a few false positive samples, the Confirmation Layer was able to detect this systematic misclassification without the need to retrain the whole Search-Net.

At the same time, the 2-pass approach significantly reduces the time required for supervised learning. As discussed, analyst feedback is incorporated into the Confirmation Layer. The Confirmation Layer only processes defined parts of images and does not scan the whole source image as is required for the Search-Net. Hence, the Confirmation Layer can be re-trained to incorporate the user feedback within minutes. On the other hand, a complete training of the Search-Net will take, on the hardware used for this study, several hours to achieve good convergence of training results.

The 2-pass approach also allows to tune sensitivity and specificity depending on the requirements of the task at hand. For our test data set, we were able to increase the specificity from 85% to 95% without losing too much sensitivity (93 % to 87 %).

So what do these numbers mean for the daily workload of an analyst? Let's consider the following case: An analyst has obtained a data set with 10.000 images from a social media source and he wants to evaluate if members of that group pose with weapons on some of these photos in order to assess their threat potential, while it is not necessary to detect all occurrences of weapons. Let's assume that 10 of the 10.000 photos show a person with a weapon. Without technical support, the analysts would have to go through 10.000 / 10 = 1000 photos on average until he finds the first one showing a weapon. An automatic detector with a sensitivity of 93% and a specificity of 85% will find, on average, 9.3 pistols and 1499 false positives (15% out of 9990 possible false positives in 10.000 images) in the data. This means that (1499 + 9.3) / 9.3 ~ 162 images, on average, have to be checked to find the first picture showing a weapon. If the presented 2-pass object detector with a sensitivity of 87% and a specificity of 95% is used, this number once again decreases to (499 + 8.7) / 8.7, i.e. ~ 58 images. If the analyst checks 0.5 images per second, his workload for this specific analysis would have been reduced from initially about 33 minutes to about 2 minutes.

The presented object detection technique is not restricted to weapons but can be trained on any object. To scan for car plates and street signs can help to get evidence about the location where the photo has been taken and to identify group members. Scanning for symbols and logos can help to gain information about group affiliation.

We believe that this or a similar technique for image object recognition can greatly increase the efficiency of police work while potentially increasing privacy of users by limiting the amount of content explicitly monitored by police analysts.

Acknowledgements

This work was partially funded under the project "INTEGER" by the Federal Ministry of Education and Research, Germany, reference number FK 13N14377.

References

- Abadi, M. et al. (2015) TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems.
  Available from: http://download.tensorflow.org/paper/whitepaper2015.pdf
- Dai, J.; Li, Yi; He, K. & Sun, J. (2016) R-FCN: Object Detection via Region-based Fully Convolutional networks.
  Available from: ArXiv:1605.06409
- Flickr (2017),
  See: https://www.flickr.com
- He, K.; Zhang, X.; Ren, S. & Sun, J. (2016) Deep residual learning for image recognition. In The IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 770-778.
- Huang, J.; Rathod, V.; Sun, C.; Zhu, M.; Korattikara, A.; Fathi, A.; Fischer, I; Wojna, Z.; Song, Y.; Guadarrama, S.; Murphy, K. (2017) Speed/accuracy trade-offs for modern convolutional object detectors.
  Available from: https://arxiv.org/abs/1611.10012
- Internet Movie Firearms Database (2017),
  See: http://www.imfdb.org/wiki/Main_Page
- Szegedy, C.; Vanhoucke, V.; Ioffe, S.; Shlens, J.; Wojna, Z. (2015) Rethinking the Inception Architecture for Computer Vision.
  Available from: ArXiv:1512.00567,
- Wikimedia (2017),
  See: https://commons.wikimedia.org/wiki/Main_Page

Licenses of images used

The following images from Wikimedia under a Creative Commons / attribution license were used in this paper. The use of these images does not mean the copyright holder endorses this work. Please see link for details of licenses.

1. https://commons.wikimedia.org/wiki/File:Anca_Verma_with_SIG_SAUER_rifle_at_DefExpo_India_2012.JPG
2. https://commons.wikimedia.org/wiki/File:USS_Mitscher_(DDG_57)_150129-N-RB546-055_(16433068885).jpg
3. https://commons.wikimedia.org/wiki/File:120516-A-WC501-101_(7325177330).jpg
4. https://commons.wikimedia.org/wiki/File:Flickr_-_Official_U.S._Navy_Imagery_-_Sailors_fire_M9_service_pistols_during_arms_qualifications..jpg

The following images from Flickr under a Creative Commons / attribution license were used in this paper. The use of these images does not mean the copyright holder endorses this work. Please see link for details of licenses.

1. Vesselin Dochkov, Tools, https://www.flickr.com/photos/vesselin/24270513429/
2. U.S. Army Europe, Training tools, ttps://www.flickr.com/photos/usarmyeurope_images/9266950263/

Critical Success Factors for OSINT-Driven Situational Awareness

Babak Akhgar
Douglas Wells
CENTRIC, Sheffield Hallam University, United Kingdom[1]

Abstract:
A critical element of successful intelligence-led law enforcement operations is the ability of the police and other security services to obtain timely, reliable and actionable intelligence concerning the problem, incident or investigation under focus. As well as traditional investigative techniques and information sources, open-source intelligence (OSINT) can provide additional capabilities for Law Enforcement Agencies (LEAs) to manage an investigation or address the intelligence requirements of a given incident. This position paper introduces the concept of OSINT, identifies and discusses existing effective practices and critical success factors for the fusion of OSINT with traditional intelligence sources. This paper is written as a position piece based upon CENTRIC operational involvement in 14 UK based LEA open source investigations over the years 2015 to 2017.

Keywords: OSINT, Situational Awareness, Law Enforcement.

Introduction

The private sector has, over recent years, increasingly began to use information from open online source, including social media, to measure customer loyalty, track public opinion and assess product perception (Neri et al., 2012). Coinciding with this trend, Law Enforcement Agencies (LEAs) are applying techniques to enhance their investigative capability towards improving their response to against criminal threats (Gibson 2004; Bell & Congram, 2012). As a result, Open Source Intelligence (OSINT) tools and techniques are increasingly used to be a part of law enforcement's investigative repertoire in the identification of criminals and their activities; including activities targeting recruitment, transfer of money, information and the coordination of illicit activity (Omand et al., 2012).

This paper examines the criteria used by law enforcement to utilise, deploy and maintain effective OSINT investigative tools and tactics, based on experiences gleaned from collaboration, cooperation, training and bespoke investigative work undertaken alongside regional UK police forces. Moreover, the paper highlights critical areas of consideration for modern OSINT practitioners. However, defining the specific characteristics of OSINT is not a straightforward task, the context and definition for the use of OSINT often changes dependent on the country and organisation of origin. The ambiguity of the term is explored in detail later in the 'Current Challenges and Dilemmas' section. Despite this contextual ambiguity, for the purposes of this pa-

1 Corresponding author's email: d.wells@shu.ac.uk

per a working definition of OSINT is used, following the three following defining principles; *1) OSINT consists of data collected from 'publicly available sources', 2) it is data to be used in an 'intelligence context', and 3) the data collection can be performed in an overt manner.* Furthermore, from an ontological perspective the paper considers OSINT to be part of a LEAs situational awareness capabilities. Situational awareness, in the context of our discussion is defined as; 'the capability to identify, contextualise, visualise, process, and, comprehend the critical elements of intelligence about particular areas of concern. These areas of concern may be anything from an investigation to the management of a major crisis.

The authors acknowledge - and later explore in detail - the strengths and limitations of these terms and how they also allow for flexibility through their interpretation. These three defining statements are rough outlines rather than literal definitions and are explored in the section "Emerging Challenges to OSINT Interpretation". Indeed, it is worth noting that RIPA (Regulation of Investigatory Powers Act 2000) may be interpreted to have been written for the capacity for flexible and dynamic interpretations, and not to be an inconvenience or destructive restriction upon law enforcement.

Importance of Social Media

OSINT is increasingly focused on internet based and social media analysis (SOCMINT). To this extent the UK NPCC (National Police Chiefs Commission) have debated over whether to continue calling it OSINT, or internet investigations (NPCC National Open Source Intelligence and Investigations Conference, 2017). Whilst this may seem like a trivial point, it shows the prevalence and dominance of online and social media aspects of contemporary OSINT investigations over traditional 'offline' approaches. Currently, it appears that the use of internet based OSINT, especially regarding big data analytics are primarily used for intelligence gathering and investigations, and not for general community-policing. As of 2015, it was noted that in general, the majority of police forces and OSINT practitioners used; "social media… to inform strategies such as pre-emptive arrests, interceptions of activities, approaching particular individuals and groups, or change of tactics during events… (the lack of identifying community needs) is not yet part of police practice and raises concerns within police about the level of overlap between intelligence and engagement" (Carey, 2015). As with many aspects of law enforcement and other relevant security practitioners, levels of engagement towards social media largely differ between forces, with most mainly using it to engage with community regarding ad-hoc notifications, such as public information announcements, and petty crime announcements. This in itself may concerns members of the public whom may feel that OSINT monitoring may be a 'two-way mirror'[2], with intelligence practitioners able to observe and investigate, with minimum community engagement and interaction.

It is essential to understand and respect that many elements of OSINT investigations benefit from refraining full disclosure policies towards the specific tactics and solutions used. It should be made increasingly clear to the public, the tight rules and regulations that warrant and authorise deployment, as well as that public security and safety may benefit from the indiscretion and minimized disclosure of engagement which may help to track down community threats, protect vulnerabilities and to maximise order. It may also be beneficial to reassure public opinions that the police and other OSINT certified practitioners have to adhere to far stricter standards, than the majority of private corporations and enterprises that utilise big data analytics and collect, store and correlate personal data. To the computer-literate generations, the loss of control and ownership over personal data to organisations and corporations is not a revolutionary, or particularly terrifying revelation, however it may prove beneficial to reassure the collective, that OSINT has to adhere to far stricter protocols than agencies such as; Google, Facebook, Microsoft, and Amazon.

LEA Requirements in the Age of Austerity

Contemporary use of internet-based OSINT has helped increase the capacity and efficiency of police forces, this holds a direct knock-on effect for situational awareness capabilities. One of the leading benefits of OSINT is through the reallocation and reduction upon traditional resources. OSINT allows for relatively low-resource operations, these have the potential to save great amounts of physical and financial cost compared to traditional policing as they may carried out

2 A two way mirror has connotations of surveillance, spying and monitoring without their knowledge: https://dictionary.cambridge.org/dictionary/english/two-way-mirror.

remotely, securely with surveillance and investigative practices often requiring far less manpower than the physical presence of officers 'on the scene'.

Additionally, OSINT training is seen to require relatively low cost and time investments when compared to other police force specialisations. The majority of UK based OSINT courses offer on average 2-7 day training packages, whereas undercover officer, firearms, covert surveillance, traffic, financial and corruption officer training courses often require intensive engagement courses of up to 18 months or longer (Nottinghamshire Police, 2008). Indeed, as of 2014, open source e-learning modules are available from the College of Policing consisting of condensed 35 minute long assignments (College of Policing, 2014) and requires little training for investigators compared to other policing specializations. Furthermore, if procedure, regulation and legislation are properly adhered to, OSINT operations are usually low risk due to the non-physical involvement, with mainly reputational and organisational damages on the line. Indeed, whilst reputational and organisational concerns surrounding online privacy and free speech are increasing, leading to increased force scrutiny from both public, judicial and NGO agencies, OSINT situational awareness also is increasingly utilised, perhaps paradoxically (Barnes, 2006), for public relations monitoring and post-event feedback as a necessary tool in improving community policing approaches.

Noticeably as IoT (Internet of Things) devices increasingly permeate all aspects of modern civilisation, all investigations now have a cyber element, this is especially true of considerations for police contamination of crime scenes through device connections to routers, local WiFi's, etc. potentially compromising evidential material. This concern also encompasses the branches of OSINT situational awareness, one example being officers trained in basic social media search queries alongside traditional note-taking to assist in community roles such as identification of alleged perpetrators. Furthermore, OSINT can be used to parallel intelligence, this capability allows LEAs to protect undercover and embedded agents as well as evidence and intelligence derived from. Closed sources may be passed onto OSINT teams to recreate the same information and leads from publicly available information.

Overall, OSINT is one of the few areas that LEAs and other security practitioners may 'bring the outside in', allowing for (vetted) external expertise and advice. Indeed, conveniently the motto of the UK Army's SGMI (Specialist Group Military Intelligence, whom routinely utilise open source analysis, is; 'bringing the outside in'. Due to the nature of the open source material OSINT situational awareness may be expanded in more convenient manners to the protocols surrounding covert and classified data. For example, the outsourcing of security work to researchers and analysts may allow for taskings that anonymise or mitigate data and intelligence concerns, instead focusing on specific lines of enquiry. For example, when investigating a particular individual, social media pictures may be doctored to hide the subject of enquiry but keep in the background imagery, allowing for external actors to seek intelligence on the desired location without compromising the information of the individual.

Core Requirements for Situational Awareness

The ability to covertly monitor individuals, suspected of involvement in serious criminal or terrorist activity, has obvious benefits for the LEA and the wider security community. OSINT techniques can be used effectively in response to a range of law enforcement issues, from enhancing community safety, tackling anti-social behaviour, through to fighting serious and organised crime and combating terrorism. Any covert technique, including undercover or publically undisclosed OSINT surveillance and monitoring must be used sparingly, appropriately and where OSINT is deployed, that it is transparent, auditable and in accordance with relevant legislation. CENTRIC OSINT involvement has observed seven priority requirements for emerging situational awareness trends:

1. Counter Terrorism focus of Situational Awareness

As notoriously publicised by the technical and disseminatory skill of the Islamic State in its prime operating years of 2014-2016 (Winter, 2017. p.6.), online open sources play a crucial role in the radicalisation, recruitment, training, financing and incitement of terrorist objectives. Counter terror (CT) situational awareness priority requirements have been observed to revolve around three key vectors:

A) Defensive measures to reduce the vulnerability to attack of populations, territories, infrastructure*, and communication systems of interest.*

B) Offensive measures to locate, prevent, deter and interdict terrorist activities.
C) Measures to limit the consequences of terrorist attacks and to stabilise the situation in the aftermath of such attacks, in support of civilian authorities.

Regarding defensive measures, OSINT situational awareness can greatly assist through measures such as counterintelligence and red-teaming wherein potential target locations and individuals may be examined by researchers to reveal potential data leakage and information freely available that may compromise their security. Offensive situational awareness OSINT measures may predominantly consist of traditional researcher and analyst investigative roles, locating, monitoring and reporting on terrorist sources. Limiting the consequences of terrorist actions are reactive measures including suitable public announcements, open source monitoring from a command and control perspective and may also include the crowdsourcing of intelligence for example when the FBI requested public help unmasking the Boston bombers of 2013 (Bruinius, 2014).

2. Cyber Focus

Cybercrime, cyberwarfare and cyberterrorism have each evolved rapidly and dynamically over the past decade. Although the perception of OSINT may traditionally be considered to be of lower technological finesse than conventional cyberattacks, threats and vulnerabilities, it however has proven to be a valuable tool in identifying emerging cyber trends and promoting greater resilience. One such important area is in the investigation of - and subsequent automated crawling of - forums and dark web markets promoting, encouraging, and selling guides on hacking as well as data and hardware exploitations. Increasingly, there is the demand for LEAs to utilise automated monitoring systems to alert OSINT investigators and analysts to indicators of such behaviours. This may include cross validation of news and public sources reporting discovered data breaches, personal info dumps with cross references to increased activity or keyword appearances on illicit sites such as identified darkweb forums.

3. Threat Financing

A key challenge facing LEAs and the wider security community is in identifying and obstructing the funding of hostile actors. Players participating in terrorism activities are likely to parallel organised crime groups (OCGs) financing tactics which are already proven and known to avoid the scrutiny of the financial and government watch teams. However, despite seeking the same objectives from a financial perspective the two groups may be argued to hold different end objectives: OCGs seek to gain as much profit as possible operating in a stable environment. Usually with a consumer reliant on their activities. It is usual for OCGs in close proximity to operate in some agreed harmony in the best interests of each OCG. On the other hand, terrorist organisations usually harbour a radical and political agenda that requires funding for organisational and operational capacity; as such they are less likely to be limited by considerations to conflict with any partner.

One of the leading and more complex challenges for situational awareness focused OSINT lies in identifying and classifying requirements for the relationship between criminal and terrorist funding, as well as being able to pinpoint when criminal activities may become terrorist financing and escalating to the suitable countermeasures and procedures. Subsequently, the priority approach for OSINT situational awareness of threat financing is:

1. *Establish the identity of funding streams to terrorists*
2. *Identify the bad actors within an OCG who is funding terrorism*
3. *Identify apparently legitimate financial streams that subsequently leads to terrorism.*

4. Analysis of Cryptocurrencies

One increasingly difficult element of threat financing is attached to blockchain cryptocurrencies. Whilst currencies such as bitcoin and Ethereum are publicly available and hold open ledgers, the tracing and monitoring of illicit exchanges requires highly specialised and trained individuals, often operating in the cybersecurity and espionage spheres.

The use of "spinners" or "tumblers" can make it frustratingly difficult for LEAs to track and trace online blockchain transactions (Darknetmarkets, 2017). Whilst it is appropriate to ensure that this funding method is not overlooked by OSINT and situational awareness focused departments, the actual proven cases appear limited; additionally, they appear to rely on a lengthy and complex period of comparing online marketplace details against individual blockchain transactions.

5. Weak Indicator Analysis

Weak indicators can be particularly useful in dealing with situations such as human trafficking, illegal migration, arms and explosives manufacture, and in relation to terrorist funding. Weak indicator crawling analyses the 'ingredients' of potential threats or areas of interest, for example weak indicators, or ingredients, may be rise in hawala networks, increased ivory trade or sim card customs seizures, relating to generating money for terrorist groups. Each individual ingredient isn't a useful indicator of the overall potential funding, however when clustered together, these automated captured ingredients may reveal areas of interest that indicate a wider problem.

When utilising big data solutions and weak indicator analysis, it may be encouraged to split OSINT situational awareness teams between human led investigators and analysts and data scientists and researchers dealing with the interpretation of quantitative data. CENTRIC operations allow for the close proximity of the teams to mutually reinforce the direction of the investigation. One example of harmonious working is through the analysis of alleged terrorist recruitment social media profiles - these profiles may consist of thousands of separate individual connections. The human led operation may focus upon individuals whose profile pictures appear to support terrorist badges, emblems or carry firearms during time restrictions, however the data interpreter may assist leading the investigation towards other profiles, for example female accounts (Dearden, 2017) whom whilst not suspicious looking, are priority accounts mapped out in relation to their connection and prevalence throughout the suspect networks. Here, successful OSINT situational awareness utilises the 'human in the loop' alongside the cognitive objectivity of big data and weak signal analysis. Indeed, 'the major difference between basic and excellent OSINT "operations" lies in the analytical process' (Hribar, et al. 2014), fusing both human led knowledge with machine based capabilities.

6. Data Capture

When conducting research, operators should be encouraged to keep all tabs open, this allows a recollection of how the user got from A to Z and assist them in explaining any links if required by a senior officer. Additionally, the use of secure logbook tools such as OSIRT (OSIRT, 2017) are actively encouraged for managing histories, logging details, data capture and encrypted storage as well as for hashing documents with time stamps. Overall, the tasking document for a specific investigation or operation is the single most important article in the process. All providers should make every and all efforts to ensure all information is provided, including historic emails, mobile numbers, landlines, associates etc. Custodial records often hold a wealth of data that can often be overlooked.

One such recommended approach for data collection best practices is modelled upon the; 'The JAPAN Approach'. First developed in 1998 following the introduction of the Human rights Act by Kent Police; it is broken down in the following diagram and plays an essential role in guiding OSINT and situational awareness practice:

Justified	The actions must be justifiable in the current circumstances. For example; can the 'need for' and 'method of acquisition' to view, collect, store, and, share personal or potentially sensitive information be deemed reasonable.
Authorised	Depending on the circumstances, there may be a need for the authorisation of specific actions or focuses of the investigation. Either the individuals involved should have suitable authorisation to carry out such tasks, or it has been cleared/designated by a manager responsible for such actions.
Proportionate	The actions and data collection of the investigation must be proportionate, it must be ensured that they could not be collected reasonably and efficiently from other means, and it is necessary to pursue them altogether.
Auditable	The chain of evidence gathered from the investigation should be auditable and sufficient enough to hold up in a case of law. There must be evidence and clear presentation of how each step of the investigation is linked and developed.
Necessary	The investigator must ensure that the sought after investigation results are of importance and are being pursued in the best practice.

7. Emerging Challenges to OSINT Interpretation

Despite the best efforts to define OSINT at the beginning of this paper, the term itself and its defining characteristics are not absolute. Indeed, regarding the three defining characteristics of situational awareness OSINT there are significant criticisms of their ambiguity and how they are actually interpreted by law enforcement (Hulnick, 2010). Leading criticisms of the interpretation of OSINT are primarily focused on the definition points one and three (Gibson, 2004) (Holland, 2012), they are explored below:

1) OSINT consists of data collected from 'publicly available sources',
2) It is data to be used in an 'intelligence context',
3) The data collection can be performed in an overt manner.

Regarding the first defining point, 'publicly available sources' used in a policing intelligence context also includes financial data (such as credit reports and bank details), vehicle registration data (such as from DVLA databases and insurance providers) as well as additional data supplied to law enforcement from specialists companies that deal in bulk data and communications information. UK based companies such as Connexus GBG (GBG, 2017) and Cosain 9 (Gov.uk, 2017) utilise mobile and social media data, however only sell their specialist services to LEAs, or on occasion to other specialists. The access to such data opportunities is particularly contentious as, despite branding, they are not openly available to members of the public.

Additionally, relating to the third defining factor; the point of challenge relates to the mention that the data collection 'can' be carried out in an overt manner, but rarely does so. Indeed, such online aspects of OSINT require anonymity and discretion, in part due to data protection and policing standards, and, therefore will not be noticeable. For example, the viewing of social media profiles, without direct interaction and communication, will usually never notify the target profile they are being viewed, this is similar for the police use of specialist companies and services as detailed above for big data and communications information.

Sound usage of OSINT situational awareness must therefore include proper situational awareness that reflects on such emerging criticisms as open source investigations and intelligence increasingly become mainstream avenues of enquiry as well as becoming more prominent in the public's general knowledge thanks to modern investigative journalism and media programs. Given the ongoing debate of security and liberty between political groups, members of the public and the current government, the relatively modern integration of internet-based OSINT capabilities for surveillance and investigation, are potentially volatile topics in the post-Snowden era (Rigoglioso, 2014).

Conclusion

Overall, contemporary OSINT situational awareness is largely and increasingly dominated by online research and investigations. Due to the nature of these actions being somewhat ambiguous it is imperative that efforts are made by LEAs to balance a degree of transparency alongside protecting specific methods and tactics. Modern OSINT situational awareness has assisted LEAs with increased capacity and operational effectiveness, additionally its format allows for a degree of outsider support networks through outsourcing tasks to experts and vetted individuals. In particular, this approach has helped through emerging security concerns such as terrorist networking, cybercrime actors and threat financing trends. The inclusion of experts, analysts and security personnel into modern OSINT is an essential factor for success - the importance of the 'human in the loop' is critical for efficient, accountable and proportionate intelligence gathering. Indeed, modern tools supplied to LEAs are often of great value when used to cut away the noise and help focus investigations.

All contemporary OSINT situational awareness should be captured to the highest level of accountability, integrity and proportionality, such as through the 'JAPAN' approach described, by doing so this helps safeguard modern OSINT situational awareness methods against some of the emerging challenges, which include potential negative fallout from increasing public awareness of modern surveillance operations..

References

- Barnes, S., (2006) A Privacy Paradox: Social networking in the United States.
  Available at: http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394/1312%2523 (Accessed online: 17/12/2017)
- Bell, P. & Congram, M. (2013) Intelligence-Led Policing (ILP) as A Strategic Planning Resource in the Fight against Transnational Organized Crime (TOC). International Journal of Business & Commerce, 2 (12), 15-28.
- Bruinius, H., (2014) FBI asks Americans to help IS masked Islamic State Jihadi. Good idea?
  Available at: https://www.csmonitor.com/USA/Justice/2014/1008/FBI-asks-Americans-to-help-ID-masked-Islamic-State-jihadi.-Good-idea (Accessed online: 17/12/2017)
- Carey, Z., Denick, L., Hina, P. & Hintz, A. (2015) Managing 'Threats': Uses of Social Media for Policing Domestic Extremism and Disorder in the UK.
  Available at: http://www.dcssproject.net/files/2015/12/Managing-Threats-Project-Report.pdf (Accessed online: 17/12/2017)
- College of Policing (2014) e-Learning Release Bulletin.
  Available at: http://www.ncalt.com/file/October%202014%20E-Learning%20Release%20Bulletin.pdf (Accessed online: 16/12/2017)
- Darknetmarkets (2017) Best Bitcoin Mixers 2017.
  Available at: https://darknetmarkets.co/category/btc-mixer-tumber/ (Accessed online: 17/12/2017)
- Dearden, L. (2017) How Isis attracts women and girls from Europe with false offer of 'empowerment'.
  Available at: http://www.independent.co.uk/news/world/europe/isis-jihadi-brides-islamic-state-women-girls-europe-british-radicalisation-recruitment-report-a7878681.html (Accessed online: 17/12/2017)
- Denick, L., Hintz, A., et al., (2015) Managing 'Threats': Uses of Social Media for Policing Domestic Extremism and Disorder in the UK.
  Available at: http://www.dcssproject.net/files/2015/12/Managing-Threats-Project-Report.pdf (Accessed online: 09/04/2018)
- GBG (2017) Introducing GBG Connexus.
  Available at: https://www.gbgplc.com/uk/products/gbg-connexus/ (Accessed online: 18/12/2017)
- Gibson, S. (2004). Open source intelligence: An intelligence lifeline. *The RUSI Journal*, 149(1), pp.16-22.
- Gov.uk (2017) Digital Marketplace: Cosain 9.
  Available at: https://www.digitalmarketplace.service.gov.uk/g-cloud/services/945108024310388 (Accessed online: 18/12/2017)
- Greenberg, J., "Why Facebook and Twitter can't just wipe out ISIS online". Wired Online, November, 2015.
  Available at: https://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/ (Accessed online: 01/02/2017)
- Holland, B. (2012) Enabling Open Source Intelligence (OSINT) in private social networks. Graduate Theses and Dissertations, 12347.
  Available at: https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3354&context=etd (Accessed online 09/04/2018)
- Hribar, G., Ivanusa, T. & Podbregar, I., (2014) OSINT: A 'Grey Zone'? International Journal of Intelligence and Counter Intelligence, 27(03), 529-549.
- Hulnick, A. (2010) The Dilemma of Open Sources intelligence: Is OSINT Really Intelligence? In: Johnson, L.K. (ed.): The Oxford Handbook of National Security Intelligence. DOI:10.1093/oxfordhb/9780195375886.003.0014
- Kent Police (1998) The JAPAN Test.
  Available at: http://www.kelsi.org.uk/__data/assets/pdf_file/0003/26706/Japan-Test.pdf (Accessed Online: 13/01/2017).
- Neri, F., Aliprandi, C., Capeci, F., Cuadros, M., & By, T. (2012) Sentiment analysis on social media. Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining, 919-926.
- Nottinghamshire Police (2008) Procedure on Firearms Learning and Development V.20.
  Available at: https://www.nottinghamshire.police.uk/sites/default/files/documents/files/pd%20514%20Firearms%20Learning%20and%20Development%20-%20PROCEDURE%202008%20-%202010.pdf (Accessed Online: 16/12/2017)
- Omand, D., Bartlett, J., & Miller, C. (2012) Introducing Social Media Intelligence (SOCMINT). Intelligence and National Security, 27 (6), 801-823.
- OSIRT, (2017). The Browser Made for Open Source Intelligence.
  Available at: http://osirtbrowser.com/ (Accessed online: 17/12/2017)
- Rigoglioso, M. (2014) Civil Liberties and Law in the Era of Surveillance. Stanford Lawyer, 91.
  Available at: https://law.stanford.edu/stanford-lawyer/articles/civil-liberties-and-law-in-the-era-of-surveillance/ (Accessed 09/04/2018)
- SRIEE (2017) Personal Communication, West Yorkshire Police Cybercrime Officer, Tallinn Estonia.

- Strauss, J, S., (2004) Dangerous thoughts? Academic freedom, free speech, and censorship revisited in a post September 11th America. Washington University Journal of Law & Policy, 15(01).
  Available at: http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1290&context=law_journal_law_policy (Accessed online: 01/02/2017)
- Stone, G. (2009) Free Speech and National Security. University of Chicago Law School. Chicago Unbound, 84.
  Available at: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2975&context=journal_articles (Accessed online: 01/02/2017)
- UNSC (2016) Security Council Presidential Statement Seeks Counter-Terrorism Committee Proposal for 'International Framework' to Curb Incitement, Recruitment.
  Available at: https://www.un.org/press/en/2016/sc12355.doc.htm (Accessed online: 01/01/2017)
- Winter, C. (2017) Media Jihad: The Islamic State's Doctrine for Information Warfare. Institute for Strategic Dialogue.
  Available at: http://icsr.info/wp-content/uploads/2017/02/Media-jihad_web.pdf (Accessed online: 16/12/2017)

The T-Factor – New Technologies and Intelligence Analysis Learning

José María Blanco
Guardia Civil, Spain[1]

Jéssica Cohen
Yaiza Rubio
Félix Brezo
Private Sector, Spain

Abstract
The world is continuously evolving in regards to the so-called VUCA environments (volatility, uncertainty, complexity, and ambiguity). If we adopt a PESTLE analytical model (which includes political, economic, social, technological, legal, and environmental factors), we can see that new technologies are the great "game changers". This concept, usually considered in foresight and future studies, can be defined as a new introduced element of factor that changes an existing situation or activity in a significant way. This technological factor (T-factor) is changing the way that we live, think, interact, communicate, or access services in an increasingly digital society.
Considering what Lowenthal (2013, 2015) has pointed out, intelligence tradecraft is in a permanent process of *"fatigue reform"*. This paper will identify how Information and Communication Technologies (ICT) are: first, affecting the so-called intelligence cycle; second, offering new opportunities to collect, evaluate and integrate old and new sources of information; third, generating new corporative and personal risks for intelligence analysts, especially in the cyberspace; fourth, introducing new bias; fifth, modifying classical skills usually developed in intelligence analysts; sixth, offering new tools to support the daily work of the analysts: big data, predictive systems, semantic analysis; and seventh, changing the way in which intelligence products are disseminated, with more visual contents: maps, infographics, and diagrams.

Keywords: Intelligence, analysis, technology, VUCA, learning

1 Corresponding author's email: blanco.josemaria@gmail.com

"Whatever the complexities of the puzzles we strive to solve and whatever the sophisticated techniques we may use to collect the pieces and store them, there can never be a time when the thoughtful man can be supplanted as the intelligence device supreme"

(Kent, 1965, p. xviii).

1. Technologies affecting the so-called "Intelligence Cycle"

The accelerated process of innovation also affects criminal phenomena. It is not a coincidence that EUROPOL has chosen *"Crime in the Age of Technology"* as a subtitle for this year's SOCTA report (2017, p. 24), stating that *"for almost all types of organised crime, criminals are deploying and adapting technology with ever greater skill and to ever greater effect. This is now, perhaps, the greatest challenge facing law enforcement authorities around the world, including in the EU"***.** In its report *"Exploring tomorrow's organized crime"*, EUROPOL identifies eight key drivers for change. All of them are linked to information technologies and other related technologies: internet and deep web, social media, big data, cloud computing, mobile applications, Internet of Things, nanotechnology and smart cities.

Considering that technologies are a key factor in new criminal trends, Law Enforcement Agencies need to strengthen their efforts in order to improve their intelligence capabilities. Professionals from police forces and/or criminal intelligence departments need continuously new and specialized training to counter new threats and to take advantages of new opportunities. New technologies are at the same time both part of the current security problem and part of the solution as well. Since the 9/11 attacks (National Commission on Terrorist Attacks, 2004), there has been a continuous effort to improve the capabilities of intelligence analysts. The intelligence community has been always questioned after the attacks, due to the simple fact that it is too easy to carry out analysis from outside, always after the main event has happened and once all the information is available. This situation which originates intense media chatter.

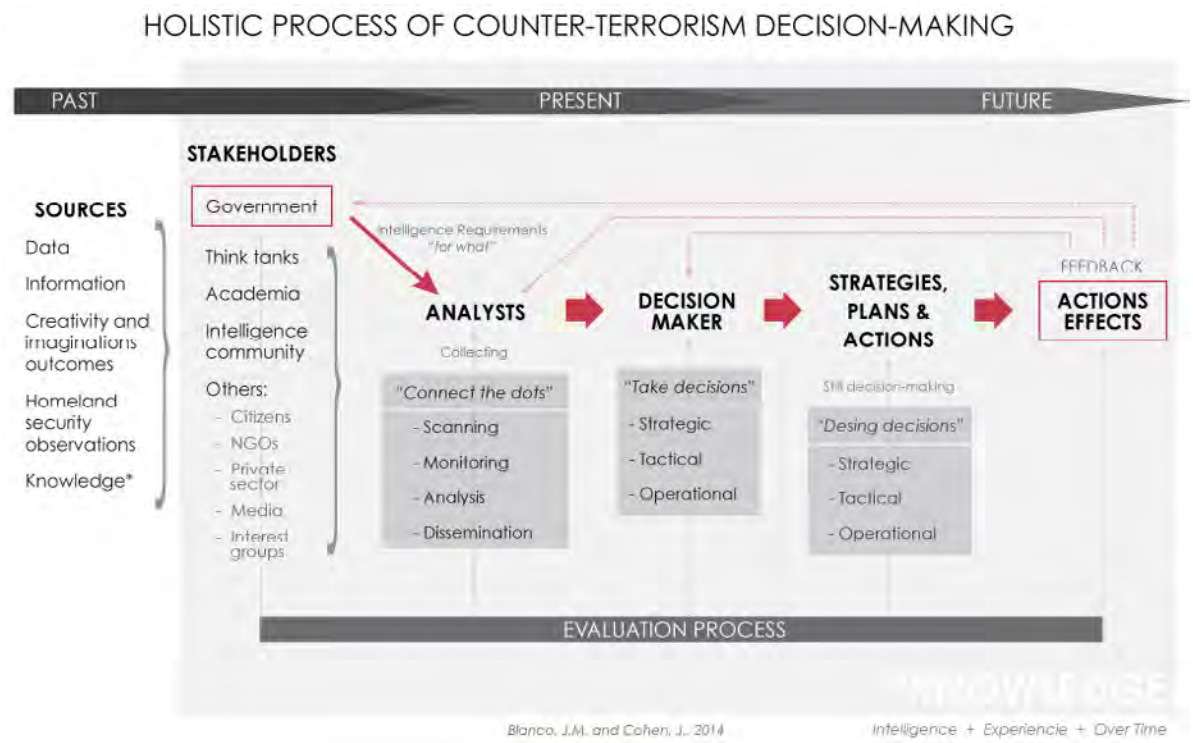
1.1 The end of the intelligence cycle

The intelligence cycle appears in many manuals, articles and training courses as the center of the whole intelligence discipline. It is pointed out that the cycle is an excessively theoretical construction that translates an unreal image of work into intelligence, leading to thinking that it is sequential, and cyclical. Several official models do not incorporate key tasks such as evaluation. As far as this chapter is concerned, and with the idea of "tools" in mind, it is evident that the current technological development is modifying the whole process in its classical conception:

- New technologies allow the incorporation of new tasks in the phase of collecting, including some tasks that had always been considered part of later steps. For example, open source management systems allow the extraction of entities and are able to immediately perform information integrations based on them. New technologies are capable, with an increasing degree of success, of synthesizing texts, as well as translating information into maps and other geolocation applications. We also work on approaches to automate the evaluation of information, for example, contrasting the same facts in different sources.
- The monitoring of information is becoming by itself a whole specialization. Systems can be feeding other basic and current intelligence systems on a continuous basis.
- Several technologies can support analysis tasks: ACH, decision support systems, statistical packages or integrated platforms (IBM i2).
- Technologies also modify the way in which information is presented, with a growing incorporation of visual and multimedia elements in intelligence reports, to the detriment of the text, which makes the work of analysts and decision makers easier and saves time.
- Technologies can also be useful in the training of intelligence analysts, improving their skills: serious gaming, simulations, or case studies.

Because of these reasons, we propose a broader concept such as the process of intelligence, which can be defined as the *"set of activities developed in an organization, by analysts, and aimed at obtaining information and analysis to support decision making in time, place and form"* (Blanco & Cohen, 2014, 2016).

Figure 1. Intelligence Process. Source: Blanco and Cohen (2014 & 2016)



1.2 The need to avoid "technological solutionism"

Our current society is characterised by the intensive use of technologies, especially in the field of ICT. Their contribution has been fundamental in providing new services and features to citizens, who can interact at any time and place. But they can also generate new risks and threats. New technologies are the great "game changer" of our time.

Among the critical views, or at least those that try to warn of the negative effects of the technologies, we can highlight the works of Eugeny Morozov. In 2013, Morozov criticized what has been called "technological solutionism", i.e., the vision of technology as an objective instead of a means to get different objectives. For Morozov, every problem has a technological solution. There are even technological solutions aimed to face problems that do not exist. In the field of intelligence analysis, it is possible to find technological warnings, such as those pointed out by Lowenthal in reference to Big Data (2013). Perhaps the most coherent position would be to rely on the benefits of the technologies, but maintaining a "situational awareness" towards them. New technologies are the source of new threats and risks, but, at the same time, they are part of the solution.

The possible debate on technologies and intelligence analysis raises two possible scenarios: technological automation of the analysis versus technological support to the analysis (or enhancers of the analysis through technology). Intelligence analysis is a human-driven process, and can be technology-enabled at the same time.

In the field of innovation in Europe, some projects have been financed by the European Commission, such as RECOBIA, which have shed a light on the difficulties faced by organizations in the identification of tools that meet analytical needs. Proprietary applications are expensive and require time for development. Commercial developments present additional risks, including: high prices due to the short life cycle of technological innovation, risks in information and data security, or technological proposals that cannot yet be considered mature. This situation leads to a situation of technological paralysis.

Intelligence analysis tools, in the opinion of the analyst community, are not being effective in separating *"the signal from noise"* (Silver, 2015) or in reducing uncertainty. There is a clear gap between what is offered technologically and the analysts' expectations.

Badalamante and Greitzer (2005, p. 5) pointed out that *"the complexity, uncertainty and ambiguity in which the analyst moves to reach judgments about future events and actions will remain for a while despite the improvement of the capabilities of the software tools"*.

There is, however, a high degree of consensus on the technological support for intelligence analysis, as a way to:

- Manage complexity;
- Limit cognitive biases: warning about them and their impacts;
- Manage volume, volatility and variety of information, especially in its unstructured character (text format, imagine, video, etc.);
- Overcome the human limitation to process and interpret large amounts of data and information;
- Support analytical tasks;
- Improve the presentation of intelligence products, especially through the support of visualization tools;
- Training and developing new skills, through simulations and serious gaming.

It is possible to differentiate between two large groups of technological challenges in intelligence analysis, external (environment and specific current characteristics of information) and internal (organizations and analysts).

Table 1. Technological challenges in intelligence analysis

External	Environment VUCA	Identification of trends	Prospective challenge
		Wild Cards	
	Information	Infoxication	Quantitative challenge
		Reliability of sources and credibility of information	Qualitative challenge
Internal	Organization	Leadership Change management Digital transformation	Organizational challenge
	Analysts	Cognitive biases Impacts of technology on cognitive skills Obsolescence of knowledge and skills Cybersecurity concerns	Cognitive challenge

External challenges

In a VUCA environment, there are two main challenges for analysts. On one hand, they must detect technological trends that affect either the subject matter of the analysis or their own function as an analyst, under a dual perspective in both cases: new threats and new opportunities. On the other hand, it is advisable to develop a prospective exercise that allows to anticipate technological "wild cards" (Petersen, 1997), facts of low probability and high impact, in order to adapt the present strategies.

It is understood by infoxication, infobesity or information overload the situation produced because of having too much information to follow a topic or support the decision making. The incessant generation of content, a low relation between signal (valid information) and noise (disposable information), and the ignorance of the average citizen on how to handle information contribute to this effect, which in its English terminology ("information overload") was coined in 1970 by Alvin Toffler in "The Shock of the Future", although it was previously mentioned by Bertram Gross (1964, *The Managing of Organizations)*.

The current world, in which the concept of post-truth has recently been coined, shows us how the invocations of emotions are above the facts themselves. Lies, propaganda, misinformation, and deception often find support in new technologies, both as facilitator and enhancer (Viner, 2016). The great challenge a decade ago was managing the amount of information. Now, we face another difficult challenge: the evaluation of all this volume of information when, increasingly, part of it is false or has been manipulated.

Internal challenges

Internally, the new environment affects both the intelligence organizations (thinking both of the public and private sectors) and the analysts themselves. Organiza-

tions, as part of today's society, must develop a continuous monitoring of the desires and expectations of the people that they serve. Again, the technological component is a key factor, leading to the development of ambitious digital transformation strategies and plans. Organizations must promote and manage change. Surely, success will be in the hands of those organizations that change the rules of the game, and not in those who only know how to adapt. The digital transformation requires an external dimension (towards the client) but also an internal one, taking the digital gap among its workers as one of the biggest challenges to face.

Biases are unconscious mental errors resulting from the instinctive propensity to simplify decision-making, leading to shortcuts or deviations in judgment. They are usually based on memory, experience, education, cultural baggage or ideologies. Biases are a consequence of the quantitative and qualitative challenges presented by the information. Kahneman (2012) has detailed that there are basically two types of thinking, one fast and intuitive, and other slow and logical. The first is useful to tackle known and familiar environments, being a thought that is always activated and does not generate fatigue. The problem is to respond in the fast mode to complex problems. For that purpose we need to activate slow thinking, which is exhausting, demanding high cognitive resources and cannot be kept active continuously. Admitting the existence of biases should lead analysts to be cautious.

Some of the bias inducted by technologies are originated by the way in which search engines are used. Eli Pariser (2012) has pointed out the "filter bubble". Algorithms guess what information a user would like to see based on previous information about them, such as their location or their search history. Users become isolated from information that disagrees with their viewpoints, keeping them in a bubble. Technologies could strengthen other classical biases: proximity of information, confirmation (Cook and Smallman, 2008), completion, anchoring or heuristics.

In the same way, technologies may already be affecting some of the analysts' cognitive abilities. Some effects have been pointed out in recent times. As an example, because they are well known, we will highlight:

- "Google effect": We use Google and the Internet in general as a supplementary memory. We reduce the personal demands of memorization, trusting that we can easily recover information on the Net.
- "The Shallows" effect: Nicholas George Carr (2010) develops an argument: The Internet can have detrimental effects on thinking that damage the capacity for concentration and contemplation, which causes a deficit in the memory's storage capacity and in the processing of the information. Reading long articles and books has become an arduous task. Precisely, multitasking, a sign of our times, is a possible cause.
- "Focus effect": Goleman (2013) highlights the difficulties in focusing on a single task, a situation in which the great human technification and its dependence on a multitude of informational inputs greatly influence our cognitive capabilities. The solution he proposes is meditation, in order not to damage this human and necessary capacity. For Goleman, multitasking does not exist, it is not a human capacity.
- "Addiction effect": Dopamine is asking us to receive continuously new informational inputs. This limits our capabilities to analyze and to go deeper inside them.

These observations, controversial in part, but very popular nevertheless, require to look for points of consensus. Technologies do affect the brain, but it may perhaps be noted that there is no loss of mental abilities, but rather an adaptation that, in addition, only occurs in the long term. The plasticity of the brain causes an adaptive process.

This situation presents specific challenges in the intelligence process:

Table 2. Technological challenges in the intelligence process. Blanco and Cohen

TASKS	CHALLENGE
Planning and direction	Technological surveillance Technological requirements Identify end-user requirements Option: own development or commercial product Cost-benefit analysis Security concerns
Collecting, monitoring and processing	Collecting tools. Crawls. Entity extraction. New demand in intelligence services: Tools for verification Training using OSINT tools Security concerns
Analysis	Previous agreement: human-driven analysis and technology-enabled analysis Training using analytical tools. Complex, because implies knowledge in different domains (data mining, statistics…) Develop computer support for structured and advanced techniques of analysis (for example ACH with Bayesian support)
Dissemination	Developing of visualization tools, integrated with analytical capabilities Complexity needs training (for example Tableau)

2. The T-Factor - New skills for intelligence analysis

In the 1990s, the US Army outlined what would be a new military training program. Its parameters were defined with a clear objective: to develop the capacity of its members to act under highly complex contexts. This was a new need that emerged after identifying the main characteristics that would determine future scenarios, coined as VUCA environments (acronym for volatility, uncertainty, complexity and ambiguity, see figure I). As a result of this initiative, in 2004 the first results of a new program known as Thinking Training Method and Think like a Commander (TLAC) were published. The final conclusions were defined in the first lines of the document: "*Success in future operations will depend on the ability of leaders and soldiers to think creatively, decide quickly, take advantage of available technology, adapt easily and act as a team*".

This scenario is not an option but a reality, and is a challenge for analysts, with the added complexity of not being trained for it, as if it were the TLAC program.

Table 3. VUCA elements

COMPLEXITY Each event is conditioned by a multiplicity of causes and factors, each of which is interrelated with third events. This situation generates a high level of confusion that prevents us from having a clear vision of the situations that we face.	**VOLATILITY** Changes are rapid, almost unpredictable, making it difficult to identify trends or patterns and reducing the stability of processes. The type, the magnitude, the volume and the speed with which they occur make analysis tasks difficult.
AMBIGUITY The answer to the key questions (who, where, why, when...) is difficult to establish. Errors of interpretation and the plurality of meanings is a cause and effect of confusion, resulting in an increase in imprecision.	**UNCERTAINTY** Many of the changes that take place are disruptive, evidencing that the past does not have to be an indicator of the future, and hindering our preparation in the face of future scenarios.

If we do not have this VUCA environment in mind, it is impossible for the next generations of analysts to be well trained. In the same way we will fail in the recruitment processes. It is very complex to properly select a profile of analysts when there is blindness to the tasks that they are supposed to do.

Therefore, it is necessary to consider, not only the limitations of the present, something that is already conditioning us, but also what the future will be like: understanding what challenges and opportunities it will offer us and what skills we have to train in order not to be overwhelmed by its complexity.

Precisely to respond to these limitations, a second acronym of VUCA emerged, as an antonym, trying to focus on the perspective from which these environments must be understood, "VUCA Prime": vision, understanding, clarity and agility (Figure 2). It is configured as a set of inexorable skills needed in the present and future times of our societies (Blanco & Cohen, 2017).

Table 4. VUCA Prime Responses

CLARITY over COMPLEXITY Even chaos can make sense. Generate knowledge maps. Make a dynamic tracking of the existing analyses to detect new evidences (monitoring). Understand each phenomenon from within and from the global perspective simultaneously. Do not use simplistic, mono-causal or mere chance explanations, trying to answer all possible questions. One of the great challenges is knowing and knowing how to use constantly changing information from disparate sources.	**VISION over VOLATILITY** Think in future as a habit. Imagine scenarios and analyze them in a back-casting process to detect indicators, in order to avoid future risks and threats. The objective and methodology applied must be clearly defined. We must be able to rapidly integrate large amounts of information without the process or tools used, resulting in less precision and speed.
AGILITY over AMBIGUITY Maximize the ability to learn, make mistakes, communicate, respond and adapt. It requires rapid problem solving and constant decision-making. It must be proactive and be focused on the problem to anticipate the effects even before adopting the answer. The technologies used as support have to be agile and adaptable to users and needs, leaving behind generalist solutions.	**UNDERSTANDING over UNCERTAINTY** The phenomenon that we face must be fully understood. The answer should go beyond our own previous experience and knowledge. It needs to build knowledge networks, with trust and credibility, and use new technologies to strengthen the whole process and progressively improve reasoning skills.

Taking into consideration these previous definitions about the way in which the future has materialized, from our daily experience as analysts, but also as managers of analysis units and professionals of new technologies, we point out the need to use new principles for training new analysts: the use of serious gaming, the focus on skills and not only on knowledge, the shift of the teaching approach in favor of the learning approach (empowering students) and the need to consider any organization as a center of continuous learning, without leaving this work (responsibility) only in the educational sector.

2.1. Game as a transversal skill

When we refer to the game, we allude both to the need for its existence in the training processes (serious gaming), and to its value in terms of attitude, which we will call gaming-mind.

The training in which the game is allowed goes beyond the theoretical content, making it easier for the analysts to put into practice, both individually and as a group, the skills that are required before a given question or problem, without being exposed to the risk that would involve doing so in a real situation. It is a "learning based on experience" process that makes it easier to immediately obtain feedback and that also trains the agility of response and allows the analyst to be exposed to rapidly changing dilemmas. These demands are highly related to the growing demand for discovery, collection, evaluation, integration and synthesis of data from the use of new technologies.

Under this type of activities, the didactic level is maximized, because not only the theoretical content is contemplated, but also its development and use, having to deal in a simulated way with the problems that the reality would generate.

However, this problem is evident from an early age, where the anachronistic teaching methodology of the current educational centers detracts from this component, perhaps because it is perceived as a waste of time, perhaps due to not knowing how to visualize it outside the children's environment.

While it is true that agencies like the CIA have been using games for years as a training tool for their agents, the use of these techniques is not widespread. This is even more palpable in general formations of profiles that, a priori, have not decided to focus their professional career within the intelligence analysis, as is the case of the police bodies, whose position is finally defined by many other rather organizational criteria (conditioned by vacancies, promotions, countries of work, categories, etc.).

However, this not only facilitates the highlighted processes, but can work as: a source of ideas; an improvisation generator; and a creativity enhancer. It can also facilitate the search for alternatives; the decision making; as well as contribute to an improvement of the social skills and a greater training in the control of biases. All of them are relevant areas for every intelligence analyst.

Highlighting among these benefits human ingenuity, experience and creativity, is a relevant factor in intelligence analysis, but also in our need to work with machines and to be different from them. If the empowerment of people that is today allowed by the use of new technologies is answered with greater creativity, not only at the individual, but at the organizational lev-

el, it will be easier to make smarter decisions, to solve more complex problems.

2.2. Abilities and skills, not only knowledge

In 1970, Alvin Toffler described the symptoms of the "shock of the future". The speed at which the change occurs comes to generate greater implications than the direction in which it materializes. Events happen so quickly that we have to be able to talk about the past and the future simultaneously. Managing complexity, Toffler pointed out, would be the major problem for societies in the future. A context that, by pure definition, is being harmful to those people and organizations that are rigid and have difficulties adapting to vertiginous change. This context is having a great impact on an essential element: knowledge.

The creation, transmission and assimilation of knowledge advances and is modified in the same way as society, science, technology as or communications. In this sense, Toffler himself stated (p. 414) that *"the illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn"*. He was using words from the psychologist Herbert Gerjuoy of the Human Resources Research Organization[2]: *"the new education must teach the individual how to classify and reclassify information, how to evaluate its veracity, how to change categories when necessary, how to move from the concrete to the abstract and back, how to look at problems from a new direction—how to teach himself. Tomorrow's illiterate will not be the man who can't read; he will be the man who has not learned how to learn"*. Toffler added that training persons would not be based on immovable knowledge that you have in your mind, but in function of the abilities needed at every moment

Years later, in the conference "*New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities*" (Rome, Italy, 31 March - 2 April 2004), it was showed that, after the fall of the Iron Curtain, the intelligence requirements changed completely. It was not a sudden transformation, but it was a challenge in terms of the training of the analysts, who were forced to pay attention to other environments hitherto neglected, such as larger, global scenarios that require both short and long term for their understanding, with multiple new cultural connotations and linguistic differences.

Imagining, listening, experimenting, making mistakes, creating and destroying creatively, using intuition, are key skills to live in the future. Knowledge will become a set of skills, not of immovable knowledge and its use, in line with the opportunities provided by new technologies, will be a key factor of success. The objective will be to create differential value through a specific skill at a given moment. As Toffler said, by teaching students how to learn, unlearn and relearn, new dimensions can be incorporated into education.

2.3. Learning, not teaching

The aim of education is learning, not teaching. The book *"Turning Learning Right Side Up: Putting Education Back on Track"* (Ackoff and Greenberg, 2008) focuses precisely on trying to answer why we keep trying to teach people to be machines and not to enhance their abilities as humans, as highlighted in the previous section.

Memory is confused with learning and that conditions us so that we will hardly remember in our adult life what was taught to us. However, what was learned (talking, walking, how to dress) will remain, in general, in our imprint in a perennial way.

It is about generating the same dynamics that generate learning before a new job. In this process, the teaching, if any, is minimal. However, learning arises from the observation, imitation, the need, the explanation of reference examples, but not the talk.

Learning escapes the standardized and standardized formats of what an adult is supposed to be in society. You learn by trying, failing, sharing, interacting informally to get answers and sharing what you have internalized.

Learning through explanation is another pillar of this vision. The "explainer" is required an extra effort that the teacher is not required, the need to put themselves in the mind of the other to be able to answer their question. A practice that involves developing "environmental culture": not only taught based on what is known, but it is explained based on the difficulties that a third party poses. You learn to "learn from others". In this context there is a need to use experienced analysts as mentors for those more novices, thus sharing experience, training and skills.

2 The book's notes state that Gerjuoy's comments are from an interview with Toffler.

2.4. Learning organizations

Following the previous scenario and taking into account that new technologies allow us a greater daily diffusion between the biological, the physical and the digital, it is also possible to talk about the learning needs within organizations.

Peter Senge's vision of a learning organization as a group of people who are continually enhancing their capabilities to create what they want to create could have a clear use in intelligence analysis teams. According to Peter Senge (1990, p. 3) learning organisations are: *"…organisations where people continually expand their capacity to create the results they truly desire, where new and expansive patterns of thinking are nurtured, where collective aspiration is set free, and where people are continually learning to see the whole together" (The Fifth Discipline).* For this to happen, it is argued, organizations need to "*discover how to tap people's commitment and capacity to learn at all levels*" (*ibid.*: 4).

Senge points out different ways of learning. *"Survival learning"* or *"adaptive learning"* is important and necessary, but it is not enough, and organizations need to develop a *"generative learning"* that enhances the organizational capacities. This is why an intelligence department must be continuously looking for the way it can improve knowledge and especially develop new skills.

This concept has several links with the new skills needed to survive in VUCA environments. For this purpose, organizations should cultivate five disciplines:

1. Systems thinking: ability to comprehend and address the whole, and to examine the interrelationship between the parts.
2. Personal mastery: organizations learn only through individuals who learn.
3. Mental model: learning to unearth our internal pictures of the world, to bring them to the surface and hold them rigorously to scrutiny.
4. Building shared vision: unearthing shared "pictures of the future" that foster genuine commitment and enrolment rather than compliance.
5. Team learning: aligning and developing the capacities of a team to create the results its members truly desire.

All of these 5 disciplines are key elements in intelligence analysis, in which there is a need of holistic approaches to have the "big picture" about security phenomena, and a strong critical thinking philosophy to challenge previous or intuitive judgements. Individual and team learning must be balanced, taking into consideration that intelligence analysis is a team work.

This learning must be guided by the shared vision about their mission, and the aim of improving the intelligence process and the intelligence final product, in order to facilitate decision taking. This must be favoured not only by governments or institutions, but also by teachers, human resources, managers and analysts themselves.

Table 5. How to survive - abilities needed in a VUCA world

CLARITY over COMPLEXITY	VISION over VOLATILITY
Adaptive thinking Lateral thinking Knowledge Management **Information overload management** Diversity management Intellectual curiosity Star-busting creativity techniques Cognitive biases management **Data analysis** Operating with estimates (Lowhental[3]) General / holistic approaches as well as **t**echnical vision **Information media literacy** Observation Explainers (Ackoff & Greenberg)	Learn to learn Knowing how to unlearn Continuous training Anti-fragility (N. Taleb, 2013) Creativity Agility Motivation humility Cognitive adaptability Collaborative intelligence Knowledge management based on the team Diagnosing collaboration barriers **Self-taught use of new technologies** **Gaming-mine** Evaluative vision **Social media relations ability**
AGILITY over AMBIGUITY	**UNDERSTANDING over UNCERTAINTY**
Critical thinking Experimentation Learned lessons Learn to doubt Dismisses the superfluous Self-driven learning Social pressure management Proactivity **Decision-making engineering** Team-based decision making quality Adaptation of the methodologies to the study objective Finding solutions Intelligence analysis process development Crisis management Time and priorities management **Serious gaming techniques** Talent management Critical writing Resolution / decision-making	Transparency Confidence Managing overconfidence (honestly introspective) Collaboration / teamwork **Technological awareness** Creating scenarios / simulations Idea Generation **Validation of acquired knowledge** Inter-personal skills Intelligence of the crowds **Leadership In virtual and transcultural teams** **Information visualization techniques** High performance team development **Management of virtual teams**

The future, no matter how disruptive or distant it may seem, is not immune to our control. As organizations, analysts and citizens, we all have the ability, if not the responsibility, to intercede in their evolution with our decisions. Having the necessary skills to make these as accurate as possible is only the beginning, having become a condition *sine qua non* to our future.

3. OPSEC and privacy in online investigations

Operational security (OPSEC) is a process designed to protect intelligence analysts from being identified by third parties. Its implementation results in the development of countermeasures, which do not have to be necessarily technical, in order to prevent possible leaks. We are now going to discuss some examples of this.

3.1. Identity management in the network

When carrying out research activities on the network, the analyst will need to authenticate in certain services in order to obtain additional information. In this process, the management of numerous identities can be an obstacle if it is not properly planned from the very moment of the creation of those profiles.

The reuse of real profiles implies the risk of exposing the analyst's identity through their usernames, emails, photographs, comments, affiliations or even IP addresses. The large number of leaks of information made public over these years, which have involved top-tier companies such as LinkedIn, Adobe, Dropbox or Yahoo are just a reflection that the exposure of sensitive information of users is not only possible in low-profile websites. Websites like HaveIBeenPwned.com[4], maintained by Australian security specialist Troy Hunt, or Hacked-Emails.com[5],by José M. Chia, are some examples of this.

A protection tool for analysts is the use of password managers like KeePass[6]. These managers are applications in which the user can store different passwords for each profile that will be used, generating them randomly and storing them in a database encrypted with military standards such as AES256. As a consequence, the analyst will prevent the leaking of information in one of the resources they use from exposing sensitive data from other platforms, as the passwords for every platform are different from each other. Obviously, the user will have to take care of the security of this database, using a very robust password to prevent that, in case of loss or theft, a third party has access to their data.

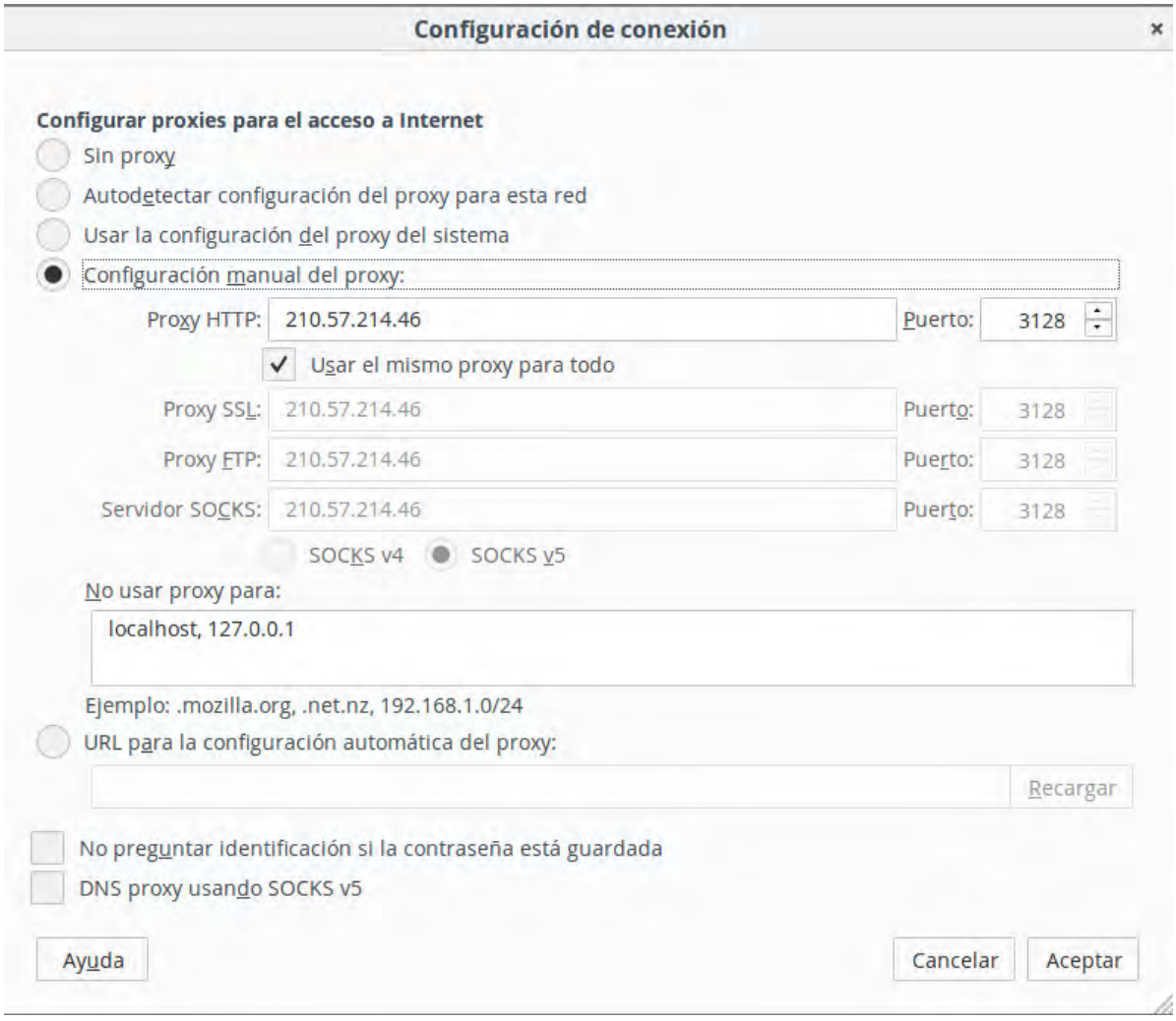
3 http://www.tandfonline.com/doi/full/10.1080/02684527.2017.1328856

4 https://haveibeenpwned.com

5 https://hacked-emails.com

6 https://keepass.info

Figure 2. Configuration window for HTTP, HTTPS, FTP and SOCKS proxies in the Firefox browser.



Creating profiles on the best-known social networking platforms can be difficult if the analyst's aim is to act as anonymously as possible. The analyst has to be aware that platforms like Twitter will offer recommendations based on the account's location, its activity, the people it follows, the accounts with which it interacts, the *tweets* in which it participates or the email address used in the registration process, thus establishing links with real contacts of the original profile. Mail providers such as Gmail or Outlook request numerous personal information and establish a series of mechanisms that are difficult to dodge from the moment they begin to suspect that too many accounts are being created from the same location. Therefore, many end up opting for email providers such as ProtonMail[7] (or mail2tor.org, cock.li, airmail.cc, mailcatch.com or guerrillamail.com) that will offer email accounts without performing too many checks.

7 https://protonmail.com

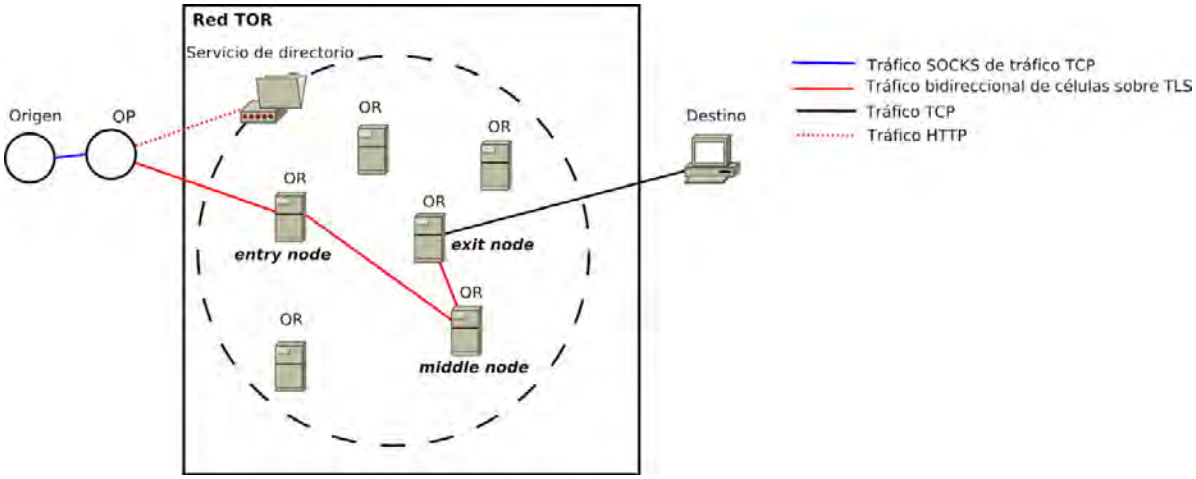
3.2. Masking the identity of the analyst

One of the problems that analysts have to face when conducting an investigation is the masking of the connections' origin. Normally, the IP addresses from which we connect are visible to the services we visit, since the point from which the requests are made can be registered.

The use of proxies

A proxy server is an element that acts as an intermediary between two systems, so that both ends of the connection do not interact except through this intermediate agent. In this regard, each system only has visibility of this intermediate agent, which in practice has the effect of masking the origin. There are a lot of lists of public proxies located in different places like free-proxy-list.net or freeproxylists.net.

Figure 3. Operation diagram of the Tor network. Source: Fercufer (Wikimedia)



The configuration of these proxies in the browser is quite simple. Just take note of the country from which you want to exit and adjust the parameters of the proxy settings. For this case, we have chosen a proxy from Indonesia, whose IP address is listed as 210.57.214.46 through port 3 128.

The main problem presented by these lists, regardless of their availability and latency, is that the user has no real way of knowing what these intermediaries do with their data.

VPN

While *proxy* servers only act as intermediaries between two points, a VPN is a more complex technology that allows extending the extension of a domestic or corporate local network beyond its physical location. Although they can also be used as a gateway to avoid revealing the real IP address, their functionalities go far beyond those of a mere intermediary, since they allow, for example, that employees working outside an office have access to shared resources. The connection between the user and the physical network itself is tunneled so that the traffic circulates in an encrypted and safe way.

The Tor network

The Tor project[8] was conceived with the aim of offering users an additional layer of privacy in the use of the internet. Thus, the use of the Tor network for conventional navigation protects the origin of the real user's request by exposing only the output node requesting a particular resource. Tor is a free *software* designed to help activists, journalists and Internet users to evade mass surveillance by routing encrypted traffic through a series of nodes that make up this network.

The user, instead of connecting directly to his destination, chooses a node of the Tor network as an entry node after connecting to a directory of available nodes. The exit node is the one that will connect to your destination and your IP address will be the only one that the destination will have a record of.

Navigation through Tor is not an absolute guarantee for 100% anonymous navigation. Unfortunately, a recently discovered bug related the way publish local links are published could expose the user's real IP address of the user on Mac and GNU / Linux systems. The bug has been quickly corrected not only in Tor Browser Bundle but also has been moved to the project on which it is based, the Firefox browser itself.

Footbridges towards the Tor network

To facilitate access to the hidden services without having to configure any software, there are known as Tor gateways that act as an intermediary between the user who tries to access a resource.onion and the resource itself, collecting the result and serving it again. There are multiple platforms on the internet that offer these services, mainly based on the Tor2Web project. Examples of this type of platforms are onion.city, onio.cab, onion.plus and onion.link among others.

However, the use of gateways implies that the user renounces to a significant part of their anonymity by granting the intermediary information that was not available to the final server. For the user, these practices carry the risk that, not only the requests made may be registered by a third party together with their real IP address, but also that the responses received have been adulterated by the intermediary.

8 https://torproject.org

Other alternative networks

Apart from the Tor network, there are other types of networks that can be mentioned, such as I2P (Invisible Internet Project)[9]. This project focuses on offering a layer of abstraction of communications within the network in order to offer anonymous web pages, chat clients or file transfer platforms. The main difference with the Tor network is that I2P has been conceived to be used as a gateway to the conventional network. Lately, the IPFS system has also been gaining importance[10], Inter Planetary File System. It is a distributed protocol in which the different nodes of the network share disk space and replicate the content for all the nodes of the P2P network. The project is used in combination with blockchain technology to store content on a continuous basis.

3.3. Operating systems

There are some operating systems whose main objective is to preserve the user's safety. Although each of them puts the focus on a different aspect of security, they all assume that the user will be exposed to vulnerabilities and failures that can compromise both their identity and the integrity of their system. Some of these operating systems are:

- Tails[11] (acronym for The Amnesic Incognito Live System). This is a distribution designed to protect privacy and anonymity by requiring that all connections of this Debian system be made from the Tor network through the use of Birdy[12] (a plugin to use Tor with Thunderbird), with Pidgin or KeePassX for managing passwords. Unlike conventional operating systems, it has been specifically designed to be executed from a Live CD or USB so that it leaves as little fingerprint as possible in local storage;
- Whonix[13] is distributed in a virtualized environment with two virtual machines. One of them has the sole mission of acting as a gateway to the Internet, routing all the traffic generated by the other, which acts as a work station, towards the Tor network;
- Qubes OS[14],an operating system that has been designed with security in mind and that implements the concept of security by isolation and is defined as a "reasonably secure operating system". If an application is compromised, it cannot affect other applications outside the domain in which it is present. Different security levels are applied, for example, to execute banking transactions or consult mail.

Conclusions

This paper has identified how technologies are affecting the so-called intelligence cycle. New technologies offer new opportunities to collect, evaluate and integrate old and new sources of information, to analyse data and information third, and to disseminate the final product in a seductive way.

But, on the other hand, new technologies are generating new corporative and personal risks for intelligence analysts, especially in the cyberspace, and introducing new bias. Clearly, it is possible to point out a set of technological challenges in intelligence analysis. Some of them are external factors: the technological landscape in continuous evolution and the characteristics of information (infoxication and increasing difficulties to evaluate sources and pieces of information). Other factors suppose internal challenges, both for organizations and analysts: digital transformation, new leadership, new cognitive bias, obsolescence of knowledge and skills, or new security concerns.

This paper proposes a roadmap to improve the learning of intelligence analysis, with three main pillars: first, focus on learning instead of teaching; second, focus on organizational learning; and third, focus on learning by gaming and doing. Agreeing that technologies are a key factor in new criminal trends, Law Enforcement Agencies need to strengthen their efforts in order to improve their intelligence capabilities. For this purpose, an adaptive VUCA framework can show us the main challenges we face to analyze and interpret this world, and especially its criminal phenomena, letting us to identify new knowledge and new skills needed to tackle old and new threats and risks.

Finally, intelligence analysts face new concerns, because of their possible high digital exposition. Operational security (OPSEC) is a process designed to protect them from being identified. In this process of continuous evolving technologies, cloud computing, artificial intelligence, OPSEC is a relevant content training for new and old intelligence analysts.

9 http://geti2p.com/

10 https://ipfs.io

11 https://tails.boum.org/

12 https://addons.mozilla.org/en/thunderbird/addon/torbirdy/

13 https://www.whonix.org/

14 https://www.qubes-os.org/

REFERENCES

- Ackoff, R. & Greenberg, D. (2008) Turning Learning Right Side Up: Putting Education Back on Track. FT Press.
- Badalamante, R. V. & Greitzer, F. L. (2005) Top Ten Needs for Intelligence Analysis Tool Development. Proceedings of the First Annual Conference on Intelligence Analysis Methods and Tools. Richland. Pacific Northwest National Laboratory, 2005.
  Available from: https://www.pnnl.gov/coginformatics/media/pdf/topten_paper.pdf [Accessed 10th September 2017]
- Blanco, J. M. & Cohen, J. (2014) The future of counter-terrorism in Europe. The need to be lost in the correct direction, *European Journal of Future Research*. Vol. 2, No. 1.
  Available from: from: https://link.springer.com/article/10.1007%2Fs40309-014-0050-9 [Accessed 10th September 2017]
- Blanco, J.M. & Cohen, J. (2016) Knowledge, the great challenge to deal with terrorism. Revista de Estudios en Seguridad Internacional, RESI.
  Available from: http://www.seguridadinternacional.es/revista/?q=content/knowledge-great-challenge-deal-terrorism [Accessed 10th September 2017]
- Carr, N. (2010) The Shallows: What the Internet Is Doing to Our Brains. W. W. Norton & Company.
- Cook, M.B. & Smallman, H.S. (2008) Human factors of the confirmation bias in intelligence analysis: decision support from graphical evidence landscapes. *Human Factors* 2008 Oct, 50(5): 745-54.
- EUROPOL (2017) SOCTA: Crime in the Age of Technology.
  Available from: https://www.europol.europa.eu/newsroom/news/crime-in-age-of-technology-%E2%80%93-europol%E2%80%99s-serious-and-organised-crime-threat-assessment-2017 [Accessed 10th September 2017]
- Global Futures Partnership of the Sherman Kent School for Intelligence Analysis (2004) New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities. Conference Rome, Italy, 31 March - 2 April 2004).
- Goleman, D. (2013) Focus: The Hidden Driver of Excellence. Harper Collins US Brand Code.
- Gross, B. (1964) The Managing of Organizations: The Administrative Struggle. The Free Press of Glencoe.
- Kent, S. (1965) Strategic Intelligence for American World Policy. Hamden, Conn., Archon Books.
- Khaneman, D. (2012) Thinking Fast and Slow. New York: Farrar, Straus and Giroux.
- Lowenthal, M. M. (2013) A Disputation on Intelligence Reform and Analysis: My 18 Theses. *International Journal of Intelligence and Counterintelligence,* Vol. 26, pp. 31-37.
- Lowenthal, M.M. & Marks, R.A. (2015) Intelligence Analysis: Is It As Good As It Gets?, International Journal of Intelligence and CounterIntelligence, 28:4, 662-665.
- Morozov, E. (2013) To Save Everything, Click Here: The Folly of Technological Solutionism. Public Affairs.
- National Commission on Terrorist Attacks (2004) The 9/11 Commission Report. New York: Norton.
- Pariser, E. (2012) The Filter Bubble: What The Internet Is Hiding From You. Penguin.
- Petersen, J. (1997) Out of the Blue How to Anticipate Big Future Surprises. The Arlington Institute, 2nd ed. Lanham: Madison Books.
- RECOBIA. REduction of COgnitive BIAses in Intelligence Analysis. FP7-SEC-2011-1.
  Available from: http://cordis.europa.eu/project/rcn/102068_en.html and https://www.recobia.eu/ [Accessed 10th September 2017]
- Senge, P. (1990) The Fifth Discipline: The Art and Practice of the Learning Organization. Currency.
- Silver, N. (2015) The Signal and the Noise: Why So Many Predictions Fail--but Some Don't. Penguin Books.
- Toffler, A. (1970) Future Shock. Random.
- U.S Army Research Institute for Behavioral and Social Sciences (2004) Think like a Commander.
  Available from: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA425737 [Accessed 10th September 2017]
- Viner, K. (2016) How technology disrupted the truth. *The Guardian* (12/07/2016).
  Available from: https://www.theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth [Accessed 10th September 2017]

Applications of Data Science in Policing: VeriPol as an Investigation Support Tool

Federico Liberatore
Department of Statistics and Operational Research, Faculty of Mathematics, Complutense University, Madrid, Spain

Lara Quijano-Sánchez
UC3M-BS Institute of Financial Big Data, Universidad Carlos III de Madrid, Getafe, Madrid, Spain

Miguel Camacho-Collados
Secretaría de Estado de Seguridad, Ministerio del Interior, Madrid, Spain.

Abstract
Data Science is an interdisciplinary field involving the development of processes and systems to extract knowledge and understanding from data in different formats and from different sources. Considering the large amount of data generated and managed by public safety agencies, *Data Science* applications in the police sector are numerous. More important are the advantages that the different applications of *Data Science* could provide the police on issues such as the optimization of resources, the increase of efficiency and effectiveness, the modernization and its exemplariness when compared with other institutions. In this paper we present different potential applications fields of Data Science for the police. In addition, we focus on the case of *VeriPol*, a tool for automatic detection of false violent robbery reports, currently under development by the Spanish National Police. In particular, we illustrate a detailed analysis of the results of a recent pilot study aimed at assessing the effectiveness of the tool.

Keywords: Data Science, Policing, Optimization, *VeriPol*.

1. Introduction

Every day we are in contact with systems that collect large amounts of information in order to model our behaviour. Spotify does it to recommend artists who might like you, based on the songs you listen to; Netflix builds a profile for each user, allowing to customize each person's experience, and even some banks use it to detect fraudulent transactions.

To transform these huge amounts of data into knowledge, it is necessary to design and use statistical and computational tools. The interdisciplinary field that concerns the development of processes and systems to extract knowledge and understanding from data in different formats and coming from different sources is called Data Science. In Data Science, techniques and theories, which derive from many fields within diverse areas such as mathematics, statistics or computer sci-

ence, are used. These include for example: probability and uncertainty models, automatic learning and statistical learning, data mining, information retrieval and retrieval, pattern recognition and visualization, and predictive analysis.

These techniques and sciences have achieved a dramatic reduction in the cost of storing and processing information and have led Data Science to become a technological trend that continues to grow. You could say that at present there is not a single Fortune 500 company that is not investing human and economic capital in any area related to Data Science, with Facebook and Google being two of the most notable cases. Data Science influences the economy, business and finance (Patil & Davenport, 2012). From a business perspective, Data Science is an integral part of competitive intelligence.

The use of Data Science techniques is not limited to companies seeking to retain their customers to increase their profits (such as Spotify, Netflix, Facebook or Google), there are also use cases in which these same methods have been used to tackle problems with a great social impact. This is the case of "*The Data Science for Social Good Fellowship*" of the University of Chicago[1]. Data analysis can help us to improve decision making in companies, provide new perspectives to our entrepreneurs and be a powerful ally to combat problems of social development and public health.

This paper relates to this last social and public interest and describes the applications that *Data Science* can have in security and safety. More concretely, the applications that the Spanish National Police is considering developing in the near future and in particular the case of *VeriPol*, a tool for automatic detection of false violent robbery reports, currently under development by the Spanish National Police.

2. Applications of Data Science for Security and Safety

The importance of data analysis for police and citizen security activities has been recognized even by the former President of the United States, Barack Obama, who in 2015 launched the Task Force on 21st Century Policing initiative[2]. Within this is the Police Data Initiative which recommends the use of innovative Data Science techniques to improve police action, relations with citizens and public safety.

Considering the large amount of data generated and managed by the different National Police Institutions around the world, the applications of Data Science in the police sector are innumerable. Specifically, in this paper, the focus will be in the different applications that Data Science could provide to the Spanish National Police, with issues such as resource optimization, efficiency and effectiveness, modernization, or exemplarity compared to other global institutions. Next, some of these ideas are detailed.

2.1 Prediction of Crimes

Predictive Policing is the use of police data to identify individuals, locations and events with a high risk of crime. The prediction of crimes allows to focus the police effort in the areas with greater risk in a dynamic way and that adapts to the criminal tendencies of the moment and of a specific territory. Numerous pilot projects (Miami, Chicago and London, among others) have proved useful. *PredPol*, an initiative in Santa Cruz, California, uses historical data to point out to agents 10 to 20 high-risk areas (Perry, 2013). The result has been a reduction in the first year of the 27% of the thefts and of 11% of the robberies in houses.

The interest for the definition of reliable crime prediction models is evident. Currently sponsored by the National Institute of Justice, a competition is underway for the definition of predictive models with economic awards totalling $1.2 million dollars[3].

2.2 Definition of Police Districts and Patrol Optimization

The prediction of crimes represents the first step towards the definition of a protocol of police action that fits the profile of each police beat or shift duty. Through optimization techniques it is possible to define the distribution of patrol agents in a district to improve different objectives, assuming an improvement in the distribution of the workload between agents and an improvement in the efficiency in the actions (Camacho-Collados, Liberatore & Angulo, 2015; Camacho-Collados & Liberatore, 2015; Liberatore & Camacho-Collados, 2016).

1 https://dssg.uchicago.edu/

2 https://cops.usdoj.gov/policingtaskforce

3 https://www.nij.gov/topics/law-enforcement/strategies/predictive-policing/Pages/welcome.aspx

2.3 Itinerant Crime and Criminal Series

Methodologies such as the Series Finder (Wang, Rudin, Wagner & Sevieri, 2013), developed at MIT in collaboration with the Cambridge (MA) Police Department, can identify criminal patterns and detect crime series. More specifically, this tool builds profiles of *Modus Operandi* and detects crimes that belong to the same series. In a pilot study with theft crimes in housing Series Finder has excluded crimes from crime series previously identified by police. This has reduced the number of suspects automatically.

2.4 Gender Violence Risk Estimation

Applying learning methodologies such as Case-Based Reasoning (Aamodt & Plaza, 1994) it is possible to obtain very powerful and effective models based on similarities with previous cases for the estimation of the risk for abused women. These models could also provide information on risk factors and their relevance by introducing machine learning predictive models (Bishop, 2006).

2.5 Analysis of Organized Crime Network Vulnerabilities

The Social Network Analysis (Bishop, 2006) discipline provides tools for studying social networks and identifying major actors as well as hidden structures. Among their techniques are methodologies to identify the most important elements of these networks and the communities within them. In the context of policing, similarly to what is presented in Baker and Faulkner (Baker & Faulkner, 1993), these basic applications could identify the most important individuals within an organized crime network, differentiating the different roles (central and linking elements). More advanced models (i.e., interdiction and fortification optimization models) can be used to define network vulnerabilities, that is, which individuals "attack" (stop or damage) to dismantle the network in the most efficient and effective way (Liberatore, Scaparra & Daskin, 2011; Liberatore, Scaparra & Daskin, 2012; Liberatore, & Scaparra, 2011). This model would require the evaluation of the relation between the actors, leading to the application of Tie Strength models (Liberatore & Quijano-Sanchez, 2017).

2.6 Analysis of Images of Police Cameras

Police cameras (e.g., body, helmet, and vehicle cameras) are a powerful tool that generates a large amount of data daily. However, the large amount of information produced makes an analysis by experts impossible. Fortunately, it is possible to develop tools (Wu, Liu, Li, Gu, Si & Tan, 2009; Hampapur, 2008) that process the recordings automatically to search for information of interest, both *a posteriori* (for example, identification of sequences of persecutions) and real time (reading of license plates, identification of faces of suspects).

2.7 Analysis of Work Productivity

At present, the productivity measurement of a police station does not take into account the work of crime prevention, which has the advantage of reducing costs for both the police, the judiciary system and society as a whole, as well as the economical and human benefit associated with avoiding the conversion of a citizen into a criminal. By applying statistical and optimization models (D'Amico, Wang, Batta & Rump, 2002) it is possible to design more sophisticated productivity measures that take into account all factors of police work. In addition, these models would allow the identification of police stations where good work is being done in particular, allowing them to model their techniques and to open the possibility of training courses to other police stations or agents, thus sharing expert knowledge that would increase national performance.

2.8 Detection of False Reports

False allegations represent an expense of money and resources for the Police. In addition, this type of crime is often accompanied by other crimes, such as fraud. Early detection of such complaints would allow inspectors to focus more efficiently. This type of Data Science tool is currently being built at the Spanish National Police. In the following Section the description of such tool and in particular, a detailed analysis of the results of a recent pilot study aimed at assessing the effectiveness of the tool are presented.

3. Case Study: *VeriPol*, a decision support tool for false violent robbery reports detection

Police investigations that are carried out in the different police departments of the Spanish territory are generally influenced by quantitative parameters, although many of them also consider qualitative ones. Generally, these investigations start from a report made by a person harmed or offended by an illegal act that, directly and by legal imperative, it forces the officers of the Security Forces to undertake the investigation and clarification of what has been brought to his/her attention.

The referred investigations cover all types of crimes contained in the Spanish Penal Code, although in some cases it is easily determined who the author is. In others, it is very difficult, even at times impossible, to determine the culpability of the crime. In those cases that are not possible to close, uncertainties and doubts usually appear in the course of the investigation, including whether the complainant has told in the report everything in his/her knowledge, or if this complainant has any malicious interest in his story, or even if he/she is openly lying to get a benefit.

Articles 456 and 457 of the Spanish Penal Code concern false reports and the simulation of crimes respectively, that is, they punish the fact of falsely filing a report before a judicial or administrative to provoke procedural actions such as the police investigation. In certain cases, the police responsible for these investigations, after a time spent collecting information about the complainant and the information provided by the complainant, may suspect that it is a false report or a simulation of crime. However, since the majority of these complainants are respected citizens and, above all, they are not criminals, care must be taken in dealing with them and with the facts to be investigated, always without violating the principle of presumption of innocence that every person has.

In recent years it has been observed that, partly motivated by a social phenomenon such as an economic crisis, a very high percentage of "normal" citizens, that is, not ordinary criminals, are being detained or charged with a crime that they had never known existed as such, although it does not justify their action. This situation entails an additional cost of time and resources to the National Police that could be invested in other more appropriate tasks.

This fact is causing great concern among those in charge of criminal control, since the statistical indices of false reports have reached a very high level of concern. Not only because it is a statistical modulator index, but because when analysing this phenomenon in depth, the following conclusions, that are quite striking and that directly and indirectly affect police effectiveness, can be drawn.

- Firstly, it affects the beginning of the investigation. Since it should be presumed that the information coming from the complainant is truthful, these falsehoods hinder and delay the beginning of the police action.
- More often than not, in the course of the investigation, it is found that the reason that motivates the investigative police intervention is not true.
- This hampers police work and calls for new investigation in another direction, thus generating unnecessary stress and strain. A properly targeted approach from the start would undoubtedly have a better outcome.

Motivated by the analysis of the current situation, an innovative project has been carried out within the scope of "predictive policing," the result of which is, *VeriPol*, a computer tool to estimate the likelihood that a violent robbery report is false. The program takes the text of the complaint as input. Therefore, it does not need any information on the part of the user and is completely automatic. In addition, it integrates perfectly with the SIDENPOL system (Police report system). That is, the system entry consists of a document (in PDF format) of each complaint, from which the descriptive text of the complaint is obtained. The program processes the text, extracting useful characteristics for its classification using techniques of Natural Language Processing (Winograd, 1972). These characteristics are passed to a mathematical model that uses Artificial Intelligence techniques (Michalski, Carbonell & Mitchell, 2013) and estimates the likelihood of falsity of the complaint. The output of the program is the probability that the complaint entered is false. Empirical experiments show that the accuracy of the tool is more than 90%.

The purpose of this novel project is the creation of a global and automatic system for the detection of false allegations, in addition to the definition of a research protocol for this type of crime. In this first phase, the problem has focused on the specific case of allegations of violent robbery. The promising results inspire to continue with this process and design of successive models for other types of reports.

3.1 Pilot Study

To test the efficacy and effectiveness of *VeriPol*, a pilot study has been undertaken in the urban areas of Murcia and Málaga, Spain. More in detail, the pilot study was run in Murcia (four police departments involved) from the 5th to the 9th of June 2017, while it took place in Málaga (six police department involved) from the 12th to the 16th of June 2017.

In each destination, two agents, experts in false report detection and in *VeriPol,* were sent to install the software, give a short course on its use to the local agents and investigators, and supervise all the activity. After

that, all the new violent robbery reports as well as all the open violent robbery cases of 2017, were analysed by *VeriPol*.

The results of the pilot study are shown in Table 1. As it could be observed, the implementation of *VeriPol* allowed for an impressive increase in productivity in terms of number of false cases of violent robbery detected and successfully closed.

Table 1: Comparison between the number of false violent robbery cases closed during the pilot study and the average number of false violent robbery cases closed in June.

Destination	Number of false violent robbery cases closed during the pilot study	Average number of false violent robbery cases closed in the month of June, years 2008-2016
Murcia	31	3,33
Málaga	49	12,14

3.2 Survey

To understand the level of acceptance and satisfaction associated with the use of *VeriPol*, all the agents and officials that participated in the pilot study were asked to answer to an anonymous questionnaire (illustrated in Table 2) on a voluntary basis.

Table 2: Questionnaire structure. For each question, the original text in Spanish and a translation to English are provided. The third and the fourth columns show the type of question and the allowed answers, respectively.

#	Question	Type of question	Allowed answers
1	Would you like the National Police to explore new methodologies to reduce costs and decrease the workload? ¿Te gustaría que en la Policía Nacional se exploraran nuevas metodologías para reducir costes y disminuir la carga de trabajo?	Multiple choice	Yes, No *Sí, No*
2	Do you think that the national police should provide investigator staff of more and better technological means to deal with the crime? ¿Crees que la Policía Nacional debería dotar al personal investigador de más y mejores medios tecnológicos para enfrentarse a la criminalidad?	Multiple choice	Yes, No *Sí, No*
3	Have you worked in the investigation of violent robberies? ¿Has trabajado la investigación de robos con violencia y/o tirones?	Multiple choice	Yes, No *Sí, No*
4	Did you use *VeriPol*? ¿Has usado VeriPol?	Multiple choice	Yes, No *Sí, No*
5	Do you think that *VeriPol* could be useful for the investigation of violent robberies? ¿Crees que VeriPol podría ser útil para la investigación de robos con violencia y/o tirones?	Multiple choice	Yes, No *Sí, No*
6	How useful do you think that *VeriPol* is as a investigation tool? ¿Cómo de útil crees que es VeriPol como herramienta investigativa?	Linear scale	1 (Not at all, *Nada*) to 5 (A lot, *Mucho*)
7	Do you think that *VeriPol* would be easy to integrate into your daily tasks? ¿Crees que VeriPol sería fácilmente integrable en tus tareas diarias?	Linear scale	1 (Not at all, *Seguro que no*) to 5 (Absolutely, *Seguro que sí*)
8	If you had *VeriPol* available, would you use it on a regular basis? ¿Si tuvieras VeriPol a disposición, lo usarías de forma regular?	Linear scale	1 (Not at all, *Seguro que no*) to 5 (Absolutely, *Seguro que sí*)
9	Do you think that *VeriPol* would expedite the investigation of cases? ¿Crees que VeriPol agilizaría la investigación de los casos?	Linear scale	1 (Not at all, *Seguro que no*) to 5 (Absolutely, *Seguro que sí*)
10	Would you like to have *VeriPol* installed in a way regular in all the National Police computers? ¿Te gustaría que VeriPol se instalase de forma regular en los ordenadores de la policía?	Linear scale	1 (Not at all, *Seguro que no*) to 5 (Absolutely, *Seguro que sí*)

#	Question	Type of question	Allowed answers
11	Do you think that it would be useful to extend *VeriPol* to other types of complaints? ¿Crees que sería útil que VeriPol se extendiese a otros *tipos de denuncias?*	Linear scale	1 (Not at all, *Seguro que no*) to 5 (Absolutely, *Seguro que sí*)
12	Would you like to receive training to learn new interrogation techniques? ¿Te gustaría recibir formación para aprender nuevas técnicas de interrogatorio?	Multiple choice	Yes, No *Sí, No*
13	Sex *Sexo*	Multiple choice	Male, Female *Hombre, Mujer*
14	Age in years *Edad en años*	Short answer	Short-answer text
15	Police Department *Comisaría*	Short answer	Short-answer text
16	Rank *Escala*	Multiple choice	*Básica, Subinspección, Ejecutiva, Superior*

21 agents and officials took part to the survey. The results are summarized in Table 3.

Table 3: Summary of the survey's result (in this context, NA means "Not Answered"). For each question, the frequency of each answer is given. Question #14 is an exception as its answer is continuous numerical. For this reason, summary statistics (minimum, 1st quartile, median, mean, 3rd quartile, and maximum) are given.

Question #	*Answers*					
1	**Yes**: 21		**No**: 0		**NA**: 0	
2	**Yes**: 21		**No**: 0		**NA**: 0	
3	**Yes**: 21		**No**: 0		**NA**: 0	
4	**Yes**: 18		**No**: 1		**NA**: 1	
5	**Yes**: 21		**No**: 0		**NA**: 0	
6	**1**: 0	**2**: 0	**3**: 0	**4**: 8	**5**: 13	**NA**: 0
7	**1**: 0	**2**: 0	**3**: 0	**4**: 3	**5**: 18	**NA**: 0
8	**1**: 0	**2**: 0	**3**: 0	**4**: 3	**5**: 18	**NA**: 0
9	**1**: 0	**2**: 0	**3**: 1	**4**: 4	**5**: 16	**NA**: 0
10	**1**: 0	**2**: 0	**3**: 0	**4**: 2	**5**: 19	**NA**: 0
11	**1**: 0	**2**: 0	**3**: 0	**4**: 3	**5**: 18	**NA**: 0
12	**Yes**: 21		**No**: 0		**NA**: 0	
13	**Man**: 20			**Woman**: 1		
14	**Minimum**: 33.00; **1st Quartile**: 36.50; **Median**: 40.00; **Mean**: 41.45; **3rd Quartile**: 44.50; **Maximum**: 55.00; **NA's**: 1					
15	**Cartagena**: 3		**Fuengirola**: 1		**Lorca**: 4	
	Málaga Centro: 3		**Murcia el Carmen**: 1		**Torremolinos**: 8	
16	**Básica**: 16		**Subinspección**: 3		**Ejecutiva**: 2	

From the observation of the participants' answers the following conclusions can be drawn:

— There is a unanimous interest in innovation in the Spanish National Police (questions 1, 2, and 12).
— Concerning *VeriPol*, the participants reckon that:
  ° It is a very useful investigation tool (questions 5 and 6).
  ° It would be easy to adopt and they would use it regularly, as it would simplify their job (questions 7 to 9).
  ° It should be installed to all the computers of the Spanish National Police and it should be extended to include other types of crimes.

Overall, given the extremely impressive results obtained in terms of false reports cases closed and the enthusiastic answers provided by the survey's participant, the pilot study has been considered a huge success that has motivated the head of the Spanish National Police to proceed with the implementation of *VeriPol* into the reports management software.

4. Conclusions

Data Science allows us to analyse information flows, which are generally unpolished, to become valuable, organised, and hierarchical information. As an example, in recent years, multinationals such as General Electric, Banco Santander (Quijano-Sanchez & Liberatore, 2017) or BBVA have implemented the role of the Chief Data Officer or Chief Science Officer in their organizations, with the mission of making the most of their business data. As the Internet was 20 years ago, Data Science will mark a before and after in the history of technological development and will influence many more areas than we imagine. With this, we can conclude that Data Science will be the solution that requires our time, but as the famous Stephen Hawking said, *"Intelligence is the ability to adapt to change."*

In the security field, the implementation of a system and protocol such as *VeriPol*, would allow a better use of police resources (especially human resources), a reduction of crime due to greater research effectiveness, and an improvement of the quality of police data relating to crime, as it entails a significant reduction of false information in the databases. In addition, as mentioned through the paper this type of initiative could open the door to a new form of investigation individualized in the crimes of robbery with violence or intimidation, for its special incidence and social repercussion, and with the possibility of extending to any type of police investigation as this is the beginning of an unusual and innovative system.

Finally, the implementation of the tool would make the Spanish National Police the first in the world to use a system of this type. In fact, there is no other system with similar characteristics, neither at academic level nor at the industrial level, and research on detecting lies from text is still in its infancy. Similar initiatives in foreign police have had a very strong media impact. For example, the previously mentioned *PredPol* tool, developed between the Los Angeles Police Department and the University of California Los Angeles, has been named by Time Magazine as one of the 50 best inventions of 2011 (Grossman, Brock-Abraham, Carbone, Dodds, Kluger, Park & Walsh, 2011).

The implementation of the system proposed in this document would put the Spanish National Police at the forefront as one of the most advanced police in the world, with a very positive impact on its image, both nationally and internationally. Looking at the results of the Pilot Study, this is more than likely to occur.

References

- Aamodt, A., & Plaza, E. (1994) Case-based reasoning: Foundational issues, methodological variations, and system approaches. *AI communications*, *7*(1), 39-59.
- Baker, W. E., & Faulkner, R. R. (1993) The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry. *American Sociological Review*, Vol. 58, no. 6, 837-860.
- Bishop, C. M. (2006) *Pattern recognition and machine learning*. Springer.
- Camacho-Collados, M., & Liberatore, F. (2015) A decision support system for predictive police patrolling. *Decision Support Systems*, *75*, 25-37.

- Camacho-Collados, M., Liberatore, F., & Angulo, J. M. (2015) A multi-criteria police districting problem for the efficient and effective design of patrol sector. *European Journal of Operational Research*, *246*(2), 674-684.
- D'Amico, S. J., Wang, S. J., Batta, R., & Rump, C. M. (2002) A simulated annealing approach to police district design. *Computers & Operations Research*, *29*(6), 667-684.
- Grossman, L., Brock-Abraham, C., Carbone, N., Dodds, E., Kluger, J., Park, A., & Walsh, B. (2011) The 50 best inventions. *Time Magazine, Nov. 28, 2011*.
- Hampapur, A. (2008) Smart video surveillance for proactive security [in the spotlight]. *IEEE Signal Processing Magazine*, *25*(4), 136-134.
- Liberatore, F., & Camacho-Collados, M. (2016) A Comparison of Local Search Methods for the Multicriteria Police Districting Problem on Graph. *Mathematical Problems in Engineering.* http://dx.doi.org/10.1155/2016/3690474
- Liberatore, F., & Quijano-Sanchez, L. (2017) What do we really need to compute the Tie Strength? An empirical study applied to Social Networks. *Computer Communications*, *110*, 59-74.
- Liberatore, F., & Scaparra, M.P. (2011) Optimizing protection strategies for supply chains: comparing classic decision-making criteria in an uncertain environment. *Annals of the Association of American Geographers* 101(6), 1241-1258.
- Liberatore, F., Scaparra, M. P., & Daskin, M. S. (2011) Analysis of facility protection strategies against an uncertain number of attacks: The stochastic R-interdiction median problem with fortification. *Computers & Operations Research*, *38*(1), 357-366.
- Liberatore, F., Scaparra, M. P., & Daskin, M. S. (2012) Hedging against disruptions with ripple effects in location analysis. *Omega*, *40*(1), 21-30.
- Michalski, R. S., Carbonell, J. G., & Mitchell, T. M. (Eds.). (2013). *Machine learning: An artificial intelligence approach*. Springer Science & Business Media.
- Patil, T. H. D. J., & Davenport, T. (2012) Data scientist: the sexiest job of the 21st century. H*arvard Business Review*, 90 no.10, 70-76.
- Perry, W. L. (2013) *Predictive policing: The role of crime forecasting in law enforcement operations*. Rand Corporation.
- Quijano-Sanchez, L., & Liberatore, F. (2017) The BIG CHASE: A decision support system for client acquisition applied to financial networks. *Decision Support Systems*, *98*, 49-58.
- Scott, J. (2017) *Social network analysis*. Sage.
- Wang, T., Rudin, C., Wagner, D., & Sevieri, R. (2013) Detecting Patterns of Crime with Series Finder. In *AAAI (Late-Breaking Developments)*.
  Available at: https://www.aaai.org/ocs/index.php/WS/AAAIW13/paper/view/7018/6750
- Winograd, T. (1972) Understanding natural language. *Cognitive psychology*, *3*(1), 1-191.
- Wu, J., Liu, Z., Li, J., Gu, C., Si, M., & Tan, F. (2009) An algorithm for automatic vehicle speed detection using video camera. In *Computer Science & Education, 2009. ICCSE'09. 4th International Conference on* (pp. 193-196). IEEE.

Acknowledgments

We would like to thank the Spanish National Police Corps and, in particular, Agent Romera-Juarez for all the participation in all the phases of the project *VeriPol*, Commissioner Álvarez for his support in the initial stages and believing in *VeriPol* since the beginning. A special thanks to Commisioners Florentino Villabona and José Antonio Mateos for promoting *VeriPol* in the *Ministerio del Interior* (Spanish Ministry of Interior) and providing all the resources necessary to the development of the pilot study, as well as supporting the implementation of *VeriPol* in the Spanish National Police.

The research of Liberatore was supported by MINECO [grant number MTM2015-65803-R]. All financial supports are gratefully acknowledged. The information and views set out in this paper are those of the author(s) and do not necessarily reflect the official opinion of the financial supporters.

Decision Support Systems in Policing

Don Casey
Phillip Burrell
London South Bank University, London

Nick Sumner
Metropolitan Police Service, London

Abstract
Decision Support Systems (DSS) are widely used in industry, finance and commerce to assist users with the large and rapidly growing amount of data that these institutions have to deal with. Police organisations have been slow to investigate the benefits that such systems can offer but this situation is changing. As well as seeking to improve operational performance, there are now pressing economic reasons for using I.T. systems to assist crime analysts and investigators. A short review of some of the more striking findings of psychological research in decision-making is followed by a survey of a selection of recent research into crime linkage and predictive policing using Artificial Intelligence and some of the systems currently being used in Police jurisdictions.

Keywords: decision support systems, crime analysis, predictive policing, crime linkage, artificial Intelligence

The amount of data generated by, and available to, organisations through their computer systems increases exponentially year on year and this phenomenon is accelerating. In order to deal with some of the problems that this creates for decision-takers computer programmes generically entitled "Decision Support Systems" (DSS) have been developed and are in use throughout commerce, industry and finance (Turban, et al., 2007). Police departments face the same problems in assessing and acting on information and are adopting the same strategies to assist in deploying their resources and assisting investigators. This paper is a review of systems and approaches currently being undertaken in developing and employing DSSs in Police contexts, emerging research including Artificial Intelligence (A.I) solutions, and more widely a discussion of expert decision-making.

The major areas of application for systems are in prediction of crime "hot spots" and linkage of offences. The former is normally used in cases of "volume" crime like burglary and vehicle offences while the latter is applied to more serious offences such as rape and homicide. A 2014 survey (PERF, 2014) indicated that 38% of responding Police departments in the US were already employing "Predictive Policing" systems that are claimed to improve deployment of Police resources and reduce crime by deterring offences in areas identified as high-risk. And that 70% expected to be using this strategy within two to five years.

This field is one that lends itself to the cross-fertilisation of disciplines and the most widely discussed predictive policing system, "PredPol" (PredPol) is an innovative collaboration between Environmental Criminology, Anthropology and Mathematics that employs an algorithm first employed in Seismology to predict geological disturbances.

A criticism of Predictive Policing (Robinson & Koepke, 2016) is that by relying on historic data it predicts where crime has already occurred and that it inevitably directs the attention of Police to areas and communities that are likely to report offences. It may also be that in the case of drug abuse or other "discretionary" offences that systems become subject to a confirmation bias of continuous reinforcement of decisions as offences are uncovered in specified areas, i.e. precisely the kind of systematic distortion of the evidence that non-human decision support is supposed to be immune from.

The possibility of this process becoming a racially biased "feedback loop" where prejudiced police action is directed towards areas with high levels of minority occupation, and as a result creates increasingly distorted inputs to systems has been raised by several authors. And even that a context of incomplete and often poor recording of crime is likely to lead to invalid conclusions that: "...legitimizes the widespread criminalization of racialized districts" (Jefferson, 2018). The legal environment of predictive policing has also been questioned: Ferguson (2017) concentrates on the threat, as he sees it, to the U.S. 4th Amendment rights of suspects to be protected from "unreasonable searches and seizures" and 14th Amendment right of citizens to equal protection under the law. While accepting that predictive technology is certain to be increasingly adopted using ever more sophisticated algorithms it is argued that there must be a substantive framework of oversight to police it.

The ability to link serial crimes is of great importance to law enforcement agencies. Once a link has been established between a number of crimes then evidence collected can be combined to provide a richer profile of a criminal's activity. The result of this combined evidence provides the opportunity for the earlier apprehension of the offender, particularly where the serial crime is of a serious nature. In this case, amongst other approaches, Artificial intelligence (AI) techniques have been employed. These have included supervised and unsupervised neural networks, fuzzy systems, data-mining, scenario generation and Bayesian and natural language–based systems.

Decision Making

It is often assumed that human decision-making must be superior to any other form of decision-making system and that this becomes more obvious as the area in which decisions are to be made increases in complexity. Surprisingly there is a very large volume of psychological research going back many decades that strongly suggests that this assumption is not true. If this is indeed the case, then the practicability of embedding decision-making into computer-based decisions becomes not only achievable but highly desirable.

The influential work of Meehl (Meehl, 1954) into the comparative accuracy of predictions made by trained professionals and simple statistical algorithms across a wide variety of areas including academic success, criminal recidivism, and length of hospitalisation for mentally ill patients overwhelmingly demonstrated the superiority of the latter. A much later meta-analysis of 136 studies of expert as compared to statistical or algorithmic (actuarial or mechanical) predictions concluded:

"Superiority for mechanical-prediction techniques was consistent, regardless of the judgment task, type of judges, judges' amounts of experience, or the types of data being combined" (Grove, et al., 2000, p. 19).

This position has been even more forcefully expressed in a survey of over 200 studies comparing expert and statistical predictions in "low validity" environments i.e., domains with a "significant degree of uncertainty". In activities ranging from credit risk assessment to predictions of longevity of cancer patients algorithms were found to perform significantly better than expert opinion in 60% of cases leading to the unconditional assertion: "*In every case the accuracy of experts was matched or exceeded by a simple algorithm*" (Kahneman, 2011, p. 223).

In practice a "draw" between a highly trained decision-maker and a statistical method represents a win for the algorithm in terms of the financial investment required. There is also an advantage in the reliability of the two "systems" in that the algorithm can always be

depended upon to return the same result given the same input. This is an outcome that cannot be guaranteed in the judgement of human decision-makers even in such highly skilled occupations as radiology and clinical psychology (Goldberg, 1968). In a study of clinical diagnosis by radiologists as to whether tumours were benign (Hoffman, et al., 1968) major discrepancies were not only discovered between radiologists but individual radiologists were also found to contradict themselves in 20% of cases when presented with the same x-ray at a later date.

Some of these studies are 50 to 60 years old and their findings have been replicated many times since. They indicated that what appear to be quite complex decisions can be generated by relatively simple methods long before the astounding advances that have since been made in Computer Science and Artificial Intelligence yet the adoption of advanced decision support into areas of complexity and importance has been patchy.

The compelling implication of these findings is that such statistical techniques could be equally effective when applied to fields relating to identifying links between offences and predicting where offences are most likely to occur. There is some direct evidence that calls into question the ability of human versus "mechanical" judgement in crime analysis.

For instance, a lack of support has been reported for the supposition that analysts and investigators have a heightened ability in linking offences. An early study (Canter & Heritage, 1991) asked 28 "highly experienced" detectives to link the offences committed by 3 stranger rapists who had each committed 4 offences. The majority of subjects performed at no better than chance and when links were suggested by the subjects, the researchers commented: *"Links made by the officers were often not based on a logical combination of the material they had"* (p 4).

Comparable results have been found in a series of studies (Bennell, et al., 2010; Santtila, et al., 2004) and a similar observation made: *many trained linkage analysts rely on an experience-based, subjective, idiographic approach for selecting linking cues* (Bennell, et al., 2012, p. 630). The consequences being that the linkage of crimes was unsystemised and individual to the experimental subject.

The conjunction of the huge, disparate and ever-increasing volume of data available to police services and the evidence that human decision-making is often not only inaccurate but also unreliable is concerning. When judgements are not only wrong but inconsistently wrong this clearly supports the proposition that some form of assistance is required in order that the best and most effective decisions can be reached.

The term 'decision support' is often used and not always accurately, a very early definition of Decision Support Systems by the authors who coined the term is still useful and widely employed: "*Interactive computer-based systems which help decision-makers utilise data and models to solve unstructured problems.... fuzzy, complex problems for which there are no cut and dried methods"* (Gorry & Scott-Marton 1971).

Originally, these systems were intended to support and assist the decision making of the user and designers were insistent that they were not to replace them. They were not to be automated decision-makers but advances in A.I. in association with the proven effectiveness of "mechanical" methods bring this into question.

An area of crime analysis that has been the subject of a great deal of attention has been that of serious sexual offences. The two most recent reports on the investigation and prosecution of rape in the U.K. (HMIC/HMCPSI, 2012) and the Metropolitan Police Service (Angiolini, 2015) have emphasised the critical importance of identifying rape series at an early stage. Apart from the reasons already given there are pressing economic grounds for adopting computerised support in crime analysis as is clearly demonstrated when considering the case load of The Serious Crimes Analysis section (SCAS) in the United Kingdom (Angiolini, 2015). SCAS is a national unit *which works to identify the potential emergence of serial killers and serial rapists at the earliest stage of their offending* (NCA) and deals with the most serious offences including murder with a sexual motive, stranger rape and abductions The unit employs a version of the Violent Crime Linkage Analysis System (ViCLAS) which is in practice the standard database employed for crime linkage. In 2015 4,442 crimes were referred to SCAS for analysis but the figures show a dramatic rate of 'attrition' at each stage of the process. Only 36% of suitable crimes are even input to the system, and of those over a quarter are discarded. As a result, only 26% of crimes agreed by SCAS to meet the criteria are analysed. In practice this means that the

large majority of offences will never be subject to linkage analysis as the cohort of unexamined rapes grows at three times the rate of those analysed. Consequently, a series of two that could be found in the eligible set of offences has a probability of 0.07 of both crimes being scrutinised and this decreases rapidly as series length increases: three crimes have a probability of less than 2% of all of them being seen. The chance of any offence proceeding to analysis is small and the probability of all offences in a series being analysed rapidly decreases as the series lengthens. It should be remembered that these offences are committed by some of the most dangerous criminals in society and the aim of SCAS is to identify them *at the earliest stage of their offending*. However, the odds against even identifying their crimes are very high with the result that the chances of finding these offenders at an early point in their criminal careers is very unlikely.

Crime Linkage

Currently there are two computer systems that dominate the area of serious crime linkage and analysis: ViCAP, the Violent Crime Apprehension Program (Howlett, et al., 1986) and ViCLAS, the Violent Crime Linkage System (Royal Canadian Mounted Police). ViCAP is the creation of the FBI at Quantico, is in use throughout the United States and has been in existence in differing forms since 1985; its use has historically been linked with theories of Douglas, Ressler and other FBI agents as outlined in the Crime Classification Manual (Douglas, et al., 1982). ViCLAS is an enhancement of ViCAP and was developed by the Royal Canadian Mounted Police (RCMP) in the early 1990s; this system is used in the UK, most of the European Union and Australasia and is licensed by the RCMP, for a fee, in these jurisdictions. Both ViCAP and ViCLAS were developed primarily by practitioners and criminologists and are essentially repositories of data which are dependent upon the training and experience of the user to maximise their potential. The influence of Computer Scientists in this arena has been slight and there has been no apparent involvement by researchers in A.I or Decision Support, functionality is restricted to the proprietary software on which the databases run and amounts to simple query and retrieval. As a result, none of the advances that have been made in these areas are incorporated in either system and they remain essentially unchanged in the last 20 – 25 years.

A research initiative between the University of Arizona and the Tucson Police Dept. produced the COPLINK system (Chen et al., 2003)multiple data sources are used, each having different user interfaces. COPLINK Connect addresses these problems by providing one easy-to-use interface that integrates different data sources such as incident records, mug shots and gang information, and allows diverse police departments to share data easily. User evaluations of the application allowed us to study the impact of COPLINK on law-enforcement personnel as well as to identify requirements for improving the system. COPLINK Connect is currently being deployed at Tucson Police Department (TPD which offers decision support in the form of a large knowledge management system. This system uses a number of linked knowledge sources from police records, criminal histories, and reports and various textual mining and linguistic analysis methods to produce a comprehensive map of the criminal activity related to a crime under investigation and to elucidate relationships within the data. An example would be where associates, locations or vehicles were associated with a suspect. This system has now been developed into a commercial application and is available to law enforcement agencies.

A similar collaboration between the Memphis Police Department and Memphis University in the U.S.A. resulted in CRUSH - Criminal Reduction using Statistical History[1]. The system utilises IBM's statistical package SPSS to analyse data from a number of crime databases to create multi-layer hot spot maps to detect patterns and trends in criminal activity. Consequently, it is claimed that police resources can be more effectively utilised and that the system has contributed to an average reduction in violent and property crime of over 15%. The Homicide Investigation Tracking System (HITS) (Washington State: Office of the Attorney General) is an application developed in Washington State in response to a number of high profile murders that is similar to ViCAP/ViCLAS in that it serves as a source of detailed information on a large number of violent and sex related crimes over a wide geographical area in the American North East.

An interesting approach (Wang, et al., 2015) employs established techniques of pattern detection in data-mining to find similarity coefficients between offences to detect series of residential burglaries in Cambridge, Massachusetts. These relate to "pattern-general

1 http://www-03.ibm.com/press/us/en/pressrelease/32169.wss

similarity" that represents elements of crime that are common in most crime series such as geographical and temporal proximity and "pattern-specific similarity" that reflects within-series similarity. The use of pattern-general similarity over the set of offences generates a similarity graph where edges between crimes indicate similarity. The hypothesis being that the majority of crime series have a number of offences that exhibit the identifying features of or "core" of the series or pattern. Once cores are identified then series are found by merging overlapping cores. This hypothesis is based on the intuition of analysts and the research methodology can be summarised as: learn a similarity graph, based on previous crime series, and then mine and merge cores.

Visual Analytics for Sense-Making in Criminal Intelligence Analytics (VALCRI) is an ongoing E.U. research project that attempts to make connections in crime reports that may be missed by analysts and to present them in visual form. It employs semantic text processing and the A.I. concept of "ontologies' which are formal specifications of concepts that can be interpreted and processed by computer systems. It aims to find clusters in crime reports, which is crimes with similar features that may not be immediately apparent, using a similarity metric. Once similarity values between offences have been computed a lattice can be generated that encapsulates the relationships in the data. In one part of the system (Sacha, et al., 2017) offenders' temporal and spatial activities can be represented and answers to questions about their activities answered by moving up or down through the lattice. This also allows for the use of "association rules" to extract information about useful relationships (Qazi, et al., 2016). Lattices can also be composed on any other aspect for which there is data such as offenders' crime histories and associations and crime hot spots. This project is very strongly envisaged as tool to assist analysts: *VALCRI acknowledges that technology works best when it augments the cognitive abilities … of the analyst* (Pallaris, 2017).

A collaboration between the Metropolitan Police Service (UK) and London South Bank University (Casey & Burrell, 2009; Casey & Burrell, 2010; Casey & Burrell, 2013) in which a large release of rape data was made available employs multi-dimensional scaling and fuzzy clustering to automatically generate a taxonomy of stranger rape in order to identify behavioural similarities between offences with the aim of discovering series of crimes. The strength of this approach is that real-life descriptions such as "violent", "middle-aged" and "controlling" that are commonly used by investigators and analysts to describe crimes can be given valid numeric values. By so doing "degrees of membership" of behavioural or descriptive dimensions such as the above can be assigned and thereby characterise the similarity between offences.

Predictive Policing

The following is widely employed classification of approaches in predictive policing (Perry, et al., 2013):

1. Methods for predicting places and times of crimes. These are essentially a police resource management tools for deploying officers to areas and at times when they are most likely to deter or encounter crime
2. Methods for predicting offenders and identifying individuals likely to commit crimes. For identifying those most probable to offend in future
3. Methods for predicting perpetrators' identities. In order to generate offender profiles for specific offences
4. Methods for predicting victims of crimes. Used to determine those individuals or groups most at risk of becoming victims

In general, the focus of research activity and the development and implementation of systems has been heavily focussed on the first of these elements although there are instances of predicting offenders based on criminal histories and social network analysis. The most notable of these is the Strategic Subject List (SSL) more commonly known as the Chicago Heat List. In an attempt to curb the high level of gun crime in the city, all persons arrested in Chicago are given a *score* generated by an undisclosed algorithm that predicts their likelihood of perpetrating or being a victim of gun crime. It was hoped that by so doing effective interventions could be made by visiting those high on the list either to warn them of the threat or to inform them *that if they don't keep in line, there's a jail cell waiting for them* (Stroud, 2016). Currently there are over 400,000 citizens of Chicago on the SSL and its existence has unsurprisingly proved highly controversial in identifying suspects (Gosztola, 2017). There have also been objections that while an individual's presence on the list does not indicate that they are more or less likely to be a victim of a shooting they are more likely to be

arrested for a shooting (Saunders, et al., 2016). There is no data relating to convictions.

The main focus of predictive policing however is undoubtedly the prediction of locations and times where crime is most likely to occur and there are a large and increasing number of systems that promise to be able to achieve this. A selection of some of the most well-known applications are shown at table 1. The background to the recent emergence of predictive policing systems can be traced in a direct line from the work of Brantingham. P and Brantingham. P, (1981) on the geography of crime and crime pattern theory through the research of their student Rossmo (2000) on geographic profiling of crime to the work of Jeffrey Brantingham (Brantingham, et al., 2012) on the anthropology of criminal gangs and PredPol.

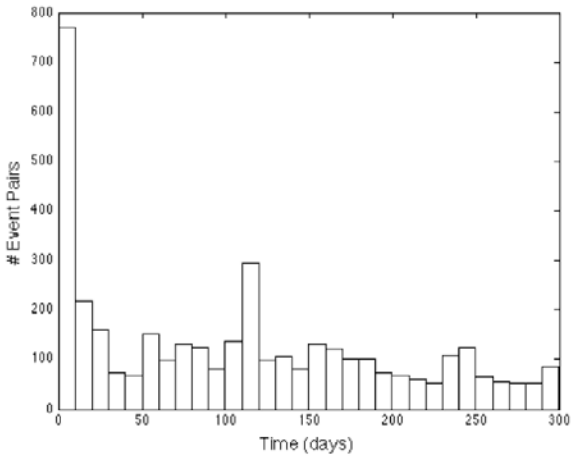
Table 1: Predictive Policing Systems

	Location	Crime types	Method	DATA
Crime Anticipation System (CAS)	Amsterdam	Property and violent	Machine learning: Neural networks	200 demographic, socio-economic & crime variables
PreCobs	Germany Switzerland	residential burglary	Undisclosed	Spatio-temporal Premises type Modus Operandi
PredPol	60+ US cities Kent, UK	Property and violent	self-exciting point process	Spatio-temporal
HunchLab	Miami	Property and violent	Machine learning: stochastic gradient boosting	"several hundred" variables: "risk terrain", crime, weather etc
CrimeScan	Chicago, Pittsburgh	Violent	Clustering:Kernel density estimation	Spatio-temporal Social indicators

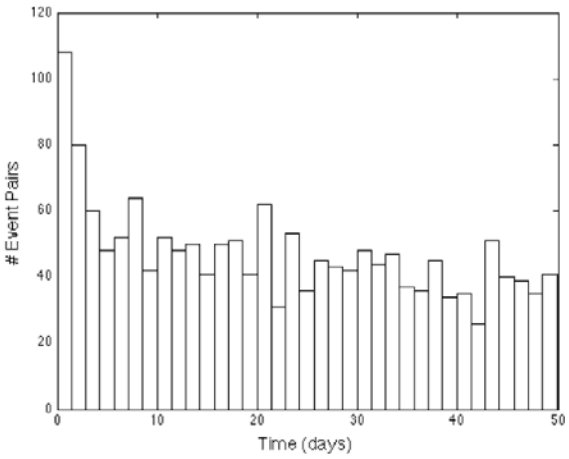
based on *Hardyns & Rummens (2017)*

It may appear that the more data sources that a system has that the better its performance is likely to be but, as has been seen from the evidence of psychological experiment into decision-making this does not appear to be the case; simpler seems to be better. A large number of sources also requires a corresponding effort to gather and evaluate data and most importantly some method for standardising and measuring evidence so that data with different character and attributes can be effectively combined. Some of the data sources shown in table 1 are so varied that is hard to see how this could be achieved. PredPol has the advantage of using a very small number of data variables that relate exclusively to time, date, and location of the offence and are easily evaluated and encoded. It employs a technique known as "self-exciting point process" (Mohler, et al., 2011) which is usually employed to model aftershocks from earthquakes. The issue of the use of algorithms and transparency in modelling crime prediction as a problem for enforcement agencies and public confidence has been raised (Ferguson, 2017). Neural networks employed by CAS exemplify the "black box" in that by their nature their internal workings are not amenable to examination but as with other techniques, they depend entirely on their success for the quality of data input to them. Other systems that are commercial products do not make public the operation of the algorithms they employ for obvious reasons but equally obviously the question of transparency is apparent. The similarities between the temporal and geographic incidents of aftershocks of and the "near repeat" occurrence in burglary are shown at Figure 1. The near-repeat phenomenon found premises near to a recent burglary are at a greater risk of being subject to an offence but that risk decreases over time (Johnson & Bowers, 2004)

Figure 1 Earthquake events in S. California and near repeat burglaries - Mohler et al, (2015)



Southern California earthquake events of magnitude 3.0 or greater within 300 days < 110 km apart



Times (less than 50 days) between burglaries separated by 200 meters or less

A research study that compared the effectiveness of a prediction system based on the earthquake model and crime analysts (Mohler, et al., 2015) ran a randomised control trial in three divisions of the Los Angeles Police Department and two divisions of the Kent Constabulary (U.K.). In this study, analysts were asked to predict locations of crimes on their sections and this was compared to the epidemic-type after shock sequence (ETAS) algorithm that is used by PredPol to generate its forecasts. Cells of 150 x 150 metres were specified as patrol areas and the predictions were randomly allocated to patrol staff for a 24-hour period; no patrolling officers, control or supervisory staff were aware of which prediction type they were dealing with. It was found that the ETAS model predicted areas with 1.4 – 2.2 the amount of crime that analysts did using intelligence reports and mapping software. Where officers were deployed to predict areas the ETAS forecasts were successful in reducing the crime rate in patrolled areas by 7.4% while analyst forecasts showed no significant effect on crime reduction.

Conversely a randomised field trial run by the Shreveport, Louisiana Police Department (Hunt, et al., 2014) that used logistic regression models (PILOT -Predictive Intelligence Led Operational Targeting) did not show a statistically significant reduction in crime in the identified cells. In this trial "leading indicators" were input to predict property crime within "block-sized" squares (400 x 400 feet – approximately 150 x 150 metres). The authors accept that there were problems with this research around issues of "dosage" and "fidelity" by which is meant the consistent level of police activity in identified areas and the extent to which interventions were delivered as intended. This raises the question of the difficulty of effectively implementing trials of experimental tactics in policing related issues when they are necessarily conducted in an environment in which unpredictable levels of demand are made on finite resources.

The Crime Anticipation System (CAS) in contrast to PredPol uses a large number of variables and predicts more offences including violent, theft and vehicle crime. Using neural networks, it produces a two-week prediction of crime based upon three years' worth of data across Amsterdam and in response, police units with a city-wide remit are sent to those areas identified as most high risk. It has been reported (Hardyns & Rummens, 2017) that in a trial from October 2013 to July 2014 that the system was successful in predicting 15% of house burglaries within a 125 x 125 metre cell and 36% as "near misses", i.e. it predicted a burglary in the neighbouring cell to where one actually occurred. The figures for street robbery or mugging are also impressive in predicting 33% of locations accurately and 57% as near misses. As always however it would be valuable to know what the baseline or "hit rate" of conventional predictive analysis running concurrently would be. It appears from the work of the Brantinghams (Brantingham & Brantingaham, 1981) and others that crime, particularly violent crime, is often highly localised so predicting its future occurrence may not be as complex as might be imagined.

PreCobs (Pre – Crime Observation System) is a predictive system in use in Germany that is restricted to house

burglary and like other systems is based upon near-repeats. This system is currently in use in several German cities (Hardyns & Rummens, 2017) but there is little information available on its performance or its operation. A very recent report (Gerstner, 2017) concludes that its effect on crime reduction is unclear but is only likely to be moderate. In considering the utility of near-repeats to other types of crimes apart from property offences the similarity of near-repeats and the temporal representation of violent gang-related events in Figure 2 is striking and suggests that the seismological model introduced to crime analysis may be generalisable.

Figure 2: Timeline of violent incidents between two Los Angeles gangs – Mohler et al. (2015)

01/01/2000 05/15/2001 07/02/2002

HunchLab (Azavea) employs a very high number of variables in its operation, which presents the difficulties referred to standardising input, and also in discerning, which are the most influential elements in the data collected. Among the factors considered are crime history, socio-economic factors, near repeat data, temporal cycles and many more; it also considers Risk Terrain Modelling (RTM) which relates to the influence of geographic features on crime (Caplan & Kennedy, 2010). The system uses a form of machine learning: a stochastic gradient boosting machine (GBM) which is an enhanced application of decision trees, a widely used group of A.I. algorithms that assist in determining the best decision for a set of circumstances. There is no information currently available as to this systems performance. CrimeScan, now known as CityScan, has been in development since 2009 (Neill) and is a joint enterprise between Chicago Police Department and Carnegie Mellon University that uses a form of clustering known as kernel density estimation to predict incidents of violent crime around the city. Again, this model employs leading indicators such as emergency calls, minor crimes and anti-social behaviour as input and operates at block level in order to make its predictions.

Conclusions

In the current environment in which crime is rising again across most of Europe and enforcement budgets are being squeezed the need for assistance in deploying police resources to deter and detect crime is of great and growing importance. The volume of data coming into and being generated by policing organisations has never been greater and this may become overwhelming: for example, recently a series of high-profile rape cases in the U.K. have collapsed because of Police failure to find vital evidence hidden in thousands of text messages, Facebook and other social media postings. This is only one instance of the difficulties faced when dealing with the unprecedented amount of information that may be relevant to an investigation and failure to uncover such data is only likely to increase in the absence of greater resources. Given that the level of personnel is unlikely to rise then the only way to expand the capacity of police departments to deal with these problems is to improve the tools that they work with. Information Retrieval is a field of Artificial Intelligence dedicated to finding information in large datasets that satisfies users' queries. Typically it would allow investigators to frame queries in natural language to a large database and have an IR system retrieve documents and answer questions on it as well as a human (Microsoft, 2018). It is also conceivable that the emerging field of "Sentiment Analysis" (Cambria, 2016) which is currently used to assess attitudes, perceptions and even emotional responses in large databases could be used to find evidence of the nature of personal relationships.

There is a large body of well-attested knowledge from research on what constitutes effective decision-making and an enormous amount of both academic and commercial research in A.I. and other disciplines into how important relationships in data can be uncovered. Crime Analysis has been slow to become involved in this effort but this is rapidly changing. As yet the answers to the problems that law enforcement faces in the present and future are not clear but there are faint and encouraging signs that they can be found given the wide variety of approaches that are being applied and tested.

References

- Angiolini, E., (2015) *Report of the independent Review into the Investigation and Prosecution of Rape in London,* London: Crown Prosecution Service.
- Azavea (n.d.)
  [Online] Available at: https://cdn.azavea.com/pdfs/hunchlab/HunchLab-Under-the-Hood.pdf
- Bennell, C., Bloomfield, S., Snook, B., Taylor, P. & Barnes, C. (2010) Linkage analysis in cases of serial burglary: comparing the performance of university students, police professionals, and a logistic regression model. *Psychology Crime & Law,* 16(6), 507-524.
- Bennell, C., Snook, B., MacDonald, S. & et al. (2012) Computerized crime linkage systems: A critical review and research agenda. *Criminal Justice and Behavior,* 39(5), 620-634.
- Brantingham, P. J. & Brantingaham, P. L. (1981) *Environmental Criminology.* Thousand Oaks, CA: Sage.
- Brantingham, P. J., Tita, G. E., Reid, S. & Short, M. (2012) The Ecology of Gang Territorial Boundaries. *Criminology,* 50(3), 851-855.
- Canter, D. & Heritage, R. (1991) *A Facet Approach to Offender Profiling: Vol 1 Final Report to the Home Office,* London: U.K. Home Office.
- Caplan, J. & Kennedy, L. (2010) *Risk Terrain Modelling Manual.* Newark, NJ: Rutgers Centre on Public Security.
- Casey, D. & Burrell, P. (2009) *Classification of Serious Sexual Assault using Fuzzy Clustering: In Proceedings of the IADIS International Conference on Intelligent Systems and Agents.* s.l., s.n.
- Casey, D. & Burrell, P. (2010) *Lasso: Linkage Analysis of Serious Sexual Offences, In Artificial Intelligence Applications and Innovations.* Heidelberg, Springer, 70-77.
- Casey, D. & Burrell, P. (2013) *Can Fuzzy Decision Support Link Serial Serious Crime?.* Barcelona, 5th International Conference on Agents and Artificial Intelligence.
- Douglas, J. E., Burgess, A. W., Burgess, A. G. & Ressler, R. K. (1982) *Crime Classification Manual.* Hoboken, N.J.: John Wiley & Sons.
- Gerstner, D. (2017) *Domestic Burglary and Predictive Policing.* Budapest, CEPOL Research & Science Conference.
- Goldberg, L. R. (1968) Simple models or simple processes? Some research on clinical judgments. *American Psychologist,* 23(7), 483-496.
- Gorry, G. & Scott-Morton, M. S. (1971) A Framework for Management Information Systems. *MIT Sloan Management review,* 13(1), 55-70.
- Gosztola, K. (2017) *Journalists Sue Chicago Police For Records On 'Heat List' Used For Predictive Policing.*
  [Online] Available at: https://shadowproof.com/2017/06/07/journalists-sue-chicago-police-records-heat-list-used-predictive-policing/ [Accessed 6 Feb 2018].
- Grove, W.M., Zald, D.H., Lebow, B.S., Snitz, B.E., Nelson, C. (2000) Clinical versus mechanical prediction: a meta-analysis. Psychological Assessment, 12(1), 19 - 30.
- Hardyns, W. & Rummens, A. (2017) Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges. European Journal on Criminal Policy and Research, 24 (3), 201-218.
- HMIC/HMCPSI (2012) *Forging the links: Rape investigation and prosecution. A joint Review by HMIC and HMCPSI,* s.l.: H.M. Inspectorate of Constabularies / H.M. Crown Prosecution Service Inspectorate.
- Hoffman, P., Slovic, P. & Rorer, L. (1968) An analysis-of-variance model for the assessment of configural cue utilization in clinical judgment. *Psychological Bulletin,* 69(5), 338-349.
- Howlett, J., Hanfland, K. & Ressler, R. (1986) The Violent Crime Apprehension Program. *FBI L.aw Enforcement Bulletin,* Volume 55, 14-22.
- Hunt, P., Saunders, J. & Hollywood, J. S. (2014) *Evaluation of the Shreveport Predictive Policing Experiment.*
  [Online] Available at: https://www.rand.org/pubs/research_reports/RR531.html
- Johnson, S. D. & Bowers, K. J. (2004) The Stability of Space-Time Clusters of Burglary. *British Journal of Criminology,* Volume 44, 55-65.
- Kahneman, D. (2011) *Thinking Fast and Slow.* New York: Farrar, Straus & Giroux.

- Meehl, P. E. (1954) *Clinical versus statistical prediction: A theoretical analysis and a review of the evidence.* Minneapolis: University of Minnesota.
- Mohler, G., Short, M.B., Brantingham, P.J, Schoenberg, F.P. & Tita, G.E. (2011) Self-Exciting Point Process Modeling of Crime. *Journal of the American Statistical Association,* Volume 106:493, 100-108. DOI: 10.1198/jasa.2011.ap09546,
- Mohler, G. O., Short, M.B., Malinowski, S., Johnson, M., Tita, G.E., Bertozzi, A.L. & Brantingham, P.J. (2015). Randomized Controlled Field Trials of Predictive Policing. *Journal of the American Statistical Association*, 110:512, 1399-1411.
- NCA (n.d) *"A day in the life" - Serious Crime Analysis Section.*
  Available at: http://nationalcrimeagency.gov.uk/84-nca-website/index.php?option=com_content&view=article&id=799&catid=84&Itemid=703
- Nobles, M., Neill, D.B., Flaxmann, S. (n.d.) *Predicting and Preventing Emerging Outbreaks of Crime.*
  [Online] https://www.cs.cmu.edu/~neill/papers/informs2014.pdf
- Pallaris, C. (2017) *Recasting the intelligence curriculum.* Presentation at CEPOL Police Research and Science Conference, Budapest.
- PERF (2014) *Future Trends in Policing,* Washington, D.C.: Office of Community Oriented Policing Services.
- Perry, W. L., McInnis, B., Price, C.C., Smith, S.C. & Hollywood, J.S. (2013) *Predictive Policing: Forecasting Crime for Law Enforcement.,* Santa Monica, CA: RAND Corporation.
- PredPol (n.d.) [Online]
  Available at: http://www.predpol.com/ [Accessed 2018].
- Qazi, N., Wong, W., Kodagoda, N. & Adderley, R. (2016) *Associative Search through Formal Concept Analysis in Criminal Intelligence Analysis.* Budapest, IEEE International Conference on Systems, Man, and Cybernetics (SMC).
- Robinson, D. & Koepke, L. (2016) *Stuck in a Pattern.*
  Available at: https://www.teamupturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf
- Rossmo, D. K. (2000) *Geographic Profiling.* Boca Raton: CRC Press.
- Royal Canadian Mounted Police, n.d. *Violent Crime Linkage System (ViCLAS).*
  Available at: http://www.rcmp-grc.gc.ca/to-ot/cpcmec-ccpede/bs-sc/viclas-salvac-eng.htm
- Sacha, D. et al. (2017) *White Paper WP-2017-011: Applying Visual Interactive Dimensionality Reduction to Criminal Intelligence Analysis.*
  Available at: http://valcri.org/publications/white-paper-applying-visual-interactive-dimensionality-reduction-to-criminal-intelligence-analysis/
- Santtila, P., Korpela, S. & Hakkanen, H. (2004) Expertise and Decision-making in the linking of car crime series. *Psychology, Crime & Law.,* 10(2), 97-112.
- Saunders, J., Hunt, P. & Hollywood, J. S. (2016) Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. *Journal of Experimental Criminology,* 12(3), 347–371.
- Snook, B., Taylor, P. & Bennell, C. (2004) Geographic profiling: the fast, frugal, and accurate way. *Applied Cognitive Psychology,* 18(1), 105-121.
- Stroud, M. (2016) *Chicago's predictive policing tool just failed a major test.*
  Available at: https://www.theverge.com/2016/8/19/12552384/chicago-heat-list-tool-failed-rand-test [Accessed 2018].
- Turban, E., Aronson, J., Liang, T. & Sharda, R. (2007) *Decision Support and Business Intelligence Systems.* Upper Saddle Rive, N.J.: Pearson Education Inc..
- VALCRI (n.d.) *Valcri.*
  [Online] Available at: http://valcri.org/
- Wang, R., Rudin, C., Wagner, D. & Sevieri, R. (2015) Finding Patterns with a Rotten Core: Data Mining for Crime Series with Cores. *Big Data,* 3(1), 3-21.
- Washington State: Office of the Attorney General (n.d.) *Homicide Investigation Tracking System (HITS).*
  Available at: http://www.atg.wa.gov/homicide-investigation-tracking-system-hits

Acknowledgement: The paper's reviewer, Dr Peter Neyroud, whose valuable suggestions have improved it.

Predictive Policing:
Perception of its risks and benefits by police trainees and citizens

Cyril Piotrowicz
Centre de recherche de l'Ecole Nationale Supérieure de la Police (ENSP), Lyon

Abstract
In the era of Big Data, law enforcement agencies are expected to analyze data in order to solve crimes, but also to prevent it. Predictive policing software aim to anticipate the most probable place and time for an offence to occur, giving police officer the opportunity to be "at the right place, at the right time". Articles questioning the efficiency of the algorithm or the data used have been published in the past few years, but none of them step backed and search to know if the law enforcement agencies were ready for this paradigm-shift: from a reactive policing to a predictive policing. This article presents the results of the most recent (April 2018) France's project research regarding organizational resilience and resistance to change in lights of predictive policing. More than 1500 peoples have answered four surveys about predictive policing, among them: citizens, police officers, police trainees, city officials, etc.

Keywords: predictive policing, resilience, algorithm, Predpol, France

Introduction to predictive policing[1]

In the early years of the 21st century, an innovation comes into the world of homeland security: predictive policing. The most widely known predictive policing software is Predpol from the eponymous company. Since then more and more companies have entered this market: for example, Hitachi (with Hitachi Visualization Suite), Microsoft (with Microsoft Power BI), IBM (with IBM SPSS), among smaller ones.

If so many companies invest in this field, it is to supply a demand from police departments across the world.

Today, beside the United States of America, where predictive policing is quite well-deployed, we can find history or actual use of predictive policing software in South America (Uruguay), Asia (India) and major cities in Western Europe (United Kingdom, Germany, Spain, Switzerland, France, etc.). It is understandable that governments and police departments are interested in a software that is claimed to reduce crime up to 30% and cost the annual salary of one police officer (Piotrowicz, 2014).

But despite this growth in interest, there is still a misconception of what predictive policing really is and what it can really achieve.

Predictive policing can be defined as: "A policing strategy focused on the spatiotemporal anticipation of the

1 In the following, "predictive policing" will be seen only as place-oriented and as predictive crime mapping. Therefore, other form of "predictive policing", such as, person-oriented or actuarial tools will not be studied.

criminal phenomenon, or at least a part of it, in the purpose to establish an operation either of prevention, investigation or repression" (Piotrowicz, 2016).

Technically, at its core, it is a software that will create a map displaying the crime likely to happen during the next day or week. The prediction is calculated with an algorithm (predictive analytics) supported by crime data, urban data and social data. Overall, the software does not need any personal data to establish predictive crime mapping.

Presentation of our Research Project[2]

The project is leaded by University Jean-Moulin Lyon 3 and funded by France's Ministry of Interior.

Overall, in order to achieve efficiency, a tool must be used as intended by the developer by the user, and with the least possible resistance from third parties.

Applied to new technologies in law enforcement agencies, we can make two assumptions: the effectiveness of a tool and its life span are tied to its acceptance by the user (police trainees and police officers) but also to its acceptance by those to whom it applies: citizens.

For example, regarding the 'flash-ball'[3] in France, since 2015 the new model (LBD 40x46) was used more often each year by police officers (IGPN, 2017), but 42% of citizens were against its use (20Minutes, 2016). Then, France's Defender of rights, which is an independent authority, officially asked in 2018 the Parliament to ban it (Défenseur des droits, 2018).

To prevent a loss of time, money but also in trust from citizens our project aimed to evaluate the acceptance by the actors of homeland security of predictive policing software before its nationwide deployment.

Our project revolved around the following question: *Is predictive policing software received by citizens, police officers, police trainees and city officials with sympathy and endorsement or with mistrust?* In a more scientific-way, we have studied the organizational resilience of Society and Law Enforcement Agencies regarding Predictive policing.

Unlike other studies, we have not evaluated the effectiveness of the predictive policing approach. Even if measuring its effectiveness is a necessity, confirming its feasibility is a prerequisite: if the tool is not used, or misused, assessing its reliability is impossible.

This project combines, on one side, empirical researches, regarding surveys and semi-structured interviews of hundreds of police and law enforcement officers or trainees, citizens and city officials, with, on the other side, an academic study about organizational resiliency and managing resistance to change.

This project explored three objectives:

1. *Identify and evaluate the causes of resistance and/or interest* from police officers or trainees, citizens and city officials regarding predictive policing.
2. *Propose solutions to create a soft transition toward predictive policing methodologies*, in order to reduce the resistance to change and the cost associated with technological change and to increase predictive policing operational deployment speed and efficiency.
3. *Develop professional education or training and management methods* to help law enforcement agencies to use predictive policing technology at its fullest as soon as its implementation is completed.

Methodology

Including all four categories of respondents, we collected more than 1650 fully-answered survey in four months, but this article will only, in a first part, provide results regarding police trainees from the 22nd promotion of France's National Police College, which oversees training of newly recruited police officers. The 22nd promotion has a response rate of 86% and 62 fully-answered survey. The survey was a multiple-choice questionnaire self-administered, with 40 questions.

Then, we review results from citizen's survey, which had 31 questions and was deployed among citizens aged 15 and more, living in France's region of Rhone. We used a quota sampling method crossing genders and age (with a gap up to 15 years) and extract a representative sample of 384 individuals.

2 This article is a brief summary of the full report (unpublished), for more information and full results, please do not hesitate to contact: cyril.piotrowicz@wanadoo.fr

3 Rubber-bullet gun.

Police trainees and predictive policing

How do they perceive predictive policing?

Prior to the survey, 63% of police trainees had already heard about predictive policing. But even without knowing what predictive policing exactly is, 87% of them had a good idea of what it is ("anticipate the place of the next offence").

Before specific training, 79% of police trainees thought that predictive policing should or could be used by police forces and 68% think about predictive policing as a "scientific tool". But, at the same time, only 8% see it as a "reliable tool" and less than 2% thought that they had enough knowledge and information.

After a brief explanation of what predictive policing is and where and how it's used, 74% of police trainees admit they have learned new information about it. The explanation made a small but significant difference to their perception of predictive policing: after the briefing 85% were thinking of predictive policing as a "scientific tool" (+17 points), 23% as "reliable" (+15 points), but even so, 82% were unsatisfied with these explanations.

One of the major concerns about predictive policing is the potential threat to civil rights and liberties. Prior to the explanation, 35% of police trainees thought of predictive policing as harmless for civil rights: after the briefing, this rose to 56% (+21 points).

Finally, 71% of police trainees wanted police forces to use predictive policing but with guarantees such as transparency about algorithms and data (47%) and strengthening the control of police activities (47%).

How do they want to use predictive policing?

Police trainees are not unanimous on how they want to use predictive policing: 32% of them are in favour of a prevention policy, 23% favour an enforcement policy and 45% prefer a hybrid approach.

When asked "What could justify the use of predictive policing?", the top answers were:

— Tackling crimes such as robberies or violence (66%);
— Tackling serious offences such as murder or rape (45%);
— Dealing with the feeling of insecurity and minor offences such as fixed penalty notices (40%).

Furthermore, 52% of them think that identity-checking an individual, without any other suspicion, based only on a predictive crime map is justified, but only 29% see this action as legal.

Indeed, when asked about the "major difficulties of predictive policing", legal issues are on the top of the list (77%), followed by a lack of acceptance from citizens (65%) and then the professional training (52%).

Police trainees ask for a specific formation regarding predictive policing (73%) and they all wanted that to be delivered by police officer who had previous experience with predictive policing.

Citizens and predictive policing

How do they perceive predictive policing?

Unlike the police trainees, most French citizens had not heard of predictive policing prior to this survey (70%) but they still had a good idea of its purpose ("anticipate the place of a future offence", 63%).

More curiously, despite not knowing what predictive policing is, they pictured the tool as "scientific" (59%).

As we could have expected, they were undecided regarding its "reliability" ("not knowing", 54%) and its risk regarding civil rights and liberties ("not knowing", 36%). Overall, they found that predictive policing had been insufficiently explained to them (85%) and they wanted to be better informed about it (73%).

But this lack of information, did not prevent them supporting predictive policing since 59% of them thought that police forces should or could use it.

Following our brief explanation of predictive policing, 85% of citizens considered it as useful, and it was a first explanation for 56% of them.

It also had a positive influence: they were more likely (now 83%) to see predictive policing as a "scientific tool" (+24 points), and they were less undecided regarding its "reliability" (- 14 points) and risks (-12 points).

Finally, 61% of citizens wanted police forces to use predictive policing but with guarantees such as strengthening the control of police activities (65%) and strengthening the rights of the defense (57%).

How do they want predictive policing to be used?
Unlike police trainees, citizens are more in favour of a predictive-based prevention policy (54%).

When asked "What could justify the use of predictive policing?", the top answers were:

— Tackling crimes such as robberies or violences (53%);
— Tackling serious offences such as murder or rape (49%);
— Fighting terrorism (44%).

Furthermore, 59% of them accept the idea of an identity-check performed against an individual, without any other suspicion, based only on a predictive crime map.

Regarding the "risks of predictive policing", citizens are worried about misuse by the police forces (71%) and risks linked to the technology, such as unreliable data or hacking (61%).

An interesting point is that citizens surveyed did not think that predictive policing would degrade the trust between them and police forces (61%).

Conclusion

Thanks to this survey, we have learned that:

- Police trainees have a reasonable understanding of what predictive policing is and they are interested in using it in the field. However, they are less sure about its reliability, they ask for guarantees about its legality and they feel that they need specific training.
- Citizens have less understanding as to what predictive policing is, but they agree police forces should be using it, even if they think it could be dangerous. They also want strengthened accountability.

Knowing that citizens and police trainees have a broadly similar thought regarding the desirability of predictive policing (reliability and risks of the software, for example) but also some differences (such as public policy regarding predictive policing), France's National Police College is now able to create for police trainees a specific training, and for citizens a specific information campaign. Both will tend to generate a favorable prior situation to a nationwide deployment of predictive policing software preventing misunderstanding, misusing and unproven fear or resistance.

By analyzing our brief explanation of predictive policing and its impact on the answers, we will be able to design a public communication strategy to reassure citizens prior to a nation-wide predictive policing deployment. By fully informing citizens, based on this research, we aim to raise awareness and reduce concerns. It is also an opportunity to fight the spreading of fake news or misunderstanding regarding an important matter: public safety.

Based on the results from this survey, we are now able to create a specific training that will meet the needs of our police officers, will reinsure them regarding predictive policing and made them to be aware of the capabilities of the software. Therefore, we hope that they will gain even more interest in predictive policing and will use it as it was intended to: as a decision-support tools, not as a tool making decisions for them.

Finally, one of the major issues of predictive policing concerns its legal implications. As shown in the survey, both citizens and police trainees agree to an identity-check solely based on a predictive algorithm.

Is it legal?
Police trainees, who often have a criminal law degree, must take criminal law courses during their training, and yet they are still uncertain. However, when looking back to France's Criminal Procedure Code, it appears that article 78-2 al.8 may provide a suitable basis, even if this has not been brought yet before a court of justice.

Until this is clearly resolved, we need to prevent the uncertainty, the risk of a procedural defect, by harmonizing the practice and sensitizing our future police officers to what can, and can't be legally done, solely based on an algorithm.

References

- Défendeur des droits (2018) *Rapport annuel d'activité 2017*. Paris, p.3.
- IGPN – Inspection Générale de la Police Nationale (2017) *Rapport annuel d'activité 2016*. Paris, 34.
- Piotrowicz, C. (2014) *Statistics and Crime Prevention*. LLM, University Jean-Moulin Lyon 3
- Piotrowicz, C. (2016) Criminological study of "predictive policing" about Homeland Security: toward a "predictive prevention"? In: D. Bourcier, *Open data & big data*, 1st ed. Paris: Mare & Martin, 163-191.
- 20Minutes (2016), Faut-il interdire l'utilisation du flash-ball par les forces de l'ordre? 20Minutes [online].
  Available at: https://www.20minutes.fr/societe/sondage-4847-faut-interdire-utilisation-flash-ball-forces-ordre

Using Predictive Policing to Prevent Residential Burglary - Findings from the Pilot Project P4 in Baden-Württemberg, Germany

Dominik Gerstner
Department of Criminology
Max Planck Institute for Foreign and International Criminal Law, Germany[1]

Abstract
In October 2015 the 'Pilot Project Predictive Policing' (P4) was started in the German federal state of Baden Württemberg. A predictive policing strategy was applied in the context of residential burglary. An evaluation study of the first six months of the pilot was carried out by the Max Planck Institute for Foreign and International Criminal Law. The article describes how the strategy was applied and summarizes the main findings of the evaluation study. Despite some positive findings the impact remains unclear and the expectable crime reducing effects appear to be moderate. Within the police force the acceptance of predictive policing is a divisive issue. Future research is recommended.

Keywords: Predictive Policing, PRECOBS, residential burglary, evaluation study

Introduction

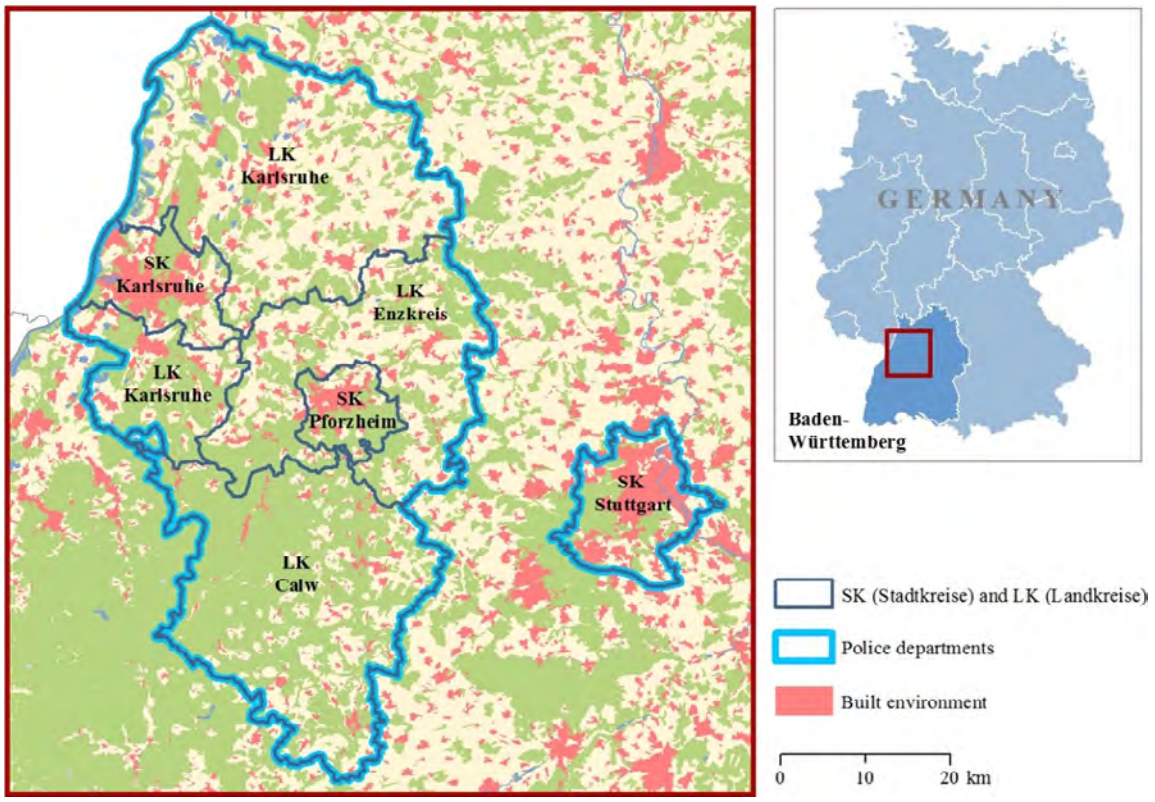
As in other federal states of Germany, also in Baden-Württemberg the number of residential burglaries has increased immensely (until 2015) since about 2008 after more than 15 years of decrease. In response to this development, different measures were introduced to stop or, ideally, reverse this trend. In this context, methods of predictive policing are being applied and tested in some of the federal states of Germany (cf. Egbert 2017; Sommerer 2017). Although the burglary rate is relatively low compared to some other German states, on October 30, 2015 the 'Pilot Project Predictive Policing' (P4) was started in Baden-Württemberg (Innenministerium Baden-Württemberg 2015). Coordinated by the State Office of Criminal Investigations (Landeskriminalamt), the project was conducted in the police departments of Karlsruhe and Stuttgart (Figure 1). The area included the urban districts (Stadtkreise) Stuttgart, Karlsruhe and Pforzheim and the more or less rural districts (Landkreise) Karlsruhe (LK), Calw and Enzkreis.[2] The police department of Stuttgart is equivalent to the urban district. As in Bavaria (*Bayrisches Staatsministerium des Inneren* 2015) and some areas of Switzerland (Balogh 2016), the commercial predictive policing software PRECOBS, offered by the German company 'Institut für musterbasierte Prognosetechnik' (IfmPt), was employed to predict near-repeat burglary events and to apply subsequent target-oriented operational planning.[3]

1 Corresponding author's email: d.gerstner@mpicc.de

2 EU NUTS 3 regions. For further information, see http://ec.europa.eu/eurostat/web/nuts/national-structures-eu, http://ec.europa.eu/eurostat/documents/345175/7451602/nuts-map-DE.pdf [14.03.18]

3 www.ifmpt.de, http://www.ifmpt.de/projekte/, English site: http://www.ifmpt.com/ [14.03.2018]

Figure 1: Pilot area, Stadtkreis (SK) = urban district, Landkreis (LK) = rural district (data source: Federal Agency for Cartography and Geodesy of Germany, own graphic representation)



The project was designed to produce open-ended and unbiased results and therefore included an external scientific evaluation conducted by the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany. Automatically generated predictive policing data were analyzed to obtain assessments of practicality and information concerning crime preventive aspects. In addition, semi-structured interviews with the police officers operating the software and an online survey with more than 700 participants were carried out. This paper describes the functional principle of PRECOBS in a nutshell and summarizes the main findings of the evaluation study.[4]

Predictive Policing

Since the TIME Magazine (Grossman et al. 2011) ranked the application of predictive policing in Santa Cruz (US-CA) as one of the most important inventions in 2011, the term has received increased attention in media as well as in academia. During the last years predictive policing strategies were applied mainly in the USA but also in European countries and recently the topic is broadly discussed in China and Japan.[5] With the widespread application of different predictive policing strategies a precise definition has become difficult. A general description might be that predictive policing is "a multi-disciplinary, law enforcement-based strategy that brings together advanced technologies, criminological theory, predictive analysis, and tactical operations that ultimately lead to results and outcomes – crime reduction, management efficiency, and safer communities" (Uchida 2014: 3871). The interplay between those different aspects has also been described as "prediction-led policing business process"

4 The author would like to thank the State Office of Criminal Investigations of Baden-Württemberg (Landeskriminalamt) for the close cooperation, provision of data and support with the online-survey and interviews with operators. Thanks are also due to the IfmPT for providing additional data. The evaluation study can be obtained online (German version): https://www.mpicc.de/en/forschung/forschungsarbeit/kriminologie/predictive_policing_p4.html [14.03.2018]

5 For example: http://www.scmp.com/news/asia/east-asia/article/2130980/japan-trials-ai-assisted-predictive-policing-2020-tokyo-olympics; https://www.japantimes.co.jp/news/2018/02/28/asia-pacific/social-issues-asia-pacific/china-using-big-data-predictive-policing-xinjiang-region-round-perceived-threats-hrw/

(Perry et al. 2013) with the authors emphasizing that accurate predictions require adequate subsequent action to decrease crime. Another important issue is the subject of predictions. Here, predictive policing can be divided into two subcategories, namely "place-based predictive policing" and "person-based predictive targeting" (Ferguson 2017). While the first one includes predictions about the likelihood of crimes occurring in certain areas during a certain time, the latter one makes predictions about particular people who might be offenders or victims. Thereby the scientific community agrees that predictions have to be considered as non-binary probabilities rather than certainties (e.g. Perry et al. 2013: 8, Degeling & Berendt 2017). This 'difficulty' varies with the type of offences and becomes most important when making predictions about distinct individuals or groups of people. Recent literature gives broad information about the basic principles, challenges, different developments and ethical aspects of predictive policing (Perry et al. 2013, Hunt et al. 2014, Uchida 2014, Mohler et al. 2015, Saunders et al. 2016; Degeling & Berendt 2017, Ferguson 2017, Shapiro 2017). This paper focusses on one example of place-based predictive policing and gives short insight into different components of an applied prediction-led policing process.

Predictive Policing with PRECOBS in Baden-Württemberg

In Germany predictive policing is solely applied as place-based predictive policing in the context of residential burglary.[6] Accordingly, PRECOBS does not predict distinct burglaries committed by certain offenders but rather assesses the likelihood that certain areas will experience burglaries during a certain timespan. For an understanding of the evaluation study's findings, a short description of what kind of data is analyzed to predict burglaries and how predictions are made with PRECOBS is provided briefly. More information can be found in the detailed evaluation report (Gerstner 2017) or in Schweer (2015).

To forecast burglaries PRECOBS utilizes the *near repeat phenomenon,* which is the observation that crime events are often followed by further events in spatial and temporal proximity (illustrated in Figure 2, subgraph A). Numerous empirical studies lend support to this observation for residential burglary (Townsley et al. 2003, Bowers & Johnson 2004, 2005, Sagovsky & Johnson 2007, Short et al. 2009, Bernasco et al. 2015, Nobles et al. 2016, Ornstein & Hammond 2017, Piza & Carter 2017) but also other types of offences (for an overview see Johnson & Bowers 2014: 3244). The rationale behind near repeat burglaries lies in the assumption that burglars act rational and behave like an *optimal forager* (Johnson et al. 2009), this results in patterns which are to some extent predictable.

Though only a certain amount of burglaries trigger subsequent events, PRECOBS uses the near repeat phenomenon for crime prediction. In advance of active field operation the software is configured with data from the past. The procedure identifies attributes of residential burglaries which point towards near repeat series. The system primarily analyzes the circumstances of an offence and the geographic location. *Trigger criteria,* indicating expected future near repeats, as well as *anti-trigger criteria*, speaking against near repeats, are being identified and listed in reference tables covering attribute groups stolen goods, modus operandi and locality (method of entry, type of house, etc.). Additionally, areas with high chances of near repeat burglaries are identified. A retrospective simulation study verifies in which of those 'near repeat affine' areas promising predictions are possible (Schweer 2015), the performance is measured via accuracy of simulated predictions. Promising areas, so called *near repeat areas* (Figure 2, subgraph B), will be activated in the real-time operation.

During daily operation PRECOBS only needs a limited amount of data which derives from police investigations and is mainly recorded when a residential burglary is reported to the police and information is entered into the case processing system (in Baden-Württemberg ComVor). Besides the attributes related to trigger criteria, the address[7], date and time of the initial event are needed. The precision of information has an impact on the precision of the predictions. During the

6 Usage with other offences like robbery and theft from cars is apparently planned in some areas in Germany (https://www.heise.de/newsticker/meldung/Predictive-Policing-Die-deutsche-Polizei-zwischen-Cyber-CSI-und-Minority-Report-3685873.html [14.03.18]). In the context of Islamist radicalization the Radar-ITE program (*Bundeskriminalamt* 2017) is sometimes connected with the term predictive policing in media (https://www.heise.de/newsticker/meldung/Precrime-BKA-meldet-erste-Erfolge-der-Gefaehrderanalyse-mit-Radar-iTE-3921293.html [14.03.18]).

7 Due to requirements of the federal data protection officer the processing within PRECOBS and the predictions do not refer to addresses but are assigned to micro units with a minimum of five households.

Figure 2: (A) Example of near repeat burglaries; 9 offences from 5 years. The blue event (originator) and red events (near repeats) happened within three days (real time and distance data, location spatially blurred). (B) near repeat area (solid line, fictitious example) and according fringe area (dashed line), (C) Initial offence triggering an automated prediction (fictious) and operational circle (blue). Background maps by Stamen Design under CC BY 3.0

pilot, data was directly transferred into PRECOBS three times a day. After the import, the software compares attributes of recent burglaries with reference tables of triggers and anti-triggers. If attributes match and the burglary took place in a near repeat area, an *automated prediction* is made. Predictions are checked for plausibility by the operators – the police officers operating the software – and accepted or denied. When accepted, an alert is being relayed to the local police station. The PDF document contains a map, recommendations for patrol as well as information about the initial event. The patrol area is called *operational circle* and contains a circular area around the originator (the burglary that triggered the alarm) with a radius of 500 meters (Figure 2, subgraph C). In this area a heightened risk of near repeat burglaries is assumed for usually seven days. Although close to near repeat areas, automated alerts cannot be produced in fringe areas (Figure 2, subgraph B). Nevertheless, the software provides the operator with an overview of burglaries in these areas with information about matching trigger criteria. The operator checks if a burglary might be a trigger for near repeats and decides whether an alert should be created manually (*operator alert*). The PDF, the relay and what follows the alert is equivalent to *automated alerts*. The option for *free prognoses*, detached from *near repeat* or *fringe areas*, is not described as this was used only four times during the evaluation period.

As patterns of burglary differ over seasons, PRECOBS has separate configurations for standard time and daylight saving time. Furthermore, geographical distribution and attributes of near repeat burglaries are not stable over time, which leads to a recalibration (areas, triggers, etc.) with each new configuration.

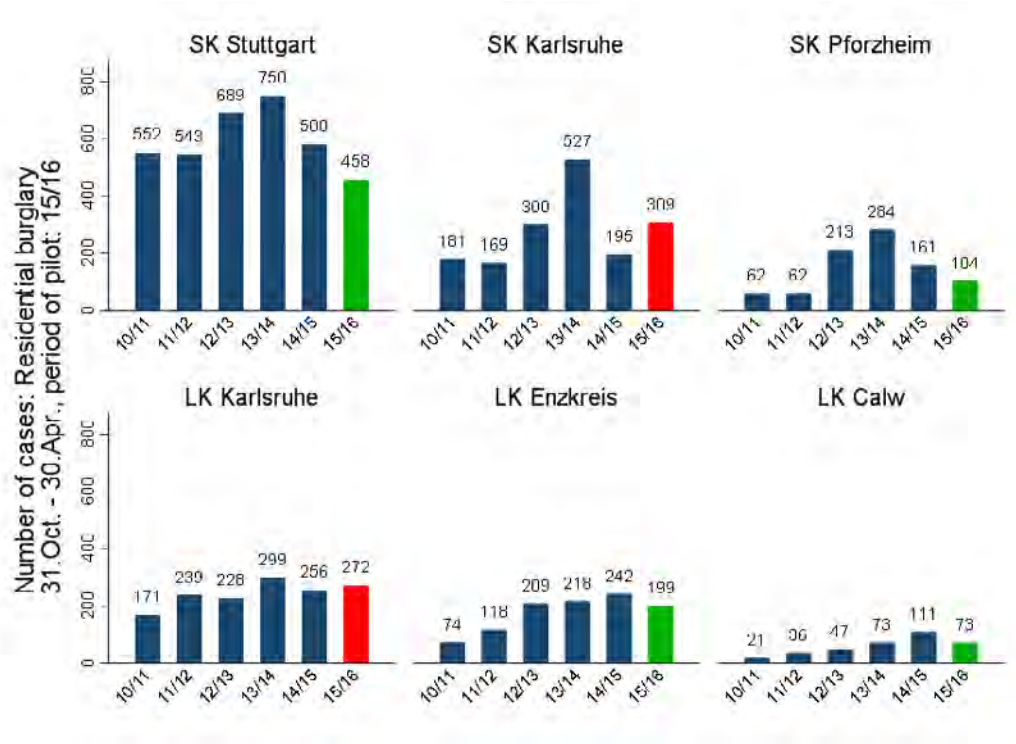
To sum up, PRECOBS is not designed to predict all burglaries but to predict potential burglaries following an initial event in spatial and temporal proximity. The method of how predictions with PRECOBS are made is not based on a complicated algorithm and doesn´t include elements of machine learning or artificial intelligence. The logic behind the predictions is comprehensible for the police. Although some additional data is included in the system (e.g. types of streets, population structure) to enrich the individual decision-making of the operators, the data processed for prediction is sparse and originates from everyday police work. The main goal of police operations following the alerts is deterrence.

PRECOBS alerts

During the six months evaluation period there were 183 alerts which mainly affected the urban districts Karlsruhe, Pforzheim and Stuttgart. In rural areas only few predictions and subsequent alerts occurred, caused by the fact that only few of the offences fell into the relevant near repeat or fringe areas. For example, in the district of Calw (Landkreis), these were only three out of sixty-nine burglaries (4.3 %). By contrast, in the urban district of Karlsruhe (Stadtkreis) 63.9 % out of 274 offences were committed in relevant areas. For this reason, the effectiveness of predictive policing in rural areas can hardly be assessed.

The processing and relay of the alerts usually went quick. The timespan between data import and relay of the alerts was reasonably short (median = 2 hours). On average the timespan between the originator event

Figure 3: Number residential burglaries in subdivisions of the pilot area. Evaluation period of pilot (31.10.2015 – 30.04.2016) compared to equivalent period in the years before (data source: ComVor-database LKA BW, own calculation)



and the relay was about 30 hours on average and 61 % of the alerts were relayed in less than 20 hours. This could be considered as reasonable, since the duration of the alerts was seven days and near repeat events – when appeared – happened within 60 hours on average (median = 50) after the initial event.[8]

What followed the alerts was a measurable increase in patrol activity. Via anonymized GPS data from police cars, an approximate measure for police density was applicable to compare states of active and inactive alerts in the respective operational circles. In about 94 % of the alerts the presence of police increased by 73 % on average (median = 49 %) during an alert. Manually recorded data by patrol officers allowed to estimate different police activities during a single alert. On average 48 hours of patrol activity were carried out by 2.8 officers. Besides patrolling in vehicles, foot patrol was also applied by uniformed or plain clothed officers (Zivilbeamte). Spatial and temporal focused identity checks (mean = 16.5) and vehicle inspections (mean = 9.4) were carried out and sometimes the resident population was contacted. These kind of measures are carried out regularly (especially during dark winter months) in areas not affected by PRECOBS alerts without a focus on predicted areas and periods.

Efficiency of predictive policing in the context of P4

In the police department of **Stuttgart** the total number of cases during the evaluation period declined considerably (Figure 3). It is hard to assess whether this was related to PRECOBS because this development also occurred during in the comparative period one year before and crime rates vary naturally over time. An indicator of the efficacy is the decline of significant near repeat patterns (500 meters / 7 days) in the near repeat areas. In the reference periods of the preceding years, there were significant near repeat patterns in the near repeat areas as well as in the total district. The ratio of near repeats was higher in the near repeat areas (Table 1, row A&B, columns A-D), which stresses that the areas were meaningfully defined by the software developer. For the evaluation period there was still a significant pattern present when examining the district in total, but for the near repeat areas (Table 1, row B, column E) a significant pattern didn't exist. The same applies to the **police department of Karlsruhe** (Table 1, rows C&D).

8 The calculation uses the midpoint of the timespan the crime occurred as reference.

Table 1: Results of near repeat analyses, overall areas and near repeat areas. Own calculations with „Near Repeat Calculator" (Ratcliffe 2008). Data source: ComVor-database LKA BW, PRECOBS database

		significant near repeat-pattern (7 days /1 –500 meter)				
		W†12–15 A	W12–13 B	W13–14 C	W14–15 D	W15–16†† E
SK Stuttgart	A Total	1.69**	1.79**	1.29*	1.51**	1.64**
	B ***NR-Areas***	***2.25****	***2.51****	***1.52****	***1.85****	***1.23***
PP Karlsruhe	C Total	2.03**	1.66**	1.59**	1.57**	1.62**
	D ***NR-Areas***	***2.35****	***2.42****	***1.75****	***2.19****	***1.39***
SK Karlsruhe	E Total	1.71**	1.29	1.45**	1.14	1.48*
	F ***NR-Areas***	***1.92****	***2.22****	***1.67****	***1.65***	***1.49***
SK Pforzheim	G Total	1.55**	1.65**	1.47*	0.96	1.3
	H ***NR-Areas***	***1.71****	***2.68****	***1.4****	***1.16***	***0.69***

SK = Stadtkreis, urban district, PP = Polizeipräsidium (regional police department), larger Area with urban and rural districts, Stuttgart PP is equal to SK.

** p<0.001, * p<0.05 (Monte Carlo simulation with N=999 iterations)

Example: 1,85: The chance of another incident is about 85 percent greater than if there were no discernible pattern.

†W = Winter-Configuration: November, December, January, February, March

††W15–16: P4 evaluation period

In the **police department of Karlsruhe** the absolute number of burglaries remained more or less constant compared to the preceding period. This was due to a strong activity of burglaries during November and December 2015 in the **urban district of Karlsruhe** and the surrounding **rural district of Karlsruhe** (Figure 3). If the number of cases had been higher without PRECOBS remains unclear. Compared to the preceding period, the number of cases declined in the other areas of the police department. This is especially true for the **urban district of Pforzheim**, whereas the numbers had also declined in the penultimate period (Figure 3).

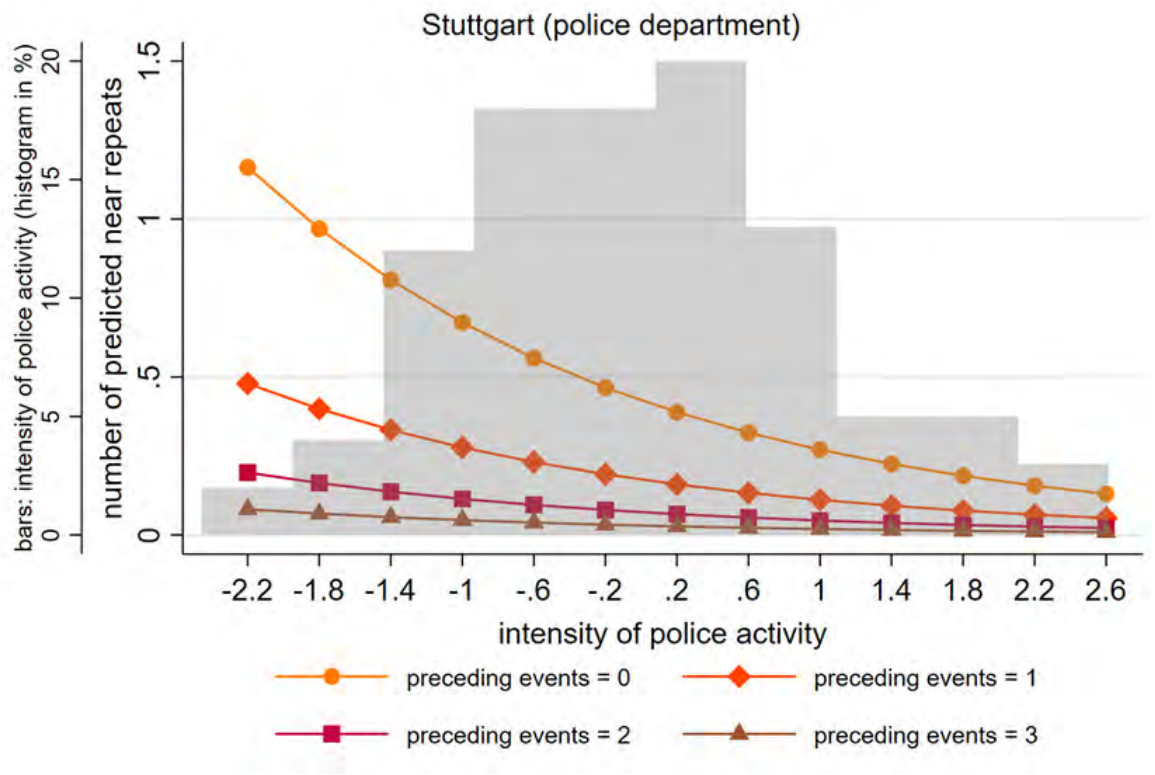
Despite the considerable increase of burglaries (+100 cases compared to the year before) in the **urban district of Karlsruhe**, there was no significant near repeat pattern observed in the near repeat areas for the evaluation period (Table 1, row F, column E). The ratio was even slightly lower than in the period before, which experienced only very few burglaries. This could be rated as another indicator for crime reduction through near repeat prediction, but causality cannot be derived from these findings.

In the **police department of Karlsruhe** correlations between police density and the number of near repeat burglaries subsequent to an alert triggering event (7 days / 500 meters) were indicated. Alerts with a stronger increase in police density showed a lower tendency for near repeat events (Spearman´s rho = -0.24, $p < 0.05$, n=72). Another correlation, only significant on the 10 % level, was found for the number of predecessor burglaries which were possibly related to the originator event due to spatial and temporal proximity. With more events preceding the originator, the probability for near repeat events decreases (Spearman´s rho = -0.21, $p < 0.1$, n=72). In multivariate analysis no significant effects were found.

A similar finding can be reported for the **police department of Stuttgart**. Though no significant correlations with the police density via GPS data was found, a correlation between manually recorded police activity[9] and the number of near repeats was found. An index (PCA factor score) including the variables "sum of operating hours", "number of identity checks", "number of vehicle controls", and "number of direct contacts to residents" gives a summary of how alerts differ in intensity of patrol activity. With a higher intensity less near repeats were to be expected (Spearman´s rho = -0.21, $p < 0.05$, n=100). This finding also holds in a multivariate framework where the dependent variable was the number of near repeats following an alert (negative binomial regression). Effects can be reported for the "intensity" (b= -0.46, $p < 0.01$) and the "number of potentially preceding events" (b= -0.89, $p < 0.1$). The remaining predictors, "time between the originator and the relay of the alert" as well as the "ratio of patrol officers in plain clothes" do not show an effect. On aver-

9 The manual documentation started with a delay, which resulted in a reduced number of cases. The sample size in the police department of Karlsruhe was too small for these analyses.

Figure 4: Predicted values for different values for „intensity of police activity", conditioned by „number of preceding events" (data source: ComVor-database LKA BW, PRECOBS database, own calculation)



age the effect of intensity is rather small. With a change in "intensity" from the 10th percentile to the 90th percentile – which corresponds to the boundary of the middle 80 % of the distribution - the amount of estimated near repeats by the model only changes by -0.78 burglaries (average marginal effect = -0.18, p <0.01). Within the interquartile range the number of predicted events changes only by -0.23 (25th percentile=-0.69, 75th percentile=0.63) – this effect appears to be rather small. As nonlinear-regression is affected by inherently multiplicative (or conditional) effects (for further explanation see Oberwittler & Gerstner 2014, Gerstner & Oberwittler 2018) interesting moderating effects between "intensity" and the "number of potentially preceding events" are observable (Figure 4). With no preceding events the effect of the intensity of police activity appears to be strong. With more than one preceding events the effect is practically not present. As the results are based on small sample sizes and only a short period of time, they have to be treated with caution. Nonetheless, these findings point to the importance that detecting small series of burglaries at an early stage can improve crime prevention. Future research should follow this issue with experimental designs.

Assessment by PRECOBS Operators

PRECOBS operators are officers who operate the software, evaluate automated predictions, manually generate predictions and relay the alerts. The basic tenor of semi-structured interviews was that PRECOBS was assessed as a useful supplement, especially during phases with a high load of burglaries. According to this, the application in rural areas, with only few burglaries, was perceived skeptically. The software was unanimously rated as user-friendly, even though there were some initial difficulties. The support offered by the developer was gauged as good. Asked about the transparency of the automated alerts, the operators emphasized that in most cases these were comprehensible. Some of them expressed that after a certain period of usage, they required a keen eye for cases which would trigger an alert, before importing the data into the software. Finally, the operators appreciated the additional tools (not part of the evaluation study) implemented in PRECOBS for the analyses of local crime activities.

Online Survey with Police Officers

An online survey with more than 700 police officers made it possible to capture how predictive policing with PRECOBS was perceived by patrol officers and officers in the upper service. One important finding was that predictive policing is a divisive issue (see Figure 5). About one half of the respondents sees a promising concept in applied predictive policing, the other half has the opposite view. The question of continuation was rated more positive in the police department of Karlsruhe, where 62 % of the respondents agreed to a further use of the software. In the police department of Stuttgart only 41 % agreed to this. The highest agreement was found in the group of the higher management level (65 %, höhere Führungsebene), followed by the respondents of the middle management level (57 %, mittlere Führungsebene). The lowest agreement was found in the group with mainly patrol officers (46 %, Sachbearbeiter).

A remarkable finding was that those confronted with lots of alerts during their everyday service, assessed the benefits of predictive policing with PRECOBS more negatively and disagreed more often to a continuation (Figure 6). This is possibly due to the fact that some of the respondents reported about additional workload or about other work left undone during active alerts. This problem was mainly perceived by officers in Stuttgart. Another explanation might be that success is not immediately measureable. Predictive policing with PRECOBS aims at preventing burglaries by deterrence rather than catching criminals. In this context it is hardly surprising when frequent PRECOBS alerts break established routines and therefore negative perceptions are reported by some of the respondents. This is another connection point for future research.

Figure 5: Perceived value of predictive Policing. Mean score out of 7 items (Cronbach's Alpha = 0,912): "Predictive policing (PP) is a useful addition to regular police work", PP is more annoying than useful"*, "PP is a suitable auxiliary tool for targeted planning", "An added value is not given with PP"*, "In my opinion PP remains gazing into a crystal ball"*, "It is worth thinking about using PP with other offences", "The financial resources of the pilot could have been used better elsewhere"* (n = 552, *reverse coded, PP Stuttgart/Karlsruhe = police departments, Data source: P4 online-survey).

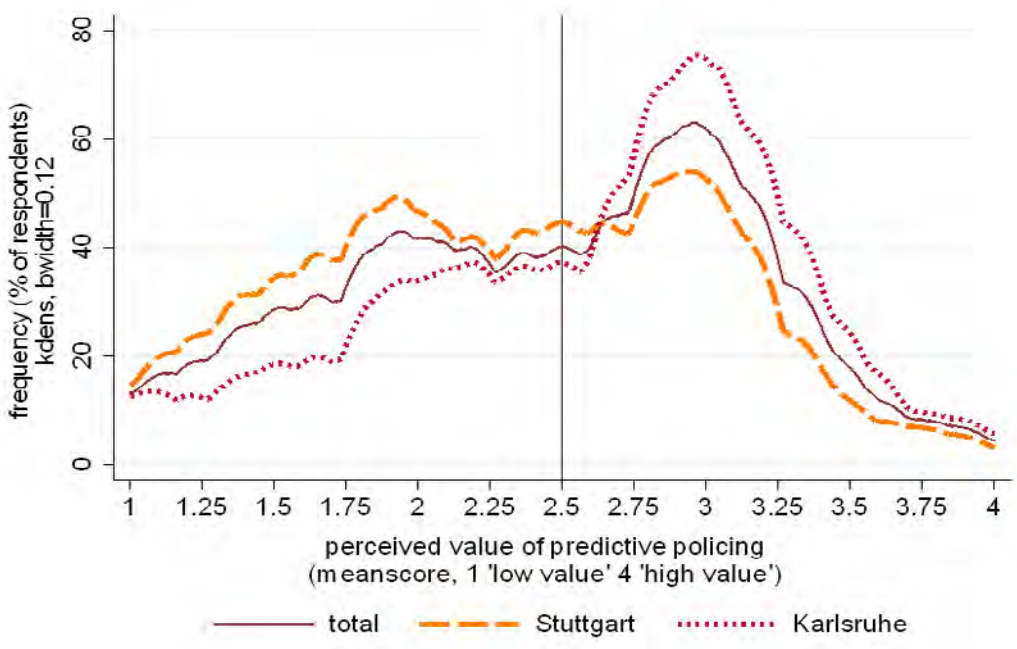
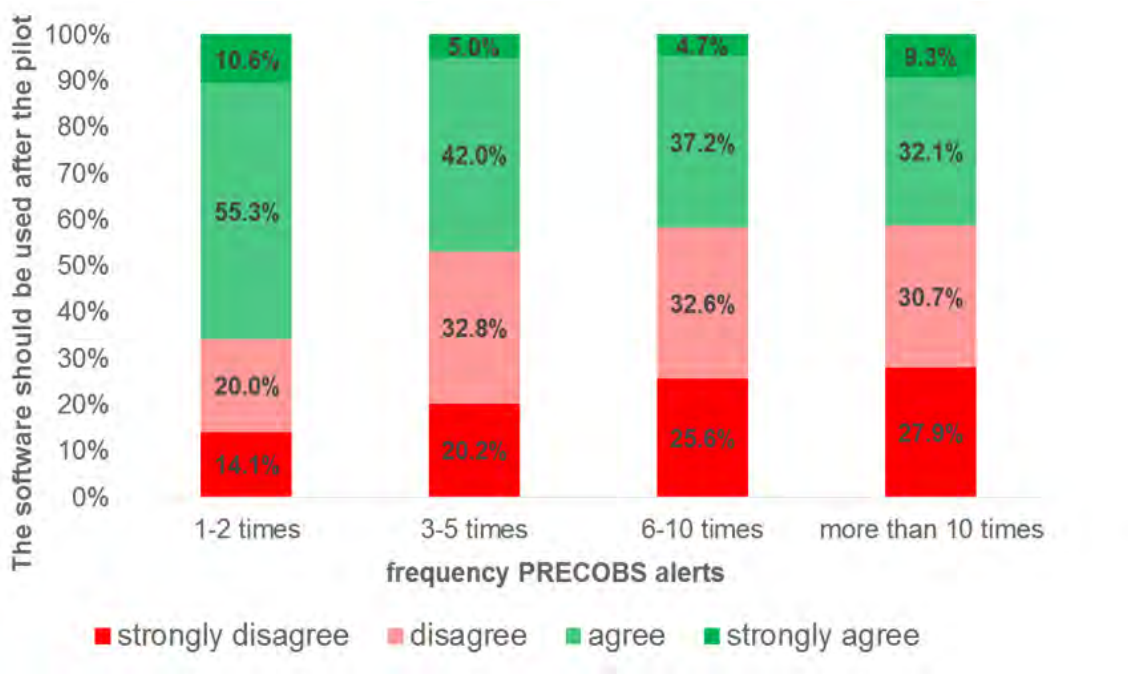


Figure 6: "The software should be used after the pilot" in relation to the frequency patrol officers had to serve PRECOBS alerts (n=430, Data source: P4 online-survey)



Concluding remarks

After the evaluation of the P4 pilot project and despite some positive indications, it still hard to assess whether and to what extent predictive policing can contribute to the reduction of residential burglaries. Some relevant conclusions can be drawn on the basis of available data related to alerts based on predictions, also on data about police activity as well as the analyses of numbers and patterns of burglaries. Furthermore, it could be demonstrated that predictive policing is more than making predictions. With regard to crime reducing effects, it is important to note that the results have to be treated with caution due to the short evaluation period, the lack of an experimental research design and a small size of trial areas. As crime rates usually show natural variation, a comparison with previous periods or other regions can only give limited insights. Only few studies with an experimental research design have been carried out in the field of predictive policing (Hunt et al. 2014, Mohler et al. 2015, Saunders et al. 2016). Since predictive policing has become a hot topic in many European countries, such studies are desirable for future research in order to gain knowledge about how predictive policing can reduce crime. Nonetheless, with the analyses of near repeat patterns and near repeat events subsequent to alerts, the evaluation study found that certain crime reducing effects are indicated, however these effects appear to be moderate. The integration of the software into everyday business worked without much difficulty and police actions following an alert-triggering burglary took place in a timely manner. The small group of officers who operated the software, assessed it as a useful supplement – especially during times with a high load of residential burglary. In a larger group, including patrol officers, the perceived value of predictive policing with PRECOBS was a divisive issue. In particular, officers who were confronted with many alerts tended to disapprove of a continuation of predictive policing. This might be due to perceived additional workload but also due to the fact that the preventive effects of deterrence cannot directly be perceived. The acceptance and assessments of predictive policing within police forces provide additional connection points for future research.

The Baden-Württemberg Police is using the software for another trial period in the same pilot area since August 2017 in order to get a higher degree of certainty about benefits of predictive policing in the context of residential burglary. This includes a further scientific evaluation by the Max Planck Institute for Foreign and International Criminal Law in Freiburg. Besides the extended timespan, an experimental research design is applied to increase the meaningfulness of the results.

References

- Balogh, D. A. (2016) Near Repeat-Prediction mit PRECOBS bei der Stadtpolizei Zürich. *Kriminalistik, 2016* (5), 335 - 341.
- Bayrisches Staatsministerium des Inneren, f. B. u. V. (2015) Press release: Herrmann berichtet über Erfahrungen des Precobs-Tests in München und Mittelfranken. München.
- Bernasco, W., Johnson, S. D. & Ruiter, S. (2015) Learning where to offend: Effects of past on future burglary locations. *Applied Geography, 60*, 120-129.
- Bowers, K. J. & Johnson, S. D. (2005) Domestic Burglary Repeats and Space-Time Clusters. *European Journal of Criminology, 2*(1), 67-92.
- Bowers, K. J. & Johnson Shane, D. (2004) Who commits near repeats? A test of the boost explanation. *Western Criminology Review, 5* (3), 12-24.
- Bundeskriminalamt (2017) Press release: Neues Instrument zur Risikobewertung von potentiellen Gewaltstraftätern. RADAR-iTE (regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos - islamistischer Terrorismus).
- Degeling, M. & Berendt, B. (2017) What is wrong about Robocops as consultants? A technology-centric critique of predictive policing. *AI & SOCIETY*, doi:10.1007/s00146-017-0730-7.
- Egbert, S. (2017) Siegeszug der Algorithmen? Predictive Policing im deutschsprachigen Raum. *Aus Politik und Zeitgeschichte, 67*(32-33), 17-23.
- Ferguson, A. G. (2017) *The rise of big data policing. Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.
- Gerstner, D. (2017) *Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl. Evaluationsergebnisse zum Baden-Württembergischen Pilotprojekt P4* (1. Aufl. ed., forschung aktuell | research in brief, Vol. 50). Freiburg im Breisgau: Max-Planck-Inst. für Ausländisches und Internat. Strafrecht.
- Gerstner, D. & Oberwittler, D. (2018) Who's hanging out and what's happening? A look at the interplay between unstructured socializing, crime propensity and delinquent peers using social network data. *European Journal of Criminology, 15*(1), 111-129.
- Grossman, L., Brock-Abraham, C., Carbone, N., Dodds, E., Kluger, J., Park, A., et al. (2011) The 50 best inventions. *Time Magazine, 178*(21), 55-82.
- Hunt, P., Saunders, J. & Hollywood, J. S. (2014) *Evaluation of the Shreveport Predictive Policing Experiment*: RAND Corporation.
- Innenministerium Baden-Württemberg (2015) Press release: Polizei startet Einsatz der Prognose-Software „precobs". Stuttgart.
- Johnson, S. D. & Bowers, K. J. (2014) Near Repeats and Crime Forecasting. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of Criminology and Criminal Justice* (pp. 3242-3254). New York, NY: Springer New York.
- Johnson, S. D., Summers, L. & Pease, K. (2009) Offender as Forager? A Direct Test of the Boost Account of Victimization. [journal article]. *Journal of Quantitative Criminology, 25*(2), 181-200.
- Mohler, G. O., Short, M. B., Malinowski, S., Johnson, M., Tita, G. E., Bertozzi, A. L., et al. (2015) Randomized Controlled Field Trials of Predictive Policing. *Journal of the American Statistical Association, 110*(512), 1399-1411.
- Nobles, M. R., Ward, J. T. & Tillyer, R. (2016) The Impact of Neighborhood Context on Spatiotemporal Patterns of Burglary. *Journal of Research in Crime and Delinquency, 53*(5), 711-740.
- Oberwittler, D. & Gerstner, D. (2014) Die Modellierung von Interaktionseffekten in Erklärungsmodellen selbstberichteter Delinquenz – Ein empirischer Vergleich von linearer OLS-Regression und negativer Binomialregression anhand der Wechselwirkungen von Risikoorientierung und Scham. In S. Eifler and D. Pollich (Eds.), *Empirische Forschung über Kriminalität* (pp. 275-301). Wiesbaden: Springer Fachmedien
- Ornstein, J. T. & Hammond, R. A. (2017) The Burglary Boost: A Note on Detecting Contagion Using the Knox Test. [journal article]. *Journal of Quantitative Criminology, 33*(1), 65-75.
- Perry, W. L., McInnis, B., Price, C. C., Smith, S. C. & Hollywood, J. S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*: Rand Corporation.
- Piza, E. L. & Carter, J. G. (2017) Predicting Initiator and Near Repeat Events in Spatiotemporal Crime Patterns: An Analysis of Residential Burglary and Motor Vehicle Theft. *Justice Quarterly*, 1-29.

- Ratcliffe, J. H. (2008) Near Repeat Calculator (version 1.2). Temple University, Philadelphia, PA and the National Institute of Justice, Washington, DC.
- Sagovsky, A. & Johnson, S. D. (2007) When Does Repeat Burglary Victimisation Occur? *Australian & New Zealand Journal of Criminology, 40*(1), 1-26.
- Saunders, J., Hunt, P. & Hollywood, J. S. (2016) Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. [journal article]. *Journal of Experimental Criminology, 12*(3).
- Schweer, T. (2015) „Vor dem Täter am Tatort" – Musterbasierte Tatortvorhersagen am Beispiel des Wohnungseinbruchs. *Die Kriminalpolizei, Heft 1*, 13-16.
- Shapiro, A. (2017) Reform predictive policing. *Nature, 541*(7638), 458–460.
- Short, M. B., D'Orsogna, M. R., Brantingham, P. J. & Tita, G. E. (2009) Measuring and Modeling Repeat & Near-Repeat Burglary Effects. *Journal of Quantitative Criminology, 25*(3), 325-339.
- Sommerer, L. M. (2017) Geospatial Predictive Policing – Research Outlook & A Call For Legal Debate. *NK Neue Kriminalpolitik, 29*(2), 147-164.
- Townsley, M., Homel, R. & Chaseling, J. (2003) Infectious Burglaries. A Test of the Near Repeat Hypothesis. *British Journal of Criminology, 43*(3).
- Uchida, C. D. (2014) Predictive Policing. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of Criminology and Criminal Justice* (pp. 3871-3880). New York, NY: Springer New York.

Predictive Policing - Is It Really an Innovation?

Lúcia G. Pais
Instituto Superior de Ciências Policiais e Segurança Interna, Lisbon, Portugal[1]

Abstract
The novelty of predictive policing, its goals and promises, are put under criticism and discussion. In the last few years predictive policing has been presented as a new model for law enforcement activities. Predictive policing is based on the special skills of statisticians and computational scientists who run sophisticated techniques to analyse data available in disparate sources, to anticipate and prevent crime and disorder. Hence, a shift in the police work could be envisaged; a change of 'paradigm' (T. Kuhn). This "new" model appears to be rooted in the last century 70s and 80s 'new penology' with its actuarial approach, where numbers produce the individual. Further back in time, its roots can also be found in the 19th century vision of J. Bentham, when he proposed a 'moral arithmetic' for the benefit of governmentality (M. Foucault). A predictive regime requires organisational capabilities and structures, a new way of thinking and (perhaps) new leaders. Police forces would have to be able to effectively make use of the findings of predictive research. Yet, some police forces still don't recognise the criticality of science and research. And, let's not forget that information *is not* knowledge, as it is 'indifferent' to meaning and does not consider people's 'intentional states' (J. Bruner). So, it seems the individual is lost in the mechanics of discovering patterns. But it takes only one person to disrupt society...

Keywords: innovation in police activities; policing models; predictive policing.

Introduction

The novelty of predictive policing, its goals and promises, are put under criticism and discussion. Three main ideas are the core of this discussion: (1) some of the roots of predictive policing, and what appears to be the design of a 'new' individual; (2) the preparedness of police forces to ingrain predictive inputs, and the shift in the police work; and, (3) the way the outliers from a normal distribution are treated when the widespread practices induce to consider group traits.

In the last few years predictive policing has been presented as a new model for law enforcement activities, or as being the future of law enforcement (Haberman & Ratcliffe, 2012; Munk, 2017; Pearsall, 2010; Perry et al., 2013). Predictive policing is a model based on the special skills of statisticians and computational scientists who manage to operate sophisticated techniques to analyse all data available in disparate sources, with the major goal of anticipating and preventing crime and disorder.

1 Corresponding email: lgpais.25@gmail.com

The roots of predictive policing

To achieve equilibrium within and between States, each one has to know the figures about its population, production, commerce, natural resources, financial situation, and so on... This information became available during the XIX century, when statistics started to be systematically published and the confidence in the rigour of numbers and measures was increasingly asserted (Smith et al., 2000).

How was statistics established? Foucault (2007: p.411) said 'it can be established precisely by police, for police itself, as the art of developing forces, presupposes that each state exactly identifies its possibilities, its virtualities. Police makes statistics necessary, but police also makes statistics possible'.

The roots of the actuarial approach can be found in the XIX century vision of Jeremy Bentham, the father of utilitarianism, where his *Introduction to the Principles of Morals and Legislation* (Bentham, 1781/2000) and '*Pannomion: Complete Body of Law* – a complete and rational code aimed at «command and instruct»' (Ost, 2001: p.291) – would provide for the principles of a legislation dedicated to search for the greatest amount of happiness for the greatest number of people through a 'moral arithmetic' and the calculation of pleasures and pains.

He criticised the legal system as well as society and proposed the reform of some institutions that were supposed to discipline people and society, like prisons, schools and welfare services. In his most known proposal – the *Panopticon* – he presented an architectural model that presupposes confinement, inspection (observation), vigilance, discipline, and, of course, registering. If correctly applied, these principles would allow for the control of the whole society, thus enabling the 'disciplines' to operate as 'techniques for assuring the ordering of human multiplicities' (Foucault, 1995: p.218) or to assure 'governmentality' (Foucault, 2007). But he struggled with the absence of numbers that would let governments to adequately rule their societies. Bentham took advantage of some statistical methods to collect, record, and analyse data from the institutions, so that it could be useful to its managers, and even sent them some questionnaires to be completed (Brunon-Ernst, 2007). His interest in the use and utility of numbers was applied to morality, which could be mathematically calculated through the balance of pleasures and pains, thus presenting an economy of pleasures (Bentham, 1840).

To sum up, we can see that the actuarial methods were, already in the XIX century, in place to support governance and governmentality. On the other hand, this "new" model appears to be rooted in the last century 70s and 80s 'new penology' with its actuarial approach, where numbers produce the individual, putting aside idiosyncrasies, wishes, fears, and of course responsibilities.

The 'new penology' is an expression coined by Malcolm M. Feeley and Jonathan Simon in 1992. One central feature of this 'new discourse', as they argue, is the substitution of 'a moral or clinical description of the individual with an actuarial language of probabilistic calculations and statistical distributions applied to populations' (Feeley & Simon, 2000: p.367). Building on the use of a strategy to acquire knowledge about the criminal phenomenon, it would allow for a different perception of the existing problems and potential solutions, and thus for greater effectiveness of the employed resources at the lowest possible cost.

The individual – the ancient unit of analysis and intervention – is to be replaced by behaviours or 'observable data' (Cohen, 1995: p.147), enabling the segregation of the dangerous from the rest of the population. This resulted in the spreading of several offending behaviour programmes targeting specific groups of offenders (e.g. violent, sex, drug and alcohol related offenders), following the 'what works' (Martinson, 1974) and 'nothing works' debate regarding the effects of rehabilitative interventions on recidivist offenders (e.g. Hollin & Palmer, 2006). This movement of criticism had its most prominent force during the last quartile of the XX century, when the increasing violence of some criminality as well as the recidivism of 'treated' offenders and the cost of the rehabilitation techniques was in the centre of the debate, leading to the rejection of the idea of treatment of offenders (Ancel, 1985). Mainly during the 80's, there were some political and public opinion sectors demanding for an adequate response to that violent criminality 'through a rigorous repression, opposing the legal violence to the illegal one' (Di Argentine, 1991: p.26). As some had put it, 'the «resocialisation treatment» was the big idea (or the great illusion) of the 50s' (Ancel, 1987: p.10), and its evaluation led to its abandonment and the emergence of a more neutral one: the idea of intervention (Tsitsoura, 1990).

Resting upon actuarial techniques allowing for new ways of managing the social order, the new penology 'employ[s] the language of social utility and management, not individual responsibility' (Feeley & Simon, 2000: p.367). As Cohen (1995: p.147) wrote, it is 'the most radical form of behaviourism imaginable – prevention of the act of crime by the direct control of whole populations, categories and spaces'. Indeed, the main idea was to be able to respond quickly and locally, to limit contagion effects and manage social risk.

So, *'(…) the new penology is neither about punishing nor about rehabilitating individuals. It is about identifying and managing unruly groups. It is concerned with the rationality not of the individual behaviour or even community organization, but of managerial processes. Its goal is not to eliminate crime but to make it tolerable through systemic coordination.'* (Feeley & Simon, 2000: p.368)

As such, the new criminologists, for instance, are increasingly 'trained in operations research and systems analysis' (Feeley & Simon, 2000: p.375), rather than sociology, psychology, or social work. Furthermore, this new approach provides significant information about the successful intervention strategies and the performance of the institutions themselves. So, even if at the beginning the individual characteristics were searched and highlighted for comprehensive intervention or parole issues, for instance, today, in the actuarial criminology, as Feeley and Simon (2000: p.376) argue, *'the numbers generate the subject itself. (...) [By] rationalizing the operation of the systems that manage criminals, not dealing with criminality (...) [, these techniques] can be used to improve the penal system's efficiency'*. In addition, this also illustrates what happens in many curricula at some police academies: the disinterest in human and social sciences.

On the other hand, Loader (1999: p.373) wrote about the 'commodification of policing and security'. He argued that *'since the early 1980s especially, the imperatives and vocabulary of the market have come increasingly to infuse the rhetoric and practices of the public police'* (Loader, 1999: p.375). The police appeared to be more and more 'business-like' – managerialism; the police was delivering a 'professional service' to the 'consumers' (citizens) of that service – consumerism; and, the police was embracing the task of openly promoting its 'product' – promotionalism. It is so, nowadays. Though maintaining its basic legally-based bureaucratic model, the police are increasingly operating within the market paradigm.

This business analysis and management approach, with the outcomes mainly treated in terms of numbers, became prevalent. The financial constraints police face nowadays demand for it. So, the language of numbers is deeply embedded in the police activity; its managerial costs, the crime figures, what the citizens want and embrace, and the number of followers and likes in different platforms. As Harcourt (2007: p.16) put it, *'risk assessment, algorithms, and criminal profiles now permeate the field of crime and punishment'*. The question one must ask, here, is if this is to minimise the costs for society or police organisations.

It might be said that statistics shape our world, leading us to perceive reality differently. Statistical data help to reinforce stereotypes because of the way data is collected, categorised, run by computational programmes, and analysed. The unshakeable faith on actuarial methods, 'by accentuating and aggravating the correlations between group traits and criminality' (Harcourt, 2007: p.192), will end by changing our world with us behaving differently and relate differently with each other.

The preparedness of police forces to ingrain predictive inputs

A predictive regime requires organisational capabilities and structures, a new way of thinking and (perhaps) new leaders. In this regard, a shift in the police work could be envisaged; a change of paradigm in the sense of Thomas Kuhn (1970). That would mean a new way of perceiving reality, new tools to analyse and intervene, and new shared discourses. But it also means that there would be

'a criterion for choosing problems that (...) can be assumed to have solutions. To a great extent these are the only problems that the community will (...) encourage its members to undertake. (...) [This also means that some] socially important problems (...) [might be discarded] because they cannot be stated in terms of the conceptual and instrumental tools the paradigm supplies' (Kuhn, 1970: p.37),

which is to say, in this case, the police organisation and culture supplies. Numbers generate the individual and also the social problems, determining which ones

should be carefully dealt with and rejecting others. And it is somehow imaginable the interest some political forces might be willing to devote to this matter.

To begin with, police forces would have to be able to effectively make use of the findings of predictive research. Yet, some police forces still don't recognise the criticality of science and research (Jaschke et al., 2007; Weisburd & Neyroud, 2011), though the language of numbers appear to find a definite space in police organisations. At least with regard to budgetary demands... This "new" model seems to accommodate a police force that is not so demanding with what knowledge application is concerned. Rooted in the works of Drucker (1995) who coined the expression 'knowledge work', and Ericson and Haggerty (1997) who saw the police as 'knowledge workers', Brodeur and Dupont (2008) stress that

'the police are considered to be knowledge producers, but they do not even fulfil the requirement of being knowledge appliers, which is to have a formal education. Unless the requirements for formal education are made much more rigorous, this situation is a prescription for disaster.' (p.17)

But from what is known today, there are still many 'police agencies [which] do not see science as critical to their everyday operations' (Weisburd & Neyroud, 2011: p.3), and do not see the need of an academic degree to join a police force or to be promoted as senior police officer. On the other hand, even though police forces show the curiosity and motivation to accept and incorporate new technologies in their activities, they usually have no deep knowledge to evaluate the studies prior to its presentation or to study its effects on police work (Weisburd & Neyroud, 2011). Besides, the police institution is usually suspicious about anyone who shows some interest in its activities (L'Heuillet, 2001), and so there is still a great deal of scepticism regarding the scientists and researchers' work within the police contexts. This is, nevertheless, a strange posture if we think how helpful and powerful an external validation of some practices can be. In fact, police decision-makers could 'benefit immensely from having a respected academic representative (...) affirming that the choices and decisions made by the police follow best practices developed by research, study, and assessment' (Engel & Whalen, 2010: p.106).

Welten (2010: p.12) once said that 'a brave police force deserves courageous scientists'. But as scientists became increasingly courageous and interested in researching in police topics it is also important that the police institution do not see researchers and research results as a verdict of guilt. The idea of being evaluated is fierce, and restrains either the possibility of developing research or the publication of its results in scientific journals because they can damage the image of the police (Weisburd & Neyroud, 2011).

That is to say police officers may not be – or feel – obliged to have a formal education to be knowledge appliers. Rather, they may simply fulfil the task of collecting information as its analysis will be performed by others – now by men, further ahead by machines. It seems 'we have allowed technical knowledge, somewhat arbitrarily, to dictate the path of justice' (Harcourt, 2007: p.3). The resulting knowledge – or, shall we say information? – will be mostly used by police managers to better plan police operations, as it allegedly allows for accurate deployments considering the identified patterns and forecasted trends. This last goal seems to be, nowadays, a major issue given the financial constraints police forces are facing. Furthermore, the increased scrutiny by the citizens raises the question of whether they are willing to pay for the police service, and for which kind of police service. And here, we have to agree with Weisburd and Neyroud (2011) when they state that 'what is most striking about policing is that we know little about what works, in what contexts, and at what cost' (p.11).

The way the outliers are(n't) treated

A major concern in predictive policing relates to how and by whom the data is collected and registered, which data is relevant for analysis, and how it will be transformed in knowledge. Perry et al. (2013) have presented some myths of predictive policing, being one of them the belief that the computer will do all the work. However, as they say,

'even with the most complete software suites, humans must find the relevant data, process these data for analysis, design and conduct analyses in response to ever-changing crime characteristics, review and interpret analysis findings (and exclude erroneous findings), recommend interventions, and take action to exploit the findings and assess the impact of interventions.' (Perry et al., 2013: p.XIX)

So, though we are moving back again to the faith in numbers and measurements as it happened in the 19th century with the development of statistics, let's not forget that information *is not* knowledge, as it is 'indifferent' to meaning and does not consider the people's 'intentional states', in the words of Jerome Bruner (1990). So, it seems the individual is lost in the mechanics of discovering patterns. Actually, 'we seem increasingly indifferent to individual cases and small numbers' (Alschuler, 1991: pp.904-905), favouring a nomothetic approach instead of an idiographic one. As Brodeur and Dupont (2008: p.22) state, 'there is a crucial difference between information, disinformation, and trusted intelligence (knowledge) in the field of HUMINT [human intelligence], with the central concern being the question of validity'.

But, even in statistics the outlier is important because it disturbs the normal distribution of data. And that is precisely what we are looking for: the extreme cases, or the cases that pop-up from the population. Indeed, it takes only one to disrupt society...

Today, this is a major concern for the police forces: the lone terrorist, the one single person who puts all of us in a permanent state of alert and for whom we demand an immediate response. And, as far as we know, there is some evidence that predictive policing doesn't work in this specific context, because of the 'mistakes due to a randomness bias' (Brodeur & Dupont, 2008: p.22) that can result in the identification of too many 'false positives' (Brodeur & Dupont, 2008; Munk, 2017). Actually, together with the given unreliability of 'public and private databases (...) the emphasis placed on decontextualized relational features produces 'false positives' and leads to the identification of innocents as terrorists' (Brodeur & Dupont, 2008: p.25).

Predictive policing does not capture the particularities of the individual, or a specific set of behaviours, or the different sorts of relationships established with other people while assuming different roles when moving through the different social scenarios. It can be said that the police is mainly concerned with maintaining social peace and order, not exactly with the specific offender. But, if this is it, other policing models will also have to be thought over.

This being said, it seems the major topic is the supposedly successful police-control metrics instead of evaluating the police activities in terms of the citizens' well-being. In other words, it fails to comprehend the background of the phenomena the police forces have to deal with. New forms of criminality, social disruption, individual or group behavioural disorders, must be tackled by being educated about its roots, developmental history, more or less visible relationships with other social actors and within institutions, and assuming the far-reaching effects that each individual's actions have, backed – or captured? – by the communication technologies. In fact, 'the determinist speculations at the core of data-mining algorithms fail to account for life's coincidences, which are not governed by the laws of causality' (Brodeur & Dupont, 2008: pp.25-26).

Conclusion (?)

The 'network society' (Castells, 2010) confronts us with immense and immediate information. As a consequence, we feel free to ask for urgent responses to old and new problems and this requires a systematic vigilance of all people by all people. These are the characteristics of the 'risk society' (Beck, 1992). Also, people travel more and more, for business or holidays… or to commit crimes. The changes in demography and labour market result in changes in labour relations and the position people occupy in the social structure. Police forces are no longer confronted with just the natives but also with the foreigners. Thus, what derives from the political and economic management of this reconfigured society is something new the police forces have to deal with. Clearly, the police forces have to rethink and redesign their methods, be aware of the scientific and technological developments and, most of all, be adaptable to differences according to the spaces and times people occupy in their lives.

As discussed, the use of statistics is not new and, even more so, it seems that real people are left behind. Let's be wise not to be absorbed by and transformed in numbers.

References

- Alschuler, A. W. (1991) The failure of sentencing guidelines: A plea for less aggregation. *University of Chicago Law Review*. 58, 901-951.
- Ancel, M. (1985) Reforme pénale et politique criminelle dans les dernières années du XXe siècle. *Mélanges Offerts à Robert Legros*. Bruxelles, Editions de l'Université de Bruxelles, pp.1-11.
- Ancel, M. (1987) De l'individualisation de la peine a la dépénalisation: Un courant moderne de politique criminelle. Separata do *Boletim da Faculdade de Direito de Coimbra*, 1-14.
- Beck, U. (1992) *Risk Society: Towards a New Modernity*. London, Sage.
- Bentham, J. (1781/2000) *Introduction to the Principles of Morals and Legislation*. Kitchener: Batoche Books. Available from: https://socialsciences.mcmaster.ca/econ/ugcm/3ll3/bentham/morals.pdf [Accessed 25th November 2017].
- Bentham, J. (1840) *Théorie des Peines et des R*écompenses (rédigée en français d'après les manuscrits de Bentham de 1775 par Étienne Dumont, et publiée pour la première fois à Londres en 1811). Bruxelles, Société Belge de Librairie.
- Brodeur, J.-P. & Dupont, B. (2008) Introduction essay: The role of knowledge and networks in policing. In: Williamson, T. (ed.), *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions*. Chichester, UK, John Wiley & Sons, pp.9-33.
- Bruner, J. (1990) *Acts of Meaning*. Cambridge, MA, Harvard University Press.
- Brunon-Ernst, A. (2007) *Le Panoptique des Pauvres: Bentham et la Réforme de l'Assistance en Angleterre*. Paris, Presses Sorbonne Nouvelle.
- Castells, M. (2010) *The Information Age: Economy, Society, and Culture – Volume 1. The Rise of the Network Society*.2nd ed. Chichester, UK, Wiley-Blackwell.
- Cohen, S. (1995) *Visions of Social Control: Crime, Punishment and Classification* (repr.). Cambridge, UK, Polity Press.
- Di Argentine, A. B. (1991) L'influence de l'œuvre de Marc Ancel sur le mouvement de défense sociale. *Revue de Science Criminelle et de Droit Pénal Comparé*. 1, 25-28.
- Drucker, P. F. (1995) *Managing in a Time of Great Change*. New York, Truman Talley Books / Dutton.
- Engel, R. S. & Whalen, J. L. (2010) Police-academic partnerships: Ending the dialogue of the deaf, the Cincinnati experience. *Police Practice and Research*. 11 (2), 105-116. doi:10.1080/15614261003590803
- Ericson, R. V. & Haggerty, K. D. (1997) *Policing the Risk Society*. Oxford, UK, Clarendon Press.
- Feeley, M. M. & Simon, J. (2000) The new penology. In: Muncie, J., McLaughlin, E. & Langan, M. (eds.), *Criminological Perspectives: A Reader* (5th repr.). London, Sage in association with The Open University, pp.367-379.
- Foucault, M. (1995) *Discipline and Punish: The Birth of the Prison*. 2nd ed. New York, Vintage Books.
- Foucault, M. (2007) Security, territory, population. In: Davidson, A. I. (ed.), *Lectures at the Collège de France, 1977-78*. London, UK, Palgrave-Macmillan.
- Haberman, C. P. & Ratcliffe, J. H. (2012) The predictive policing challenges of near repeat armed street robberies. *Policing: A Journal of Police and Practice*. 6 (2), 151-166. doi:10.1093/police/pas012
- Harcourt, B. E. (2007) *Against Prediction: Profiling, Policing, and Punishment in an Actuarial Age*. Chicago, IL, The University of Chicago Press.
- Hollin, C. R. & Palmer, E. J. (eds.) (2006) *Offending Behavioural Programmes: Development, Application, and Controversies*. Chichester, UK, John Wiley & Sons.
- Jaschke, H.-G., Bjørgo, T., Romero, F. B., Kwanten, C., Mawby, R. & Pagon, M. (2007) *Perspectives of Police Science in Europe: Final Report*. Bramshill, UK, CEPOL European Police College.
- Kuhn, T. S. (1970) The structure of scientific revolutions (2nd ed. enlarged). In: Neurath, O., Carnap, R. & Morris, C. (eds.), *International Encyclopedia of Unified Sciences* (Vol. 2, nº 2). Chicago, IL, The University of Chicago Press.
- L'Heuillet, H. (2001) *Basse Politique, Haute Police: Un Approche Historique et Philosophique de la Police*. Paris, Fayard.
- Loader, I. (1999) Consumer culture and the commodification of policing and security. *Sociology*. 33 (2), 373-392.
- Martinson, R. (1974) What works? Questions and answers about prison reform. *The Public Interest*. 35, 22-54.

- Munk, T. B. (2017) 100,000 false positives for every real terrorist: Why anti-terror algorithms don't work. *First Monday: Peer-Reviewed Journal on the Internet*. 22 (9).
  Available from: http://firstmonday.org/ojs/index.php/fm/article/view/7126/6522 [Accessed 26th November 2017].
- Ost, F. (2001) *O Tempo do Direito* [The time of law]. Lisbon, Instituto Piaget.
- Pearsall, B. (2010) Predictive policing: The future of law enforcement? *National Institute of Justice Journal*. 266, 16-19.
- Perry, W. L., McInnis, B., Price, C. C., Smith, S. C. & Hollywood, J. S. (2013) *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA, RAND Corporation.
- Smith, L. D., Best, L. A., Cylke, V. A. & Stubbs, D. A. (2000) Psychology without p values: Data analysis at the turn of the 19th century. *American Psychologist*. 55 (2), 260-263.
- Tsitsoura, A. (1990) La politique criminelle de la fin du XIXe siècle à la fin du XXe siècle. In: van der Vorst, P. & Mary, P. (Dirs.), *Cent Ans de Criminologie à l'U.B.L.: Adolphe Prins, l'Union Internationale de Droit Pénal, le Cercle Universitaire pour les Etudes Criminologiques*. Bruxelles, Bruylant, pp.107-123.
- Weisburd, D. & Neyroud, P. (2011) Police science: Toward a new paradigm. In: *New Perspectives in Policing*. Washington, DC, National Institute of Justice.
- Welten, B. (2010) A brave police force deserves courageous scientists (after-dinner address at CEPOL Police Research and Science Conference 2009). *European Police Science and Research Bulletin*. 3, 12-15.

Technopoly and Policing Practice: Critical reflections on innovations in police control technology

James Sheptycki
Department of Social Science, York University, Toronto, Canada

Abstract
The paper defines Technopoly as 'totalitarian technocracy' in which all forms of social, cultural and economic life are brought under the aegis of technological governance. Policing here is understood in terms of a transnational assemblage of institutions and police practice is marked by two defining features: the capacity to undertake surveillance and use-of-force in the service of governance. This paper looks at innovations in policing technology, regarding them as symptoms of broader historical shifts in global culture, society and politics. The essay points to worrying questions concerning the democratic basis of techno-policing. The discussion emphasizes the continuing need to normatively ground policing practice in concerns about social justice.

Keywords: Predictive Policing; surveillance; use-of-force; police militarization; social justice

Introduction

Although it is difficult to agree on what to call the period we are living through, it seems inescapable that it is one of revolutionary social transformation. Perhaps it is due to the revolutionary nature of our contemporary times that we cannot agree how to label them. The 'global networked society' and the onset of 'liquid modernity' represent two powerful ways of conceptualizing the depth of change that emphasize the cultural consequences of the shifting morphology of the state and capitalist relations in a transnational world (Bauman, 2000; Castells, 2011; Sennett, 2006; Sklair, 2000). The bewildering uncertainty of the age raises unavoidable questions for would-be democratic police policy-makers (Brodeur, 2010; Ericson, 2007; Manning, 2010). Democratic policing is more paradoxical than authoritarian policing because it seeks to maintain the conditions of democracy with non-democratic means (Mazower, 1997). Authoritarian policing imposes authority on the basis that authority is there to be imposed (Bloom, 2016). Assuming that the rapid pace of technological innovation and change that is on-going within policing organizations across Europe and around the world does not, however inadvertently, lead towards authoritarian ends requires a fundamental commitment to social justice (Goldsmith & Sheptycki, 2007; Wood & Dupont, 2006).

These ideas have been repeatedly expressed by David Bayley over many years – in sum: that police professionalism, absent democratic roots, will not achieve lasting social justice no matter how efficient and effective the technologies of security-control appear to be (Bayley, 1990; Bayley, 2006; Bayley and Stenning, 2016). All too often police technical success undermines the dem-

ocratic legitimacy of the police. Social philosophers attempt to provide highly nuanced explanations concerning the pernicious effects of the 'securitization of society' (eg. Schuilenburg, 2015). However, as Peter K. Manning has observed, work of this kind does not translate well into policing policy (Manning, 2010: 107). Yet the danger is that, left unchecked, un-examined and un-criticized, the technological revolution that is underway in the global networked society poses serious challenges to democracy and democratic policing. Many anxiously perceive a drift towards authoritarian control in emergent techno-policing. How best to steer democratic policing in another direction?

These complex issues and choices are greatly simplified by looking at innovations in police technology through the lens of Neil Postman's prescient 1992 book *Technopoly; the surrender of culture to technology* (Postman, 1992). Postman argued the purveyors of technical innovation have been deified. In his words, our culture "seeks its authorization in technology, finds its satisfactions in technology and takes its orders from technology" (p. 71-72). It suffers from a surplus of information generated by that very technology which, in turn and paradoxically, requires new technological tools in order to cope. Technological fascination has become the source of direction and purpose for society and the individuals that comprise it. Extrapolating Postman's view, the information technologies that we play and work with every day – our smartphones and tablets – are the nearly perfect basis for technological totalitarianism.

Computerized information processing establishes sovereignty over all areas of human experience because technology 'thinks' better, faster and more exactly than humans can. It follows that some people have a 'knowledge monopoly' in these domains, and the great gurus of Technopoly – Bill Gates, Mark Zuckerberg, Elon Musk, and the rest of them – have arguably been granted undeserved prestige, authority, and influence over human affairs. In Postman's vision, the Masters of Technopoly "elevate information to a metaphysical status". The belief that machine-thinking is superior to lax, ambiguous and complex human thinking and judgment has much in common with the principles of scientific management espoused by Fredrick Taylor in an earlier times and all of this has direct implications for policing (Sheptycki, 2017a; 2017b). The values of efficiency, precision and objectivity are encoded into machine-thinking. The value of social justice is not.

The emergence of predictive analytics and a whole range of other innovations in law enforcement should be understood in this broader context. We need to think more critically about the technological transformations that are occurring. It is generally agreed that, in our present period, technological change has come at a faster pace than at any time in recorded history and we are all strongly encouraged to welcome the opportunities to innovate. But technological transformation has a price that is not borne equally across society. Not everybody benefits and some benefit more than others. Police control technology is central to a growing discomfort that police efficiency metrics disguise.

Innovations in policing - an example and some considerations

The new technologies of security-control get between the police and the public. This is not properly recognized. Contemporary security control is mediated by a host of technological wonders: Big Data, predictive analytics, and a myriad of surveillance technologies can be cited here. Purveyors of the new technologies of social control seductively promise an elevated ability to achieve social order through more effective law enforcement (Sanders & Sheptycki, 2017). With that view, the problem becomes one of ensuring that police leadership can successfully implement technological innovations, following which presumably the functional aim of enforcing social order is supposedly assuredly achieved. Let's consider that critically.

Since its inception in the late 19th and early 20th century, professional policing has been at the cutting edge of technological change. Historically, the adoption of new communications technologies especially has affected the organization of policing. Most people in the police profession (and certainly the academics who study them) are aware that in the early-20th century urban police used centralized police 'call box systems' to coordinate walking police patrol. This eventually gave away to sectorial and functional differentiation within police organizations with the advent of two-way mobile radio systems. During the mid to late 20th century, virtually all urban police agencies were heavily dependent on mobile radio communications and telephones with fixed landlines to coordinate field operations. By the end of the century, with the invention of mobile telephones and mobile data terminals, police organization was again transformed by the possibility

of direct point-to-point communication. There can be little doubt that for the last century, police organization has been in a more-or-less permanent state of technological revolution (Dupont, 2001; Manning, 2001; Nogala, 1995; Sheptycki, 2013).

The move to radio-dispatched police patrol cars in the middle years of the 20th century changed the organizational practice of policing in fundamental ways, but not all were necessarily positive. Here it is instructive to take note of Mollie Weatheritt's long ago told 'cautionary tale' about the unintended consequences of innovations in policing (Weatheritt, 1986). As she told the story, in the late 1950s traditional policing in the British Isles was largely achieved through a broadly dispersed system of police patrol supervised through a myriad number of highly localized constabularies. In larger centers this was supplemented by a 'fixed point' system of police call-boxes which allowed police agencies in larger geographical locales to provide some level of supervision and communication to officers working their beats.

Weatheritt documented a number of police 'experiments' productive of a consensus that radio-dispatched car patrol was more efficient and effective than the previous model, but in so doing she argued that these demonstration projects were not true experiments. Rather, they were 'foregone conclusion research' designed to arrive at the results that everybody wanted, which in this case was to demonstrate the speed and efficiency of radio-dispatched patrol cars. Years later, Weatheritt observed, it was subsequently realized that putting police in cars created a barrier between police and public. Simplifying for the sake of brevity, when police patrolled their beats on foot, there were a variety of opportunities for 'non-adversarial contact' between police and public, but by putting police officers in cars, mobilized for fast response to radio calls, these opportunities for non-adversarial contact diminished and what remained were the more complex, conflictual and often adversarial kinds of police-citizen interaction. At the time, nobody envisaged that putting police in cars would decrease the number of non-adversarial contacts in proportion to other kinds of police-citizen interaction and, in the process, change the cultural expectations of both police and citizens eventually contributing to the erosion of police legitimacy. But that is what happened.

This cautionary tale was expounded in the mid-1980s, when academic research on policing was beginning to seriously develop. Many of those involved at the time took the cue to embark on research concerning the effectiveness of police foot patrol and other tactical innovations, and the 'community policing' and 'problem-oriented' paradigms blossomed as police professionals and professional police researchers sought to develop and refine democratically appropriate approaches to policing innovation (Brodeur, 1998). Today the field is dominated by so-called evidence-based police research and policy, but this viewpoint largely fails to comprehend the social and political background against which police experimentation and innovation occurs. Police research of this kind creates the appearance of success using police-control metrics rather than subjecting policing activity to critical evaluation in terms of social well-being (Manning, 2010, pp. 101-106). Institutionally speaking, the police manager is subject to pressures of many kinds and often struggles to achieve diametrically opposed expectations. It is no small wonder that they are indisposed to research that might attract criticism. It is safer to police by numbers and targets. Given the constraints, the research that gets done is usually achievement-oriented and, while the problems measured are subsequently seen to be solved, the symptoms those problems express continue and may even become worse (Bowling, 2011).

At a general level, Weatheritt's cautionary tale reminds us that modern and technologically innovative changes in policing need to be gauged against normative criteria and not simply in terms of efficiency gains defined by the police organization. The distinction between adversarial and non-adversarial contact between police, and the ratio between them, presents a metric of a different kind which signals something about the *quality* of police-community relations. In general, that shifting quality has to do with an often ill-recognized yet fundamental paradox of democratic policing; that it aims to serve and to maintain the civil conditions conducive to democracy by recourse to non-democratic means. Management by numbers does not usually recognize this paradox and the degree of any consequent failure of democratic police legitimacy can be reliably gauged by the number and intensity of public accusations regarding police institutional hypocrisy.

Techno-policing in the 21st Century

'Predictive analytics' has become the new magic wand of technological policing. That is to say, 'predictive policing' is another one of those technological innovations that seems to be a foregone conclusion. It promises something short of total information awareness. It promises to orchestrate policing on the basis of superior knowledge of the situation. It promises to be cost effective. Sometime in the not-too-distant future, public policing will be more fully automated, focused through the technological wizardry of mass surveillance, co-ordinated by centralized command-and-control systems and more demonstrably efficient than ever (Caplan, et al, 2011; McCue, 2014; Perry et al, 2013). This model is being heavily promoted and not only because of its presumed benefits in terms of increased social control, but also especially because of costs savings. According to *The Police Chief*, a magazine for law enforcement managers in the United States:

> *'The strategic foundation for predictive policing is clear enough. A smaller, more agile force can effectively counter larger numbers by leveraging intelligence, including the element of surprise. A force that uses intelligence to guide information-based operations can penetrate an adversary's decision cycle and change outcomes, even in the face of a larger opposing force. This strategy underscores the idea that more is not necessarily better, a concept increasingly important today with growing budget pressures and limited resources' (Beck & McCue, 2009).*

Note the militaristic language. Police departments across North America are increasingly adopting the organizational principles of 'real time intelligence operations' co-ordinated through centralized fusion hubs. These organizational principles, and all of the technology that goes with it, have been transplanted directly from the US military (Harwood & Stanley, 2016). That all of it can be bought, while saving the tax-payer's money, seems a good bargain on its own terms. But again, what of social justice? The claim that "reality is wholly knowable, that knowledge necessarily liberates, and that absolute knowledge liberates absolutely" is as dubious as it is hubristic (Berlin, 1969, p. 80). Predictive policing is one of a plethora of Technopoly products being sold on the basis that police knowledge systems – based on stochastic calculation and dubious data – produce superior knowledge which can be strategically translated into operationally effective actions, like 'crackdowns' (Sherman, 1990; Koper & Mayo-Wilson, 2006). But only because the enforcement perspective is increasingly that of an occupying army trying to control 'hostiles' in 'hostile territory' and because the metrics used to evaluate success are based on those assumptions (Fassin, 2011). Increasingly in the democratic countries of the West, technologically enhanced policing does not look like or feel like policing by consent of the governed and it seems very far away from concerns about social justice.[1]

One way to illustrate this point further is to shift attention away from the magic of contemporary police surveillance and communications technology and consider another manifestation of the police technopoly-mindset. Policing is not only about surveillance since it can also involve use-of-force, that is why the increasing surveillance power of police is so contentious, because it is connected to physically coercive means. No other issue in policing is more inflammatory than police use-of-force which – in the United States especially – is frequently increasingly thought of in terms of 'police brutality'. The technological solutions found in police use-of-force training are interesting and revealing. For example, there is the Shockknife an innovative, patented and trademarked device for police edged-weapons training.[2] Quoting from the company website, the Shocknife is the "only training knife in the world that is capable of inducing FEAR" (Note that the word 'fear' is in all-capital letters). The logic is that police need to train in order to cope safely with people who are holding knives or other edged weapons. Evidently, the old-fashioned way of undertaking such training using rubber knives is insufficient because it is not 'realistic' enough. According to the webpage, the Shocknife will "revolutionize the edged weapon training industry with the only training knife that induces the necessary stress required for realistic edged weapon training." To quote further, "Shocknife is designed to improve tactical knife defense training in law enforcement, military and corrections markets around the world."

1 I am aware that the terminology of 'policing by consent' is not in use everywhere around the world. I am also aware that it is very difficult to define what we mean by democratic policing. The extent to which the general public understands and endorses what police do, one can speak about policing by consent. Indeed, it strikes me as the very opposite of democratic policing when an uncomprehending public experiences a police presence that they do not endorse. Lack of consent is an indicator of un-democratic policing.

2 http://www.shocknife.com/about.php - last accessed Feb. 17, 2018

The only reason this even makes sense in the context of policing is because, especially in the United States, people have been encouraged to think of it in terms of the 'war on crime' and the 'war on drugs' (Kraska, 2001; Parenti, 2003). If its war out there, then the training should be stressful, painful and hurtful. How else will the troops get desensitized? This is a new piece of equipment found increasingly in police training academies across North America and it needs to be read as another symptom of something very wrong with the way technological innovations are being used to shape policing transformation.

The emerging techno-policing of the 21st century looks to bring together 'ambient surveillance' (Stalcup & Hahn, 2016) backed up by police agents holding coercive means, all coordinated by centralized command-and-control systems, and it aims to be more demonstrably economic, efficient and effective than ever. It will mark another intensification of the wars on crime of the past, and the uncertainty and anxiety it provokes will further fuel the mistaken belief that "that more will work where less has not" (Ericson, 2007, p. 12). Technopoly thinking in policing is currently, and very evidently, antithetical to the democratic ideals captured in the terminology of community and problem oriented policing that were *de rigueur* in professional policing circles not so very long ago. Need it be?

Conclusion

This short essay began by observing that contemporary innovations and transformations in policing and its organization are manifestations of broader historical shifts in global culture, society and politics. These complex transformations coincide with technological changes which police policy-makers at every level of governance have historically taken enthusiastic part in. Police leaders are Technopolists *par excellence*. This paper began by defining Technopoloy as 'totalitarian technocracy' in which all forms of social, cultural and economic life are brought under the aegis of technological governance. Policing has become a transnational assemblage of governance institutions that are difficult to empirically map (Bowling & Sheptycki, 2012). Certainly all are marked in one way or another by the two defining features of police practice: the capacity to undertake surveillance and the use-of-force. If the words 'totalitarian technocracy' are passed off as a mere provocation, the expressed centrality and importance of social justice in policing is being denied.

The drift towards militaristic and authoritarian style policing in the liberal democratic countries of the West has almost the feel of a forgone conclusion. The Technopolists of law enforcement are coming closer to achieving, not without challenge, a monopoly on authoritative knowledge about the science of social ordering (Hope, 2009). In matters concerning peace, order and good governance, techno-policing does not possess the only relevant scale of value. The 'human security' that 'policing with intelligence' seeks to provide can, for example, be judged in terms of 'freedom from fear and from want' (Sheptycki, 2008). Prior to the arrival of the millennium, Neil Postman presciently observed a much wider phenomenon of ongoing and breakneck technological transformation of culture. Much like the French Revolution, say, or the Industrial Revolution, our current historical period has the feeling of a natural cataclysm which affects everyone whether they welcome it or not. From the point of view of the individual history does seem 'inevitable' in that we are all born into a stream of change which carries us along. Between a past that none can alter and an uncertain future there is the present fleeting moment in which one is free to act in ways that may affect future history. We might not be able to precisely steer that trajectory, but we can try to nudge it in the right direction. The task is difficult and sometimes it feels to me like trying to change the drift of an iceberg by pushing it with a toothpick.

References

- Bauman, Zygmunt (2000) *Liquid Modernity*, Wiley-Blackwell.
- Bayley, David (1990) *Patterns of Policing*, New Jersey: Rutgers University Press.
- Bayley, David (2006) *Changing the guard: Developing democratic police abroad*. New York, NY: Oxford University Press.
- Bayley, David H. & Stenning, Philip C. (2016) *Governing the Police: Experience in Six Democracies* New Brunswick: Transaction.
- Beck, C. & McCue, C. (2009) 'Predictive Policing: What can we learn from Wal-Mart and Amazon about fighting crime in a recession?' *The Police Chief,* Vol. 10 No. 10, 18-24.
- Berlin, I. (1969) *Four Essays on Liberty*, Oxford University Press
- Bloom, Peter (2016) *Authoritarian Capitalism in the Age of Globalization*, Cheltenham, UK: Edward Elgar.
- Bowling, B. (2011) 'Transnational Criminology and the Globalization of Harm Production'. In: *What is Criminology?* M. Bosworth and C. Hoyle (eds.) Oxford University Press;
  DOI: http://dx.doi.org/10.1093/acprof:oso/9780199571826.003.0025
- Bowling, B. & Sheptycki, J. (2012) *Global Policing*, London: Sage
- Brodeur, J.-P. (1998) *How to Recognize Good Policing*, London: Sage
- Brodeur, J.-P. (2010) *The Policing Web*, Oxford: Oxford University Press
- Caplan, J. M., Kennedy, L. M. & Miller, J. (2011) Risk Terrain Modeling: Brokering Criminological Theory and GIS methods for Crime Forecasting, *Justice Quarterly*, Vol. 28 No. 2, 360-381.
- Castells, M. (2011) *The Rise of the Network Society*, Oxford: John Willey and Son.
- Dupont, B. (2001) 'Policing in the information age: Technological errors of the past in perspective'. In: *Policing the Lucky Country*, Enders, M. & Dupont, B. (eds.) Annadale NSW: Hawkins Press, 34-48.
- Ericson, R.V. (2007*) Crime in an Insecure World,* Cambridge: Polity Press.
- Fassin, D. (2011) *Enforcing Order - an ethnography of urban policing*, Cambridge: Polity Press.
- Goldsmith, A. & Sheptycki, J. (2007) *Crafting Transnational Policing*, Oxford: Hart.
- Harwood, M. & Stanley, J. (2016) 'American Military Technology has come home – to Your Local Police Force', *The Nation*, May 19, 2016
  Available at https://www.thenation.com/article/american-military-technology-has-come-home-to-your-local-police-force/
- Hope, T. (2009) 'The Illusion of Control; a response to Professor Sherman' *Criminology and Criminal Justice*, Vol. 9 No. 2, 125-134.
- Kopper, C.S. & Mayo-Wilson, E. (2006) 'Police crackdowns on illegal gun-carrying; a systemic review of their impact on gun crime' *Journal of Experimental Criminology*, Vol. 2 No. 2, 227-261.
- Kraska, P. B. (ed.) (2001) *Militarizing the American Criminal Justice System; the changing roles of the armed forces and the police*, Boston: Northeastern University Press.
- Manning, P.K. (2001) 'Technology's Ways; Information technology, crime analysis and the rationalizing of policing', *Criminal Justice,* Vol. 1 (1), 83-103.
- Manning, P.K. (2010) *Democratic Policing in a Changing World*, London: Routledge.
- Mazower, M. (1997) *The Policing of Politics in the Twentieth Century*, Berghahn Books.
- McCue, M. (2014) *Data Mining and Predictive Analysis; Intelligence Gathering and Crime Analysis* (2nd ed.), Amsterdam: Elsevier.
- Nogala, D. (1995) 'The Future Role of Technology in the Police' in *Comparisons in Policing; An International Perspective*; J-P. Brodeur (ed.) Aldershot: Avebury, 191-210.
- Parenti, C. (2003) *The Soft Cage; Surveillance in America from Slavery to the War on Terror*, New York: Basic Books.
- Perry, W.J., McInnis, B., Price, C.C. Smith, Susan C., & Hollywood, J.S. (2013) *Predictive Policing; the Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica CA: RAND Corp.
- Postman, N. (1992) *Technopoly - the surrender of culture to technology,* New York: Vintage Books.
- Reiner, R. (2010) *The Politics of the Police* (4th ed.) Oxford: Oxford University Press.

- Sanders, Carrie B. & Sheptycki, James (2017) 'Policing, crime, and 'big data'; towards a critique of the moral economy of stochastic governance' *Crime, Law and Social Change*, Vol. 68 No. 1-2, 1-15. https://doi.org/10.1007/s10611-016-9678-7
- Schuilenburg. M. (2015) *The Securitization of Society*, New York: New York University Press.
- Sennett, R. (2006) *The Culture of the New Capitalism*, Princeton NJ: Yale University Press.
- Sheptycki, J. (2007) 'High Policing in the Security Control Society', *Policing* Vol. 1 No. 1, 70-79. https://doi.org/10.1093/police/pam005
- Sheptycki, J. (2008) 'Policing, Intelligence Theory and the new Human Security Paradigm'. In: *Intelligence Theory; Key Questions and Debates*, P. Gill, S. Marrin & M. Phythian (eds.) London: Routledge,166-187.
- Sheptycki, J. (2013) 'Technocrime, criminology and Marshall McLuhan; towards an inventory of criminological effects'. In: Technocrime, Policing and Surveillance, S. Leman-Langlois (ed.) (2013) London: Routledge, 133-150.
- Sheptycki, J. (2017a) 'Liquid Modernity and the Police Métier'. *Global Crime*, Vol. 18 No. 3, 1–17. doi:10.1080/17440572.2017.1313734
- Sheptycki, J. (2017b) 'The Police Intelligence Division-of-Labour'. *Policing and Society*, Vol. 27 No. 6, 620-635. https://doi.org/10.1080/10439463.2017.1342645
- Sherman, L. W. (1990) 'Police Crackdowns: Initial and Residual Deterrence'. *Crime and Justice* Vol. 12, 1-48.
- Sklair, L. (2000) *The Transnational Capitalist Class*, Wiley-Blackwell.
- Stalcup, M. & Hahn, C. (2016) 'Cops, cameras and the policing of ethics'. *Theoretical Criminology*, vol. 20 no. 4, 482-501.
- Weatheritt, M. (1986) *Innovations in policing*, London: Police Foundation/Croom Helm 1986.
- Wood, J. & Dupont, B. (2010) *Democracy, Society and the Governance of Security*, Cambridge: Cambridge university Press.

H2020
Research Projects

RAMSES: Internet Forensic Platform for Tracking the Money Flow of Financially-Motivated Malware and Ransomware

Holger Nitsch
University of Applied Sciences for Public Service in Bavaria, Germany

Julio Hernandez-Castro
Edward Cartwright
Anna Stepanova
Darren Hurley-Smith
University of Kent, United Kingdom

Abstract
This paper provides a discussion on the objectives, approach and findings of the European Union's Horizon 2020 research and innovation programme under grant agreement No 700326 funded RAMSES project. As the rise of the use of the Internet is followed by the rise of criminal activity on the Internet, new tools are needed for Law Enforcement Agencies to fight the crime and to collect forensic evidence. The use of ransomware and financially orientated malware is growing very fast and criminals are very innovative in creating new ways to harm citizens and companies. Within this project eleven partners from all over Europe are creating the project jointly and find solutions for the different practitioners involved in the project. This project will provide LEAs with new tools and also covers the dark and deep web. Several tools and functionalities are described such as creating a platform that can e.g. analyse malware payment and hidden files, which can be found and analysed via the platform, to create forensic evidence. The platform will have also a dashboard with different functionalities that will help LEAs in their daily work to fight cybercrime. And also the importance of game theoretic models applying to the determination of the probability and efficacy of malware being used for profit is elaborated. This shows the value of the analysis of malware by different means to help LEAs in the decision making process, which malware might be more distributed and "successful" than others.

Keywords: Ransomware, malware, banking trojans, game theory, cybercrime

Introduction

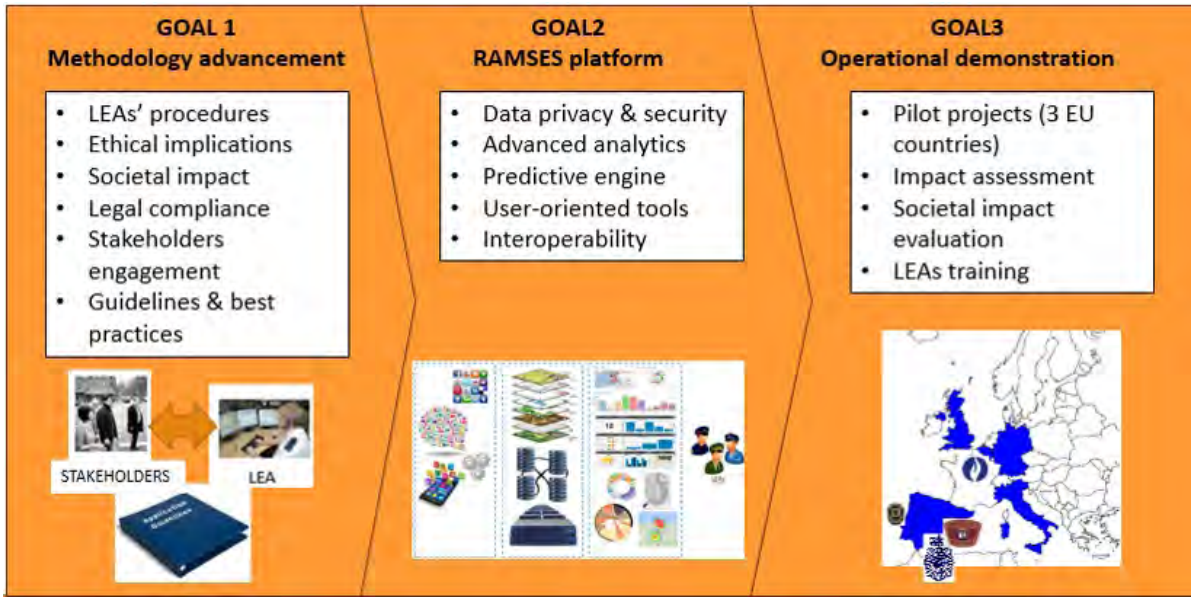
In the recent years the internet has become the key medium of communication and business activities. As business through the internet is growing also criminal activity grows. The exchange of criminal information started in forums like 4chan and has now developed into a wide variety of surface and dark web pages. The 2017 report of NTT Security from Switzerland finds that 77 % of all ransomware concerns four several sectors: administration, retail, business and professional services and health service. Three quarters of there were fish-

ing attacks and 66% of all attacks were coming from the United States. (NTT Services, 2017) The importance of Cybersecurity and information security is constantly rising. The 2016 report of Kaspersky lists a high amount of malware and related incidents. 39% of all internet users were 2016 at least once victims of a cyberattack and 77.26% attacks happened through a malicious URL (Kaspersky, 2018).

The strong rise of internet use has been followed by a stronger use of the internet for criminal activity. For some crimes it is seen by criminals as the perfect tool, because it is easier not to be in direct contact with the victim and to hide their own identity. As the above numbers prove that the numbers are rising, and some see it as a business model to sell their IT knowledge and services to less skilled criminals. So, the investment for criminal activity could be lower than before. According to the Internet Organised Crime Threat Assessment by Europol (iOCTA) (2014) the generated value of the Crime as a Service is around 300 billion dollars.

The Horizon 2020 funded EU project RAMSES to tackle the problem and support Law Enforcement Agencies (LEA) across Europe to resolve problems faster and have court relevant evidence. The RAMSES project (ramses2020.eu) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700326. It aims to design and develop a holistic and intelligent platform for LEAs for facilitate forensic investigations. The system will extract, analyze, link and interpret information extracted from the internet related with financially-motivated malware. That includes the surface web, deep web and the dark web. The RAMSES project focusses on two use cases: ransomware and banking trojans.
Another aim is to demonstrate the impact of the project through several pilots in several stages. At the end, there will be effective guidelines and collaborating methodologies developed. The following diagram shows the main goals of this project:

Diagram 1 – The main goals of RAMES 2017 project



Besides LEAs, other stakeholders like customers, developers and malware victims will be included in the process to get all possible participants throughout Europe involved. This will lead to a better understanding of the problem and the criminal activities and phenomenon. Big Data technologies must be used to extract, store and search for criminal online behaviour to handle the vast amount of structured and unstructured data.

The RAMSES Platform

The platform will include several modules for LEAs to fight malware and to gain court relevant evidence. One of the main problems is to find and extract the relevant data from the internet. The platform will be able to automatically extract this data related to malware from the surface web. This includes also social networks like

Facebook, Twitter and forums. Other challenges are the Deep Web and the Dark net due to the nature of both guaranteeing at least some degree of anonymity and obfuscation of information.The RAMSES platform will also incorporate these elements into the data mining pool and gain relevant information as forensic evidence by doing so.

Further, the platform will be able to analyse malware related payments. This is an important module to judge the importance of the detected malware, as described below in the economic modelling the likeliness of a successful ransomware that might be used more often than others.

Ransomware is often hidden in images, videos and audio files. The platform is able to detect the manipulation of these and perform steganalysis. By doing so LEAs will have the evidence that image, video or audio files were manipulated, and information was hidden, even if the contents of such messages remain unknown. Correlating image manipulation with lines of communication is a potentially powerful way of making items of evidence mutually supporting contributions to prosecution.

In another module malware samples will be extracted and analysed to gain a better understanding of the nature of malware and common trends. This will help also with the prevention of future threats to citizens and to create countermeasures for LEAs and stakeholder against this type of crime.

The results of the different analyses can be visualised in the next module to identify different trends and threats to the citizens or business sectors.

The information feeding the platform comes from a variety of sources. On the one hand, LEAs can input their data to see also their local or nationwide specialities. During the lifetime of the project this will come mainly from the project partners: The University of the Bavarian Police, Belgium Federal Police in Belgium, Policia Judiciara in Portugal and the Spanish National Police. Further information is gained from the common sources of the surface web mentioned above. For the Deep Web and the Dark net sources among others will be TOR, reddit, Pastebin, Zmap and SHODAN, which is a search engine, that is not like Google and others looking for text, but is looking for vulnerable devices (Akhgar; Yates, 2013: 243). Blockchain is another source.

Also, existing knowledge of malware analysis, steganography and multimedia forensics will be fed into the system by the academic partners, specialised on the topic.

There are certain main functionalities. After the processing of a large amount of data the user is able to search for an IP address, a nickname, a certain technology, a name of a Remote Access Trojan (RAT) or any keyword interesting for the investigator. Through to an interactive dashboard the user is able to visualize the different process of malware clustering and forensics. There is also a machine learning process included, so that the more often this functionality is used the more precise the results are according to the needs of the user.

Furthermore, an exploration function will be integrated. Using that will help to explore the relationship between different entities. This can be IP addresses, the name of a malware domains or others. By feeding the platform with information it will show important events concerning malware around the globe. This is useful for LEAs, considering that a successful malware, used in another region, could be easily turn relevant in another region in a very short time. This includes e.g. the de-anonymization of hidden services as well. The alerts are defined by the LEAs.

According to the high amount of malware around the globe, it is of high importance to have a perception of the likeliness of it being used. Therefore, the RAMSES project uses a game theoretical approach to define it.

Ransomware as a business model

Before the RAMSES approach and the findings of Kent University in the next chapter are explained a couple of key elements for the success of certain ransomware. In general ransomware has quite high fixed costs, according to design, programming, development or simply buying it, but very low costs of the use of it, meaning the actual attack. This is in contrary of a "usual" crime or compared to a hijacking, where the costs of the attack / crime are much higher. The developer of a successful ransomware can sell it much more often than an inefficient one. This plays a crucial role for the business model of for-profit ransomware. Other key factors are: if there is a distribution line or if there are certain services included, like offering the victim support in the

way of payment instructions and advice, like hotlines or helpdesks.

Other factors that might influence the success of a certain ransomware are, if there might be a global reach like WannaCry that had a global reach and has hit institutions like the British NHS and companies like Renault and the Deutsch Bahn (Briegleb, 2017). The use against institutions might create a higher ransom than against individuals, even a dual use in which different types of targets receive the same malware with different ransom demands is possible. The sophistication of the ransom demand, be it targeted or random, price discriminatory or fixed, can affect the complexity of the command and control communication required to successfully carry out the attack.

Success is not just related to the quality of the malware used, it is logical that it depends on the situation, emotive and material value of files to individuals or institutions. If the infected computer is part of important infrastructure (such as customer or patient records vital for record keeping and correct allocation of resources) the willingness to pay is much higher.

There is also a relation to the reputation of the ransomware. If the victim does not have the chance to get his data back, this will also be spread around, but if the service was "good" and the data could be restored, the success will be much more likely.

Kent University is providing the RAMSES project with a business model based on game theory to help the project to classify ransomware.

Overview of Game Theory, Economic Modelling and Ransomware

Ransomware is often viewed through the combined lenses of cyber-security and law enforcement, and quite rightly so. However, a purely technical analysis of ransomware doesn't capture the myriad decisions regarding the price of ransom, target selection, and potential negotiating strategy between criminals and victims. Economic modelling is a powerful tool that can identify the costs and revenue streams of ransomware. For the sake of brevity, this discussion focusses on profit-motivated ransomware, disregarding politically motivated or destructive variants.

Research conducted by academics from the University of Kent suggests that current criminals are not very aware of the economics of their activities. Current ransomware demands ransoms that are fixed, and low compared to the optimal price. This optimal price can be found by considering two key attributes of any ransomware victim: their willingness to pay (WTP) and their willingness to accept (WTA). WTP is a simple measure of what a victim states they are willing to pay, whilst WTA is closer to their personal valuation of their files. Horowitz and McConnell (2002) observe that WTA is usually higher than WTP, by up to a factor of 10 in some cases. The true value of files being held to ransom must therefore lie between WTA and WTP. Bateman et al. (2005) argue that the true valuation will be closer to WTA (the higher value).

Hernandez-Castro, Cartwright, and Stepanova (2017) conducted a preliminary survey of 149 adult residents of Canterbury, UK. The results of this survey showed that 9% of respondents expressed a WTA of £990 and WTP of just over £200. 20% of respondents had a WTA of approximately £400, and WTP of £92. Considering that WTA is more reflective of the victim's true valuation of their files, this suggests that charging a ransom which only 9% of victims pay is more profitable than when a larger number of individuals pay. This is because of the assorted reasons victims must refuse payment – they may be unwilling to cooperate with criminals, might place a lower value on their files, are not capable of paying the ransom, or one of any number of reasons that lead to non-payment. Criminals are charging low prices in the hopes of enticing a population who wouldn't pay regardless of how low the ransom is – all the while missing out on the potential profits that a select portion of their victims would yield by paying higher ransoms.

This assumes completely random infection and the perception of victims as individuals, intelligence-led attacks against companies could take this a step further and price-discriminate. Such pricing schemes involve the tailoring of prices to meet the likely WTA of a victim, instead of setting a blanket ransom that attempts to capture the most profitable segment of the paying population. More sophistication is required than is currently common in ransomware attacks, but Remote Access Trojans (RATs) and financial information for publicly traded companies are just two sources criminals may use to determine if they can squeeze a high-value victim for a higher ransom.

Game theory provides a means of playing through hypothetical ransomware attacks. Selten (1988) proposed a simple game of kidnapping. His 6-stage game is applicable to ransomware, if one considers the files encrypted by an attack to be the object being held to ransom. Two actors, the criminal and victim, represent the players of the game. The criminal wishes to extract a sum of money, while the victim wants their files returned, but may not wish to pay. Throughout this game, the criminal is best served by releasing the files if their demand is met or a viable counter-offer is offered. In any one instance of this game, it may appear that the criminal could delete files even after being paid, but one must remember that this game is being played on a massively parallel scale. One must also assume that some victims may communicate. Destruction of files after a ransom has been paid will be communicated, diminishing the trust, and therefore willingness to pay, of victims that are aware of the event. As the cost of infecting each victim is low, but the potential income from each is high, it is in the interests of the criminal to play fairly, but firmly.

Lapan and Sadler (1988) expand on this game by accounting for the possibility of defensive measures. In this game, the victim may spend resources on defence. Such defences reduce the probability of an attack succeeding, but may still fail (due to zero-day exploits or insufficient expenditure). However, additional costs are incurred by criminals who may have to increase the sophistication of their infection method to bypass widely proliferated defensive measures. As the successful defence of one would-be-victim's machine harms the potential profit of the attacker, this generates positive externalities for the entire population of potential victims. This means that if the criminal fails to infect enough victims, they will not be able to generate profit. Even if a portion of victims can defend themselves, profit may fall significantly below the optimal, as high-paying victims may be in the portion of targets the criminal cannot reach.

A game theoretic approach to ransomware can highlight such weaknesses in criminal enterprise and suggest more effective strategies for LEAs and potential victims of cybercrime. Communication is key, increasing the portion of individuals who refuse to play the ransom game (by refusing to pay) is highly effective. This is, however, dependent on the perceived worth of files at risk – encouraging backups can reduce the impact of high-value files being held to ransom by ensuring that the victim can restore them instead of submitting to a criminal's demands.

Economic modelling can provide deep insights into the costs, revenue streams, and weaknesses in the public domain that allow ransomware to be such a profitable enterprise. Though this overview cannot hope to encompass the complexities of current and near future ransomware, it can demonstrate than even cursory analysis of current ransomware highlights a myriad of improvements that criminals are guaranteed to incorporate in the future. Our continuing work with the RAMSES project, will explore optimised forms of ransomware, and identify behavioural and technological countermeasures to them prior to their inception by criminals, where possible.

Conclusion

As it can be expected that the threat from ransomware is not declining, but is instead rising, countermeasures are necessary to help citizens and LEAs to protect critical infrastructure and the privacy of citizens. Especially under the most likely assumption, that the Internet of Things (IoT) will continue to become more critical to daily activity for a great many individuals. The attack of WannaCry in 2017 proved that the connection infrastructure and data in the internet can and will be attacked, also in the future and the criminal activities, like in the past, will become more sophisticated and harder to detect and counter. Cyberattacks against critical infrastructure, like traffic systems, water supply or the energy system would have a very high effect on the population. But also homes and privacy are more at risk, because citizens are more and more depending on the data on the internet and some services can just be used online. The more citizens will use Apps to control their homes including the access will lead to the threat that burglary might change and the innovation for automated driving brings also certain other possibilities for criminals to attack these systems with ransomware. The financial sector is moving with high speed towards business on the internet. This forces citizens to use online banking systems, which includes the risk of infiltration of the financial business sector and the theft of data and money. Other EU funded projects, like Cyberroad (2016), have shown and analysed these risks.

The RAMSES approach will help citizens also according to the future risks to be safer in their privacy and the use of the internet. LEAs will have the possibility to retrieve information faster, respond quicker and it will help them to gain forensic evidence, which is court relevant. They will have the possibility also to create a network by signing up and share their experiences and learn from each other as the phenomenon and the criminal activity is not limited to a single region or country. One of the advantages of the project is that LEAs can use the platform and the developed tools for free, if they sign up. By doing so RAMSES will help to strengthen security for this criminal phenomenon and help LEAs to faster react to threats and speed up the process of findings of forensic evidence.

References

- Akhgar, B. & Yates, S. (2013) *Strategic Intelligence Management*. Butterworth-Heinemann.
- Briegleb, V. (2017) WannaCry: Was wir bisher über die Ransomware Attacke wissen.
  Retrieved from: https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html
- Cyberroad Website (2016)
  Retrieved from: https://www.cyberroad-project.eu/
- Europol, (2014). The Internet Organised Crime Threat Assessment (iOCTA).
- Hernandez-Castro, J., Cartwright, E. & Stepanova, A., (2017) *Economic Analysis of Ransomware*. SSRN Electronic Journal. 10.2139/ssrn.2937641
- Kaspersky Lab and Global Research and Analysis Team (2018) Kaspersky Security Bulletin 2016/17.
  Retrieved from: http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/Kaspersky_Security_Bulletin_2016_2017.pdf
- Lapan, H. E., & Sandler, T. (1993) Terrorism and signalling. *European Journal of Political Economy*, 9(3), 383-397.
- Lapan, H. E., & Sandler, T. (1988) To bargain or not to bargain: That is the question. *The American Economic Review*, 78(2), 16-21.
- NTT Security (2017) NTT Security stellt Global Threat Intelligence Report (GTIR) 2017 vor.
  Retrieved from https://www.nttsecurity.com/de-ch/uber-uns/News/detail/ntt-security-stellt-global-threat-intelligence-report-gtir-2017-vor-77-prozent-der-ransomware-in-vier-branchen
- Ramses website (2017) Project.
  Retrieved from https://ramses2020.eu/project/
- Selten, R. (1988) A simple game model of kidnapping. In: *Models of strategic rationality*. 77-93. Springer Netherlands.

Maximising the Security and Safety of Citizens by Strengthening the Connection between the Police and Communities They Serve

Holger Nitsch
University of Applied Sciences for Public Service in Bavaria, Germany[1]

Ben Brewster
Babak Akhgar
CENTRIC (Centre of Excellence in Terrorism Resilience, Intelligence and Organised Crime Research), Sheffield Hallam University, United Kingdom

Abstract
This paper provides a discussion on the objectives, approach and findings of the EU H2020 funded UNITY project. The project aims to strengthen the connection between the police and the communities they serve by providing a suite of ICT tools to improve collaboration, cooperation and information sharing between LEAs (Law Enforcement Agencies) and the communities they serve. The paper defines the underlying concept of community policing, before moving into a discussion about the developed ICTs and the empirical research underpinning their development and the subsequent approach used to test them. Within, we build upon the theoretical notion that ICTs in isolation do little to break down existing cultural, socio-economic and other embedded factors that contribute to absences in collaboration between citizen groups and the police. Instead, ICTs are an important mechanism which can be used to reinforce existing cultures of collaboration and trust, providing an additional vector through which citizens can make a contribution in their local communities, and through which police can be made contextually aware of local crime issues.

Keywords: Community Policing; Social Media, Radicalisation, Training

Introduction

Communities the world over, despite their varying social, cultural and ethnic differences, have common and shared values, and the right to safety, security and well-being. Despite living in an age of ever increasing digital connectivity, many communities remain disconnected from society at large and the public services designed to support them; including the Police.

The socio-economic landscape is complex and constantly changing, adapting to global events, and reflecting changes in wider society, shaping the perceptions and behaviours of individuals and the communities to which they belong and identify. Events such as the fall of the iron curtain in the late 80's and early 90's, and the ascension of many of these eastern bloc states to the

1 Corresponding author's email: Holger.Nitsch@pol.hfoed.bayern.de

European Union in 2004, opened up freedom of movement to millions, providing many with the opportunity to travel elsewhere in Europe for work. The culture of policing in many of these areas, and the perceptions held by the public however, is very different than that which those from relatively stable democratic states would be used to. Those from traditionally autocratic states are likely more accustomed to cultures of mistrust in policing, fuelled by perceptions of corruption and malpractice, where police are seen, in extreme cases, as an enemy and not an institution that serves the wellbeing of the public.

In parallel, and in some ways compounding these issues, are social tensions between different communities. Events such as the terrorist attacks in 9/11, and subsequent attacks in London, Paris, Nice, Brussels, Copenhagen, Berlin and Ansbach have fostered a culture of fear, anxiety and suspicion, building tensions towards specific racial and religious groups. The Islamic population in particular has been the subject of scrutiny by many as a result. At the same time, ongoing conflict in parts of Africa, Syria and Afghanistan has displaced millions. In 2015 alone more than 800,000 entered Germany, with up to 2000 people per day entering via the Austria – Bavarian border alone (Bundesamt für Migration und Flüchtlinge, 2016). Moreover, the ongoing conflict in Syria has placed ISIS and Daesh firmly into the public consciousness, radicalising some to travel to become foreign fighters in the region, and others to carry out attacks in their name on European soil. This has exacerbated tensions with the Islamic community in many areas, and contributed to the growing proliferation of right-wing ideologies, and the increased profile of right-wing political parties, in a number of areas of Europe, including the UK, Germany and France.

The near ubiquity of digital communications through the web and social media has transformed how, and the frequency at which, individuals contract, and are able to disseminate, information. These platforms are now popular vectors for the spread of misinformation, or 'fake news' as it is now commonly referred to in social parlance, and hate-speech. As a result, maligned and minority communities are commonly excluded from many aspects of normal society (Olcott, 2012). Together, these challenges pose a great challenge for the Police in addressing local crime issues.

Community policing and social capital

Despite broad and often varied underlying definitions, a common theme throughout community and neighbourhood policing strategies establishes the need to target improvements in the relationship and level of engagement between the police and the communities they serve. Community policing approaches have long underpinned a desire to move away from reactive policing models towards those which establish a more proactive philosophy, responsive to the wants and needs of the community. The near ubiquitous proliferation of smartphones and other ICTs (Information and Communication Technologies) means they are often seen as a vector through which initiatives of all kinds can instil a culture of proactive engagement with their respective stakeholder communities.

At the core of engagement, and similarly the idea of 'community' as a whole, is the concept of social capital (Huysman & Wulf, 2004). Social capital is a form of economic and cultural capital in which social interaction is vital, and in which social transactions are marked by cooperation, reciprocity and trust (Flora, 1997), and where goods, services and interventions are produced in service of common goals. The concept of community policing is underlined by the exchange of social capital between the Police, other statutory and non-statutory organisations, citizens, communities and interest groups in pursuit of social cohesion and the collective efficacy that enables citizens and groups to participate in shaping the contexts and communities to which they belong and with whom they engage (Sampson & Raudenbush, 1999). The concept of community policing itself has been discussed as an extension of the 'social contract' that exists between police and citizens placing additional requirements and demands on both parties. From a policing perspective, this requires the acceptance of citizens and communities as a partner in local safety and security, and from the perspective of those citizens, an acceptance of the police's role within their communities. But what is community policing? While the term is omnipresent in across western policing, an agreed and accepted definition of what it actually entails remains elusive (Cordner, 1998). Despite this continued ambiguity, the core philosophy of community policing, and thus a common thread across all of its contemporary manifestations, can be distilled to focus on those activities which seek to forge working partnerships between the police and communities (Peak & Glensor, 1996).

Methods and approach: The UNITY project

The empirical work drawn upon in this paper originates from the EU H2020 funded UNITY Project (UNITY, 2017). UNITY was undertaken with the objective of trying to build a greater understanding of the contextual factors that influence the engagement of citizens with the police at a local level, towards developing models of effective practice that strengthen the cooperation between police, other stakeholders from the statutory, non-statutory and third sectors; enabled through the use of technology. The project took a multidisciplinary approach, involving academics from a range of disciplines alongside policing practitioners and private sector technology providers. UNITY adopts the view that community policing is an important strategy in the contemporary policing repertoire as a means of moving away from traditional reactive practices to a more proactive, integrated and partner-oriented role that focuses on addressing lal needs (Maureen, Brudney, & Brown, 2014). Among other benefits, it is believed that by strengthening the connection and levels of communication between police, stakeholders and citizens can play a significant role in efforts to reduce crime and the associated risk of radicalisation (Wuchte & Knani, 2013).

In total, the project undertook 249 interviews across 8 EU member states; Belgium, Croatia, Bulgaria, Estonia, Germany, Finland, Macedonia and the UK, as the projects end-user pilot testing locations. Participants consisted of 82 police officers, 91 young people identified as members of country-specific minority groups and 76 representatives from intermediary organisations who work with minority groups. The research was conducted to develop a greater understanding how ICTs are currently being used to support community policing. While the results indicated that perspective on community policing varied significantly it did establish a number of key themes centred around crime fighting, information management, cooperation and collaboration, providing (or requesting) assistance and communication (Bayerl, van der Giessen, & Jacobs, 2016).

Despite the focus on technology, a common thread throughout the findings was the perceived importance of face-to-face communication in community policing. As a result of this emphasis, the report concluded that instead ICTs should act as a mechanism to reinforce existing relationships and face-to-face communication vectors between communities and the police by facilitating improvements to information, promoting visibility and accountability (Bayerl, van der Giessen, & Jacobs, 2016). Using these outcomes, UNITY undertook to develop a suite of ICTs to support the core principles it identified.

Alongside a more conventional mobile application and web platform designed to allow for information to be exchanged between police and citizens on a local community basis, the project has developed a suite of training tools; aimed at both the police and at citizens and community groups. Many of the core principles of the project's training offering have been implemented into the training of the Bavarian police at the University of the Bavarian Police, with the core development and refinement of the police training tools under collaborative development by the projects law-enforcement partners from Finland, Bavaria, Estonia and Croatia.

Training: Applied engagement for community participation

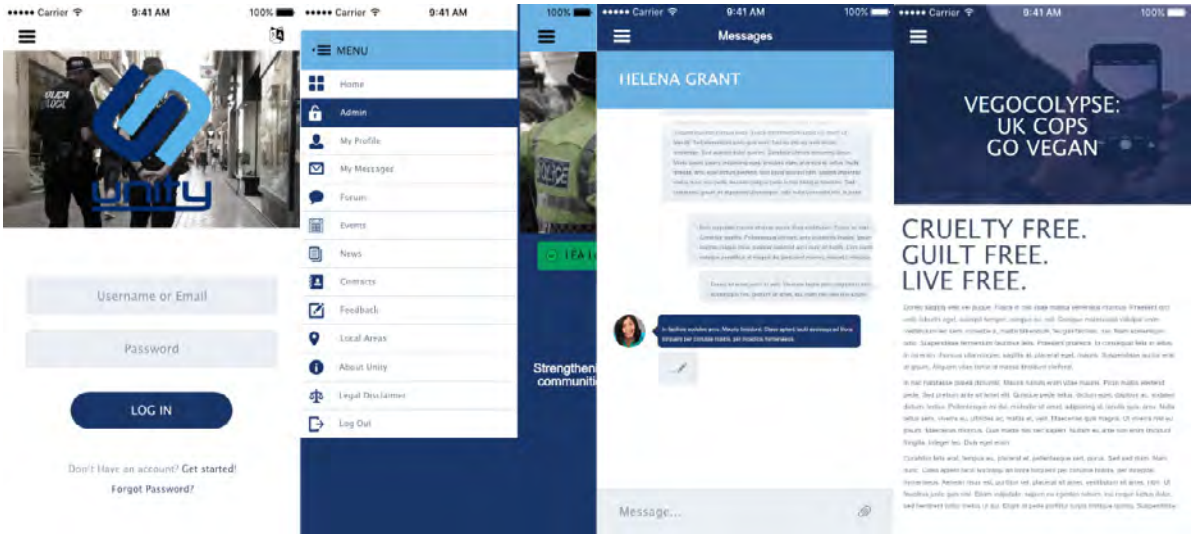
While it is possible to deploy training and education to the police and other statutory organisations that have a duty to act, the task of engaging and raising awareness within communities, especially those which may be considered underrepresented or vulnerable can extraordinarily challenging. With AEsOP (Applied Engagement for Community Participation) we set out to explore the possibilities of engaging with these communities using ICTs, specifically through the development of an educational videogame, to raise awareness of community policing within the communities themselves. AEsOP provides the user with a range of scenarios, each of focussing on different local policing issues. The game puts the user in the shoes of various community actors, including the police, allowing them to play through a range of interactive stories with branching decision paths, revealing how various community actors and forms of community participation can help prevent and reduce the impact of local crime issues. The game uses mechanics borrowed from the '2D adventure' genre, utilising a narrative driven storytelling approach. The game makes use of rich hand-illustrated art, to ensure AEsOP is approachable and suitable for use by all, from school children right through to niche community groups focusing on different activities and demographics. A piece of concept art for the game's modern slavery scenario can be seen in Figure 2.

Figure 1: AEsOP Concept Art - Modern Slavery Scenario

A common information exchange platform

Alongside the training and educational materials, UNITY provided a two core ICTs; a web portal and mobile app, designed to provide police, citizens and other intermediary organisations with a common information exchange platform. The app and platform try build upon and leverage existing cultures of information sharing through social media, cultures which are prominent across many groups in society. Some screenshots showing an overview of the mobile app developed during the project can be seen in Figure 1.

Figure 2: UNITY Mobile App



Some public organisations, such as the Munich police department already send out tweets in multiple languages at events such as the yearly Oktoberfest, where it is known or believed the target audience is not necessarily German speaking.

In the run up to Oktoberfest 2016, tightened security was put in place in response to the attacks that rocked parts of southern Germany only a few months prior to the event, while the chief of Munich police took to social media to provide reassurance, posting in English:

> *"From a policing point of view there is no reason at present for refraining from going to the Oktoberfest. That is why I have to take note of the cancelations that came out. We still have no indication of a concrete danger regarding an attack during the Oktoberfest. We have been living for the threat for many years now. This situation has not changed for this year. There is one thing you can count on: The police will do everything to ensure maximum safety during the Oktoberfest this year again. Our security concept does not start at the entrance, but includes many other measures right up at exchanging information at an international level. Nobody needs to alter the way the live. This will only play into the hands of those who want to exploit the situation for their political goals [sic]* (Andrää, 2016)".

Information such as this, designed to ease tensions, doubts and fears, can help to build trust with the target audience. While the UNITY platform does not aim to replace existing and well established social media platforms, as it would be extremely difficult to cultivate a user base to rival sites like Facebook and Twitter, thus reducing its utility, it does provide a vector where responses to more localised issues can be made.

The project's empirical research identified that most people, unsurprisingly, are already using established social media platforms to consume this kind of information – meaning that despite the presence of systems such as UNITY, which aim to provide a more localised forum for community-oriented issues, it is important the LEAs maintain an active presence on services such as Facebook and Twitter. Events such as the 2016 Oktoberfest, and also the threat to the central rail infrastructure of Munich on New Year's eve the same year (Eddy, 2016), are good examples of how powerful communication, and the dissemination of information, can be in maintaining calm.

The number of people following the Munich police twitter account rose significantly following the threats made against the city's rail infrastructure on New Year's Eve 2016. This shows that the public look to these mechanisms for information on the back of threats, showing a degree of trust in authorities such as the police. The tweets helped to reinforce a feeling of calm among citizens at the time of the events, despite the shutdown of the cities trains and subway (Eddy, 2016). The police also managed to reach a diverse audience by using multiple languages and multiple popular social media platforms, ensuring it was seen by tourists, non-native speakers and other minority communities, providing they are digitally-enabled. Examples such as these inform the training provided through the UNITY project, taking into account the specific and tailored information needs of different locales, demographics and communities.

Minority groups

The project, as part of the development of its scenarios for the pilot testing process, made efforts to identify unique contexts, groups and circumstances that would test the core principles of community policing; crime fighting, information management, cooperation and collaboration, providing (or requesting) assistance and communication. The nature of the groups identified went from ethnic minority groups and university students, to football fans, people with disabilities, and special interest groups. While it may be possible to draw parallels between the behaviour and perspectives of groups such as those with disabilities and football fans in different regions across Europe, great differences were observed among different Ethnic minority groups.

The information requirements of different groups also varied significantly. Football fans are bound to the club they support, so they are commonly interested in news around the club, safety and security information about forthcoming games, and other context sensitive information. In cases where levels of trust exist with the police exists, it can provide an opportunity to avoid the risks of being caught up in hooligan clashes, other forms of violence, travel disruption, ticketing details, and forms of security screening that may in place around specific high-profile games.

Other groups have different information requirements. For example, some forms of disability, such as blindness or deafness can cause communication problems. In such cases there is a needed to adjust communication mediums. Throughout the duration of the project, UNITY worked alongside the deaf community in the UK. To mediate communication issues the project integrated features that allowed for the posting of short videos, so that British Sign Language (BSL) could be used to communicate with the deaf community face-to-face to build trust and improve the ability to exchange information. The mobile application also allowed the deaf community to post videos to the platform. The diversity of issues was also evident in other pilots. In Bulgaria the focus was on people of Roma decent, in Germany it was refugees from central Asian and Middle East backgrounds. The Estonian pilot focused in on the Russian community, while in Belgium the Jewish community of Antwerp took part.

Pilot Testing

As has been touched upon throughout this paper, the UNITY project is built upon the real-world requirements of end-users, identified as result of empirical research conducted across the projects eight 'end-user' participants from across the EU; Croatia, Germany, Estonia, Finland, Belgium, Bulgaria, the Former Yugoslavian Republic of Macedonia, and the United Kingdom. These same countries were subsequently used to test the operational impact of UNITY's community policing principles and software tools. Each pilot was set up slightly differently to reflect the local contextual needed of the communities involved in the respective case-study scenarios. The requirements identified in the projects empirical work were used to build two contrasting schematics of community policing in each of pilot regions; the Current Operating Model (COM) and the Target Operating Model (TOM). The COM was built to reflect the projects understanding of community policing, and the challenges currently faced by police in each of the projects pilot location. The TOM was built to reflect an aspirational view of community policing in location, reflecting what community policing should look like, and how it should mediate some of the challenges identified in the COM following the implementation of the UNITY technology toolkit and the core principles of community policing established during the project. In each location the technology and UNITY approach was tested against real or indicative events and scenarios.

Conclusion

The H2020 project UNITY was established to provide LEAs, stakeholders and minority communities with a varied and broad ranging set of possibilities to build trust and accountability, and improve methods of information sharing and communication. Due to the wide range of scenarios, target groups and stakeholders, also through the advice of many experienced experts from Europe and beyond, UNITY can be used flexibly in various situations against a varied range of local community issues. UNITY also provides LEAs with training, tailored to the specific contextual needs of the user, and built on the empirical work and experiences gleaned throughout the project. The training can be completed face-to-face or online. The project also provides a mechanism to raise awareness within communities and citizen groups with AeSOP, an education game which was established to help improve understanding of community policing and to educate on how individual citizens can make a difference in the local community, making policing easier, and helping to improve the safety and security of citizens.

References

- Andrää, H. (2016) Statement from our Munich City Police Chief concerning doubts visiting the Oktoberfest. Retrieved January 31, 2018, from https://twitter.com/PolizeiMuenchen
- Bayerl, P. S., van der Giessen, M., & Jacobs, G. (2016) *UNITY - Gathering of user requirements for community policing tools*. Retrieved from https://www.unity-project.eu/wp-content/uploads/2015/12/D3.4-Gathering-of-user-requirements-for-CP-tools.pdf
- Brown, M.M. & Brudney, J. L. (2003) Learning Organizations in the Public Sector? A Study of Police Agencies Employing Information and Technology to Advance Knowledge In: Public Administration Review *63*(1), 30–43.
- Bundesamt für Migration und Flüchtlinge. (2016) *Migrationsreport*. Retrieved from https://www.bamf.de/SharedDocs/Anlagen/DE/Publikationen/Migrationsberichte/migrationsbericht-2015.pdf
- Cordner, G. W. (1998) Community Policing: Elements and Effects. In G. Alpert & A. Piquero (Eds.), *Community Policing: Contemporary Readings*. Illinois: Waveland Press.
- Eddy, M. (2016) Munich on High Alert After New Year's Eve Terrorism Threat. Retrieved January 31, 2018, from https://www.nytimes.com/2016/01/02/world/europe/munich-threat-attack.html
- Flora, C. (1997) Building social capital: the importance of entrepreneurial social infrastructure. Retrieved September 23, 2017, from http://dgroups.org/file2.axd/9cccfd87-46a6-4a00-80ab-1224c6345443/Building_Social_Capital.doc
- Huysman, M., & Wulf, V. (2004) *Social Capital and Information Technology: Current Debates and Research*. *Social Capital & Information Technology*. Retrieved from http://books.google.com/?hl=en&lr=&id=8uYbB1AeVrYC&oi=fnd&pg=PR7&dq=Social+Capital+&+Information+Technology&ots=AyDgtWDk0T&sig=YOxm20lNHzN3tHd9lYqYTi6T8YU
- Olcott, A. (2012) *Open source intelligence in a networked world*. A&C Black. Retrieved from https://books.google.co.uk/books?hl=en&lr=&id=oncloN25T38C&oi=fnd&pg=PR7&dq=Open+Source+Intelligence+in+a+networked+world,+&ots=ak-wC3JSAQ&sig=17fUvKUUOfVlv3RMsvRpncB3NvQ
- Peak, K. J., & Glensor, R. W. (1996) Community Policing and Problem Solving: Strategies and Practices, Prentice Hall.
- Sampson, R. J., & Raudenbush, S. W. (1999) Systematic Social Observation of Public Spaces: A New Look at Disorder in Urban Neighborhoods. *American Journal of Sociology*, *105*(3), 603–651. https://doi.org/10.1086/210356
- UNITY (2017) About the UNITY Project.
- Wuchte, T., & Knani, M. (2013) Countering violent extremism and radicalization that lead to terrorism: the OSCE's unique regional blueprint. *Journal EXIT-Deutschland. Zeitschrift Für Deradikalisierung Und Demokratische Kultur*, (2), 76–86. Retrieved from http://journals.sfu.ca/jed/index.php/jex/article/view/22

Developing and Testing a Community Policing Social Network in European Cities

Georgios Leventakis
George Kokkinis
KEMEA – Center for Security Studies[1], Hellenic Ministry of Interior, Greece

Abstract
Enhancing the feeling of public safety and crime prevention are tasks customarily assigned to the Police. Police departments have, however, recognized that traditional ways of policing methods are becoming obsolete; Moreover, a large number of police departments are experiencing budget cuts and are streamlining their operations while they are looking for innovative policing approaches to balance these reductions. However, when the Community Policing philosophy is appropriately applied, it provides the opportunity to identify risks and assist in solving problems related to crime and disorder. It also enhances the feeling of safety, consequently improving the quality of life in local communities.
Modern Community Policing approaches utilise Social Media and mobile applications. Due to their high level of infiltration in modern life, both of these media constitute a powerful mechanism which offer additional and direct communication channels for reaching individuals and communities. When the feedback gained via these channels is analysed by Law Enforcement Agencies the gain is twofold. These channels can be exploited to improve citizens' perception of the Police and to capture individual and community needs.
This paper presents the outcomes of the first trials of the INSPEC^{2}T system (**I**nspiring Citize**NS** **P**articipation for **E**nhanced **C**ommunity Poli**C**ing Ac**T**ions). The project is funded by the European Commission's research agenda and aims to explore the impact of Social Media on Community Policing.

Keywords: Community policing, social networks, new technologies, organisational changes, information crowdsourcing

Introduction

There is no end to the usage and purposes of the smartphone applications that are available nowadays. Over the last years, numerous instances of mobile applications with focus on local communities' safety are available. At the same time, various Law Enforcement Agencies (LEAs) across the EU have realised the importance of Community Policing (CP), an area that is rapidly evolving and transforming the policing landscape. CP provides the opportunity to communities to assist in solving problems of crime, disorder and safety, while at the same time contributes towards improving the quality of their lives and serves as an efficient decision support system for the Police, due to the crowdsourcing of information.

1 Corresponding emails: gleventakis@kemea.gr, g.kokkinis@kemea-research.gr

Researchers will agree that CP is both a philosophy (a way of thinking) and an organizational strategy (a way of carrying out that philosophy) which allows the police and the community to work together in new ways. The philosophy is built on the belief that people deserve and have a right "to have a say" in policing in exchange for their participation and support (K.J Peak., R.W. Glensor & L.K. Gaines, 1999). According to (A. Myhill, 2006) CP is the process of enabling the participation of citizens and communities in policing at their chosen level, ranging from providing information and reassurance, to empowering them to identify and implement solutions to local problems and influence strategic priorities and decisions'.

INSPEC^{2}T^2 is a three-year project that started in May 2015. It focuses on a user-centric design and development approach, and has already mobilised and engaged a critical user group mass within the EU and overseas. With special emphasis on social media, it consolidates and modernizes bidirectional communication of stakeholders, using multiple levels of anonymity to ensure data privacy. Citizens are encouraged to interact with police using a mobile application and a web portal. The proposed and modernised communication platform, and the developed social media network enhance the participation of communities in policing.

Capturing stakeholders' requirements

The INSPEC^{2}T project reached out to more than 2100 CP stakeholders using four online surveys and focus group discussions. The project partners promoted the online surveys using social media channels and electronic communications exclusively. All four surveys were structured in such a way so as to better grasp European values in regard to CP in respect to social, cultural, ethical and legal dimensions. The surveys were conducted between August 2015 and January 2016.

The first survey was aimed at communities and was promoted through the project's social media channels. The general public questionnaire received 1092 responses from citizens living in Greece, the United Kingdom, Spain, the Netherlands, Germany, Cyprus and 5 other EU countries. Most respondents were university degree holders and were employed. They mainly lived in towns, cities and metropolitan urban areas. Citizens that responded to the questionnaire were of various ages, most of them were not involved in any voluntary work and the majority of them felt safe in their communities.

The second survey was aimed at neighborhood watch members and social workers. In total 70 responses were provided from 14 EU countries (Austria, Bulgaria, Cyprus, Czech Republic, England, Germany, Greece, Ireland, Italy, Netherlands, Northern Ireland, Norway, Portugal and Spain). The third survey sought to capture the views of police colleges / universities / academies involved in the training of police students. 19 police professors from 6 countries contributed to the 3rd survey. The last survey was designed so as to capture CP practitioners' experience and views. This survey received 782 responses from police professionals from 8 EU member states.

Except for the general public survey, which was promoted using social media channels, the other three surveys had a more focused method of attracting responses. The project partner's professional networks were used to promote the surveys to CP stakeholders. The targeted respondees were Non-Governmental Organisations with an interest in CP, neighbourhood watch groups, community employees dealing with CP related issues, acting CP officers, police officers and their academia. The analysis from the online surveys provided a generic indication about the current CP status and about community preferences throughout a number of European member states which participated in the surveys.

In order to capture the "local" element and verify the findings of the online survey analysis, specific Discussion Focus Groups were formed. Guidelines about how to attract participant responses were issued and anonymous focus group interviews took place using a structured questionnaire. These focus group interviews were conducted in Greece, the UK, Cyprus, the Netherlands and Spain. Participants were questioned in two phases: the first phase concerned LEAs (10 participants from each country), while the second phase concerned citizens (60 participants in total, 10 per country). All participants, from different backgrounds, were selected with specific characteristics in mind, so as to capture a diverse set of views.

In addition to the online surveys and the focus groups, INSPEC^{2}T utilises a Stakeholder Advisory Group (SAG)

2 http://inspec2t-project.eu/en/

and an External Expert Group (EEG). These committees are made up of Law Enforcement Agency senior officers, government representatives, active citizen groups, community organizations, commercial associations, and CP visionaries. EEG members are distinguished Academics in Policing, Data Protection and subject matter experts in EU Ethical and Legal frameworks. The advisory committees, external to the project, were presented with the analysis from the responses to the online surveys and focus group interviews which were used to define the functionalities and system specifications.

The findings from the interaction with CP stakeholders are summarised herein.

Despite the fact that younger individuals are frequent users of Social Media (over 80%), the survey showed that they are nonetheless not enticed to contact the police through this medium. Only 18% of ages 20 – 39 uses social media to contact the police, while the respective percentage for ages over 40 rises to over 30%, and in some age groups it doubles (39%). The same principal applies for the use of webpages as a communication channel with the police. Despite the fact that younger ages use the internet to access web pages for a large amount of their everyday lives, they do not use the web to contact the police. Similarly, mobile apps are not an established method of communicating with the police. Only a small percentage of over 7% of younger ages use mobile apps for this purpose, a percentage that rises slightly to over 10% for the ages of 40 – 59 and drops back to less than 9% for ages above 59 years old.

Table 1: Which communication Technology do you use/will use to communicate and engage with the Police?

Communication Technology to engage with the Police	Current situation (%)	Future Situation (%)	Difference (%)
Email	24,00	60,50	+ 36,50
Phone Communication	88,30	61,20	- 27,10
New/ Social media	26,90	51,50	+ 24,60
Text Messaging (SMS)	5,20	37,40	+ 32,20
Websites / Portals	19,50	46,70	+ 27,20
Mobile Applications	8,70	45,30	+ 36,60

The surveys strongly prove that the most familiar and accepted form of communication with the police is phone communication (Table 1). When referring to the future, all responders have *shown eagerness to use the most updated technologies for their communication with the police*. Social Media has an acceptance rate of 51,50%, internet and websites have an average acceptance rate of 46,70%, e-mail communication succeeds with acceptance rates that vary between 51% and 66%, text messaging is accepted as a means for contacting the police at a percentage between 36% and 41%, while mobile apps will be used by approximately 50% of those aged under 50 and 40% of those aged over 50. *New technologies, in general, have an average acceptance rate of over 50% throughout all ages*.

Defining system functionalities

The analysis from the four online surveys and focus group interviews, as well as the interaction with the two external committees, enabled a shared understanding among police authorities and citizens about the problems to be addressed in a CP approach. A number of social, cultural, ethical, legal, security and privacy aspects of CP programmes were documented to point out differences in the interactions between LEA and certain communities. All of the above was used to produce an analysis of CP practices (D1.1 Report on best practices in community policing & gap analysis, 2016) and of the technological tools currently in use. Along with the results from Ethical & Legal Dimensions (D2.2 Legal and Ethical dimensions of INSPEC^{2}T System, 2015) and Societal & Cultural Aspect findings (D2.1 Social and Cultural Aspects of Community Policing, 2015) the consolidated End User Requirements were produced.

The end user requirements which were captured (D1.2 End User Requirements – 1st SAG Report, 2016) shaped the system architecture which was displayed using mock-ups for advisory groups external to the project. Following their feedback, suggestions and recommendations, the technical partners entered the development phase (D3.4 2nd SAG meeting report, 2016). At this stage there were a selection of 57 functional[3] and 53 non-functional[4] requirements classified as mandatory, highly desirable and desirable. In addition, there were 232 mandatory requirements resulting from the Description of Action[5]. Therefore, a total of 342 requirements were mapped into 24 use cases (Leventakis G., Kokkinis G., Papalexandratos G., 2017) which formed the operational guideline for the INSPEC^{2}T solution.

A Use Case[6] is a list of actions, typically defining the interactions between an actor and a system, to achieve an outcome. They document step by step instructions on how to test the built-in functionality and demonstrate specific features and functionalities of an advanced CP programme. The use case categories outline the interactions between users of the INSPEC^{2}T solution, first among themselves, then with other (existing) social networks and, finally, they describe the collaboration between community members and police officers. Finally, the 24 Use Cases were grouped into the following 6 categories as shown below.

[1] Advanced CP programme Interactions
[2] Communities
[3] Incident Reporting and Management
[4] Interaction with Social networks
[5] Back-End Intelligence
[6] Rules and Supporting Actions

Concept of operations - Overview

The concept of operations is presented in Figure 1. INSPEC^{2}T supports incident reporting from registered members and non-registered community members using a social media network. The citizens can fill in reports either as

1) *Registered*, where they agree to engage in two-way communications with the authorities (if required) or as
2) *Anonymous*, where they can submit reports. The anonymous users have willingly excluded themselves from being reached by other users and the system operators.

The submitted reports are intelligently processed by the system. The system's output will be used to assign CP officers to cases. The assigned resources will receive information to act upon and will have the option to interact with citizens and fellow officers. For incidents that might evolve beyond the CP context, front line police officers could interact with the system using the INSPEC^{2}T tools.

Aside from bidirectional and personalized communication, the system offers the means for community members to provide additional information (either text or multimedia files), enabling registered users to monitor the progress made on their submitted reports in real time. An advanced CP solution should possess intelligent functionalities and the overall architecture should be modular and should be based on open standard interfaces. As such, existing analysis modules and databases will be utilized and will constitute part of the advanced CP solution. The developed intelligence is made up of the following components: reporting, awareness raising, serious games, command, control and intelligence.

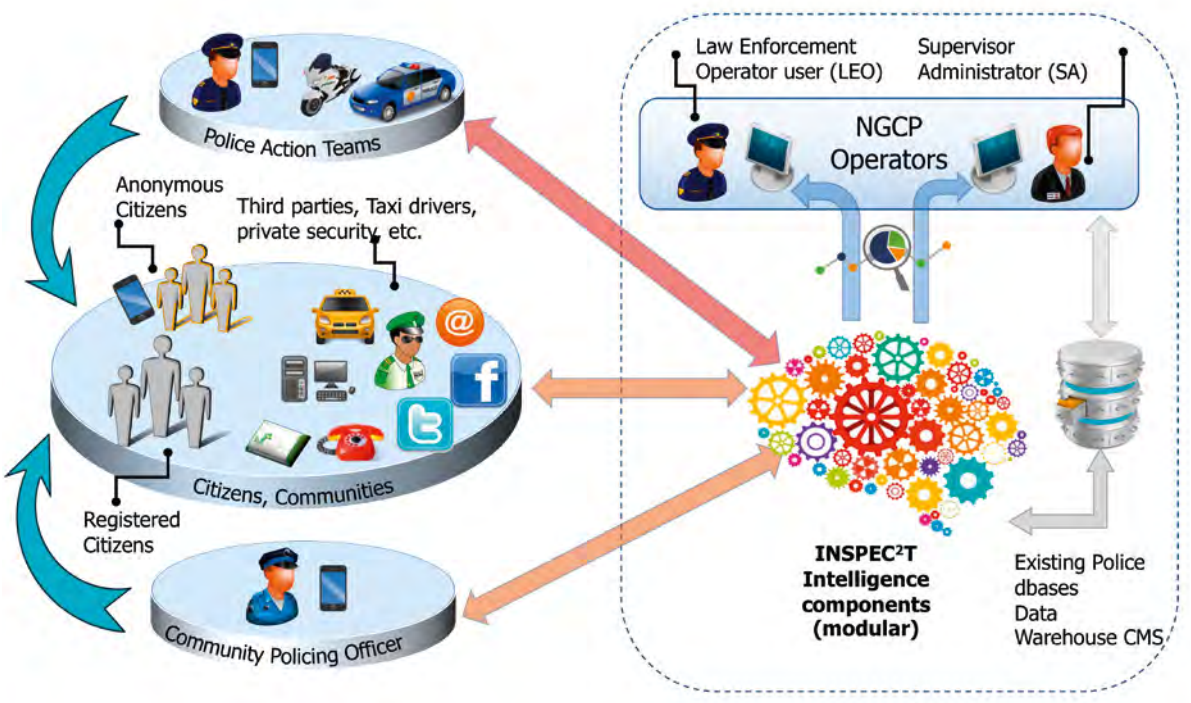
3 https://en.wikipedia.org/wiki/Functional_requirement

4 https://en.wikipedia.org/wiki/Non-functional_requirement

5 http://cordis.europa.eu/result/rcn/195176_en.html

6 https://www.ibm.com/support/knowledgecenter/en/SSWSR9_11.0.0/ com.ibm.pim.dev.doc/pim_tsk_arc_defininguse-cases.html

Figure 1: The INSPEC²T Concept



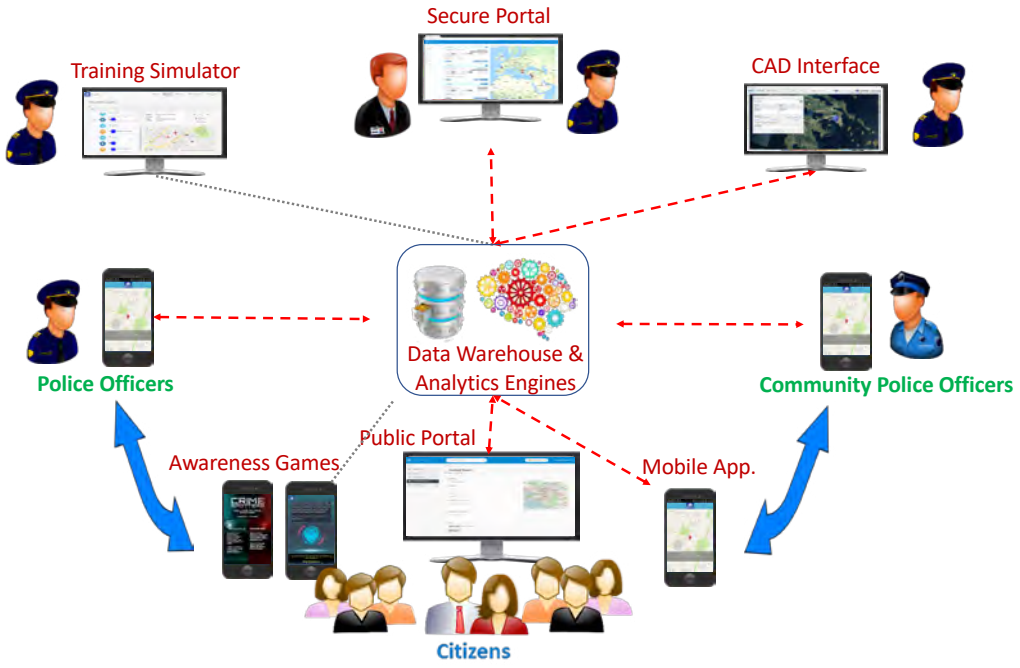
Implementing the solution

INSPEC²T is a collection of pluggable modules (Figure 2) that, as a whole, act as a user-friendly and efficient solution for strengthening community bonds. INSPEC²T consists of the following modules, each one adding unique functionalities to the platform. The smart Mobile Applications enhance incident reporting and management capabilities. The public and the private web portal promote community building and offer platform management. The data warehouse, the Geographic Information System (GIS), and the business and multimedia analytics modules augment the incident processing operations. The CAD (Computer Aided Dispatch) interface supports integration with existing CAD systems. The Serious Games facilitate awareness of CP operations and the training simulator supports the system operator's functions.

Mobile Applications (Mob App) and Public Portal (PP)

Two different incident reporting functionalities are supported. Citizens can either submit reports to the Public Portal using a computer or smartphone (without the installation of any application), or by installing the INSPEC²T mobile application on their smartphone or tablet (Figure 3). An extended (in terms of functionalities) version of the mobile application is available to CP officers for managing the reports and for further interacting with the system and its operators.

Figure 2: The INSPEC²T solution



Training Simulator and Awareness Games

The training simulator module offers realistic in-situ simulations to allow the system administrators and Secure Portal operators to get familiarized with the platform, experience the potential impact of their decisions, interact in a safe environment, analyse their approach, facilitate peer assessment and benchmark so as to enable self-reflection and improvement. Moreover, the inclusion of courses, with a focus on privacy, data protection and how the system administrators can comply with ethical, legal and societal requirements, should be mandatory items in an advanced CP training program. Apart from the mobile application and the Public Portal, an awareness game is also available. The game (Resource Force[7]) provides insight for citizens about the available CP resources and emphasises the role of community involvement. The game challenges citizens to command a limited number of CP officers and respond to a number of community requests.

Figure 3: Screenshots of the Mobile Application and the awareness game for Citizens

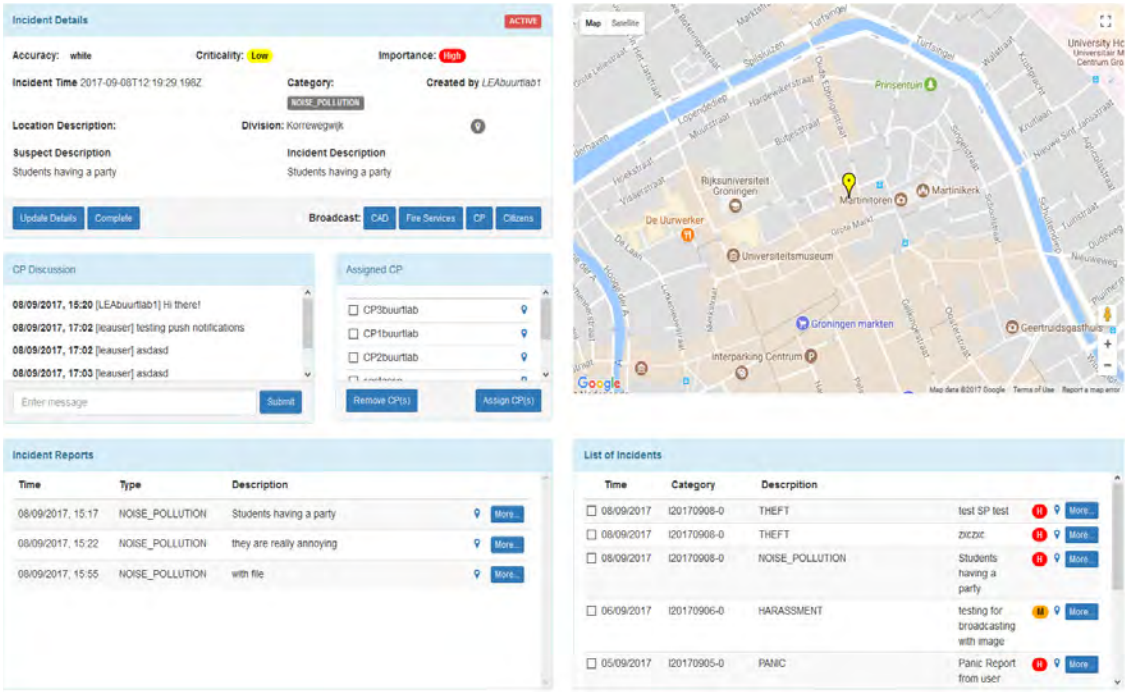
7 https://play.google.com/store/apps/details?id=com.playgen.ResourceForce

As new incidents endlessly arise and develop, the players, who are constantly under pressure, have to allocate overstretched resources while having limited information. The benefits of citizens contributing to CP are emphasised and the community members are taught that their involvement is key to safer societies.

Secure Portal (SP)

The intelligence submodules mentioned below, all feed into the Secure Portal (SP) which is the command and control interface for the entire solution. The SP is connected with the intelligence modules and present an advanced operational picture to its operators. The Law Enforcement Operator (LEO) and the INSPEC^{2}T Supervisor are in control of all CP submitted reports and, by utilising the intelligent processing of the advanced CP system, manage the reported incidents.

Figure 4: View of the Secure Portal



Intelligence

A series of intelligent modules provide processing, analytics, correlation of incident reports, archiving, and a file retention policy. The challenge of processing huge amounts of spatial data which is generated by either registered or anonymous users is addressed by the following modules:

Geospatial Complex Event Processor (GCEP). All incident reports are processed and analysed in a structural manner so as to generate meaningful information. The data submitted in the reports from multiple users are combined to infer events or patterns that suggest more complicated circumstances. The goal of complex event processing is to identify meaningful events at an early stage and respond to them as quickly as possible.

Multimedia Analytics (MMA) are capable of extracting semantic information from a wide range of multimedia data sources. Incident reports will contribute to increasing quantities of images, audio streams and videos. The MMA module first processes and then discards low quality data. The data of value is analysed to extract speech transcription, acoustic event detection (e.g. identification of a gunshot), person/face detection and other multimedia correlations.

Case Based Reasoning (CBR) is the process of solving new problems based on the solutions of similar past problems. In cases of uncertainty, or whenever decisions need to be taken based on different sources of information, this module takes action. The CBR module by design consists of two different submodules. The

first one is composed of rules that the user could adjust or modify, allowing it to make use of expert knowledge. The second submodule is equipped with a knowledge base and allows the inference of new rules and actions based on previous knowledge.

Business Intelligence Analytics (BIA) carries out the following functions: (1) computes metrics for the level of activity and engagement of both citizens and police and (2) calculates a rating for user profiles, by computing each user's activity (how frequently the user reports incidents, whether they are contributing helpful information to the system or whether they are malicious). It has to be noted that the rating essentially concerns the information provided by the users rather than the users themselves, that is BIA classifies the importance of each exchanged message, based on the author's profile ranking and other metrics.

Data Warehouse (DWH) integrates data from multiple heterogeneous sources and from different formats to support analytical reporting, structured and/or ad hoc queries and decision making. The large amounts of heterogeneous data provided by citizens and communities over time are arranged into abstracted subject areas with time-variant versions of the same records, with an appropriate level of data grain or detail to make it useful for the intelligent modules described above to retrieve and analyse them. In addition, **Data Processing Ageing (DPA)** can be configured according to the corresponding regulatory frameworks. Records may only be stored following a legitimate reason (massive storage of preventive data should not be allowed). Record lifetime and criteria for deletion have to be defined in accordance to Data protection legislation. The renewal of an item's date of expiration is possible and needs to be initiated from a user with the appropriate access rights. A mandatory description field justifying the need for this operation ensures that all data preservation actions are permanently retained for future reference and Ethical screening.

CAD interface supports legacy incident reporting systems and acts as the gateway which feeds CP related reports, which reach the call centre, into the INSPEC^{2}T system. In addition, the CAD interface is used to supply the required information, with the location of police resources, to LEO operators.

Testing and assessing the developed solution

The first working INSPEC^{2}T version undertook trials in Belfast, in April 2017. CP Officers from Police Service Northern Ireland, in cooperation with fellow Officers from Lancashire Constabulary, participated along with residents from the Holyland community and members of Ulster University in the execution of the CP scenarios. The second pilot and a demonstration of the solution to SAG and EEG committees took place in Egkomi, Cyprus in May 2017. In Cyprus, the consortium conducted a series of small scale pilots and solution demonstrations which engaged municipalities and LEAs. The third pilot took place in Valencia, Spain in May 2017. Further to Valencia local police and local community involvement, there were police representatives from San Sebastian and Guardia Civil.

The main scope of the first three pilots was twofold. One was to demonstrate and validate the strategic objectives of the project and second to present a working solution which satisfies the majority of end user requirements and requested functionalities. In addition, the empowerment of communities through the facilitation and delivery of a more personalised service, where citizens collaborated with the police in setting their CP agenda, was also tested. The output of the assessment was used to provide further input to system developers to fine-tune the system for the second testing phase which was scheduled to take place between October and December 2017.

The feedback from participants, (community members, neighbourhood watch associations, LEAs, CP visionaries) focused on the following three areas:

1) Reporting tools
2) Backoffice – Intelligent components
3) Issues primarily related to data protection and the compliance of the submitted intelligence with national and EU frameworks.

Following the development of the INSPEC^{2}T solution, an assessment toolkit was required to verify whether the implemented functionalities satisfy the end user requirements. The THOR approach, which was developed by the CAMINO[8] project was adapted and used for the assessment of the INSPEC^{2}T solution. The de-

8 http://cordis.europa.eu/project/rcn/185485_en.html

livered solution was analysed in four dimensions as follows:

Technical – Assess if the implemented solutions will assist the uptake of CP and whether they will provide the intelligence mechanisms required to efficiently analyse the user supplied information.

Human - Evaluate how a series of human factors, behavioural aspects, privacy issues, ethical, societal and CP awareness-raising activities will influence CP practices and create more safe and secure communities.

Organisational – Examine if the proposed processes, policies and procedures will enhance cooperation between Communities and LEAs and if the project will result in better CP.

Regulatory - Inspect the project for adherence to laws, standards, data protection and the legal framework at a national and EU level.

Following the execution of three pilots, feedback was collected by 1) using face to face interviews with CP/police officers using a structured questionnaire and 2) via an online survey made available for members of the public. The results recorded, were used to identify gaps and challenges that need to be overcome. The interaction of the THOR dimensions for the identified participant/user categories for the Use Case groups is shown in Figure 5.

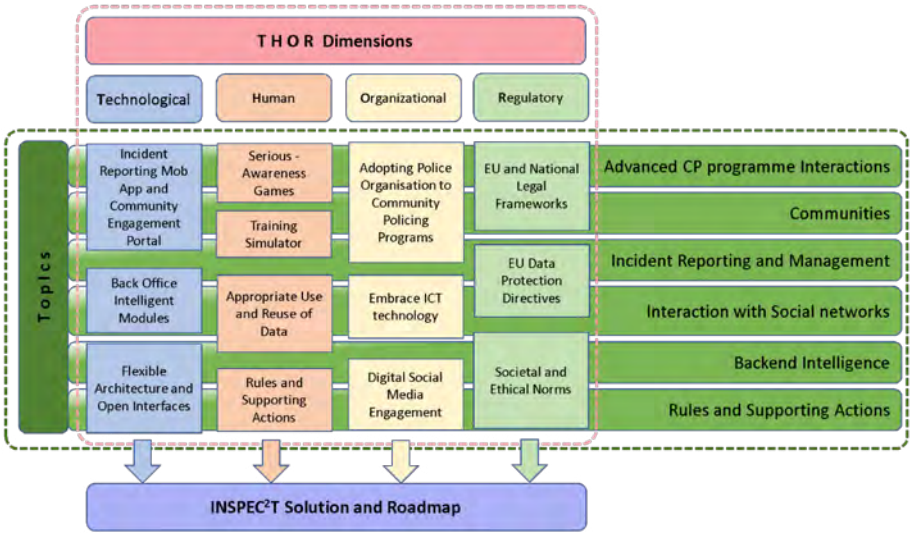
Assessment findings

The succeeding sections outline how each one of the THOR dimensions constitutes a CP verification framework and how each one of the use-cases are mapped under a specific dimension to provide the assessment criteria and verify whether the stakeholder requirements have been addressed and, if so, to what extent.

Technology

The improvements recorded by the adoption of new offered technologies and utilising it in current CP practices underlies the importance of understanding which technology solutions will introduce additional value. Introducing IT into police operations is a complex and demanding task and "it is not clear which technologies are more usable and effective in the context of a police organization" (Custers, B., 2012). Using a structured questionnaire, the INSPEC²T members requested from the SAG and EEG committees to provide their feedback and guide the consortium endeavours to shape and finalise the solution to be tested in the phase-2 pilots. Concerning incident reporting through the use of mobile applications, 93% of the experts indicated that they offer the greatest potential for improving CP. Similarly, 71% prompted that the application for LEAs is a great asset for CP officers in the field. For the public portal, 50% of the experts valued its use and ranked it at the top, along with mobile applications, as a component that could help in assisting and improving on community building and empowering citizen participation in CP tasks.

Figure 5: THOR model applied to INSPEC²T system



The independent advisors indicated that cutting edge police command and control centers are already using a number of intelligence subsystems. Therefore, the integration of "back office" components, like MMA, GCEP, BI, CBR, and DWH to support CP operations is well perceived. The experts also acknowledged that incident reporting, if processed intelligently, is a valuable intelligence source. Therefore, multimedia enriched content which is embedded in citizen reports should be treated as a valuable information source. The findings of (Kelling and Bratton, 2006) for "intelligence gathering and analysis" are confirmed for CP operations. Lastly, the INSPEC^{2}T open interfaces can be utilized for forwarding incidents to other authorities, such as municipalities, or environmental agencies.

At the end of each pilot, debriefing sessions with community representatives were held. The findings of the INSPEC^{2}T public survey (D1.2 End User Requirements – 1st SAG Report, 2016), were confirmed. Both CP officers and citizens indicated that using a mobile application will result in more frequent reporting.

Human

The INSPEC^{2}T training simulator is a scenario driven tool that simulates the submission of citizen reports and trains police operators on the functionality of the platform. The option of training CP system operators received positive feedback from SAG and EEG members and it is a mandatory prerequisite for police organisations to offer customisation to their needs and operational training to their CP Officers. The community and police relations in a social-media-like ecosystem will be studied in detail in the second phase of pilots. Therefore, the rules and the supporting actions required to prevent inappropriate behaviour, and also promote community and police interactions, was tested between October and November 2017.

The end-user testimonials confirmed that one of the most fundamental aspects for improving CP is to empower communities to prevent crime or the problems that lead to it. Establishing and maintaining mutual trust is therefore the central goal of CP. (Docobo, J., 2005). The citizens need to be aware of their own role and responsibilities and should proactively respond to indications of crime and disorder in their communities.

In all three of the INSPEC^{2}T pilots that were conducted, citizens value the option to form communities either physical (a group of residents) or virtual (licensed security personnel) and participate in them. The exchange of ideas via discussion groups, the privacy of personal messages and public threads, are all acknowledged to be required functionalities to encourage citizen participation. With this in mind, in order to empower citizen participation, the INSPEC^{2}T members developed an awareness raising game[6] for citizens, which was developed for iOS and Android devices. Using a gamification approach, the citizens were trained to collaborate with the police for the benefit of their communities. Through this game, citizens confirmed that they came to the realisation that police resources are not infinite and, as such, their cooperation with police in a number of incidents will lead to better CP results.

Organisational

The first component of successful CP initiatives involves transformational changes in the organizational structure and operation of LEAs (Bureau of Justice Assistance, 1994). CP is an information-intensive task/process, and technology plays a central role in helping to provide ready access to quality information. Accurate and timely information makes problem-solving efforts more effective and ensures that officers are informed about the crime and community conditions of their beat.

At each pilot debriefing session, focused group discussions were held with CP officers to record their professional opinions. In all three pilots it is acknowledged that two-way communications, online reporting, hosting discussion forums, and citizens' feedback promotes citizens engagement in CP and increases transparency in the way CP operations take place. Both the CP officers involved and policing experts from the SAG and EEG committees agree that the option for citizens to check the status of their submitted reports online, aside from increasing accountability of the police force, increases transparency. This highlights a strong interdependency between the Human and Organisational dimensions.

It should be highlighted that police adaptation to CP programs, the inclusion of modern ICT solutions in everyday policing tasks and the strategy of the police towards digital and social media are all topics outside of the INSPEC^{2}T sphere of influence of or other similar initiatives. To this extent, the consortium studied and analysed a number of indicators which were considered essential in the implementation of CP. Fostering and developing police-community relations requires

active engagement by police organisation, individual officers and community representatives. A CP maturity model is currently being developed for the purpose of producing CP policy recommendations for the EU.

Regulatory

The topics regarding the EU legal framework and data protection directives were discussed in the debriefing sessions of all the pilots and were debated on a round-table with SAG and EEG members. All experts agreed that the topic of data protection is well defined in EU directive 2016/680 which is designed to be consistent with the General Data Protection Regulation. Whereas Police officers as a competent authority, can process personal data for the "prevention of threats to public security" (Article 1), it is not clear at the moment which are the governing rules for use and reuse of data for CP purposes. The fact that the INSEPC^{2}T solution implemented adaptable safeguards for data ageing and the archiving & retention of submitted records is well perceived.

The way forward

The INSPEC^{2}T system aims to combine the principles of CP with the affordances of new technologies. Both the actual and potential utilisation of the resulting incident reporting and management tools (Mob Apps, Public Portal) and crowdsourcing processing modules (GCEP, MMA, CBR, BIA, DWH and DPA - referenced in section 5) have to be compliant with legal frameworks so that they can be correctly implemented in participating countries. This is the biggest challenge for a next generation CP solution.

Taking into account the effects of EU directives[9,10] and legal trends across the EU, could help facilitate the exportation and application of the findings to countries that are not currently participating or associated with the INSPEC^{2}T system (D1.2 End User Requirements – 1st SAG Report, 2016). An advanced CP solution should offer safeguards to ensure Ethical, Legal, Societal and Data protection compliance.

Following the conclusion of the first three pilots, all involved stakeholders value the evolution from a CP solution to a social network system. The proposed solution allowed community members to get in touch with the police, report their problems and observe the police reaction online. At the same time, citizens can create communities to discuss their security concerns and participate in discussions with other community members. All these functionalities empower citizens to join and actively participate in modern CP initiatives. In addition, an intelligent community policing system should be capable of supplementing and feeding existing police operational systems and, if needed, should have the capability to provide facial recognition or offer acoustic event detection to alert operators.

The consortium members acknowledged all of the above and enhanced the solution with new features and improved functionalities. A second testing phase, took place in Groningen (Netherlands) between September and December 2017 and in Preston (UK) in November 2017where all new and enhanced functionalities were tested.

Acknowledgment

The work presented in this paper received funding from the European Commission, under the "H2020-FCT-2014 Ethical/Societal Dimension Topic 2: Enhancing cooperation between law enforcement agencies and citizens - Community policing" call entitled INSPEC^{2}T (Inspiring CitizeNS Participation for Enhanced Community PoliCing AcTions) under grant agreement number 653749.

9 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32016L0680 **(**protection of natural persons with regard to the processing of personal data by competent authorities)

10 http://eur-lex.europa.eu/eli/reg/2016/679/oj (protection of natural persons with regard to the processing of personal data and on the free movement of such data)

References

- Bureau of Justice Assistance, (1994) Understanding Community Policing. A Framework for Action. Washington: U.S. Department of Justice.
- Custers, B., (2012) Technology in policing: Experiences, obstacles and police needs. Computer Law & Security Review, 28 (1), 62-68.
- D1.1 Report on best practices in community policing & gap analysis (2016)
  available online http://inspec2t-project.eu/wp-content/uploads/2017/05/Deliverable-1.1-Report-on-best-practices-in-community-policing-gap-analysis.pdf
- D1.2 End User Requirements – 1st SAG Report (2016)
  available online http://inspec2t-project.eu/wp-content/uploads/2017/05/653749_Deliverable_2_D1.2-End-User-Requirements-1st-SAG-Report.pdf
- D2.1 Social and Cultural Aspects of Community Policing (2015)
  available online http://inspec2t-project.eu/wp-content/uploads/2017/05/653749_Deliverable_4_D2.1-Social-and-Cultural-dimensions-of-INSPEC2T-System.pdf
- D2.2 Legal and Ethical dimensions of INSPEC2T System (2015)
  available online http://inspec2t-project.eu/wp content/uploads/2017/05/653749_Deliverable_5_D2.2-Legal-and-Ethical-dimensions-of-INSPEC2T-System.pdf
- D3.4 2nd SAG meeting report (2016)
  available online http://inspec2t-project.eu/wp-content/uploads/2017/05/653749_Deliverable_12_D3.4-2nd-SAG-meeting-report.pdf
- Docobo, J., (2005) Community Policing as the Primary Prevention Strategy for Homeland Security at the Local Law Enforcement Level. Homeland Security Affairs 1 (1), Article 4.
  available online https://calhoun.nps.edu/bitstream/handle/10945/49819/HSAJ_Summer_2005.pdf?sequence=1&isAllowed=y
- Kelling, G.L., & Bratton, W.J. (2006) Policing terrorism, Civic Bulletin 43, September. New York: Manhattan Institute for Policy Research.
- Leventakis G., Kokkinis G. & Papalexandratos G. (2017) Community Policing Case Studies: Proposing a Social Media Approach. In: Bayerl P., Karlović R., Akhgar B., Markarian G. (eds) Community Policing - A European Perspective. Advanced Sciences and Technologies for Security Applications. Springer, Cham, 139 – 156.
- Myhill, A. (2006) Community engagement in policing: Lessons from literature. Home Office London.
- Peak, K.J., Glensor, R.W. & Gaines, L.K. (1999) Supervising the Police. In: Kenney, D.J. & McNamara, R.P. (eds.): *Police and Policing: Contemporary Issues*. Greenwood, Westport, pp.37-56.

A Virtual Platform to Train Cross-National Police Teams in Team Collaboration and Police-Interviewing

Emma Jaspaert
Geert Vervaeke
Katholieke Universiteit Leuven, Belgium[1]

Diogo Rato
Rui Prada
Ana Paiva
IST Technical University of Lisboa, Portugal

Abstract
Although transnational police collaboration has become increasingly important to effectively fight those crimes that cross borders, training in the necessary skills to achieve good cross-national collaboration and investigation is currently lacking. Indeed, organising trainings with police trainees from different countries is very expensive, time-consuming, and logistically challenging. Therefore, the European Commission is funding the Horizon2020-project 'LAW-TRAIN', in which a virtual training platform is being developed which allows police officers (and judicial authorities) from different countries to train together from their respective locations in the preparation for, and the conduct of, a police interview with a virtual suspect within the context of a transnational investigation. The current contribution will describe the goals and features of this training, the actual training trajectory, and the innovative role of the virtual trainer in achieving a standardized and automated training for police officers all across Europe and beyond.

Keywords: transnational police collaboration; investigative interviewing; PEACE; virtual platform; virtual trainer

Introduction

With the globalization came many benefits, but it also created new opportunities for criminal groups to expand their activities to a transnational level (UNODC, 2012; Vermeulen, 2002; White House, 2011). Although it is of upmost importance that actions are undertaken to effectively combat this type of crimes, the transnational element characterising such crimes makes its investigation, prosecution, and punishment much more complex (UNODC, 2012). To be successful, international police cooperation is crucial, but not easily achieved (Reichel, 2008; UNODC, 2012; Vermeulen, De Bondt & Ryckman, 2012).

Police training in conducting transnational investigations and interviews is challenging. Of course, police officers are usually extensively trained in interviewing within their home country, but these kind of trainings

1 Corresponding author's email: emma.jaspaert@kuleuven.be

tend to focus on basic interviewing competencies rather than team collaboration and the investigation of complex international crimes. Arranging such trainings with people from different countries is often very difficult to organise, time consuming, and expensive. Furthermore, effective training requires follow-up training in the field (Cyr et al., 2012; Lamb, 2016; Lamb et al., 2002), which is almost impossible to realise when it concern a cross-national team of trainees. However, with the past and current societal evolutions, training police to fight transnational crime together is imperative.

Therefore, the Horizon2020-project "LAW-TRAIN"[2] aims at developing a virtual training platform that allows police officers (and judicial authorities) from different countries to train together in the preparation for, and the conduct of, a police interview with a virtual suspect within the context of a transnational investigation. More specifically, LAW-TRAIN intends to train a Joint Investigation Team in conducting suspect interviews within the context of a transnational investigation in drug trafficking. In the present contribution, we will focus on the goals of the training platform, the different elements in the training, the training trajectory, and the way in which feedback is provided to trainees.

Goals of the LAW-TRAIN training

Cross-national investigation in the context of Joint Investigation Teams (JITs), and the interviewing of suspects within these investigations, presents a number of specific challenges, such as establishing a good and fluent collaboration among participants from different countries having different languages and (professional) cultures, and identifying a shared strategy and method of interviewing to reach the goals set forth for the interview (Block, 2008; Kapplinghaus, n.d.). Acquiring the necessary skills and accumulating the necessary experience to perform this sort of multi-national investigations and interviews, in a demanding context in terms of the protection of legal rights and admissibility of evidence, is imperative. For these reasons, LAW-TRAIN sets out two major goals in its training. The first goal is to train transnational team collaboration and decision-making skills (including team coordination). The second goal is to train interviewing competencies.

Training transnational team collaboration skills

The difference between transnational and national investigation and interviewing lies in the much more complex collaboration between police officers from different countries. Most police trainings focus predominantly on the actual execution of the police interview itself, but forget about the collaborative preparation that precedes it. Good and effective team collaboration is nevertheless crucial for conducting successful suspect interviews (Vanderhallen, 2007; Vanderhallen, Vervaeke & Holmberg, 2011).

The transnational element in a Joint Investigation Team makes effective team collaboration more difficult. These teams often consist of team members with different cultural backgrounds (e.g., different nationalities, languages, organizations, professions, habits), who might have different investigation and interviewing practices or styles, and different legal systems and legal requirements. They often have not met before, and therefore were not yet able to establish mutual trust between each other (Peñarroja et al., 2015; Pinjani & Palvia, 2013). In that sense, transnational Joint Investigation Teams of police and judiciary can be categorized as 'ad hoc teams'. Whereas traditional teams are characterized by relatively permanent memberships, ongoing and long-term tasks, routinized reporting relationships within the organisation, close proximity of team members, and good acquaintance between team members (Finholt, Sproull & Kiesler, 1990), ad hoc teams are put together for a particular purpose for a particular (short-term) time frame, consist of members who would otherwise not work together and that will dissolve once the task has been completed (Finholt et al., 1990).

Training police interviewing competencies

The interviewing itself does not really differ between transnational or national contexts. Interviews in both contexts should follow the same procedures and safeguard the same rights of the suspect. However, actual interviewing practices and trainings might differ between (and even within) countries (Walsh et al., 2015). It is possible that different techniques are being taught and used, or that similar techniques are applied differently. Therefore, a big advantage of LAW-TRAIN is the ability to train police officers from different countries in the same 'standardized' interviewing methodology. Within LAW-TRAIN, the choice was made to train police officers using the PEACE-method. This is a method within investigative interviewing that is embedded within the inquisitorial system, which is the predomi-

2 This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No. 653587

nant system in most of continental Europe. The goal of investigative interviewing is not to obtain a confession, but to gather as much truthful information as possible.

It is clear that even experienced police officers can benefit from continuous training in using and applying the correct interviewing method (e.g., Clarke, Milne & Bull, 2011; Walsh & Bull, 2010a; Walsh & Bull, 2010b). Research on actual practices still shows that many police officers do not follow the best practices in investigative interviewing and still treat confessions as their primary goal (Ponsaers, Mulkers & Stoop, 2001; Vanderhallen, 2007; Walsh & Bull, 2010a; Walsh & Bull, 2010b). By creating standardized feedback to train the interviewing competencies of trainees from different countries, based on the PEACE-method, the opportunity will be provided to commence the harmonization of police practices throughout Europe.

Different elements within the LAW-TRAIN virtual training

The training within the LAW-TRAIN virtual platform comprises of four different phases. However, before going in detail into these different phases, it is important to first briefly discuss the different elements within the training.

Actors within the training

There are four different actors present during the training: the human trainer, the virtual trainer, the trainees, and the virtual suspect. Each of these actors has a distinct role within the training.

The human trainer is the person who is responsible for the recruitment of the trainees, the setting up of the training trajectory, and for ensuring the correct procedure during the training trajectory. This will usually be the person who is in charge of national police trainings. Trainees from each country will be under the supervision of their human trainer. Thus, since LAW-TRAIN concerns transnational collaboration, different human trainers will take part in the training. The human trainers will not provide feedback to their trainees during the training trajectory. They will observe the training and will give feedback to their own trainees after the completion of the training.

The *virtual trainer* is a virtual character that will give systematic and standardized feedback to the trainees at certain stages throughout the training trajectory. He will also assist trainees and human trainers when they are having technical difficulties. Although the virtual trainer will be able to intervene during the different phases of the training trajectory, he will predominantly provide feedback in the final stages of the training. His feedback will focus on the assessment of the team collaboration and decision-making and how each individual trainee has performed within the team, and on the interviewing skills of each trainee.

The *trainee* is the person that will be trained with the training platform. The training is aimed at police officers who already have experience with interviewing suspects. Prior experience in transnational investigations is not required, although it is preferred. A further distinction needs to be made between active and observing trainees. Active trainees are those trainees who will actively participate throughout the complete training trajectory. The number of active trainees within one training trajectory will be limited to one or two per human trainer. Observing trainees are those trainees that will only observe the training of the active trainees (although they will also be active in the first phase of the training). Trainees can also learn a lot by observing others (Mayes et al., 2001; Silberman, 2006). They will also help in collecting information concerning the performance of the active trainees by filling out observation forms, allowing for peer feedback to the active trainees. Using these forms also helps the observing trainees to focus on the critical features in the training (Silberman, 2006). There is no limitation to the amount of observing trainees within a training trajectory.

Finally, the *virtual suspect* is the virtual character that will be interviewed by the trainees. There is the option to choose either a male or a female virtual suspect. The virtual suspect will reply to the questions asked by the interviewers. The way he replies to the questions and the information that he will share, will depend on the quality of the questioning.

Rooms within the training trajectory

Besides distinguishing between the actors that will take part in the training, it is also necessary to differentiate between the 'rooms' that are available. There are three different rooms that need mentioning: the videoconferencing room, the virtual interview room, and the control room.

The *videoconferencing room* is an important room within the training, since this will be the place where the trainees from different countries will meet virtually and discuss the issues that need to be settled before starting the actual interview with the virtual suspect. A videoconferencing tool has been built within the LAW-TRAIN platform, so trainees can communicate with each other and at the same time enter certain decisions made during this discussion into the system.

The *virtual interview room* is the room where the active trainees will be able to interview the virtual suspect. The virtual room can be customized by the trainees. The virtual suspect will be seated in this virtual room and the active trainees will be able to question him. The trainees will have to option to include a 'virtual lawyer' in the virtual interview room. At the moment, the virtual lawyer will be a static character that will not be able to intervene during the interview.

The last room is the *control room*. In this room, active trainees who are not interviewing the suspect and observing trainees can watch what happens inside the interview room. Active trainees will be able to chat with each other, observing trainees will not. From the control room, active trainees can easily go to the interview room when it is their turn to interview the suspect.

The LAW-TRAIN training trajectory

The training trajectory consists of four different phases: the individual preparation phase, the joint preparation phase, the actual interview phase, and the debriefing phase. The first two phases relate to the first phase in the PEACE-method, namely 'Preparation'. These two phases also relate to the first training goal: training transnational collaboration and decision-making skills. The third phase relates to the 'EAC' in PEACE, which are the phases within the actual police interview (i.e., 'Engage and Explain', 'Account, Clarification, and Confrontation', and 'Closure'). This phase also relates to the second training goal: training interviewing competencies. Finally, the fourth phase relates to the final phase in PEACE, the 'Evaluation'.

The individual preparation phase

In the first phase, each individual trainee will be able to thoroughly study and understand the case, before starting the preparation for the interview. All trainees (both active and observing) get access to the case file on the platform. This case file contains police information about the suspect and his activities in a possible drug trafficking organization. They can read the documentation, make notes, assign labels to the information (e.g., evidence, relevance), and save important pieces of information in their personal library. Not every trainee will have access to the same information in the case file. Some of the information will only be accessible to trainees from a particular country, as some of the evidence has been collected nationally, prior to the formation of the JIT. This way, sharing of information in subsequent phases is stimulated.

One trainee will be assigned as 'team coordinator'. This trainee is responsible for coordinating the next phase in the training, the joint preparation phase. During the individual preparation phase, the team coordinator will therefore have the additional task to prepare the agenda for the joint meeting (in the joint preparation phase). This agenda contains some fixed agenda points: introduction of team members, discussion of the case and exchange of information, determining the goals of the interview, evaluation of legal procedures and the admissibility of evidence, and preparation of the interview. The team coordinator will also be able to add additional agenda points. It is advised that the team coordinator already prepares some of the agenda points, for example by investigating the legal procedures that have to be followed.

The joint preparation phase

Once all trainees have completed their individual preparation, they move to the joint preparation. Here, they will all enter into a videoconference meeting, which is embedded into the LAW-TRAIN platform. All the trainees can enter the videoconference, but only the active trainees will be able to communicate with each other. During the videoconference, all the team members will be able to view the agenda prepared by the team coordinator. The team coordinator will lead the meeting and make sure that each agenda point is dealt with. For each agenda point, the team coordinator will have to insert some decisions made by the team into the system. Each of these decisions needs to be confirmed by all the active team members before it is officially logged into the system. This is a safeguard to guarantee that all the team members agree with the decisions entered. The virtual trainer will provide immediate feedback to these decisions (cfr. infra).

The actual interview phase

Once the team is prepared, they move on to the actual interview phase. During this phase, trainees will interview a virtual suspect in the interview room. Only one or two active trainees at a time can interview the suspect. The rest of the trainees (the other active trainees and all the observing trainees) will follow the interview from the control room. The active trainees in the control room will be able to communicate with each other via chat. Observing trainees will not be able to participate in the conversations. During the interview, the system will log several elements that will allow the virtual trainer to assess the quality of the interview and to provide feedback afterwards (cfr. infra).

The debriefing phase

When the actual interview phase has finished, the active trainees will be forwarded to the debriefing phase. In this phase, the virtual trainer will provide descriptive information, accompanied with feedback, on both the individual performance of the trainee during the preparation phases and the interview phase and on the team performance during the joint preparation and the interview. All the active trainees will be able to see the same team performance feedback, but will only be able to view their own individual feedback (not the individual feedback of other trainees).

Innovations of LAW-TRAIN

Focus on training team collaboration in a transnational context

LAW-TRAIN offers the opportunity to train police investigators in interviewing in a transnational context. In such a transnational context, the interview itself does not differ a lot from interviewing in a national context. The difference lies more within the more complex collaboration between team members from varying nationalities, with different habits and interview practices, and without a previously established trust between team members. Such collaborations are thus not straight-forward, yet no training program exists to prepare police investigators for these kinds of collaboration. LAW-TRAIN advances in the current state of art in police training by developing an additional, yet important, phase in the training trajectory that is specifically focused on the training of transnational collaboration (i.e., joint preparation phase). Including this phase in the training not only allows for police investigators to practice this type of collaboration, but also for further research to learn more about ad hoc virtual transnational police teams, how they function, and which elements can differentiate between effective and less effective team collaboration.

Ability to provide standardised and automated feedback

Interviewing practices trained in different countries can vary, even if they are based on the same fundamental principles. If a transnational team is being trained in interviewing, it is thus important that everybody receives the same feedback, and that trainees are not confused by differing or even contradicting feedback from different trainers during the training. Thus, LAW-TRAIN proved to be the ideal ground to explore the opportunities that arise from having a virtual training system. It allows to install, test, and validate standardized quantitative parameters that are able to predict positive interview performance.

Most of the current assessments of interviewing quality are based on self-reports, peer-evaluations or observation schemes. These assessments are thus all of a subjective nature and can differ depending on the person who does the assessment. It not only impedes standardization of practices and training across countries, but even within countries. Given the fact that LAW-TRAIN offers a virtual interview training platform, every action of the trainee can be extracted by the system. The system can as such 'log' all the activity of all the trainees during the training. Since there is little to no literature on how to quantify interview performance, possible parameters that might provide useful information on the quality of the interview were selected based on existing observation schemes and literature on the best practices in investigative interviewing and the PEACE-method. The system is then programmed as such that it collects the relevant information to provide results for these parameters. This allows for immediate presentation of performance parameters to the trainees. Since there are no norms and standards already available for these parameters, the feedback given to the trainees based on these parameters is mostly descriptive. However, LAW-TRAIN provides the innovative opportunity to systematically collect data through the continuous use of the LAW-TRAIN training system to further assess if, and to what degree, each of these parameters is truly able to differentiate between good and not-so-good performances, and to develop norms and standards for the quantitative parameters that have proven to be predictive for performance.

In what follows, we will further elaborate on the way information on the performance of the trainees is extracted by the system and is presented to the trainees by the virtual trainer.

The Virtual Trainer of LAW-TRAIN

To ensure that the training of all trainees in LAW-TRAIN follows the same methodology – and as such receive a uniform, standardized training – a Virtual Trainer (VT) was developed. The VT is a central part of LAW-TRAIN and, as an Intelligent Pedagogical Agent, aims at improving the training by providing suggestions as well as details on the given feedback (Soliman & Guetl, 2010).

The Virtual Trainer is built over the classical architecture of an Intelligent Tutoring System (ITS), which are computer systems with intelligence aimed at providing tutoring and training of a specific topic, usually without the intervention of a human tutor (Freedman, Ali & McRoy, 2000). In the context of serious games, researchers found that in ITS it is important to trace the user's activities and necessary to measure performance based on learning goals instead of the game completion (Baalsrud et al., 2014; Serrano-Laguna et al., 2014; Shoukry, Göbel & Steinmetz, 2014). Taking these findings into account, we designed the Virtual Trainer to monitor all the trainees' actions by logging their interactions with all the actors of the training in the platform. The VT then provides live feedback to the trainee as soon as the actions are registered or a detailed debriefing report at the end, grouped according to the two training goals.

To provide feedback both on the team collaboration skills and the interviewing competencies, the Virtual Trainer must log and analyze the training session from an individual trainee's point of view and from a team perspective. The need of the VT's supervision on these two levels is emphasized by previous work that shows the effectiveness of ITS in improving individual learning (Tchounikine, Rummel & McLaren, 2010), and its potential for collaborative learning has also been highlighted (Walker, Rummel & Koedinger, 2009).

The role of the Virtual Trainer

The Virtual Trainer is one of LAW-TRAIN's actors. It is a virtual entity that "exists" on the platform and is continuously supervising all the trainees' actions based on their interactions on the platform. The feedback and explanations given are personalized for each trainee. This customization allows for different levels of guidance that can be adjusted to the expertise of each police officer. However, despite adapting its feedback to the user, the introduction of the Virtual Trainer in LAW-TRAIN creates an opportunity to provide standardized feedback to all trainees across multiple countries and police agencies.

The goal of the Virtual Trainer is not to grade or judge the trainees' performance. Its role in the platform is mainly to assist the trainees during the training trajectory and to give feedback about their performance in order to support the review process between trainee and human trainer afterwards. During the training itself, the VT identifies mistakes that might compromise or even nullify the entire information gathering process and allows the trainee to immediately fix these mistakes. In the debriefing phase, the VT helps inspect the training session and highlights relevant areas of the session to increase the efficiency of the review process.

Endowing the Virtual Trainer with these intelligent capabilities creates an autonomous agent that tutors a trainee in a long and complex training trajectory, a task that is not easily done by a Human Trainer. But the addition of this virtual entity doesn't mean the human trainer is removed from the process. In the review process of the training session, the role of the VT is to create an environment that not only helps the self-evaluation of the trainee but also promotes the joint inspection and discussion of the training with the Human Trainer, therefore combining the VT's capabilities with the expertise of a police officer.

In conclusion, the Virtual Trainer's role is to supervise the performance of each trainee, identify critical mistakes when necessary and provide the tools to analyze the training session, adapting the feedback to each platform's user.

Interventions

The Virtual Trainer needs to adapt its feedback throughout the training sessions. Therefore, three distinct types of interventions are defined, based on the different phases of the training session and the type of feedback: Active Intervention, Debriefing Reports, and Interface Help.

The first type of intervention, *Active Intervention*, is associated with the reactive feedback of the Virtual Trainer. During the training session, the VT identifies errors or mistakes caused by the trainee's actions and displays either a critical error or a warning message. The first message type, critical error, is used when the trainee's action will render the information gathered in the interview inadmissible in court, by for example not presenting the suspect's rights before asking investigative questions. The second message type, warnings, is used when the trainee's actions might lead to critical errors in the future. To process the trainee's actions and generate the proper feedback, the Virtual Trainer uses a rule-based approach. The rules used are inspired by the best practices according to the PEACE-method and they are tested every time the trainee performs a new action in the platform. For instance, when a trainee asks an aggressive question to the interviewee, the Virtual Trainer presents a warning. To do so, the VT handles the question and verifies that the aggressive questions rule is triggered. Then, the VT generates a warning that is displayed to the trainee. Upon asking multiple aggressive questions, the same rule is triggered, but the VT intensifies its intervention by displaying a critical error due to the persistent aggressive stance of the interviewer.

The second type of intervention is the *Debriefing Reports*. As the name states, they are presented in the last stage of the training trajectory. In LAW-TRAIN's platform, the trainee and human trainer have several tools and charts to help them review their performance. However, inspecting the whole training session might be a complex procedure. The VT intervenes in the Debriefing Reports by highlighting the trainee's actions that might be relevant to review more closely (with the human trainer). The Debriefing Reports are grouped by Training Phase and they allow the inspection of the training from different perspectives, such as the interviewing style, the topic coverage or compliance to the PEACE method. By identifying these areas worth reviewing, the VT can facilitate systematic inspection of all the actions performed by the trainee and is able to suggest 'working points' that might require further inspection. To identify these areas, the Virtual Trainer relies on a set of patterns that are often associated with questionable practices. For instance, in the PEACE method, it is advised not to change topics too quickly during the first phases of the interview. By using a graph to display the question topic distribution during the interview, the VT looks for sequences of questions with multiple topics associated and highlights them for review.

The last intervention is the *Interface Help*. This type of intervention provides further information about the methodology that is trained. The Virtual Trainer focuses on exploring the theoretical background underlying each chart in the Debriefing Reports and how it should be used. This authored help is integrated into the platform and can be consulted at any moment without leaving LAW-TRAIN, creating a seamless flow of interaction, therefore improving the learning trajectory of the trainees.

Conclusion

Although the LAW-TRAIN virtual training tool will need further development to become a marketable product, its advantages are already clear. From the perspective of the police, this training tool will allow for continuous training in transnational collaboration and interviewing, an area in which training opportunities are currently scarce. The ease with which international training groups can be formed and the much lower cost and logistics it will require to train these teams, will improve future transnational collaboration in order to more effectively fight transnational crime. From the perspective of the European Union, LAW-TRAIN can facilitate the standardized training of interviewing practices across borders, which will help the European Union move towards a European Security Model. From a research perspective, collecting data through the LAW-TRAIN platform can reshape our knowledge and expertise on team collaboration and police interviewing tremendously. Being able to collect and automatically analyse multiple interviews will provide an abundance of information on interviewing practices (and how they differ between countries) and will allow us to analyse the descriptive information to determine more quantitative norms and standards to assess interview quality. Furthermore, LAW-TRAIN also provides the opportunity to learn more about effective team collaboration, communication and decision-making within the context of law enforcement. Research in that field has until now been scarce, yet good team collaboration is crucial to be well prepared to conduct a police interview, and a good preparation has proven to be an important predictor for a good interview. In sum, the more data that will be collected with LAW-TRAIN, the more researchers will be able to advance in the field of police collaboration and police interviewing.

References

- Baalsrud Hauge, J., Berta, R., Fiucci, G., Fernandez Manjon, B., Padrón-Nápoles, C., Westra, W. & Nadolski, R. (2014) Implications of learning analytics for serious game design. In: *Advanced Learning Technologies (ICALT), 2014 IEEE 14th International Conference on Advanced Learning Technologies*. pp. 230-232.
  Available from: doi:10.1109/ICALT.2014.73
- Block, L. (2008) Combating organized crime in Europe: practicalities of police cooperation. *Policing*. 2 (1), 74-81.
  Available from: doi:10.1093/police/pan009
- Clarke, C., Milne, R. & Bull, R. (2011) Interviewing suspects of crime: the impact of PEACE training, supervision and the presence of a legal advisor. *Journal of Investigative Psychology and Offender Profiling*. 8, 149-162.
  Available from: doi:10.1002/jip.144
- Cyr, M., Dion, J., McDuff, P. & Trotier-Sylvain, K. (2012) Transfer of skills in the context of non-suggestive investigative interviews: impact of structured interview protocol and feedback. *Applied Cognitive Psychology*. 26, 516-524.
  Available from: doi:10.1002/acp.2822
- Finholt, T., Sproull, L. & Kiesler, S. (2011) Communication and performance in ad hoc task groups. In: Galegher, J., Kraut, R. E., & Egido, C. (eds.) *Intellectual Teamwork: Social and Technological Foundations of Cooperative Work*. New York, Psychology Press, 291-325.
- Freedman, R., Ali, S. & McRoy, S. (2000) Links: what is an intelligent tutoring system? *Intelligence*. 11 (3), 15-16.
  Available from: doi:10.1145/350752.350756
- Kapplinghaus, J. (n.d.) *Joint Investigation Teams: Basic Ideas, Relevant Legal Instruments and First Experiences in Europe*. Visiting Experts' Paper from the 134th International Training Course.
  Available from: http://www.unafei.or.jp/english/pdf/RS_No73/No73_07VE_Kapplinghaus2.pdf [Accessed: 21st June 2017]
- 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*. 71 (8), 710-718.
  Available from: doi:10.1037/amp0000039
- Lamb, M., Sternberg, K. J., Orbach, Y., Hershkowitz, I., Horowitz, D. & Esplin, P. (2002) The effects of intensive training and ongoing supervision on the quality of investigative interviews with alleged sex abuse victims. *Applied Developmental Science*. 6 (3), 114-125.
  Available from: doi:10.1207/s1532480xads0603_2
- Mayes, T., Dineen, F., McKendree, J. & Lee, J. (2001) Learning from watching others learn. In: Steeples, C. & Jones, C. (eds.) *Networked Learning: Perspectives and Issues*. London, Springer, pp. 213-227.
- Peñarroja, V., Orengo, V., Zornoza, A., Sánchez, J. & Ripoll, P. (2015) How team feedback and team trust influence information processing and learning in virtual teams: a moderated mediation model. *Computers in Human Behavior*. 48, 9-16.
  Available from: doi:10.1016/j.chb.2015.01.034
- Pinjani, P. & Palvia, P. (2013) Trust and knowledge sharing in diverse global virtual teams. *Information & Management*. 50 (4), 144-153.
  Available from: doi:10.1016/j.im.2012.10.002
- Ponsaers, P., Mulkers, J. & Stoop, R. (2001) *De Ondervraging: Analyse van een Politietechniek* [The interview: analysis of a police technique]. Antwerp, Maklu.
- Reichel, P. L. (2008) *Cross-National Collaboration to Combat Human Trafficking Learning from the Experience of Others*. U.S. Department of Justice.
  Available from: https://www.ncjrs.gov/pdffiles1/nij/grants/223286.pdf [Accessed: 8th July 2017]
- Serrano-Laguna, Á., Torrente, J., Moreno-Ger, P. & Fernández-Manjón, B. (2014) Application of learning analytics in educational videogames. *Entertainment Computing*. 5 (4), 313-322.
  Available from: doi:10.1016/j.entcom.2014.02.003
- Shoukry, L., Göbel, S. & Steinmetz, R. (2014). Learning analytics and serious games: trends and considerations. In: *Proceedings of the 2014 ACM International Workshop on Serious Games*. 21-26.
  Available from: doi:10.1145/2656719.2656729
- Silberman, M. L. (2006) *Active Training: A Handbook of Techniques, Designs, Case Examples, and Tips*. 3rd ed. San Francisco, Pfeiffer.
- Soliman, M. & Guetl, C. (2010) Intelligent pedagogical agents in immersive virtual learning environments: a review. In: *MIPRO, 2010 Proceedings of the 33rd International Convention*. 827-832.
  Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5533534

- Tchounikine, P., Rummel, N. & McLaren, B. M. (2010) Computer supported collaborative learning and intelligent tutoring systems. In: *Advances in Intelligent Tutoring Systems.* 308, 447-463.
  Available from: doi:10.1007/978-3-642-14363-2_22
- UNODC (2012) *Manual on Mutual Legal Assistance and Extradition*. New York, United Nations.
- Vanderhallen, M. (2007) *De Werkalliantie in Het Politieverhoor* [The working alliance during a suspect interview]. Leuven, KU Leuven.
- Vanderhallen, M., Vervaeke, G. & Holmberg, U. (2011) Witness and suspect perceptions of working alliance and interviewing style. *Journal of Investigative Psychology and Offender Profiling*. 8 (2), 110-130.
  Available from: doi:10.1002/jip.138
- Vermeulen, G. (2002) New developments in EU criminal policy regarding cross-border crime. In: van Duyne, P. C., von Lampe, K., & Passas, N. (eds.) *Upperworld and Underworld in Cross-Border Crime*. Nijmegen, Wolf Legal Publishers, pp. 115-140.
  Available from: http://cross-border-crime.net/freecopies/CCC_freecopy_2002a_UpperworldAndUnderworld.pdf [Accessed: 18th June 2017]
- Walker, E., Rummel, N. & Koedinger, K. R. (2009) Integrating collaboration and intelligent tutoring data in the evaluation of a reciprocal peer tutoring environment. *Research and Practice in Technology Enhanced Learning*. 4 (3), 221-251.
  Available from: doi:10.1142/S179320680900074X
- Walsh, D. & Bull, R. (2010a) What really is effective in interviews with suspects? A study comparing interviewing skills against interviewing outcomes. *Legal and Criminological Psychology*. 15, 305-321.
  Available from: doi:10.1348/135532509X463356
- Walsh, D. & Bull, R. (2010b) Interviewing suspects of fraud: an in-depth analysis of interviewing skills. *The Journal of Psychiatry & Law*. 38, 99-135.
  Available from: doi:10.1177/009318531003800106
- Walsh, D., Oxburgh, G. E., Redlich, A. D. & Myklebust, T. (2015) *International Developments and Practices in Investigative Interviewing and Interrogation. Volume 2: Suspects*. London, Routledge, Taylor & Francis.
- White House (2011) *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*.
  Available from: https://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf
- Vermeulen, G., De Bondt, W. & Ryckman, C. (2012) *Rethinking International Cooperation in Criminal Matters in the EU: Moving Beyond Actors, Bringing Logic Back, Footed in Reality.* IRCP research series, volume 42. Antwerp, Maklu.

The TARGET Project: Using VR and AR to improve police training

Lola Vallès
Alicia Moriana
Rotger Garcia
Police School of Catalonia, ISPC, Spain[1]

Abstract
This paper aims to provide an outline of an ongoing research project that is funded by the H2020 programme, the TARGET: Training Augmented Reality Generalised Environment Toolkit. The project addresses the need for innovative serious gaming solutions for police and other security agents to train in low probability/high impact events. The ambition of the project is to deliver a pan-European serious gaming platform that combines Mixed, Virtual and Augmented Reality and content for training, and also incorporates a system to assess the skills and competencies of trainees. In addition, the paper provides a description of the technology components and of the six training content scenarios that TARGET has developed up to now.

Keywords: Innovation, training, virtual reality, augmented reality, scenarios

Introduction

H2020 programme

Horizon 2020 is the biggest EU Research and Innovation programme ever, with nearly €80 billion of funding available over seven years (2014 to 2020) – in addition to the private investment that this money will attract (European Commission, 2018). The programme aims to help addressing the main social challenges, promote industrial leadership in Europe and reinforce the excellence of its scientific base.

Within this programme the TARGET project was funded. TARGET stands for *Training Augmented Reality Generalised Environment Toolkit* and it responds to the FCT-07-2014 Framework entitled « Law enforcement capabilities topic 3: Pan European platform for serious gaming and training ». It began in May 2015 and will end in October 2018. It received 6 million euros in funding from the Research Executive Agency (REA) of the European Commission.

1 Corresponding authors' email: lvalles@gencat.cat

The TARGET project was designed to help Security Critical Agents [2](SCA) to:

- engage effectively with the general public;
- minimise risk to SCA and citizens;
- optimise use of available resources (pan-European collaboration);
- use existing tools, systems, and equipment already available at user sites;
- enable SCA to train for low probability / high consequence scenarios (such as a cyber-attack or CBRN incident);
- leverage virtual reality in order to optimise cost effective of current training programmes (importantly, reduce the number of trainers needed for a scenario, saving time and resources);
- empower Security Critical Agents to effectively use new technologies developed in collaboration with the technical partners in the consortium.

The TARGET Consortium

The TARGET consortium brings together sixteen partner organisations from nine EU member states. The consortium gathers the expertise of major users, leading edge technologists and best-of-class experts in technology assessment, dissemination, ethics, security sensitivity and project management. The project is coordinated by the international management services firm ARTTIC, with technical coordination by Luxembourg Institute of Science and Technology (LIST).

As we can see in Figure 1 there are three different groups of partners. In the first place, we see partners responsible for coordination, communication and ethic review. In the second place, there are partners responsible for the technology development. Finally, there are partners who are in charge of developing realistic and useful training contents. The Police School of the Institute for Public Security of Catalonia (ISPC) belongs to the third group that reunites other police research and training institutions, namely from France, l'Ecole Nationale Supérieure de Police (ENSP) at Lyon; from Germany, the Fachhochschule der Polizei des Landes Brandenburg (FHPOLBB) and the German Police University (DHPOL) at Münster; from Estonia, the Estonian Academy of Security Sciences (EASS). Other end-users included in the consortium are the Spanish Police Guardia Civil (GUCI); the Cleveland Fire Brigade (CFB) from the UK and the International Security and Emergency Management Institute (ISEM) of Slovakia.

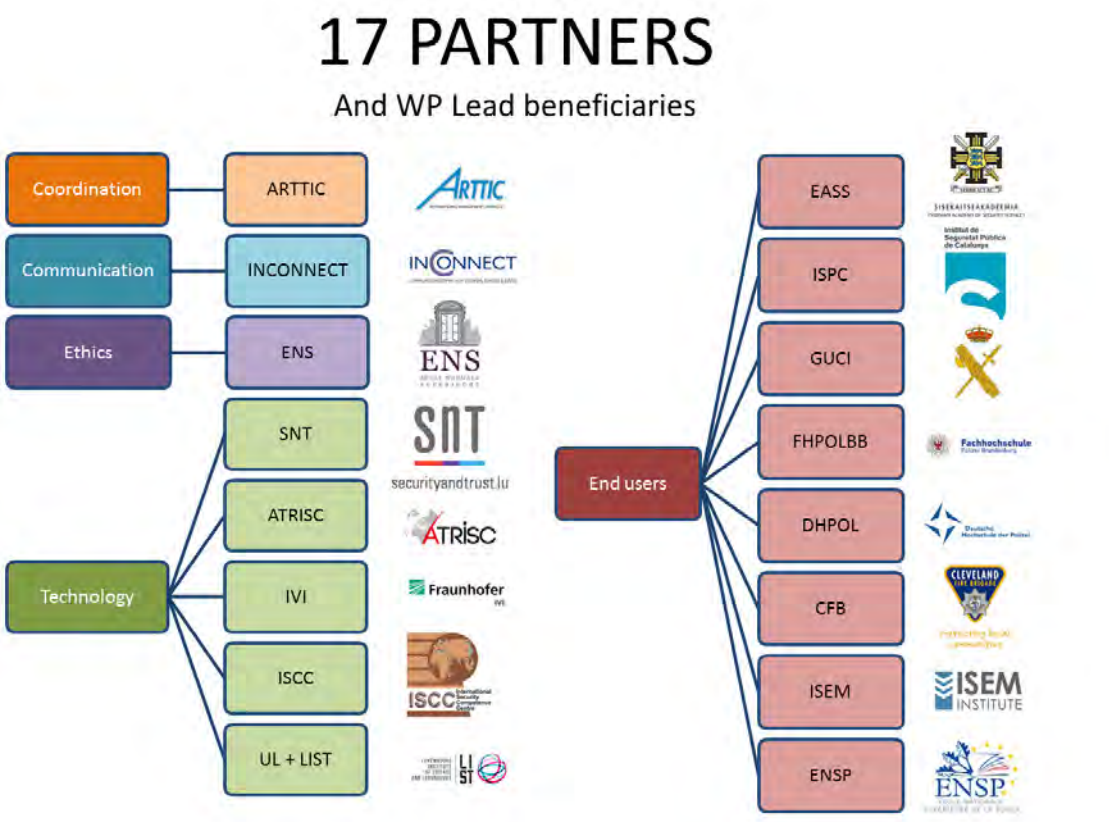
Besides the TARGET consortium there is a group of experts, the TARGET Advisory Board (TAB), who meet regularly with the consortium throughout the project. They provide technical, ethical and legal guidance, input and feedback on the TARGET technology roadmap. The TAB also advices on links with relevant interest groups outside TARGET and propose and encourage the potential interactions of the project with other projects, initiatives or activities.

Aims of the project

The project aims to enable effective Security Critical Agents training by developing pan-European training content through six training scenarios that will be developed in the course of the project. On top of that it will foster a TARGET marketplace in order to buy/sell what is available on the TARGET platform as well as associated TARGET products and services. The TARGET platform consists of architecture, development environment, technology components and a store with training content. The first version of the TARGET is already completed and has been tested at the users' sites.

2 Security Critical Agents (SCA) include all security forces such as counterterrorism units, border guards and armoured car guards, first responders such as police, fire fighters, paramedics, civil security agencies and operators of critical infrastructures.

Figure 1: Partners and their role at TARGET consortium

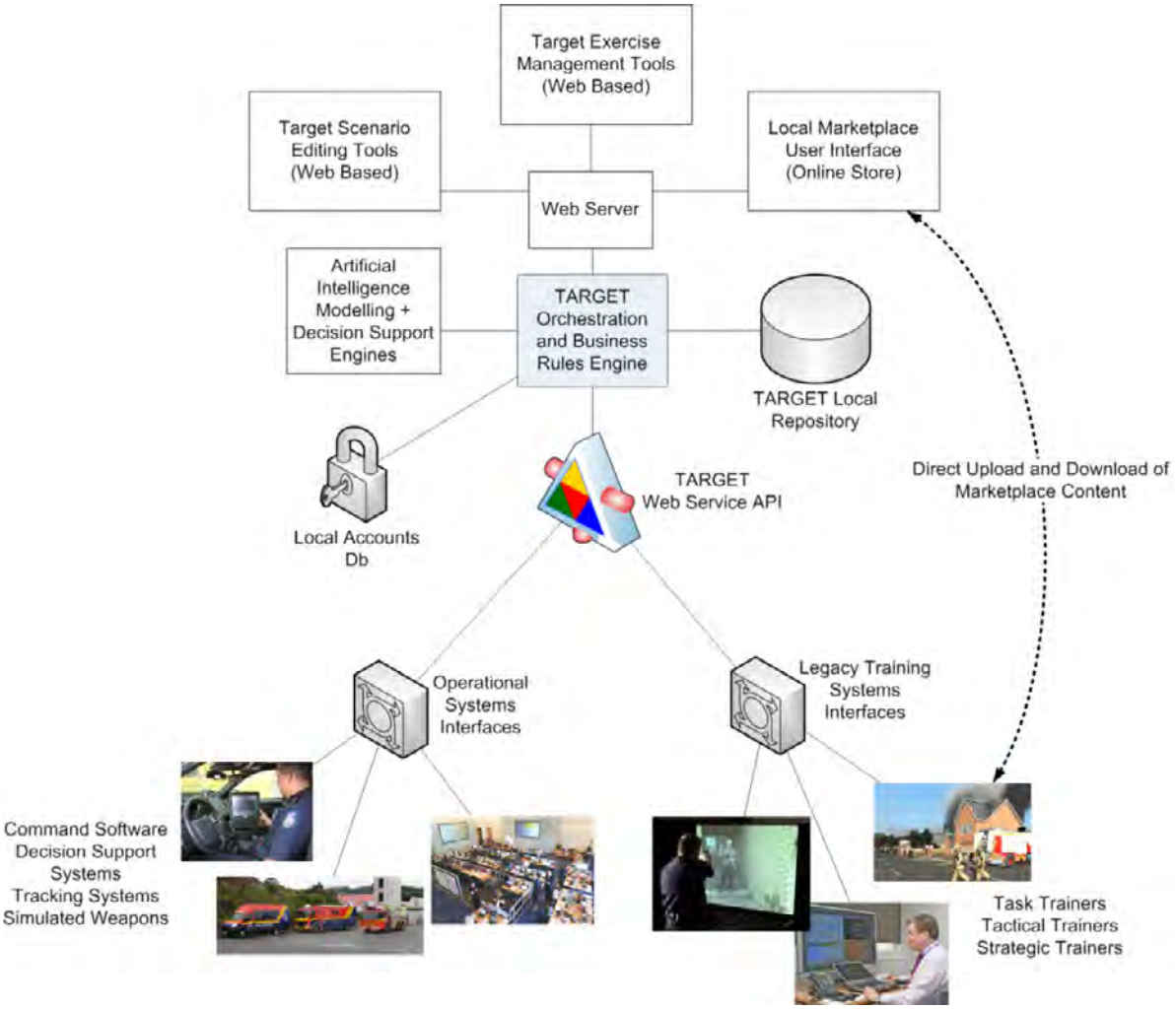


Pan-European Platform

The TARGET pan-European Platform for hybrid serious gaming includes training case development tools, standard interfaces, effective integration for third party technologies and content, support for content and technology sharing, licensing and payment.

The Platform will be customisable into local languages, legal contexts, organisational structures, existing IT systems, ensuring personalised scenarios and technologies which are useful and relevant to the user organisation.

Figure 2: TARGET System Architecture Diagram



Technology components

The TARGET Platform supports the design of training narratives, corresponding scenarios and role players, the collaborative training activity, as well as the assessment of competencies developed in TARGET. The TARGET narration builder incorporates a library of virtual threat scenarios for 3D virtual reality training and augmented reality training.

The TARGET technology components cover a number of external systems, including third party simulation systems and third party operational systems, which will be integrated into the system via the TARGET training web Application Programming Interface (API) as seen in figure 2. It includes real world command and control systems or already existing training environments, real world modelling engines (chemical plumes, power grids, or wildfires) and links to already consolidated training systems. Therefore, the TARGET system communicates directly with existing systems, and augmented and virtual environment support which can be integrated into legacy systems[3] by the TARGET API.

Training scenarios

The training content scenarios are used to improve the platform and to demonstrate it to third parties. They respond to specific needs for training law enforcement agencies (LEA) and Security Critical Agents, infrastructure operators and crisis managers. They address complex needs concerning technical skills, operational management, social (communicating with the public) and ethical issues (making the « sound » decision). The training content scenarios are led and defined by end-users from six European member states and some involve multi agency cross-border collaboration, in

3 A legacy system is an old method, technology, computer system, or application program, in other words, it is a previous or already existing computer system.

particular those related to cyber-attack and road accidents which are scenarios three and six.

The training environments of the scenarios are as realistic as possible by combining Augmented Reality (AR) and Mixed Reality (MR). They are flexible and use existing equipment of user organisations. The individual and team performance is recorded in real time and pluggable to any simulation platform. Finally, the MR environments improve the field of pervasiveness, use real world environments (existing training facilities) as effective as possible, and provide capability to assess fundamental human behaviour. The six scenarios are described in the chapter "Scenarios".

Assessment

To ensure best practices, TARGET is testing both the platform and the training content scenarios in dedicated sessions including single user and team sessions. The purpose of these trials is to improve the platform and the training content's iteratively through trial and learning. It encompasses:

- Train the trainers to prepare them to customise the scenarios to the local context, dispense and administer the serious gaming-based training to selected end-users.
- Customisation of specific usage contexts (language, legacy systems …) to ensure that the TARGET environment will be truly generic and customisable to the particularities of different EU member states and, more generally, be competitive in the global market place.
- Comparison of experiences in different cultural and organisational settings to develop best practices, some of them generic, others more specific to particular organisational categories.
- Security Critical Agents training as such.
- Evaluation of the results and feedback to the developers of the platform.

Dedicated European ecosystem

The TARGET project intends to have a significant impact by becoming the European ecosystem for European Security Critical Agents training. It intends to be a hub with easily sharable scenarios and serious games which can be modelled to local specifications. It will provide training tools for police officers, fire brigades, civil protection officers and other security professionals. In this way, it will build capacities of Security Critical Agents and contribute to EU member state security by supporting the fight against national and transnational crime.

The cornerstone of this strategy will be the set-up and development of a heterogeneous TARGET Community including practitioners-users (Security Critical Agents), their trainers, scenario providers, technology suppliers and policy makers.

Challenges of serious gaming

Nowadays Security Critical Agents are mostly carrying out virtual reality (VR) training based on "video jukebox" solutions in classroom environments. However, these solutions tend to be neither immersive nor non-linear, therefore a workaround has to be used to present to the participants the missing information. This is typically provided by the trainer taking up too much time and attention and deteriorating the evaluation (Vidal, 2011).

A possible solution for this problem can be found on VR environments. Nevertheless, those can suffer from a number of specific pitfalls: lack of maturity of the simulation models, much of the interaction within a 3D visualisation is either or is effectively puppeteered by human operators, substituting for the lack of modelling and simulation. This results in either a linear and uninvolved scenario, or huge loads on human operators having to deliver inconsistent, non-repeatable and expensive experiences. In many cases integration with existing equipment is very limited. Most training centres do not even have the adequate equipment or are designed to train only one command tier at a time. As such, they are less than immersive in their nature and tend to support only a scripted route through a particular scenario.

In addition, content dealing with social and ethical issues is generally weak. Tactical, operational and strategic decisions influence - often instantly - public opinion and behaviour. In training and exercises this influence is hardly recognised or visible. This is in spite of the increasing recognition of the importance of an effective Security Critical Agents-citizenry interface, be it to engage directly with citizens, to communicate through the media or to make difficult ethical decisions affecting individuals or groups of citizens.

Finally, the cost of developing new serious game-contents can be very significant and such investment is often subject to difficult cost-benefit trade-offs. Sharing tools, contents and best practices across different target Security Critical Agents populations, international borders and training situations would represent a significant advancement in this area, but is either ad-hoc or simply not done. A pan-European serious gaming repository for Security Critical Agents is a major step forward to support the implementation and evolution of EU policies in this field.

TARGET wants to be a turning point in VR/MR Security Critical Agents training providing a solution with the following characteristics: non-linear and immersive scenarios; able to be carried out with real tools and taking into account social and ethical issues.

The specific challenges to the TARGET project include:

- Taking experimental approaches of photogrammetry and the EU-wide geospatial dataset and merging them into a useable solution.
- Devising and implementing a simulation service that allows pre-existing decision support tools and modelling technology to be added and integrated flexibly.
- Devising easy-to-use toolsets to combine exercise snippets into rule clusters that make up a simulation.
- Providing multilingual capabilities and localisation of scenarios to local languages throughout the system.
- Supporting localisation to adapt to command & control structures and procedures, and to easily connect local classified content.

Scope of the TARGET platform

TARGET delivers an extremely realistic and flexible Augmented and Virtual Reality (AVR) simulation solution, incorporating a range of dynamic and variable scenarios. Trainees use a combination of both real and training weaponry, radio equipment, command and control software, decision support tools, real command centres and vehicles (Munro, 2017). This leads to improving the field of pervasiveness within MR by effectively using the real-world environment and its objects, and by exploring fundamental human behaviour within MR environments. TARGET facilitates new tools for joint training for police interventions with a variety of agencies.

Social and ethical content also plays an important role throughout all aspects of the project. The project supports inter-agency Security Critical Agents exercising across the EU and acts as a serious gaming repository and brokerage facility for authorised agencies to share training material and maximise re-use and efficiency in delivering complex exercises. Mixed Reality experiences immerse trainees at operational, tactical and strategic command levels with scenarios that include tactical firearms events, asset protection, mass demonstrations, cyber-attacks and CBRN (Chemical, Biological, Radiological, Nuclear) incidents (Munro, 2017).

The vision of the project is to make the TARGET Open Platform the reference for Security Critical Agents training using serious gaming across Europe creating a much needed hub for the sharing of training content and serious games that can be quickly modelled to local specifications within the European Union. A multi-language, online exercise creation and management tool will be available, allowing agencies throughout Europe to use the training content. Special support will also be provided to translators to assist the creation of local language versions of the training content modules.

TARGET covers a huge range of current European training needs. This is possible with the participation of end-users, Security Critical Agents training professional organisations, which advise technological partners in scenario edition and needs assessment. Needs Assessment reflect the real needs of TARGET trainees/end users, as well as the needs of the relevant end-user organisations. End-users have provided deep needs-analysis, which has helped them to build the efficient training content.

Scenarios

TARGET has developed six training content scenarios based on the requirements capture phase, the key training objectives and MR components. Training issues were also taken into account, the number and roles of the people involved and their interaction and interconnection throughout the command structure. It also identified the real objects and tools required,

training evaluation processes, social media injects and relations with the general public.

That is why the scenarios are prepared very carefully. Development processes have to be assessed from all possible sides and aspects. Every incorporated detail must be thought out and discussed many times. Timeline of the story in a scenario must be real but allowing sufficient time for decision-making.

The six scenarios are led by end-users from five different EU countries: France, Germany, Slovakia, Spain and United Kingdom, with the contribution of the Estonian Academy of Security Sciences. The School of Police of Catalonia is leading the scenario on fire arms training. Each training content scenario leader has paid attention to all aspects of the work (security, currently existing trainings standards, ethical and societal questions) and has taken into account all the needs defined in the needs assessment. The scenarios were prepared from the end user point of view and based on end user needs. A short description of the six scenarios is presented below.

Scenario1 - Major HAZMAT / CBRN event

Figure 3: TC1 trial in October 2017 in Bratislava, Slovakia

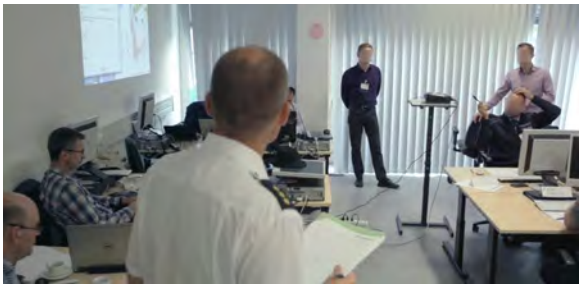
Training content scenario 1 is led by the International Security and Emergency Management Institute of Slovakia in cooperation with police and military experts. It focuses on a major HAZMAT (Hazardous Materials)/ CBRN incident. The scenario develops operational/tactical level exercises for police first responders. The idea is that two trainees enter a suspicious room, a clandestine terrorist laboratory, after having gathered intelligence about its existence and without meeting any terrorist. Supposition is that SWAT and EOD units are not needed in this case. A binary team has to follow the main steps before the Crime Scene Investigation (CSI): check the suspicious area and recognize the threats with regards to radioactive and chemical substances; find them (detect, identify, mark, sample if necessary for the identification purposes); provide safety zoning and mark sectors for CSI; make reconnaissance pictures and do all necessary actions properly without destroying evidences in order to prepare the crime scene for CSI investigators. These are the main objectives to train.

Trainees use virtual devices and dangerous (CR) substances that are virtually simulated as well. To create conditions as much real as possible, trainees have to work in protective suits on which the HoloLens are tagged. Thereafter, virtual stress triggers are used (time running, dosimeter alarm, oxygen time count down).

Using virtual items in combination with real objects brings a whole new level of training and increases greatly the ultimate effectiveness of the entire training process. This is a way to succeed in reaching Research, Development and Innovation requirements requested in projects like TARGET.

Scenario 2 - Protecting a critical infrastructure and dealing with crowds during a mass demonstration

Figure 4: TC2 trial in September 2017 in Oranienburg, Germany



Training content scenario 2 is led by the Fachhochschule der Polizei des Landes Brandenburg. This training scenario is aimed at preparing police officers as members of command post bodies for large scale police operations to deal with crowd control and protection of a critical infrastructure. The target group for this exercise are commanders and command and control personnel at a tactical as well as strategic level.

The scenario deals with crowd management and protection of an airport: an alliance of anti-immigration groups announced a public gathering in front of the terminal building of the Berlin-Brandenburg Airport in Berlin-Schönefeld. The organisers expect several thou-

sand attendees. The aim of this demonstration is to protest against the entry of further refugees and asylum seekers into Germany. Once this information becomes public, an alliance of pro-immigration groups and politicians announces another public gathering also on site in front of the terminal building.

As in scenario 1, this scenario focuses on the management of personnel and resources. In this scenario of approximately 3 hours, we are training to work under pressure to make decisions about unexpected events.

SCENARIO 3 - Response to a massive cyber-attack

Figure 5: TC3 trial in October 2017 in Hartlepool, UK

Training content scenario 3 is led by Cleveland Fire Brigade from the UK. The exercise is targeted at the strategic and tactical command levels and is based in a joint operations/emergency operations-centre environment. The emphasis is not in managing any attack technicalities, but in the response and recovery operations necessary to deal with a sustained power outage.

The scenario trains on appropriate deployment of assets, reactions to the collapse of distribution-networks, management of medium and long term aftermath, management of media injects, and public response and resilience to stress injects.

The script is based on discussions with energy distribution companies operating in the United Kingdom. It is designed to be generic so that it can be adapted quickly to any part of the European Union. The objective of the simulation is to practice teamwork and coordination among the different representatives of many different services. It has a fictitious duration of about 10 days.

SCENARIO 4 - Using personal fire arms in small tactical vignettes

Figure 6: TC4 trial in October 2017 in Mollet del Vallès, Spain

Training content scenario 4 is led by the Police School of the Institute for Public Security of Catalonia with the contribution of Guardia Civil. This is a decision-making scenario in firearms situations. The objective of the training is not to have a virtual shooting gallery, but train above all the decision making about using firearms. Security forces can find themselves in situations in which they need to use firearms. The challenge is to achieve a realistic, dynamic and safe training system with fewer resources.

The trainees have to access a building where they can find people armed or disarmed (perpetrators and victims). The trainees have to interact with these people, aiming to protect the victims and arrest/neutralize the perpetrators. It is a decision-making scenario, therefore the avatars (AR characters) have many possible reactions: obey, take a nearby weapon, drop the weapon they already have, shoot against the trainee, etc. These reactions are not pre-established; the trainer can choose the avatars' action depending on the situation.

Shooting or not shooting and the way to do it will be the most important decision trainees will have to make. The use of firearms is tracked and assessed. When the situation is escalating, one offender can take a victim as a hostage and then, if the police patrol takes the right decision, the SWAT will be required and from that moment the training will be focused on this team. SWAT is supposed to intervene in the final stage, release the hostage/s and neutralize the offender without victims.

SCENARIO 5 - Arrest of suspects after their car crash

Figure 7: TC5 trial in October 2017 in Saint Cyr au Mont d'Or, France

This training scenario is led by l'Ecole Nationale Supérieure de Police at Lyon (France). The script starts with two police officers who are in a police car, driving through the city. A car advances at very fast speed and turns in a corner crashing. The police car also turns and police officers notice that the car that had advanced them has suffered an accident. The driver is unconscious, but after a few seconds the passenger opens the door and leaves the car. From here there are multiple situations where the trainees are asked to assess the threat and neutralise suspects.

It is a scenario of decision-making under stress and good practices in detention. The scenario has a linear introduction that has no variations except for the amount of information the officers have. After the passenger of the injured car comes out of the car, different developments can occur. The agents must determine (under difficult environmental conditions) if the passenger is armed, is dangerous and the best way to arrest him/her.

SCENARIO 6 - Dealing with a major road accident involving multiple cars, victims, and high risk of explosion

Figure 8: TC6 trial in September 2017 in Münster, Germany

This training content scenario is led by the German Police University at Münster. The objective of the training is to provide a realistic training situation to encourage confidence building in large scale operations. The story line is based on a real multiple collision that took place on a German motorway with about 51 cars and more than 100 injured persons involved. The scenario setting is a rural area. The accident is caused by a rear-end-collision of two cars due to heavy fog. Fifty cars, a minivan with fifteen children and a tanker truck, loaded with more than 30.000 litres of petrol / flammable liquids, are involved. There is a high risk of explosion

In this scenario, the decision-making process and the coordination of the specialist teams in an emergency situation are sought. It combines at the same time the training of the staff of a command centre and a mobile police unit at the accident site.

Moving forward: The TARGET Place

The TARGET project finishes in October 2018. This means that the European project phase will be over, but that will not be the end of TARGET. After October 2018, a commercial phase will begin and the TARGET solution will be further developed and brought into market by TARGET Place. The objective of this commercialization is to offer the opportunity to acquire TARGET to all public and private entities that work in the training of Security Critical Agents.

This is an innovative opportunity that completely revolutionizes the traditional training system in these types of scenarios. Traditionally, LP/HI (low-probability high-impact) training has led to a great investment in preparation (time, resources and personnel).

With TARGET solutions Security Critical Agents will no longer have to prepare simulations with months in advance, hire a stack of helpers or invest in infrastructure and material. Thanks to TARGET the outlay will be limited to the initial investment in equipment (hardware) of AR/MR and acquisition of the content (software) that is wanted to train. Once this initial investment has been made, the simulation can be reproduced endlessly at no extra cost. TARGET, as a product, will not only include hardware and software but also maintenance and guidance in good practices to learn how to use it correctly.

References

- Albiero, S. (2017) *First project progress report.* [Online] Available at: http://www.target-h2020.eu/wp-content/uploads/2017/12/171207-TARGET-DL-ART-D8.05-First-Project-Progress-Report-R0.0.pdf [Accessed 29 Jan. 2018].
- European Commission. (2018) *Horizon 2020.* [Online] Available at: https://ec.europa.eu/programmes/horizon2020/en [Accessed 13 Feb. 2018].
- McCall, R. & Braun, A.-K. (2008) Experiences in Evaluating mixed Reality Games. *Psychology Journal,* 6(2), pp. 157-172.
- Munro, R. (2017) TARGET: realistic training through Augmented and Virtual Reality simulation. *Emergency service times,* XVIII(3), 25.
- TARGET Consortium. (2016) *Target H2020: Deliverables & Reports.* [Online] Available at: http://www.target-h2020.eu/wp-content/uploads/2015/10/160126-TARGET-DL-ART-WP6-TC-scenario-overviews-R0.0-FINAL.pdf [Accessed 2 Feb. 2018].
- Vidal, R. (2011) *Training Incident Management Teams to the Unexpectes: the benefits of simulation platforms and serious games.* Paris, France: ARMIR.
- Vidal, R., Frerson, C. & Jorda, L. (2001) Training Incident Management Teams to the Unexpected: The benefits of simulation platforms and serious games. In: P. Fauquet-alekhine & L. Soler, eds. *Serious Games & Simulation for Risks Management.* Paris: Dans A., 43-48.
- Wetzel, R., McCall, R., Braun, A. & Broll, W. (2008) *Guidelines for the Design of Mixed Reality Games.* Toronto, Canada: ACM.
- White, M. D. (2008) Making good cops in the twenty-first century: Emerging issues for the effective recruitment, selection and training of police in the United States and abroad. *International Review of Law, Computers & Technology,* 22(1), 119-134.

Learning Innovation(s)

Innovation Management in Police Organisations: Exploring the process from scientific innovation to police training

Sirpa Virta
Harri Gustafsberg
University of Tampere, Finland

Abstract
This article deals with the process of managing innovation(s) in the police. Innovation management is seen as an organisational response to complexity and uncertainty and therefore, also a method to improve organisational performance and to enhance organisational resilience. The case of translating scientific research results in to the police training and practices in Finland is an illustration of innovation management process that is characteristic to learning organisation. The research results of the international multidisciplinary research project of University of Toronto and Police University College of Finland show that the innovation (iPREP training program) developed in the research project has positive consequences for individual resilience of police officers and therefore, consequently, for organisational resilience too. The empirical research was conducted among police organisations in Canada, Finland and the United States in 2014-2017.

Keywords: innovation, innovation management, learning organisation, resilience

Introduction

This article deals with the process of managing innovation(s) in the police. Innovation management is seen as an organisational response to complexity and uncertainty and therefore, also a method to improve organisational performance and to enhance organisational resilience. The complexity of modern problems, such as terrorism, political and organized violence and cybercrime, place a heavy demand on the police. Traditional hierarchical command-and-control structures have served policing sufficiently so far, but are no longer up to navigating the complexity of social problems and are suboptimal for the organisational flexibility that is required to deal with them. '*Traditional hierarchical police management styles have led to a system where accountability for decisions falls upon senior managers, whereas frontline staff is expected to comply with procedures rather than think*' (Knutsson & Thompson, 2017: p. 2). Bottom-up policing innovations, based on practical ideas and inventions, as well as scientific innovations produced by international or domestic research projects, are useful for the police only when the police organisation has an innovation strategy, a flexible innovation management process and facilitative leadership, creating a creative atmosphere.

In the European Union innovation strategy – From Research to Security Union (European Commission, Migration and Home Affairs, 2017) – the EU-financed security research is seen playing an important role in developing innovations, solutions and technologies

for use by police and other law enforcement officials. The whole Horizon2020 Research Program, like the former Framework programs, is aimed at producing research and innovations, in order to meet challenges for handling security threats and fighting terrorism, cybercrime, human trafficking and natural disasters (European Commission, Migration and Home Affairs, 2017). The Security Research, Innovation and Education Event 2017, organized by the European Commission and the Estonian Academy of Security Sciences in Tallinn 14-15 November 2017, also discussed open innovations in security research and regulation and legislation as drivers or obstacles for innovations. The EU system of innovation promoting by security research funding can be seen as a European-wide innovation management process. The next steps in the process will be the establishment of a European Innovation Partnership on Security (EIP) and setting up a dedicated security Knowledge and Innovation Community (KIC) (Towards a Stronger Security Union: Current state of play and future trends in EU Security Research, 2017: 14-15).

What is innovation then? There is a wide variety of definitions. A useful definition here is that innovation is a process which brings some new method into an organisation. Therefore, something is an innovation only if it is a process that changes the manner in which an organisation performs its task. The second general definition sees innovation as a product or programme that an organisation adopts. The studies of police innovations have used the requirement that an innovation must be new to policing. The innovation types classified in the article *Measuring police innovation*, by William R. King (2000) are as follows: radical or incremental innovations, administrative (field oriented, management oriented), management / technical innovations, line-technical innovations (tactics, weapons) and programmatic innovations (crime oriented, efficiency, community) (King, 2000: 307-310). Innovation management should be included today in to the leadership and management structures and processes in the public sector too.

Scientific research in many disciplines produces innovations for law enforcement. Police sciences' and research's impact and outcome are always based on particular disciplines' (or multidisciplinary) basic and applied research, knowledge and innovations. Capacity and capability of police organisations to adapt and manage innovations are dependent on many variables like level of centralization, types of innovation, creative atmosphere, leadership, environmental contingencies, etc. Recently, it has been argued that evidence-based policing, as a policing knowledge process, is a disruptive innovation in itself (Mazerolle et al., 2017: 117). The case of translating scientific research results into the police training and practices in Finland is an illustration of innovation management process that is characteristic to a learning organisation. The research results of the international multidisciplinary research project of University of Toronto (HART, the Health Adaptation Research on Trauma Lab) and Police University College of Finland show that the innovation (iPREP International Performance Resilience and Efficiency Program) developed in the research project has positive consequences for individual resilience of police officers and therefore, consequently, for organisational resilience too. The empirical research was conducted among police organisations in Canada, Finland and the United States in 2014-2016.

The case study is introduced in Harri Gustafsberg's Doctoral thesis '*Do People Get Shot Because Some Cops Panic? Enhancement of Individual Resilience through a Police Resilience and Efficiency Training Program*' (2018).[1] The Police University College of Finland adopted the iPREP training program after the results were published in scientific journals in 2015-2016. The innovation management process of translating the research results into the everyday training practices is evaluated in this article.

Governing complexity through innovations and innovation management

The complexity of the theoretical approach to policing and police research suggests that policing and police services are parts of a complex adaptive system that has three levels: the policy system, the organisational system, and the individual practitioner level. At all levels, but especially at the policy level and the organisational level, innovation management is seen as a response to govern the complexity and uncertainty of the environment (changes and challenges of societal security, crime and disorder, threats). '*Within the context of complexity theory, arguments are made for the importance of creativity at all levels of the system and (...) novel*

1 The innovative training method is introduced in four scientific articles where Gustafsberg is a co-author (see Andersen et al. 2015a; Andersen et al. 2015 b; Andersen et al. 2016; Andersen & Gustafsberg 2016).

solutions to apparently intractable problems' (Pycroft & Bartollas, 2014: 11).

The vision of the evidence-based policing model is that research findings should be taken into the heart of practitioner decision-making so that they inform and influence how decisions are made (Knutsson & Tompson, 2017: 214). According to the definition, evidence-based policing is "*the use of the best available research on the outcomes of police work to implement guidelines and evaluate agencies, units and officers. Put more simply, evidence-based policing uses research to guide practice… It uses best evidence to shape the best practice. Evidence-based policing is about two very different kinds of research: basic research on what works best when implemented properly under controlled conditions, and ongoing outcomes research about the results each unit is actually achieving by applying (or ignoring) basic research in practice*" (Scott, 2017: 28).

Innovations are vital for the police today, in order to be able to fight crime and disorder and control and govern the ever-increasing complexity of interdependent security threats. The Intelligence-led policing model builds on knowledge and information management processes of the police, but many police organisations lack innovation strategies in their knowledge management systems. The focus being on existing knowledge and information gathering means that creative thinking, experiments and innovations get not enough attention. It has been argued in the recent article of Virta and Taponen (2017) that police organisations and regimes tend to adapt new ways of thinking and doing quite slowly. Regulation and legislation, hierarchical structures and organisational culture traditions may be obstacles for innovations (Virta & Taponen, 2017; see also King, 2000). Instead, bottom-up practical innovations and innovations based on scientific research should be included in the knowledge management processes of the police. Innovations and creative thinking should be encouraged and rewarded.

Innovation research has been divided into two major categories; one category is concerned with examining the process of adoption of an innovation (innovation process research). Another category of research has focused on the association between innovativeness of organisations and organisational performance (innovation variance research). In the fields of organisational theory and strategic management, the focus is on the identification of organisational characteristics and processes that distinguish early adopters of innovations from late adopters (Subramanian & Nilakanta, 1996: 633). In this article we evaluate the process of adoption of an innovation.

Innovation management process evaluation: the case of iPREP International Performance Resilience and Efficiency Program

It has been argued for instance by Adams, Bessant and Phelps (2006) that there is an absence of a holistic framework for covering the range of activities required to turn ideas into useful and marketable products. The measurement of innovation management at the level of the particular organisation requires a holistic framework. Innovation processes can be modelled as a series of events, as a social interaction, and as a process of communication. In the project management research approach there are a number of common elements that can be summarized as the major components of the innovation management: project efficiency, tools, communications and collaboration. The holistic framework of the innovation management process, suggested by Adams, Bessant and Phelps (2006: p. 21) consists of seven categories: inputs management, knowledge management, innovation strategy, organisational culture and structure, portfolio management, project management and commercialization. The framework can be applied also in the innovation management process evaluation of a public organisation like the police.

The police resilience and efficiency training program iPREP is a scientific innovation that has recently been piloted and adopted in the Police University College of Finland. The innovation is a result from an international multidisciplinary research project led by the University of Toronto. According to the leader of the research project, Professor Judith Andersen, in the BBC News interview 9th December 2016: '*In police work, strong stressors will cumulate into acute physiological stress responses that in a multifaceted process will in turn affect the cognitive, motor and sensory processes of the individual officer. Under the influence of acute stress reactions an individual's ability to perceive is changed so that rational-logical thinking is hampered, which will further have detrimental effects on problem solving and decision-making capacity. The ability to sustain good situational awareness and make decisions*

based on it is a professional skill of utmost importance in police work. A panic state is not professional. Policing is a lifesaving occupation. We should expect that police officers receive the best scientifically proven training that is available. In 2015 US Police shot and killed 991 persons of whom 94 were unarmed' (Gustafsberg, 2018: 21).

According to evidence-based policing principles there is the need to have a good practical understanding of the problems faced by individual police officers and police organisations. The paradigm of evidence-based policing is primarily related to knowledge management, innovation management and research and evaluation methods. The innovation process that led to the research and development of the innovative training method iPREP started in a CEPOL (European Union Agency for Law Enforcement Training) seminar of European police psychologists in Finland in 2013. A co-author of this article, Harri Gustafsberg, had a presentation based on his personal experience, from for instance hostage situations, as an operative commanding leader of Karhu (the National Special Intervention Unit of the Police in Finland). The key note speaker, Judith Andersen, research director at the HART Lab of Toronto University Psychology Department, invited the Police University College to join in an international research project. The research proposal was accepted by the Head of the Police University College Kimmo Himberg in the spring 2014. This was actually the first step in the innovation management process (inputs management). In August 2014 the research project started in Finland. Later in 2014, the research project was extended to Canada and in 2015 the Police Training Institute of Illinois, US, joined in the project. In 2016 and 2017 the team conducted psychophysiological training interventions for front-line police officers in Peel, Ontario. The training proved to significantly reduce inappropriate use of lethal force upon completion of the training according to a six-month follow-up study (Gustafsberg, 2018: 23-24).

There were several phases in the research project. The three most important articles of the research team dealt with fostering resilience among the police, mental preparedness training and a training method to improve police use of force decision making: a randomized controlled trial (Andersen et al., 2015; Andersen et al., 2016; Andersen & Gustafsberg, 2016). At the same time when the original research project and interventions were going on, the researcher Harri Gustafsberg was studying in the Masters Programme of Police Management and Security Governance at the University of Tampere. The Police University College supported also this process, which means that in the innovation management process, the scientific quality of the whole research process was guaranteed in this respect too.[2]

In his thesis in 2016 Harri Gustafsberg evaluated how the Police University College integrated a new coaching method into police training. The thesis was based on the theory and concept of organisational learning, introduced by Peter Senge in 1990. The evaluation focused on the pilot phase of the adoption of the innovation. After the project had started, the pilot phase was the second step in the innovation management process. The evaluation data was mainly the interviews of lecturers and trainers of the Police University College and the main questions were: how the new coaching method had been integrated into the training schedule, what challenges if any were observed by the interviewees, and how the changes were experienced at the organisational level. The core themes were those of the learning organisation, individual professional skills and wellbeing and safety at work.

The iPREP training method was tested first with the teachers and trainers. The training provided in the course focused on the psychological and physical effects of exposure to chronic stress, which can lead to health problems and compromise police officers' work performance. The aim was to teach police officers skills that help them to

- improve their mental and physical health,
- build tolerance and develop emotional survival techniques,
- improve their work performance,
- reduce the impact of stressors on their mental and physical health, and
- lower their threshold for seeking support and help (peer support or other psychological help) within the police organisation.

The conclusions drawn brought up two challenges both of which were related to professional skills development. The first challenge was that of time constraints; according to the interviewees there is not enough time to develop professional skills to an extent

2 The co-operation between the Police University College and the University of Tampere has been close and excellent during the past 20 years and it is an illustration of the value and results of the academic-practitioner collaboration in the field of police education, science and research.

considered proper. Other concerns were related to mental models and motivation. However, it was concluded that at the organisational level the Police University College is a learning organisation. The training method was therefore successfully adopted and ready to use also in use of force –training and in other relevant police trainings (Gustafsberg, 2016).

Participation in the international research project as a researcher and in the development of the iPREP training programme was an excellent way to gather data and use it also for the PhD. The scientific articles, published with the research group, were included in the Doctoral dissertation. The research questions, led from the research data, in Gustafsberg's Doctoral dissertation were twofold:

- First, is it possible to significantly enhance situational awareness, decision making and overall performance by using the developed scientific method during interventions?
- Second, do improvements in individual resilience contribute to resilience and efficiency at an organisational level?

The point of departure in the research was that the personnel of an organisation should be able to rely on their mental resources facilitating flexibility, development and recovery from the strain of work, so as to meet the challenges they face in their organisational positions. These features of a functional individual will be referred to here as *resilience*. An organisation should offer an individual a functional environment where to apply, strengthen and develop one's human potential. Any straining work and the related mental burden cause a chain of various physiological changes with many effects on an individual's *situational awareness* and the ability to make decisions with ultimate effects being reflected on the quality of work and the effectiveness of the individual. These processes will in turn determine the reliability and relevance of the *situational picture* an organisation has at its disposal – the situational picture being a rather static tool of management and decision making and as such being dependent on the accuracy and quality of a more dynamic situational awareness of the individual.

Police work offers an excellent context for researching demanding work tasks having effects on these psychophysiological processes in the human being. A secondary derived research problem at an organisational level focused on organisational resilience to find out whether we can influence resilience, i.e. the flexibility, efficiency and productivity of an organisation by enhancing the performance of individuals. Use of force by and also the safety of law enforcement personnel have been very much in the news while the very same themes are discussed and closely analyzed as problems of increasing concern inside the police organisation. The reported results, based on data gathered in situations simulating demanding police work, show that stress reactions may change the course of operations for better or worse depending partially on the body-mind state of involved law enforcement officers (Gustafsberg, 2018: 40-42).

The results of the research show that evidence-based policing in practice – at its best – means that evidence – i.e. innovations, results and findings of scientific research – are taken seriously and that they are important in the development of police training, police work and policing in general. The results of the research show that the scientific coaching method (iPREP) improves situational awareness and the quality of decision making of police officers during demanding operative situations. This is reflected as an increased performance capacity and efficiency of police operations. It was also shown that proper preparing for operations affected positively the physiological recovery from the strain of operations. The body was thus able to bounce back from the effects of stressors more efficiently when an individual officer was able to prepare in advance for upcoming operations. It was hence posited that careful planning and high-quality training based on scientific evidence have important roles in increasing the resilience of individual officers. At the organisational resilience level, it was considered important that training processes are developed on the basis of scientifically valid information and evidence, and that administrative practices and open-minded leaders are needed in order to achieve the operational objectives throughout the organisation (Gustafsberg, 2018: 123).

Following the definition of innovation as being 'the successful exploitation of new ideas' (Adams, Bessant & Phelps, 2006: 22), we argue that the training method developed is an innovation and that the innovation management process of the Police University College of Finland has been successful in integrating the innovation into the police training. Consequently, it can be argued that the enhancement of individual resilience

of the police officers through the training will enhance the organisational resilience of the Finnish police and the quality of the police services especially in demanding circumstances and in rapidly changing working environments.

The identifiable phases in the innovation management process were inputs management, knowledge management, strategic orientation, leadership (innovation strategy) and project management. Inputs management is concerned with the resourcing of innovation activities and includes factors ranging from finance, to human and physical resources, to generating new ideas. The general research and development (R&D) intensity has frequently been used as a measure of input (Adams, Bessant & Phelps, 2006: 26), but in our case inputs management in the process was not very closely connected to the actual RDI –unit of the Police University College. However, it shows the flexibility of the overall innovation management strategy that the innovations to be adopted – inputs – can also come from outside, like in our case, as a consequence of the CEPOL seminar networking and innovation communication process. Knowledge management category, in the framework of Adams, Bessant and Phelps (2006) includes information flows, and project management includes project efficiency, tools, communications and collaboration. All these are integral parts of the innovation management process of the Police University College.

Conclusions

Although the evaluated innovation management process of the Police University College is a good example of evidence-based policing in practice in the context of the police training and education, the police in Finland lack a special innovation strategy. Innovations are discussed in other strategies but it can be argued that especially today, when the police have to face rapidly changing environments, new kinds of threats and increasing complexity in general, adaptive innovation strategy is needed in all police organisations. The most urgent and important are decisions regarding the use of technological innovations (for instance drones and artificial intelligence applications). Innovations strategy should include an adaptive and systematic innovation management process that covers all or most of the innovation management process framework categories. Adaptive innovation strategy is a critical success factor to any organisation today, but it is extremely critical to police organisations. Central to this perspective is the idea of absorptive capacity which means the organisation's ability to absorb and put to use new knowledge, and involve an ability to recognize the value of new, external knowledge, assimilate it and apply it to organisational ends (Adams, Bessant & Phelps, 2006: 29).

The authors are aware of the critique of the evidence-based model(s) of mobilization and translation of knowledge into policing practice. Research-practice co-production of knowledge is recommended in most evidence-based policing strategies but there are limitations in the models. The limitations include narrow understanding of evidence and "elite science". The hierarchy of knowledge informed by a ranking of methodology, random control trials (RCTs) at the top, refer and illusory desire to attach certainty to police operations. Evidence-based policing is also recurrently interpreted as a means for promoting legitimacy, so that evidence is seen to serve organisational legitimacy in the first place (Crawford, 2017: 199-201). Maintaining a critical distance and autonomy has to be kept in mind in research-practice co-production.

Innovations and innovation management are important elements of development and improvement of police services in all countries. In the EU Security Research, Innovation and Education event (SRIEE2017) in Tallinn in November 2017, in one of the panels, Thierry Hartmann posed a question: "what kind of an organisation is innovative police organisation?" (Hartmann 2017). He listed many elements that are essential in innovation management:

— innovation is a part of daily job, not a task of specialists,
— we should identify individuals and teams that produce innovations,
— we should open space, open the door and discuss innovations; give the opportunity,
— we should turn top-down processes upside down to bottom-up processes,
— we should create a creative atmosphere: "Feel free to present ideas".

In the end of his talk, Thierry Hartmann pointed out that there should be better integration of innovations into the processes of policing and management, and finally, that we should be "innovative in management of innovation". The very same issues and questions

were dealt with also two weeks after the SRIEE2017 conference, in the CEPOL Police Science and Research Conference in Budapest, in the end of November 2017.

Innovation processes and management are critical success factors to all police organisations today but, as shown in our analysis, leadership and strategic approach are also required: leadership that supports creative atmosphere, value scientific research and knowledge and facilitates innovation processes and strategies.

References

- Adams, R., Bessant, J. & Phelps, R. (2006) Innovation management measurement: A review. *International Journal of Management Reviews*. 8 (1), 21-47.
- Andersen, J. P., Papazoglou, K., Koskelainen, M., Nyman, M., Gustafsberg, H. & Arnetz, B. B. (2015a) Applying Resilience Promotion Training Among Special Forces Police Officers. *SAGE Open*. 5 (2), 1-8. doi:10.1177/2158244015590446
- Andersen, J., Konstantinos, P., Nyman, M., Koskelainen, M. & Gustafsberg, H. (2015b) Fostering resilience among the police. *Journal of Law Enforcement*. 5 (1), 1-13.
- Andersen, J., Papazoglou, K., Gustafsberg, H., Collins, P. I. & Arnetz, B. B. (2016a) Mental preparedness training. *FBI Law Enforcement Bulletin*. 3/10.
- Andersen, J. & Gustafsberg, H. (2016) A training method to improve police use of force decision making: A randomized controlled trial. *SAGE Open*. 6 (2), 1-13. doi:10.1177/2158244016638708
- Crawford, A. (2017) Research co-production and knowledge mobilisation in policing. In: Knutsson, J. & Tompson, L. (eds.) *Advances in Evidence-Based Policing*. Abingdon, Routledge, pp. 195-213.
- European Commission, Migration and Home Affairs (2017) *From Research to Security Union*. Luxemburg, Publications Office of the European Union.
- Gustafsberg, H. (2016) Oppiva organisaatio avuksi poliisityön stressin hallintaan [Learning organisation for managing the stress of the police work]. Master's Thesis. University of Tampere.
- Gustafsberg, H. (2018) *Do People Get Shot Because Some Cops Panic? Enhancement of Individual Resilience Through a Police Resilience and Efficiency Training Program*. University of Tampere, Juvenes Print.
- Hartmann, T. (2017) Talk in the panel of the EU Security Research, Innovation and Education event (SRIEE2017), Tallinn, Estonia 15.11.2017.
- King, W. R. (2000) Measuring police innovation: Issues and measurement. *Policing: An International Journal of Police Strategies & Management.* 23 (2), 303-317.
- Knutsson, J. & Tompson, L. (2017) Introduction. In: Knutsson, J. & Tompson, L. (eds.) *Advances in Evidence-Based Policing*. Abingdon, Routledge, pp. 1-9.
- Mazerolle, L., Eggins, E., Higginson, A. & Stanko, B. (2017) Evidence-based policing as a disruptive innovation: The Global Policing Database as a disruption tool. In: Knutsson, J. & Tompson, L. (eds.) *Advances in Evidence-Based Policing*. Abingdon, Routledge, pp. 117-138.
- Pycroft, A. & Bartollas, C. (2014) Introduction. In: Pycroft, A. & Bartollas, C. (eds.) *Applying Complexity Theory: Whole Systems Approach to Social Work and Criminal Justice*. Bristol, Policy Press, pp. 1-14.
- Scott, M. S. (2017) Reconciling problem-oriented policing and evidence-based policing. In: Knutsson, J. & Tompson, L. (eds.) *Advances in Evidence-Based Policing*. Abingdon, Routledge, pp. 27-44.
- Subramanian, A. & Nilakanta, S. (1996) Organisational innovativeness: Exploring the relationship between organisational determinants of innovation, types of innovation and measures of organisational performance. *Omega: International Journal of Management Science.* 24 (6), 631-647.
- *Towards a Stronger Security Union: Current state of play and future trends in EU Security Research.* Discussion Paper. European Commission. SRIEE2017. Security Research, Innovation and Education event. Tallinn, November 2017. Available from: http://www.statewatch.org/news/2017/dec/eu-com-non-paper-security-research-tallinn-2017.pdf
- Virta, S. & Taponen, J. (2017) Policing regimes in transition in the Nordic countries. In: Devroe, E., Edwards, A. & Ponsaers, P. (eds.) *Policing European Metropolises: The Politics of Security in City-Regions*. Abingdon, Routledge, pp. 121-143.

Management and Leadership Training in Police Organization: The EMBA in Policing

Tiina Koivuniemi
Police University College, Tampere, Finland

Abstract
Police organizations in Europe and worldwide are in the midst of change. The world has never changed as much as it has in the last decades, which means that the roles of police organizations in today's societies are also changing rapidly. Police organizations face more challenging and more complex problems in more diverse societies. As a result, the police manager's work has become more demanding. The importance of leadership to the performance of the organization has been demonstrated in various studies. Police organizations need managers who are professionals in both management and leadership. Finland's Police University College has developed a new and original management training program – the EMBA in Policing – in cooperation with Tampere University of Technology. This innovative police management training program is based on Quinn's Model of Leadership. The idea of this paper is to introduce the "EMBA in Policing" programme as a new way to train future police leaders and to research how Quinn's model serves as a theoretical framework in police management and leadership training. In this article, the author describes the model of the EMBA in Policing program, and reports the results of the pilot training.

Keywords: Management, leadership, police leadership training, development

1. Introduction

Management and leadership are crucial factors for the success of any organization. Society and the policing environment are becoming more complex, challenging, and multiform. Rapid changes are a part of everyday life now, and managing change is a manager's everyday work. This means that police and police leaders need more specific skills in addition to professional policing skills. Managing a police unit is demanding work, and managers should have special skills in managing and leadership. Many managers and supervisors in police organizations start their careers working on the front line and develop their expertise in policing. Police organizations are generally led by those who have had extensive careers, and have been rewarded by a promotions process that values police tradecraft, tradition and experience rather than formal education in leadership (Roberts et al. 2016). Effective management of police organizations and police personnel demands more.

The Executive Master of Business Administration in Policing (EMBA in Policing) is a new and innovative way to deliver management and leadership training in the police organization. The EMBA training program has been developed and implemented by the Police University College (Finland) and the Centre for Professional Devel-

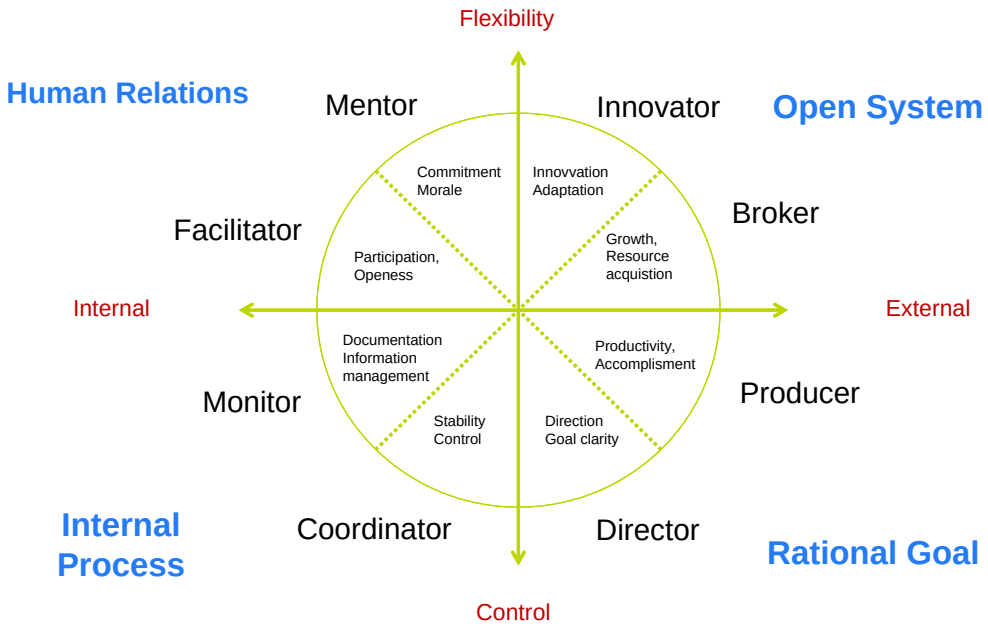
opment Edutech at Tampere University of Technology. Planning for the EMBA in Policing program began in 2014, and the first 2-year training began in 2015. The program is designed to meet the needs of police management and leadership development.

2. The Competing Values Framework of Quinn and leadership training

The impact of management on the effectiveness of an organization has been proven by several studies. Particularly in the 1990s, roles related to management became the object of special study. There are several theories related to management. Theoretical frameworks of management include the Rational Goal Model, the Internal Process Model, the Human Relations Model, Taylor's Four Principles of Management, Fayol's General Principles of Management, the Open System Model, the Contingency Theory, and Weberian Bureaucracy. All these theories have good characteristics, but they often look at management from a very narrow point of view. However, management is a complex activity, which means that in order to reach the best end result possible, several management theories should be studied simultaneously. Quinn's model combines the strengths of most theories, which has made it possible to create a framework that combines the complexity of management with identifying the different roles of a manager (Melo, Silva & Parreira, 2014).

Quinn's Competing Values Framework, developed in the early 1980s, is one of the most popular and heuristic conceptual frameworks. It is a synthesis of organizational theories, which characterize organizations in two dimensions: 1) flexibility–stability and control, and 2) internal environment–external environment. Quinn's Competing Values Framework consists of four management models, which are the open system model, the rational goal model, the internal process model, and the human relations model. Eight managerial leadership roles can be connected to the model (see Figure 1). According to Quinn, these managerial leadership models and roles are linked to the organization's culture, and reflect that culture (Morais & Graça 2013).

Figure 1. Quinn's model.



The eight managerial leadership roles identified in Quinn's model are Mentor, Facilitator, Monitor, Coordinator, Director, Producer, Broker and Innovator. Each role requires different key competencies, which are presented in the table below.

Table 1. The eight managerial leadership roles and their key competencies (Quinn et al., 2003: 23).

Managerial Leadership Role	Key Competencies
Mentor	Understanding one's self and others Communicating effectively Developing employees
Facilitator	Building teams Using participative decision making Managing conflict
Monitor	Monitoring individual performance Managing collective performances and processes Analysing information with critical thinking
Coordinator	Managing projects Designing work Managing across functions
Director	Developing and communicating a vision Setting goals and objectives Designing and organizing
Producer	Working productively Fostering a productive work environment Managing time and stress
Broker	Building and maintaining a power base Negotiating agreement and commitment Presenting ideas
Innovator	Living with change Thinking creatively Managing change

The key competencies of the different management roles can also be studied from the perspectives of the different quadrants of Quinn's model.

Key competencies are associated with the four quadrants of the competing values framework (Quinn et al., 2011: 21):

- **Collaborate:** Creating and Sustaining Commitment and Cohesion
- **Create:** Promoting Change and Encouraging Adaptability
- **Compete:** Improving Productivity and Increasing Profitability
- **Control:** Establishing and Maintaining Stability and Continuity

Quinn's Competing Values Framework is a model that is very suitable for developing management, improving the effectiveness of an organization, and creating the values of the organization. The model can be used for both private and public sector organizations. In the public sector, the model has been used in health care in particular. In contrast, police organizations do not have much experience using theoretical frameworks to develop and manage organizations.

Quinn's Competing Values Framework was selected as the theoretical framework for designing the whole EMBA in Policing training program.

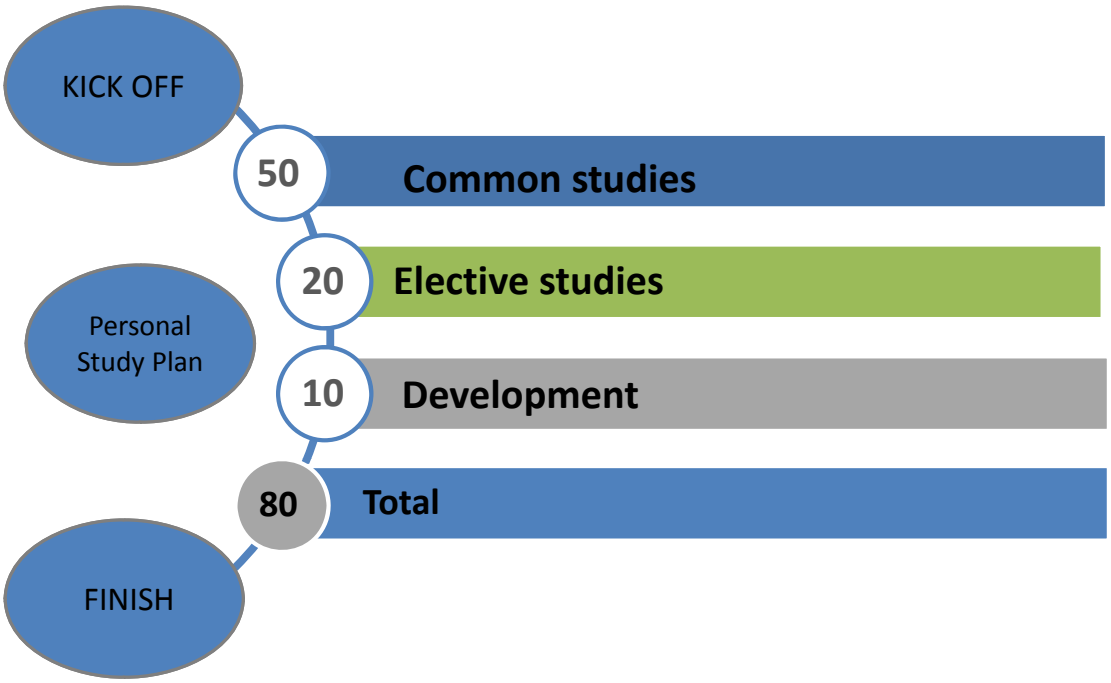
3. Case presentation: The EMBA in Policing

Police organizations need the best talents to be police leaders. The first step in the EMBA in Policing process is recruitment and selection of participants. The basic entry criteria for the EMBA in Policing program are to have a permanent appointment in the police organization, a master's degree, management and leadership experience (at least 3 years in middle management), and B2-level proficiency in English. The entrance examination consists of two phases. In the first phase, applicants apply through an online system, including a motivation letter and a statement from their police chief. In the second phase, applicants take an entrance examination. During this examination, a selection jury evaluates each applicant's motivation, professional aims and level of ambition, distinguished action as a leader, and potential for handling difficult managerial tasks. This second phase also includes psychological tests, interviews, and simulated tasks.

3.1 Structure, content, and implementation of the program

Quinn's management model (Competing Values Framework) was the framework for designing the EMBA in Policing training. The total scope of the training was 80 ECTS credits, of which 50 credits were common studies, 20 credits were elective studies, and 10 credits were a development assignment (see Figure 2). The total duration of the training was two years, including 30 classroom study days, three development seminar days, and independent work included in the courses. In addition, the participants completed elective studies, some of which consisted of previously completed studies, while others were completed during the two-year period. The EMBA in Policing was comparable to self-motivated studies, and participants completed the studies on their own time.

Figure 2. Structure of the EMBA in Policing training



Common studies

The division of common studies is based on the theoretical framework mentioned above. The studies included four subject areas, which were:

1) Strategic renewal,
2) Resource management,
3) Organizational and service structures,
4) Healthy and developing work communities.

The subject area of strategic renewal focused on analyzing the operating environment, strategic thinking, and drawing up a strategy. In addition, this study module included putting strategy into practice, working with the management group, and publicity and cooperation with stakeholders. A study module on international cooperation was also implemented in the area of strategic renewal. In the original plan, the international cooperation studies were to be implemented as a study trip. The scope of the strategic renewal study module was 16 ECTS credits.

The total scope of the resource management study module was 10 ECTS credits. The module included the management of financial resources as well as human and competence resources. In addition to the topics mentioned above, knowledge management and how to take advantage of technology were also studied in the course.

The organizational and service structures study module focused on service design and development as well as process development. In addition, change management, change communications, and organizational risk management were studied during the course. The scope of the course was 8 ECTS credits.

One fourth of the common studies consisted of the healthy and developing work communities study module. Inclusive management and dialogue as a management tool were studied during the course. The participants gained competence for managing challenging situations in the workplace, diversity management, and remote management. The scope of the study module was 10 ECTS credits.

A theme running through all common studies was the module of self-knowledge and development as a manager; its scope was 6 ECTS credits. This module included mentoring, performance skills, and managerial etiquette. Each participant had a personal mentor, and mentor meetings were scheduled throughout the two-year period in accordance with the plan and agreement between the participant and the mentor. The participants were encouraged to find mentors

outside the police administration, with the aim of broadening their views. Performance skills were practiced both during classroom studies and in connection with evening programs, during which the focus was also on management etiquette.

Elective studies

The scope of the elective studies was 20 ECTS credits. The participants had the option of including master's degree-level classes (not already included in an existing degree) to their EMBA in Policing studies. The requirement for approval was that the studies had been completed at most three years before the start of the EMBA, and that those classes promoted the personal development of the participant as a manager and were justified in the personal study plan. In addition, these classes had to complement the content offered by the EMBA program.

The elective study plan was confirmed during the personal study plan discussions, and students could propose studies supporting their professional growth for approval as elective studies. Elective studies were completed in accordance with the study requirements of other universities and institutions of higher education. During training, an agreement was drawn up between the Police University College and the National Defence College, according to which the students of the Police University College had the right to study at the National Defence College. Three students completed elective studies offered by the National Defence College. In addition, CEPOL training and FBI management training, among other things, were approved as elective studies.

Elective studies were approved by the EMBA management team based on proposals by the participants and the certificates they had provided. If the training was not at higher education degree level, the participants were asked to complement their studies, for example with extra assignments.

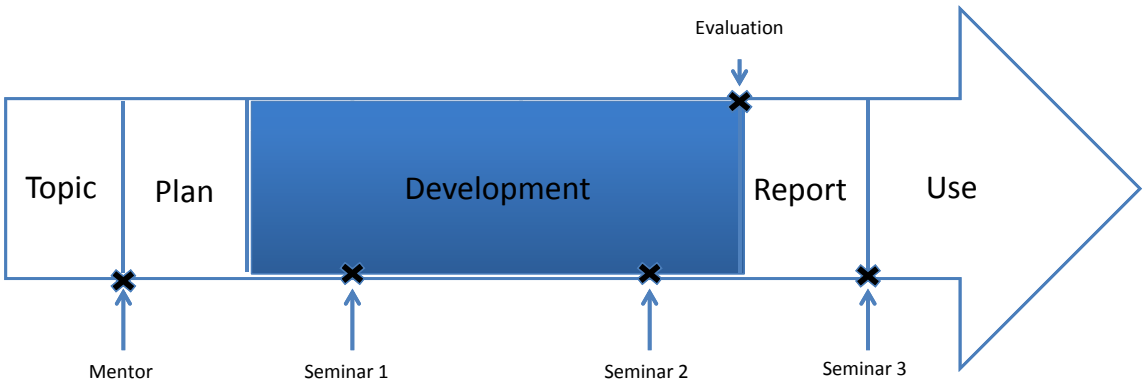
Development assignment

The scope of the development assignment included in the EMBA in Policing was 10 ECTS credits. The goal of the development assignment was to apply the lessons learned in practice and develop written communications. A development challenge or issue to be resolved essential to one's own work or organization was chosen as the theme of the assignment. The assignment was to be linked to one of the program's subject areas, or it could take advantage of all subject areas.

A report was drawn up on the completed development assignment. A clearly structured analytical work with justified conclusions was required. With the joint decision of the group, the development assignments could be published either in whole or in part within the police administration at the national level.

Development assignments started with choosing a topic and finding an advisor (see Figure 3). Next, the students drew up a subject analysis and a plan for the development assignment. After the plan was approved, the actual development assignment and a report on the work were done. Two development assignment seminars were held during the process, and the completed assignments were presented at the final seminar.

Figure 3. Development assignment process.



The themes of the development assignments served the operations of the police in a variety of ways. Some of the assignments were police department-specific projects, while others presented new innovations or involved preparing a report. The themes of the development assignments included:

- Police chief – an operative or administrative chief?
- Fewer resources – fewer policemen: How to cope with decreasing resources?
- Taking advantage of 3D-modelling in protecting targets and in planning operations
- Audit manual for intelligence-led police operations management
- Organizational development of the Finnish Prosecution Service
- Towards the target organization from the viewpoint of change management
- Strategy work at the Central Finland Police Department
- Police reserves
- Developing HR management at the South-western Finland Police Department
- Quality manual of the South-eastern Finland Police Department's forensic investigation centre as a tool of quality management – management's role in quality work
- Intelligence-led police operations management at the Eastern Uusimaa Police Department
- Developing the license service operations at the Central Finland Police Department

The scope of the development assignment was 10 ECTS credits, but most of the assignments proved to be larger than the number of ECTS credits offered, due largely to the commitment of the participants and the topics selected. A conservative estimate of the calculated value of the development assignments is approximately EUR 300,000, if the work had been commissioned from experts outside the organization.

4. Pedagogical choices

The blended learning philosophy was followed in the EMBA in Policing training. The starting point was that the training participants were active learners who used different learning methods in a variety of ways. Knowledge, learning, and insights were refined through interaction with the trainers, group members, and other people participating in the implementation of the training.

The implementation and working methods of the EMBA in Policing program were based on the competence development philosophy defined by Edutech, specifically Edutech's propositions for "Developing Competence Now", which are:

- Do development work at the grassroots level,
- Venture outside your own field,
- Take advantage of digitalization,
- Build a new network,
- Share your competence,
- Solve the problem.

The training consisted of contact teaching and independent work. Expert trainers were responsible for classroom teaching during study days. These experts came from universities, private companies offering training services, other companies, police organizations, and elsewhere in public administration. The goal was to enrich the learning process with theoretical information, practical examples, and case studies. The competence of experts was provided for the group through speeches, lectures, introductions, and so forth. The group was challenged to interact actively and question and debate issues to strengthen their own competence. Problem-solving tasks were linked to the themes, and they were done individually, in pairs and in groups, both during and in between training days. The task subjects came mainly from within the police organization. "Benchmarking" learning and thinking that supports renewal was promoted by expert trainers selected from other fields, as well as by addressing case studies.

The Police University College's Moodle system was used for online work. Teleconferencing technologies (such as Skype, Microsoft Lync, Adobe Connect Pro) were used when needed. Some of the personal study plan discussions were conducted via remote connection. During some of the classroom study periods, expert lecturers participated in the training via the TUVE video meeting application. The kyvyt.fi platform was also used as a work platform.

An additional program included cultural experiences (movies, theatre, reading assignments/recommendations) as well as training in etiquette and small talk

situations, used to coach the participants in social situations related to management.

The process of development as a manager was supported by personal study plan discussions, which were conducted twice during the program. All participants drew up a personal study plan in which they related how they intended to take advantage of the different parts of the training program to develop their own management competence and identity as a manager. In addition, the participants defined their personal learning objectives and methods for reaching them.

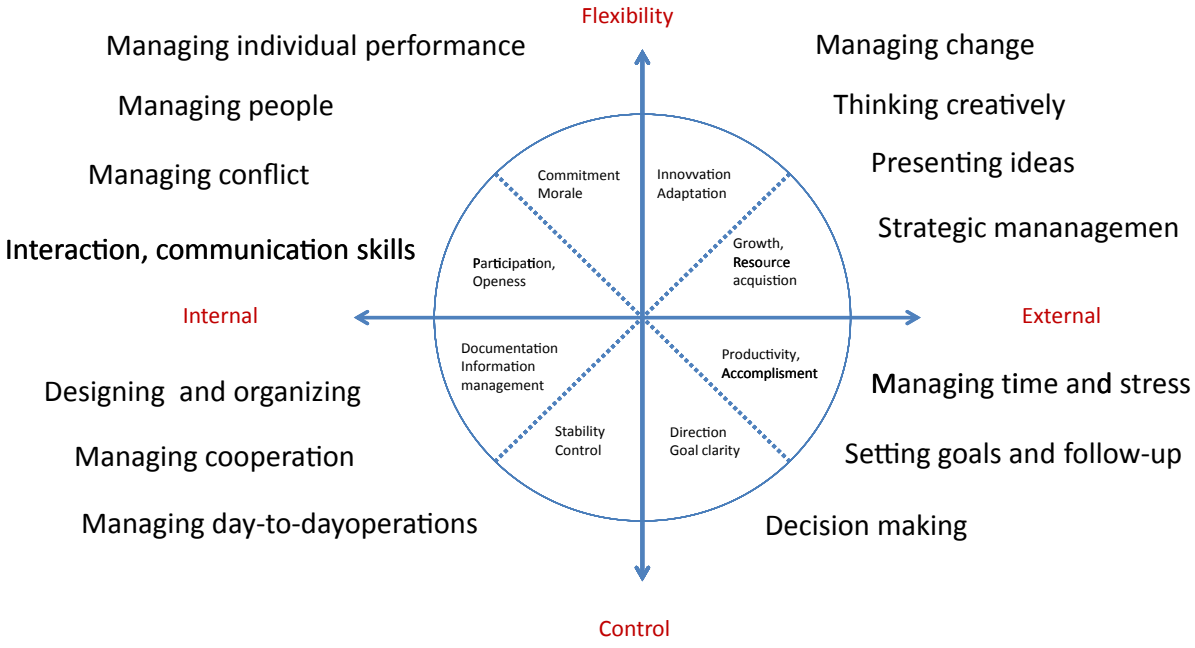
To support the self-knowledge of a manager, the psychologist responsible for the suitability test in the entrance examination described the key content of the results in the group feedback. During the program, the aim was to support the formation of groups and encourage interaction between the group members, enabling collaboration within the peer group. The peer support of colleagues in the personal development as a manager and learning from the experiences of others were an important part of the support for growing as a manager.

The idea behind mentoring was to practice management and meeting the challenges of management with an experienced manager. The participants' mentors were all experienced managers and experts in business life and public administration. In accordance with the objective, most of the mentors came from outside the police administration.

5. Learning outcomes

In addition to the course-specific feedback, a self-assessment on professional growth was collected from the participants. The feedback was collected through an online Webropol survey. A series of structured questions formed the first part of the self-assessment. The questions were constructed to measure progress in the different areas of Quinn's model (see Figure 4). In addition, the participants evaluated the change in their own development of competence.

Figure 4. Self-assessment areas



The participants of the EMBA in Policing training were asked to assess their own development during the program by selecting one of four options that best described their own development:

1 = No change, I have not developed.
2 = I have developed somewhat. However, my competence is basic and largely at the level of knowledge.
3 = I have developed a fair amount. I occasionally apply what I have learned to my own work.
4 = I have developed a great deal. I use what I have learned in my work. I have started to use new methods and apply what I have learned to my own work regularly.

The most positive development in the participants' competencies could be found in change management, HR management, performance management, creative thinking by the manager, and presentation of new ideas (see Table 2). The least positive development could be found in the area of time and stress management. Changes occurred in the competencies of all respondents during the program.

Table 2. Self-assessment of the participants' competence development.

Competence area	1 No change	2 I have developed somewhat	3 I have developed a fair amount	4 I have developed a great deal
Strategic management	0 %	0 %	70 %	30 %
Setting goals and monitoring	0 %	20 %	50 %	30 %
Presenting new ideas	0 %	10 %	20 %	70 %
Creating and maintaining cooperation with internal and external stakeholders	0 %	20 %	50 %	30 %
Change management	0 %	0 %	50 %	50 %
Managerial creative thinking	0 %	0 %	20 %	80 %
Planning and organization	0 %	30 %	40 %	30 %
Time and stress management	0 %	60 %	40 %	0 %
Performance management	0 %	0 %	50 %	50 %
Operations management	0 %	10 %	60 %	30 %
Decision-making	0 %	0 %	60 %	40 %
Acting in difficult situations in the workplace	0 %	30 %	40 %	30 %
HR management/Leadership	0 %	0 %	50 %	50 %
Interaction	0 %	10 %	50 %	40 %
Development	0 %	10 %	50 %	40 %

To summarize, it can be said that much positive development occurred in all areas of Quinn's model. The most significant areas of development were in creativity and cooperation.

In addition to the structured questions, the participants were asked to name the three competence areas in which they felt they had developed the most during the EMBA in Policing program. Half of the respondents said that their strategic thinking had developed especially well during their studies. Other competence areas often mentioned included the development of one's own thinking, new innovations, gaining confidence in presenting one's thoughts, and increased competence in implementing opportunities for experimentation.

Next, the respondents were asked to assess the EMBA in Policing training in their own words. As a rule, the program and the studies were considered as a good experience and a positive step on the career path. During the program, nine of the participants progressed in their careers.

In the view of the participants, implementing the program in cooperation with Edutech has been positive and beneficial. The use of experts and trainers from outside the police administration was considered to broaden views and develop competence. Applying new ideas and information to the police administration was felt to promote competence. The opportunity to apply lessons learned to one's own work in the form of assignments immediately after classroom study periods was also considered beneficial.

In the participants' opinions, networking between the participants has absolutely been one of the strengths of the training. Experienced and motivated students were selected for the training, which was evident in the interactions during the learning situations, which led to learning from colleagues in the best way possible.

The program was seen as challenging. The participants completed it on their own time, which means a considerable personal investment in competence development. Their feedback raised a concern about the appreciation of the EMBA in Policing training in the police administration. The open-ended responses expressed a desire for appreciation by the employer, and a hope that the new competencies would be used.

A course on international cooperation was planned for the EMBA in Policing training, and the intention was to implement it as a study trip abroad. The course program had already been drawn up well in advance, and study visits had been arranged with the receiving organizations and individuals. However, the time of the study trip had to be moved due to a lack of joint policy, and in the end, the study trip was cancelled completely. The course was implemented instead as a three-day course in Finland. The participants were very disappointed by the cancellation of the originally planned course, and the international cooperation course received the worst feedback in the course-specific assessments.

Finally, the participants were asked if they would recommend the EMBA in Policing program for other people working in police administration. All respondents except for one would recommend the training. If a respondent chose not recommend the program for others, they were asked to provide reasons why. One reason given was that certain requirements were set in advance, such as the use of time and policies concerning the group. In addition, the concern was raised that the work community and the employer did not appreciate the training program enough.

The assessment of the students' competencies development showed that the learning objectives were reached very successfully. The success of the program is also reflected in the fact that the careers of ten participants in the training program (out of 14 total) have progressed significantly. The career development of three participants has continued outside the police organization.

The effectiveness of the training program was also assessed by interviewing the police chiefs of the participants' own police departments. With one exception, the chiefs were very pleased with the results of the program, because, according to them, participation in the EMBA in Policing training program benefited their departments. They had noticed positive changes in the participants' management behaviours; examples included a deeper vision of management and increased strategic thinking. The participants' views of management have broadened. In management behaviour, the increased importance of networking, cooperation and valuing others is clearly visible in the enthusiasm and readiness to develop operations together with stakeholders and other actors.

6. Conclusion

In police organizations, advancement to management or a supervisory position has traditionally been based on seniority. Regrettably, the recruitment criteria have usually not included assessing leadership characteristics or the ability to work in management positions. For this reason, the person selected for the task has often lacked managerial training. An organization's effectiveness, strategic management, and leadership suffer if the people in management positions do not have sufficient general management competence.

The case of the EMBA in Policing showed that Quinn's model is a successful choice for the theoretical framework of a management training program. The training program was organized in cooperation with Edutech at Tampere University of Technology. The cooperation created new aspects of training, and the competencies and expert networks of the educational institutions complemented each other well. Traditionally, police

organizations are very closed and insular, but during training, the participants studied management and operations extensively outside the police organization, which gave them plenty of new ideas and views on management. Opening the police organization and benchmarking with the private sector and other public administration organizations is also particularly recommended in future management training programs.

As a whole, the EMBA in Policing training program was successful. The feedback from participants was good with an average rating of 4.02 on a scale from 1 to 5 in an assessment concerning the content, implementation, and arrangements of the modules as well as the participants' own activities. Positive changes were observed in the operating methods of most participants, including a broader view of management, improved use of information in management, and development of stakeholder cooperation skills. Some of the police chiefs noticed that the position and previous management experience affected the development of participants' management skills as a result of the training. The police chiefs consider a strategic management training program directed at unit management and upper-level commanding officers as necessary, and the EMBA training program as useful for their own unit.

In police organizations, more attention should be paid to the management profiles of the people recruited to management positions, and their suitability for supervisory duties should be assessed. An emphasis was placed on suitability assessment during the recruitment to the EMBA in Policing program, and the selection process as a whole was clearly successful. Police organizations should invest in the training of leaders and managers. The training should be sufficiently demanding, and it should focus on the challenges of the operations, organization, and leadership in a variety of ways.

References

- Melo, R. C., Silva, M. J. & Parreira, P. (2014) Effective leadership: Competing values framework. *Procedia Technology*. 16, 921-928.
- Morais, L. F. & Graça, L. M. (2013) A glance at the competing values framework of Quinn and the Miles & Snow strategic models: Case studies in health organizations. *Revista Portuguesa de Saúde Pública*. 31 (2), 129-144.
- Quinn, R. E., Faerman, S. R., Thompson, M. P. & McGrath, M. R. (2003) *Becoming a Master Manager: A Competency Approach*. 3rd ed. Hoboken, NJ, John Wiley & Sons.
- Quinn, R. E., Faerman, S. R., Thompson, M. P., McGrath, M. R. and Clair, L. S. (2011) *Becoming a Master Manager: A Competing Values Approach*. Hoboken, NJ, John Wiley & Sons.
- Roberts, K., Herrington, V., Jones, W., White, J. & Day, D. 2016. Police leadership in 2045: The value of education in developing leadership. *Policing: A Journal of Policy and Practice*. 10 (1), 26-33.

Effectiveness of Simulation-Based Learning in Basic Police Training

Andrea Beinicke
Department of Psychology, University of Würzburg, Germany

Albin Muff
Department of Police Training and Further Education, Bavarian Police, Bamberg, Germany

Abstract
Simulation-based learning is an important element of police training and further education. In the Bavarian police system (Germany), the curriculum of basic training includes 500 hours of simulation-based training for apprentices. This considerable amount of training necessitates a great deal of facilities and human resources. After a long period of practical experience, we investigated a training evaluation study in cooperation with the University of Würzburg (Germany) to measure the effectiveness of the simulation-based training in Bavarian police officer trainees.
The results of the study indicate that the simulation-based training appears to be both objectively and subjectively effective. Regarding measures of objective training success, trainees' overall performance as well as their factual and applied knowledge significantly increased over time in the simulation-based training.
Regarding measures of subjective training success, we found a highly significant increase in effectiveness over time in simulation-based training, with the largest effects found in trainees' perceived usefulness, application to practice, the feeling of personal and professional advancement, and the satisfaction with the simulation-based training.
To optimize simulation-based learning activities, more constructive feedback by trainers is necessary in terms of information about the individual learning process. Additionally, more standardisation across trainers, classes, training modules, and different training centres is necessary.
We conclude that role playing as a form of simulation-based learning is effective in basic police training, even in the long term. When combined with traditional classroom training, such simulation-based training can improve police trainees' training success.

Keywords: police training – simulation-based learning – training evaluation – training effectiveness – transfer of training

Introduction

Vocational training faces great challenges in teaching professional knowledge at the cognitive level, shaping methodical skills at the behavioural level, and strengthening both self and social competences. As constructivist learning theories point out,

> '(…) learning always occurs individually and in an experienced-based way. (…) The application of knowledge is not independent on the situation it was being learned in. The more similar the learning and application contexts are, the more securely can knowledge be converted into successful action.' (OECD, 2007: pp.226-227)

Even though traditional classroom training is commonly used as a necessary method of teaching profound knowledge in practice, it is not the only sufficient method for training in most professions. More recently, simulation-based learning has been identified as a key method in combining different levels of learning (Hochholdinger & Beinicke, 2012). Simulation-based learning is 'a technique (not a technology) to replace and amplify real experiences with guided ones, often «immersive» in nature, that evoke or replicate substantial aspects of the real world in a fully interactive fashion' (Lateef, 2010: p.348). In practice, simulations can be applied to many different disciplines and types of trainees (Gaba, 1999).

Various challenges apply to vocational training, especially in terms of police officers. First, many police officers' daily practices are dangerous. The officers can be exposed to threats of deadly violence to themselves, colleagues, or the public at any time, and they can even experience this deadly violence first-hand (Andersen, Litzenberger & Plecas, 2002). Furthermore, police officers face situations that require zero tolerance for any deviation from set standards (e.g., violence against police officers). As a result, not every situation can be trained in real life.

Second, creating realistic training settings that provide the best and most realistic training possible for police officer trainees–including situations that can arise in their working lives–is challenging. In addition, a great deal of manpower, equipment, and infrastructure need to be invested to adequately prepare future police officers for their profession.

Simulation-Based Learning In Police Training

The great advantage of simulation-based learning is that it enables trainees to develop professional knowledge, skills, and attitudes while protecting themselves and others (e.g., society) from unnecessary risks. More specifically, simulation-based learning helps to reduce the chance of making mistakes and can simultaneously provide safety. Taking these significant advantages into account, police colleges and academies–which are responsible for basic police training and further education–use simulation-based learning in professional training (Issenberg et al., 2005). Today, training in simulation scenarios (i.e., in realistic scenarios) is a vital part of modern police education (Artwohl & Christensen, 1997; LittleJohn-Shinder, 2001). Implementing simulations as an important part of their curriculum for training future police officers has been well-established, for example, in Finland (Kalalahti, 2016) and Germany (Muff & Beinicke, 2017; Schmalzl, 2008). Moreover, Gadeceau (2015) emphasizes the importance of interactive learning (such as simulation-based learning) for adults in police training programs, which form part of the '*Interpol Guide to Effective Training*'. This observation raises the question of the extent to which simulation-based training settings are effective and help trainees to maximize their learning outcomes.

Effectiveness Of Simulation-Based Learning

A large meta-analysis by Hattie (2009) revealed the main principles of scenario-based training – such as feedback (d=0.73), problem solving skills (d=0.61), and simulations (d=0.33)–to be effective teaching and learning methods. Studies on simulation-based learning in professional workplace settings provide guidelines for the effectiveness of simulations. For example, in a meta-analysis comprising 289 studies, significant effects for simulation-based training were found in a cohort of 18,971 trainees in health professions (Cook et al., 2013). In that study, the main factors for the success of learning were repetitive practice (effect size d=0.68), range of difficulty (d=0.68), cognitive interactivity (d=0.65), multiple learning strategies (d=0.62), and feedback (d=0.44).

Focusing especially on the field of police training, empirical studies on the effectiveness of police training are rare (e.g., Bull & Horncastle, 2008). For example, Vuorensyrjä (2013) investigated 105 Finnish police officers two years after their graduation in addition to analysing their supervisors (n=88). The most valuable method in police training was an integration of case

exercises, including exercises that covered the whole procedure from the beginning to the end and that dealt with cases that are common in alarm or patrol missions, in traffic enforcement, and in criminal investigations.

Sjöberg and Karp (2012) assessed police officer trainees in realistic scenario-based training in Sweden. When video-based debriefing was used in addition to regular debriefing, the trainees significantly improved in motivation and performance scores. In other studies within this work group, the authors identified key factors for effective scenario-based training, namely authenticity and 'simulation competency' of the acting police officer trainee (Sjöberg, 2014) as well as the high quality of the instructor's preparation (Sjöberg, Karp & Söderström, 2015). Such findings confirm the positive impact of simulation-based learning in recent decades.

Objectives Of The Study

The focus of this study was on investigating a training evaluation study to measure the effectiveness of simulation-based training as well as on further verifying whether the vast investment is effective in trainees' learning process. The study covers an important and interesting issue of law enforcement training by examining a simulation-based learning environment.

Main Study - Method

Study Context

The study investigated basic police training at the Bavarian Police College. Bavaria is a federal state in south-eastern Germany with a population of 12.9 million. The Bavarian police has a staff of 42,000 employees, including 3,200 trainees in apprenticeship (2017). During basic police training, every trainee has to complete 5,000 hours of training within two and a half years. The majority of the curriculum consists of lessons in law and other theoretical subjects, practical training in typical work situations (such as traffic checks and interventions in cases of domestic violence), and some additional subjects (such as politics, professional ethics, and physical training). Additionally, the curriculum comprises two individual practical training periods in real police workplace settings during which every trainee has to work in a police station with a senior police officer (i.e., law enforcement official) as a mentor for four weeks (Period 1) and again for twelve weeks (Period 2). A considerable proportion of the curriculum is constituted by 500 hours of simulation-based learning activities, which lead to the final practical exam at the end of the apprenticeship. Each simulation-based learning activity consists of scenario-based training exercises that are typical of the real workplace. Each exercise is completed according to a strict manuscript with detailed instructions for (a) trainers and (b) police officer trainees, who act as the intervening officer or play the role of suspects or witnesses. The trainer is responsible for planning, connecting the content to the theory in class, and providing feedback after the scenario has been completed.

Participants And Procedure

Researchers from the University of Würzburg (Work and Organisational Psychology) and police trainers from the Bavarian police investigated a sample of 220 trainees in basic police training at the Bavarian Police College. The trainees were 21 years old on average (median, age ranged from 17 to 33) and were 72.3% male and 26.4% female. All trainees had participated in two weeks of basic police training. During the first week, the trainees attended traditional classroom training with theoretical lessons in police law, criminal law, and additional subjects. During the second week, the trainees took part in simulation-based training in small groups of eight. The simulation comprised two specific scenarios: Checking a foreigner with a non-valid visa and an instance of disturbance of the peace by youngsters lighting fireworks. We assigned active and non-active parts to each scenario. For the active parts, one trainee played the role of an intervening officer and another trainee acted as the securing officer. Two further trainees assumed an acting role, namely that of the offender, victim, or witness. For the non-active parts, all other trainees from the group were observers. Some trainees had special assignments, such as observing the scenario and providing feedback to the active role players afterwards or merely observing the scenario.

Instruments

To measure the effectiveness of the simulation-based training, we applied objective and subjective training success measures (e.g., Beinicke & Bipp, 2018). First, police trainers and researchers from the University of Würzburg developed customized tests to measure objective training success by assessing trainees' performance in percentage regarding factual and applied knowledge (a multiple-choice test with 70 items and four response options for each item).

Second, training success was assessed subjectively in terms of trainees' self-reporting on various training success scales using the Questionnaire for Professional Training Evaluation (Q4TE: Grohmann & Kauffeld, 2013; Kauffeld, Brennecke & Strack, 2009). Kauffeld and colleagues developed and validated this self-report measure, which is time-efficient, psychometrically sound, and widely applicable across different training contents and settings (Grohmann & Kauffeld, 2013). The Q4TE scales cover all four levels of Kirkpatrick's (1959) framework: *satisfaction*, utility referring to Level 1: reaction; *knowledge*, *self-efficacy* referring to Level 2: learning; *application to practice* referring to Level 3: behaviour; and *individual results* referring to Level 4: results (global organisational results was not assessed due to irrelevance in this study). The questionnaire consisted of 22 items that were rated on an 11-point response scale ranging from 0% (completely disagree) to 100% (completely agree) with increments of 10% each.

We collected the data directly after the traditional classroom training (T1), directly after the simulation-based training (T2), and four weeks after the simulation-based training (T3).

Results

Increase In Effectiveness Of Simulation-Based Training

Overall, the results of the study both objectively and subjectively demonstrate that the simulation-based training was effective (see Table 1; Beinicke, 2016a, 2016b). Cohen's *d* for repeated measures was calculated according to Morris and DeShon (2002).

Regarding measures of objective training success, a paired samples-*t*-test showed that trainees' overall performance significantly increased over time (before and after the simulation-based training) with a large effect, $p<.001$, $d_{\text{repeated measures}}=0.93$. The greatest effects of trainees' objective performance were found in factual knowledge with a large effect, $p<.001$, $d_{\text{repeated measures}}=0.82$; however, applied knowledge also significantly increased over time with a medium effect size, $p<.001$, $d_{\text{repeated measures}}=0.53$.

With regard to the different roles, differences in performance gain was only found on a descriptive level (all *p*'s>.05): The intervening officer had the greatest gain in applied performance (*M*=7.72%). Observers who had been required to provide feedback (*M*=6.34%) learned more compared with their colleagues who had "merely" observed the scenario (*M*=4.42%). The actor showed the lowest gain in applied performance (*M*=3.81%).

Regarding measures of subjective training success, we found a highly significant increase in effectiveness over time in the simulation-based training perceived by the trainees. Specifically, satisfaction with the simulation-based training (*d*=0.40), usefulness of the simulation-based training (utility, *d*=0.48), self-efficacy expectations (*d*=0.31), application to practice (*d*=0.46), and the feeling of personal and professional advancement (individual results, *d*=0.45) increased significantly over the survey period.

Table 1 Descriptive statistics and comparison of time points of objective and subjective training success measures immediately after the traditional classroom training (T1) and directly after the simulation-based training (T2)

Level	Scale	*n*	T1		T2		*p*	*d**
			M	*SD*	*M*	*SD*		
Objective training success								
	Factual	219	51.07	9.66	59.34	9.68	.000	0.82
	Applied	219	52.63	12.16	58.30	13.51	.000	0.53
	Total	219	51.33	8.67	58.31	9.69	.000	0.93
Subjective training success								
Reaction	Satisfaction	216	58.74	14.18	64.79	16.46	.000	0.40
	Utility	220	65.11	15.69	74.45	18.44	.000	0.48
Learning	Knowledge	217	74.16	12.67	63.13	19.89	.000	-0.65
	Self-efficacy	219	67.92	15.69	73.79	17.31	.000	0.31
Behaviour	Application to practice	217	60.19	17.18	66.09	14.62	.000	0.46
Results	Individual results	215	56.44	14.26	62.68	16.14	.000	0.45

Note. Objective and subjective performances are presented in percentage. ***M***=mean; ***SD***=standard deviation; ***d****=effect size $d_{\text{repeated measures}}$

Conclusion

How to Optimize Simulation-Based Training

The results of the study confirm findings on the effectiveness of simulation-based learning. This observation is in accordance with the (subjective) perceptions of police trainers and responsible individuals in the Department of Police Training and Further Education. Role playing as a form of simulation-based training in real police workplace settings has an effect on subjective and objective training success. Combined with traditional classroom training, such simulation-based training can improve factual and applied knowledge, trainees' satisfaction, their perception of the training's usefulness, and their self-efficacy. These effects are even evident in the long term.

Nevertheless, there is room to optimize the simulation-based training. First, trainees qualitatively reported more appreciation for the constructive feedback provided by trainers concerning information about the individual learning process. Appreciation is one of the key factors in motivating individuals to work and study and in increasing their self-esteem in addition to helping them maintain their interest in becoming a professional police officer (Beinicke, 2016a). However, there are limitations to trainers' ability to express their appreciation due to regulations under the Civil Servant Law and exam regulations in Bavaria as well as in most of the other federal states of Germany and in Europe. Trainers have to ensure that the grades of a group of examinees range from an A to an E. All members of the cohort are not allowed to receive only A's or B's.

Second, an easier – but initially exhausting – method of optimisation is via a standardisation of the simulation-based training that involves standardisation across trainers, classes, training modules, and different training centres. Standardisation can be realized in the preparation, conducting, and debriefing of the tutorials. Recording specific training roles is important for planning various scenarios in the long term. Ideally, every trainee should act as an intervening officer, securing officer, actor, and observer within a six-month training period. Moreover, all individual training roles should be recorded to ensure that every trainee has acted in each different role during the entire training period. Other methods of standardisation can involve precise descriptions of acting roles and lists of questions provided by the police college that every trainer can use for the debriefing of simulation-based training. Constant feedback is critical to trainees' objective performance level and is important for individual learning and knowledge-building. The trainees should receive helpful comments and support as often as possible, especially in short and small feedback units. Multiple-choice tests are a very useful tool in providing objective feedback and can be provided by the police college (Beinicke, 2016a).

References

- Andersen, G. S., Litzenberger, R. & Plecas, D. (2002) Physical evidence of police officer stress. *Policing: An International Journal of Police Strategies and Management*. 25 (2), 399-422.
- Artwohl, A. & Christensen, L. W. (1997) *Deadly Force Encounters: What Cops Need to Know to Mentally and Physically Prepare For and Survive a Gunfight*. Boulder, Paladin Press.
- Beinicke, A. (2016a) *Evaluation Polizeilicher Einsatztrainings*. Presentation, Würzburg, Germany.
- Beinicke, A. (2016b) Polizeiliche Einsatztrainings unter der Lupe. E*inblick: Online Magazin der Universität Würzburg*. 38, 16-18. Available from: https://opus.bibliothek.uni-wuerzburg.de/frontdoor/index/index/docId/14535. [Accessed 8th November 2017].
- Beinicke, A. & Bipp, T. (2018) Evaluation training outcomes in corporate e-learning and classroom training. *Vocations and Learning*. 1-28. Available from: https://doi.org/10.1007/s12186-018-9201-7 [Accessed 13th March 2018]
- Bull, R. & Horncastle, P. (2008) Evaluation of police recruit training involving psychology. *Psychology, Crime and Law*. 1, 143-149.
- Cook, D. A., Hamstra, S. J., Brydges, R., Zendejas, B., Szostek, J. H., Wang, A. T., Erwain, P. J. & Hatala, R. (2013) Comparative effectiveness of instructional design features in simulation-based education: systematic review and meta-analysis. *Medical Teacher*. 35 (1), e867-e898.
- Gaba, D. (1999) Human work environment and simulators. In: Miller, R. D. (ed.) *Anesthesia*. Philadelphia, Churchill Livingstone. pp. 18-26.

- Gadeceau, J. F. (2015) Collective intelligence as an effective tool for learning. *European Police Science and Research Bulletin*. 12, 43-50.
- Grohmann, A. & Kauffeld, S. (2013) Evaluating training programs: development and correlates of the questionnaire for professional training evaluation. *International Journal of Training and Development*. 17 (2), 135-155.
- Hattie, J. (2009) *Visible Learning: A Synthesis of Over 800 Meta-Analyses Relating to Achievement*. London, Routledge.
- Hochholdinger, S. & Beinicke, A. (2012) Potenziale und Herausforderungen netzbasierten Lernens in der Weiterbildung. *Personalquarterly: Wissenschaftsjournal für die Personalpraxis*. 2, 16-23.
- Issenberg, B. S., McGaghie, W. C., Petrusa, E. R., Gordon, D. L. & Scalese, R. J. (2005) Features and uses of high-fidelity medical simulations that lead to effective learning: a BEME systematic review. *Medical Teacher*. 27 (1), 10-28.
- Kalalahti, J. (2016) How are simulations used in security sector training in Finland? *European Police Science and Research Bulletin*. 13, 70-76.
- Kauffeld, S., Brennecke, J. & Strack, M. (2009) Erfolge sichtbar machen: das Maßnahmen-Erfolgs-Inventar (MEI) zur Bewertung von Trainings. In: Kauffeld, S., Grote, S. & Frieling, E. (eds.) *Handbuch Kompetenzentwicklung*. Stuttgart, Schäffer-Poeschel, pp.55-78.
- Kirkpatrick, D. L. (1959) Techniques for evaluating training programs. *Journal of American Society of Training Directors*. 13, 21-26.
- Lateef, F. (2010) Simulation-based learning: just like the real thing. *Journal of Emergencies, Trauma and Shock*. 3 (4), 348-352.
- Littlejohn-Shinder, D. (2001) Maximizing the effectiveness of role-play scenario training exercises in development of police crisis intervention skills. *Journal of Police Crisis Negotiations*. 1 (2), 19-27.
- Morris, S. B. & DeShon, R. P. (2002) Combining effect size estimates in meta-analysis with repeated measures and independent-groups designs. *Psychological Methods*. 7 (1), 105-125.
- Muff, A. & Beinicke, A. (2017) *Effectiveness of simulation-based learning in basic police training*. Presentation at the European Police Research and Science Conference, Budapest, Hungary.
- Organisation for Economic Co-Operation and Development (OECD) / Centre for Educational Research and Innovation (2007) *Understanding the Brain: The Birth of a Learning Science*. Paris, OECD.
- Schmalzl, H. P. (2008) *Einsatzkompetenz: Entwicklung und Empirische Überprüfung eines Psychologischen Modells Operativer Handlungskompetenz zur Bewältigung Kritischer Einsatzsituationen im polizeilichen Streifendienst*. Frankfurt, Verlag für Polizeiwissenschaft.
- Sjöberg, D. (2014) Why don't they catch the baby? A study of a simulation of a critical incident in police education. *Journal of Vocational Education & Training*. 66 (2), 212-231.
- Sjöberg, D. & Karp, S. (2012) Video-based debriefing enhances reflection, motivation and performance for police students in realistic scenario training. *Procedia: Social and Behavioral Sciences*. 46, 2816-2824.
- Sjöberg, D., Karp, S. & Söderström, T. (2015) The impact of preparation: conditions for developing professional knowledge through simulations. *Journal of Vocational Education & Training*. 67 (4), 529-542.
- Vuorensyrjä, M. (2013) Learning in police recruit training: findings from the Finnish police recruit training evaluation project. *European Police Science and Research Bulletin*. 8, 4-8.

Integrated Concept for the Training of Trainers Within Police Cooperation of the EU Member States

Žaneta Navickienė
Mykolas Romeris University, Lithuania[1]

Vidmantas Vadeikis
Lithuanian Criminal Police Bureau, Vilnius, Lithuania

Abstract
This paper presents the outcomes of the EU-funded Twinning Light Project "Setting up the SIRENE Office: Strengthening capacities of SIRENE operators and end users of the Schengen Information System II (CRO SIRENE)". This international assistance and support project was conducted throughout 2016 by the Lithuanian Police in cooperation with the beneficiary administration, the Ministry of the Interior of the Republic of Croatia. This paper familiarises readers with the system and integral parts of the qualification improvement process assessed in the Project. The mechanism for the preparation of instructors within public administration bodies in the EU Member States could be seen as an integral process, whereby selected staff members receive initial subject-matter training, deepen their knowledge in advanced subject-matter training, participate in andragogic training sessions, practice their training skills during live training activities, have the possibility to compare working procedures in other EU Member States, and exchange best practices as well as make use of specific tailor-made methodological tools. The creation of new pedagogic standards is relevant in a way that by standardizing process of preparing police instructors, main integral educational tools are identified and applied (i.e. optimal proportion between the form and content of training is determined, training participants are involved into training evaluation process, methodical recommendations for instructors are prepared etc.). Pedagogic standards, which was developed, practically tested and presented by the authors of the research could contribute to the better commitment and ownership of the beneficiary organizations with regard police training under the EU Internal Security Strategy. Furthermore, it could be applied also in other EU Member States by organizing training activities and shaping international network of police instructors.

Keywords: Schengen Area, Second Generation Schengen Information System (SIS II), Supplementary Information Request at National Entry (SIRENE), training of trainers, trainer, instructor.

1 Corresponding author's email: zaneta.navickiene@mruni.eu

Introduction

This paper presents the findings of research conducted within the EU-funded, Twinning Light Project entitled "Setting up the SIRENE Office: Strengthening capacities of SIRENE operators and end users of the Schengen Information System II (CRO SIRENE)" (hereinafter referred to as "the Project"). As the following narrative explains, the Project supported the preparation of training programmes, training materials formed by theory and practice, study visits, and workshops with the aim of developing active, operational national SIRENE offices. The offices' central function is to coordinate cross-border information exchange using the Schengen Information System (hereinafter referred to as "SIS II"). Therefore, they are significant elements in the EU Internal Security Strategy. The main goal of this research was the analysis and presentation of the integrated training of trainers' concept as the contemporary pedagogic standard, which enables sustainable improvement of knowledge of employees of a police organization.

We propose the adoption of a systematic approach towards understanding of the integrated training of trainers' system. Namely, it should comprise of initial subject-matter training, advanced subject-matter training, and andragogic training, practicing training skills while assisting other trainers, comparison of working procedures in other EU Member States and exchange of best practices as well as of using specific tailor-made methodological tools. It is understood that implementation of integral training of trainers' scheme will facilitate long-term results and sustainability in developing and maintaining internal training system within public administration body.

Relevance of the research

We argue that the achievement of the key priorities of the EU Internal Security Strategy (Conclusions of the Council on the Renewed European Union Internal Security Strategy 2015-2020, 2015) is dependent on the qualifications and professional skills of the employees of Member States' law enforcement agencies who are tasked with the important duty of delivering on those priorities. Only the development of their competence by consistent, reliable, and diverse methods can deliver the levels of professionalism and expertise that staff need to perform their duties effectively not just in their homeland but also in the context of international cooperation (Navickienė *et al.* 2016). We argue that the effective training of trainers, capable of instilling that knowledge and expertise in staff is an essential precursor to the professional development of staff. The implementation of the key priorities of the EU Internal Security Strategy is fully dependent on the qualification and skills of the personnel of law enforcement community. Only by developing the competence of police employees by consistent, reliable, and diverse methods, can one ensure the appropriate level of professionalism in officers and adequate preparation for their operation in the homelands and in the context of international cooperation.

The training of police trainers should therefore be understood as a dynamic process of developing instructor's competences and skills not by classical monotonic training methods, but involving complex practices. In that regard, we argue that new (or at least modified) forms of training, substantiated by empirical experience should be used more broadly, Nowadays, scholars pay much more attention to the content of the training of trainers and the impact of complexity on policing (Paullet *et al*, 2017). However, that is not yet reflected broadly enough in the police training literature. It has been noted that police officers have to have integrated knowledge and capabilities (for example; forensic and technical knowledge, relevant to the investigation of modern hardware, software and wider information technologies (Freiling & Zoubek, 2017). Vrij *et al.* (2015) and Freiling and Zoubek (2017) have argued persuasively that complex training is a significant factor in the preparation of skilled and effective police instructors.

That reflects the increasing complexity of the social world and of the tasks that police staff are required to undertake. In the modern era, the acronym 'VUCA' is used to characterise the kinds of challenges that professionals increasingly face. The term was coined by the US Military in the 1990s but it quickly found its way into the business community. It describes the experiences of many people who struggle with decision-making because of the volatility, uncertainty, complexity and ambiguity that is associated with modern workplaces. The term seems particularly relevant to police decision-making, an activity that often is undertaken in environments characterised by high risk and high stress.

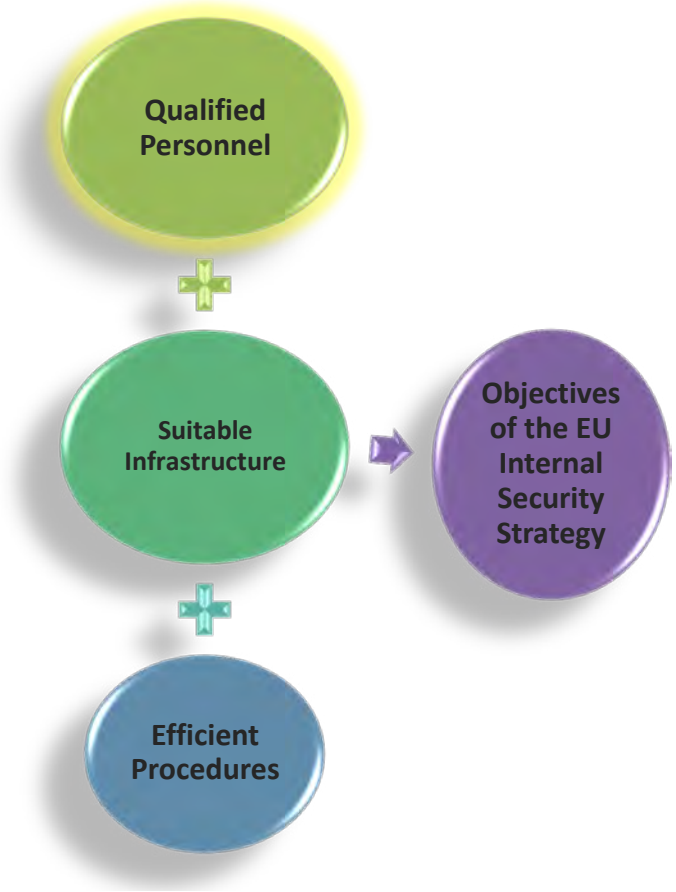
Research methods

In this publication, the following academic and empirical research methods have been used: descriptive-comparative, analytical-critical, content and non-fiction analysis.

The Project

Within the Project, a substantial proportion of activities was related to the organization and delivery of training. One activity within the Project's work plan was directly dedicated to the preparation of trainers. From the authors' point of view that was not enough and we proposed an integrated approach to the training of trainers. The idea found support within the beneficiary administration and in close cooperation was put to practice. The involvement of the beneficiary administration in systematic and demanding approach towards preparation of trainers facilitated the sustainability in outcomes of international aid instruments. We went on to explore the extent to which the competence levels of law enforcement personnel could be raised by applying complex methods involving theoretical and practical training, internships, simulations and testing.

Figure 1 – Achieving the objectives of the EU ISS



Integrated approach to the concept on training of trainers

The Project supports the view that professionalism within the police organizations is achieved through complex training, where knowledge from different areas are combined and the synthesis of that knowledge is embedded and verified by developing and applying targeted practical situations during training events. *Inter alia*, various innovative administrative, technical tools and technologies are broadly developed and introduced in policing. Therefore, it is seen that in the new concept on training of trainers the classical emphasis on learning in classrooms is shifted to innovative and integral forms of training so that the complex approach to training of trainers would dominate. New forms of training are implemented: imitation and decision making in practical situations related to policing; case studies; role-plays etc. In this way, practical training reinforces trainees' relations with their surrounding social environments, allowing them later to synchro-

nize available knowledge and apply their learned behaviours in practice. That is even more important in case of the qualification of police officers. According to researchers such as Steve Tong (2016), besides traditional police capabilities, police officers need additional capabilities to capitalise on various new technological developments.

The concept of preparing the modern instructor inevitably has to change and involve more training events of practical nature into the training of trainers. This is important for the instructor in the future to be capable of acting in the role of a lecturer in a more involving, interesting and purposeful way to the trainees. Sofie de Kimpe (2016) argues that innovation in police training depends upon pedagogical science and greater expertise in the process of police training and education. Pedagogic knowledge, applied to police training, should allow for more consistent and systemic forms of proficiency, which ultimately will allow trainers and students to master training material. We argue that it is an essential feature in the training of trainers because only systemic and coherent understanding of training material allows police officers to be capable of smooth and focused delivery of information while acting as instructors. During the course of developing the new integrated concept of the training of trainers, the authors took into consideration global trends, modern training principles and practices. Two stages could be identified in the organization of training within the Project:

1. Three training programmes were developed for the training;
2. Implementation of integrated training of trainers.

Firstly, training programmes were prepared according to the needs identified by the beneficiary administration. The first training programme was formulated to identify existing professional level of police officers employed at the central unit responsible for international information exchange and to do a refreshment of their competences and skills. The second training programme aimed to form new advanced professional competences and to present the peculiarities of specific skills related to work with the SIS II, main challenges, problems, and solutions for the efficient operation at the central information exchange unit. Furthermore, the second training programme also included the basics of andragogy, different learning methods, and management of training as main principles of efficient implementation of organizing training activities. Whereas, the third training programme was developed solely for police practitioners in the field and is focused mostly on strengthening of their practical skills in daily work. It could be said that the creation of every training programme was followed by identifying target group and was based on principle to include development of both theoretical knowledge and practical skills.

Secondly, the implementation of the concept on the integrated training of trainers was formed from interdependently correlating elements. These purposeful elements mean that the implementation process starts with initial subject matter training as a reference point to refresh existing knowledge and end with the creation of methodological tools for the future tasks for instructors. The authors propose a systematic approach towards the understating of integrated training of trainers.

Figure 2 – Elements of the integrated concept on the training of trainers

The elements of the integrated concept shown in Figure 2 could be further elaborated as follows:

- **Initial subject-matter training** – is the basic professional information necessary for daily work under specific functions;
- **Andragogic and advanced subject matter training** – advanced professional information for

operation under more complex conditions/situations at work and information related to theoretical and practical training delivery skills;

- **Practical training** – practicing instructors' training skills through assistance to experienced trainers during training activities to other officers;
- **Study visits** – visits dedicated for comparison of working procedures existing in other EU Member States and exchange of best practices or internships;
- **Use of guidebooks** – utility of specific tailor-made methodological tools by instructors during their practice as trainers.

We argue that the implementation of the integrated training of trainers' scheme will facilitate long-term results and sustainability in developing and maintaining internal training system within police organization or other public administration body.

During the realization of each element of integrated training of trainers, the balance between theoretical and practical knowledge is set. For example, while organizing first to third elements of the integrated training of trainers, the proportion of time allocated for theoretical and practical sessions was equal and amounted to 4 hours of theory and 4 hours of practical exercises (role-play, simulation, case analysis etc.) (see Figure 3).

Figure 3 – "Andragogic and advanced subject matter training" in detail

Conclusions

The proposed conceptual shift in the training of trainers was practically tested by the authors of the research in the project. It is supposed that the new scheme will contribute to the greater commitment and the ownership of the beneficiary organizations with regard to achieving the objectives of the EU Internal Security Strategy. The concept of preparing contemporary instructor inevitably is changing by involving to the training of trainers more targeted practical training in the area of andragogy. All that makes instructor capable to perform as a trainer sharing his or her professional knowledge to the trainees.

Having regard to the identified aspects of the training of trainers' mechanism, it could be said that the process for the preparation of instructors within police organisations (or other public administration bodies in the EU Member States) needs to be perceived as an

integrated process, a new pedagogic standard, whereby selected staff members receive initial subject-matter training, andragogic and advanced subject matter training, practice their training skills, have the possibility to compare working procedures in other EU Member States and exchange best practices as well as make use of specific tailor-made methodological tools.

References

- Council Conclusions on the Renewed European Union Internal Security Strategy 2015-2020 (10 June 2015, 9798/15).
- De Kimpe, S. A. (2016) A European quality assurance system for police education: a challenge for CEPOL. In: Nogala, D. et al. (eds.) Global trends in law enforcement training and education - Contributions to 2016 CEPOL European Police Research and Science Conference. Budapest, Hungary 5-7 October 2016. *European Police Science and Research Bulletin,* Special Conference Edition Nr. 3, 139-144.
- Freiling, F. & Zoubek, Ch. (2017) Do digital investigators have to program? A controlled experiment in digital investigation. *Digital Investigation*, 20, 37-46.
- Navickienė, Ž., Šileris, E. & Vadeikis, V. (2016) Training of trainers within the EU Twinning Project aimed at capacity building of police organization in Croatia in the field of Schengen cooperation. *Security of Society and Public Order: proceedings of scientific articles*, 17, 158-176.
- Paullet, K., Pinchot, J. & Mishra, S. (2017) Implementing a Successful Train-The-Trainer Program in Mobile Forensics and Security. *Issues in Information Systems*, 18, 1, 173 -179.
- Tong, S. (2016) Professionalizing policing: seeking viable and sustainable approaches to police education and learning. In: Nogala, D. et al. (eds.) Global trends in law enforcement training and education - Contributions to 2016 CEPOL European Police Research and Science Conference. Budapest, Hungary 5-7 October 2016. European Police Science and Research Bulletin, Special Conference Edition Nr. 3, 171-178.
- Vrij, A., Mann, S., Leal, S., Vernham, Z. & Vaughan, M. (2015) Train the Trainers: A First Step towards a Science-Based Cognitive Lie Detection Training Workshop Delivered by a Practitioner. *Journal of Investigative Psychology and Offender Profiling*, 13, 2, 110-130.

Applied Innovation

The Police Café – An efficient method for improving the dialogues between the police and the community

Katalin Molnár
Erna Uricska
National University of Public Service, Budapest, Hungary[1]

Abstract
Nowadays there is an urgent social demand for safer and more liveable communities because of the intensification of national safety problems, international, and transnational threats.
In this article an initiative method will be introduced that was first used by the Belgian Police. The method is called *the Police Café,* after the original method which was called *the World Café*, a structured conversational process. The primary aim of the initiative, that is unique within the Hungarian Police, is to reach the most intensive involvement of the members of the Police and civilians in order to restore and maintain safety.
According to the methodology of *the Café,* the police invite professionals who are somehow responsible for the public safety of the given precinct of a city representing different professions or organisations to carry out an unconventional and innovative conversation.
The protection of safer and liveable communities is our common social responsibility and with this innovative method, the first step can be taken.

Keywords: the Police Café, liveable communities, partnership between the police and the community

The origin of the method

The Police Café is based on the method called the World Café that was invented for community development purposes by Juanita Brown, a leader of an American organisation, 21 years ago (Brown, 2002; Brown & Isaacs, 2005).

At the World Café, the participants of a special area are selected deliberately and they are expected to activate their common thinking by exploiting their collective wisdom through open communication among the partners. In this way, they should communicate efficiently. The purpose of the meetings is to identify, define, name and explore the problems of the area and analyse their causes. Then the participants start to find the solutions, while making precise and serious personal common commitments and taking responsibility. Or more precisely: they try to find the most appropriate solution there and then.

The Police Café also tries to facilitate this creative process, with the difference that the aim here is to evoke cooperation through dialogue among the members of the police and the community, in order to improve local safety. Ideally, the method is preventive in nature

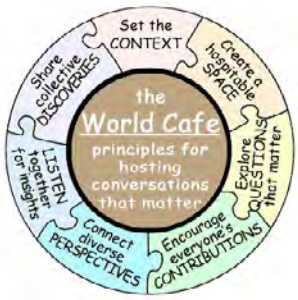
1 Corresponding authors emails: molnar.katalin@uni-nke.hu, uricska.erna@uni-nke.hu.

but it can be applied as brilliantly as a problem solving method, if a specific security deficit occurs.

The meeting has to be carried out as it is laid down in the original methodological principles; only in this way can it be called a *Café*. The methodology of the Police Café is based on the serious protocol of the World Café, but three special principles were added. Table 1 illustrates these principles.

Table 1 The Principles of the World Café and the Police Café

The seven principles of the World Café	The 7 + 3 principles of the Police Café
Set the context.	Set the context.
Create hospitable space.	Create hospitable space.
Explore questions that matter.	Explore questions that matter.
Encourage everyone's contributions.	Encourage everyone's contributions.
Connect diverse perspectives.	Connect diverse perspectives.
Listen together for insights.	Listen together for insights.
Share collective discoveries.	Share collective discoveries.
	The organisation of a Police Café is not compulsory.
	Give the freedom of the selection of the themes to the organisers.
	Do not urge anything. Let the things go in their own speed.



At the same time, the method is relatively cheap. There are some expenses depending on the local needs: besides the establishment of the hosting space in harmonisation with the principles and the expenses of minimal catering (coffee, mineral water and some snacks), it is necessary to spend on the training of the table hosts and to pay the honorarium of the moderator; but these expenses can be regarded as an investment for the whole community in the long run.

How does the Police Café operate?

This Café is called the Police Café because the table hosts are police officers. The participants sit around smaller tables of 6 or 8 and the table hosts who are actually police officers go from table to table with their own special topic and lead the conversations around the tables within a certain time frame. All of the topics represented by a police officer must be addressed by all of the members at the tables. Sometimes the participants may argue and try to chase each other. They argue, ask and answer. They say, show and draw. Finally, the table hosts summarise and compare the comments and the moderator closes the forum.

If it is a Police Café, surely there must be a topic in connection with the police: legislation, legal compliance, misdemeanours or offences? Not really. What is more, sometimes there are not any words about these topics. The main topic is safety. We talk about how to feel good where we live, work, go out and travel. We also

talk about when our living places, streets, workplaces and schools are liveable or when they are not. The police officers, who lead the conversations also live, work, go out and travel with us and they know a lot about safety. But they do not and cannot maintain it without us; but instead help us to create and maintain it. So, this is the reason why we have to talk to each other. And these conversations are supplied by the Police Café.

The beginnings of the Police Café in Hungary

In 2007 a colleague, a well-known figure of Law Enforcement science in Hungary, brought the news of the Police Café to Hungary from Belgium, where the Belgian Police had applied the method to similar purposes. We immediately fell in love with the method. As a result, in 2008, when the master training of the Faculty of Law Enforcement of the National University of Public Service was introduced, we presented the method to the students; but they did not really understand it. We offered the method to others as well - but we were not able to try it out anywhere.

Unfortunately, an unexpected chance arrived in 2014. After a brutal murder of a police psychologist in Pécs, there was an opportunity to come up with an innovative method in order to strengthen local safety (Gaál & Molnár, 2013). We organized four meetings in four precincts of Pécs, just to start the history of the Hungarian version of the Police Café (Gaál & Molnár, 2015) - and at that time we just hoped that it could be a success story.

Since then, Pécs had the first-mover advantage: on 12 May 2015 - a year after the first event - we organised a one-day Police Café training, where the police officers of the 8th district of Budapest could learn the method from their colleagues from Pécs within the framework of the neighbourhood police program. They were the first members, who could organise a thematic Police Café on 9 November 2016 as they had the opportunity to choose a special topic connected to safety, out of the general questions. In 2017 we also tested the method in a Consultation Forum of Public Safety in two districts of Bóly and Sásd to the great satisfaction of the local communities.

Training and supervision for police officers

From the beginning we have considered it a very important element of guaranteeing a good outcome to insist on a prior training before organising a Police Café. It was a great achievement when we succeeded in creating its organisational framework.

The National Crime Prevention Council accredited an 8-hour long, 8-credit training course called *The Police Café – methodological and communicational training course for police officers* in the training system of the Public Procurement Authority in Hungary in the spring of 2016. The registration number of the training is 3/M/2016/5468.

The training lasts a day and it is the best when there are 12-25 persons. Its speciality is that it is an self-experience based learning, so the participants can learn the method while practising it as well. They learn and try everything that is necessary to organise a successful Police Café. Its main advantage is that the trainer can go to the educational place and the participants are able to work out the details focusing on the local specialties and human resources together with the help of the trainer, since the professional content cannot be prescribed.

The year 2017 brought a breakthrough, as we realised that the Police Café series can be arranged in a larger area as well. It requires not only a careful preparation but also an aftercare process. Therefore, we started to organise supervision meetings for the organisers and the contractors of the program by following the classical rules, but also applying the Café methodology as well. Up to now (2018), there were two such events: one of them in Kiskunhalas on 5 July, 2017 and the other in Budapest on 19 July, 2017.

The first significant breakthrough – a webpage was born

A good method is worthless, if it remains unknown - and that is why some marketing was required. On 24 August 2017 a brilliant opportunity appeared that would have been a pity to miss: the methodology of the Police Café could be shown at the inauguration of the National University of Public Service in a 20-minute presentation. At the same time, it went public, as we

had been working with professional marketing experts on the webpage of the Police Café. Finally, we had to wait 5 more weeks for its start.

It was a great pleasure that 10 percent of the attendees had heard about the method earlier from different sources: from Facebook, from a police superintendent, who had been a host in several Cafés, civilian patrols and colleagues. Some of them had already tried the method based on their personal experience from a 'real' Police Café, or acquired through learning, from home or abroad.

After a three-month preparation, on 2 October 2017 the webpage called www.policecafe.hu went online. We try to do our best to reach more and more people with the news of this initiation. Thanks to the person who initially brought the method to Hungary ten years ago and those who helped to make the dream come true!

Finally, the method could have went out to a wider audience. It is not a secret intent of the webpage that those people who are interested in the method, can find all of the continuously updated information that could be useful, valuable and interesting for them easily, in a structured way and in one place.

The origin of the method, the methodological description and the details of the application for the training are the most important sections. But if you glimpsed into the atmosphere of the Police Cafés, you might search in the photo gallery in each location as well. You can find where and when we organised Police Cafés and our presence in the media can also be traced.

The target audience of the webpage can be divided into three groups: police officers, civilians and their communities. Additionally, we would like to raise the awareness of the institutions too. This Police Café is for all of us, together who are more and more often confronted with the safety challenges of the modern world in our everyday lives. The Police Café explores the answers for these questions and if we follow the protocol, we will have a good chance of finding the answers as well.

We encourage communities to initiate and support the opening of the Police Cafés, help the organising process and once there has been a Police Café for a while, please visit it as often as it is possible. In the meantime, please enter the hall of a Police Café and visit the webpage.

The history of the Police Café in Hungary in numbers

The webpage is improving continuously, the forthcoming Police Cafés can be seen, the previous cafés are documented with professional experience reports and they are illustrated with pictures. For result-oriented organisations such as the Police, data can tell a lot, especially when this data is compared to other data. Let's have a look at the history of the Hungarian Police Café in numbers.
In 2014, when the initiation was introduced in Hungary we organised four meetings in one Hungarian city, Pécs.
In the following year there were only two cafés: one of them was in Pécs again and the other one was held in Budapest, the capital.
In 2016 there were nine Police Cafés in nine cities, which is a promising increasing tendency.
But the year of 2017 was even more significant as there were 21 Police Cafés in 12 cities. This can be called a real breakthrough, not only in the arrangement of Police Cafés but in the methodological training of police officers as well. As 40 police officers participated in the 8- hour long training on three occasions in 2016, there were four training occasions and 80 police officers were able to participate in the training in 2017.
If we play with the numbers, let's have a look at the number of the civil participants of the 21 Police Cafés in 2017. We will get this number if we take 18 participants per an occasion. There were 14-24 people around 2 or 4 tables. So, the proper number is 378, because there were 21 Police Cafés. If we deduct the number of those persons who came to several cafés, the number of the participants is still above 300 throughout the country, beside the organisers, hosts, table-hosts and naturally, the moderator. Because of their significant roles in the future, we can state that these persons can be counted as 150 people again. So, there are more than 500 people who were concerned within a year. And this is a number that we may be proud of.

But this is enough about the quantitative measures that can be expressed in numbers. This is not important or relevant for the organisers, hosts and guests but rather they can become parts of qualitative conversations who can sit around a table with a cup of coffee and they can exchange ideas, thoughts and opinions – namely words- about the safety of their surroundings.
It is a great honour for us that through our conference presentation and article, the Hungarian Police Café was able to appear on the colourful methodological map of the European law enforcement.

Impact assessments – for now, at an early stage

It was evident, from the amount of positive feedback supplied to the team, that the project had widespread support. It was very important because a person can believe in the importance of a case but only the feedbacks are able to express the real value of something. In order to express these opinions -based on their own experience about the Police Café - it was necessary to create its proper forums. On the one hand, there is a chance on the webpage for writing comments to the posts. On the other hand, in January 2018 a separate block was created under the title 'Police Café Extra' where there is a chance to leave longer, professional comments.

Evidently, we also try to collect objective feedback about the individual opinions. An analysing summary is being prepared after completing a questionnaire about the 8-part Police Café series in Budapest and the results will be presented, although it is impossible to present them at the moment because of its incompleteness. Within the police officers participating in the project, the aftermath of the same series will be examined as well. It is extremely important to be aware of their opinions and thoughts as well.

To be continued… more Police Cafés

After the description of the method, it is obvious that we would like to bring the method to a wider audience faster but we do not want to be seen as unsatisfied. However, it is necessary to mention the difficulties that we are facing.

One of the most important difficulties in Hungary is the attitude. In spite of the fact that one and a half decade had passed after the first attempts (Cserép & Molnár 2005), it has not become a kind of philosophy - which should have made his way into the entire system of law enforcement: that law enforcement should focus on the communities and their local problems.

In contrast to many excellent projects in this scientific area, the Police Café is not a periodic program but it is such a method with which law enforcement professionals can directly experience its significant role in creating and maintain safety of the community with learning and testing the method. Moreover: they realise that this role can be more serious that they think and sometimes it is even more important for the law enforcement organisations. The regular dialogues that started and were maintained by such communication methods about the local safety can make the partners' common responsibility continuous, which is the key asset to safety.

When the question arose that how we could have a Police Café, it should be noted that organising a Café requires solid professional expertise. One of the purposes of the webpage was that this expertise could be reached. The realisation of the previous trainings and Police Cafés was supported by the National Crime Prevention Council in the form of tenders in Hungary. It is worthwhile looking for the opportunity from the same source but the training and the arrangements can be financed from other sources as well (e.g. municipal, foundation, civil organisation).

With this, we highlighted the other most difficult circumstance, namely the lack of the financial sources. Common thinking presupposes the learning and development demands of the communities for which we have to spend time, energy and money - lots of them. It is not an immediate action, but a long-term investment. Those who learn the method of the Police Café and feel its power in shaping the safety within the community by its application, they believe in it. And not too soon, but in the end, they realise that it is worth investing into the development of knowledge and skills.

The details- the specific topics, the invited guests, the scenes- always depend on the specifics of the local community, they require thorough reflection, careful planning and personal consultations.

Reflections and the relevance of the method

When the authors of the article saw the central topic of the CEPOL conference called *'Innovations in law enforcement – Implications for practice, education and civil society'* in July 2017, both of them thought that the focus of the conference was absolutely for them. The aims and the methodology of the Police Café fitted perfectly into the profile of the conference.

Since the conference it has been frequently asked whether the Police Café has had measurable effects in those communities where it had been tried out and applied. Despite the fact that preventive programs do not have easily measurable results according to their nature we will be able to present the opinion of the participants of the Cafés.

A longer, empirical questionnaire study will be published in autumn 2018 and another study of interviews in spring 2019. It can be said that the reception was positive from both sides of the police and the citizens. Not only the law enforcement, but the community shaping results of the dialogues can be demonstrated as well.

We are convinced that the police do have a serious corporate social responsibility (CSR) with the support of creating and maintaining security as a professional service in a modern democratic state. If it is carried out in a partnership through dialogue with the members of the local community, then it is a clear indication that they take this responsibility seriously. Therefore, the Police Café can be a possible and a prominent tool in the procedure of CSR.

References

- Brown, J. (2002) *The World Cafe: A Resource Guide for Hosting Conversations That Matter. Mill Valley, CA, Whole Systems Associates.*
  Available from: http://www.theworldcafe.com
- Brown, J. & Isaacs; D. (2005) *The World Cafe Book: Shaping Our Futures Through Conversations That Matter.* San Francisco, Berret-Koehler Publishers, Inc.
- Cserép, A. & Molnár, K. (2005) *The first steps of a community policing project*. Magyar Rendészet (2) 99-119.
- Gaál, G. & Molnár, K. (2013) *What can go wrong, does it go wrong? The role of the media in shaping safer and liveable communities.* Boarder Guards' Scientific Journal of Pécs, 131-140.
- Gaál, G. & Molnár, K. (2015) *Police Café Pécs – Innovative Consultation of Police and Civilians about Security.* Policajná Teória a Prax. Ročník. 23(4). 71-78.

Recording Hate Crime: Technical solutions in a training vacuum

Amanda Haynes
Department of Sociology, University of Limerick, Ireland

Jennifer Schweppe
School of Law, University of Limerick, Ireland

Abstract

In Ireland, police record hate crime as part of their operational duties and their remit in collecting crime data. This article addresses the impact on the quality of official hate crime statistics of a technical change to the manner in which the hate element of a crime was recorded in Ireland in 2015. The primary data were collected via two research projects conducted in 2015 and 2017. Both projects addressed the treatment of hate crime in the criminal justice process in Ireland. This article draws on interviews with members of the police and employees of the national Garda Information Services Centre (GISC) conducted for these studies. While technical advancements were made in the recording of hate crime, by 2017 awareness of hate crime recording categories had not been mainstreamed among police officers and little support had been provided to them in interpreting the meaning of categorical labels. While technical training had begun to be rolled out, training on the substantive issues involved had not been mainstreamed and did not address the recording of discriminatory motivations. The technical changes to the police recording of hate crime in Ireland evidence a progressive ethos with respect to:

- Recording the hate element of a crime beyond the limits of legislation
- Identifying victims of hate crime
- Including a wide range of identities

However, in the absence of agreed definitions and training, the impact of this technical change will, we argue, be limited.

Keywords: Hate Crime, Crime Recording, Ireland

Introduction

In Ireland, hate crime is recorded by the police as part of their operational duties and as part of their remit in collecting crime data. Police recorded data is provided by the police to the Central Statistics Office (CSO) who are responsible for assessing the quality of the data, collating statistics, and disseminating information. This article addresses the impact on the quality of official hate crime statistics of a technical change to the manner in which the hate element of a crime was recorded in Ireland from 2015.

The primary data in which the findings presented herein are grounded were collected via two research projects. The fieldwork for the first project, *Out of the Shadows' Legislating for Hate Crime in Ireland* (Haynes et al. 2015), which was funded by the Irish Council for Civil Liberties, was conducted in 2015 and the fieldwork for the second project, *Lifecycle of a Hate Crime* (Haynes & Schweppe 2017b),funded by the European Commission, Directorate-General Justice Rights Equality and Citizenship Programme, was conducted in 2017. Both of these projects related to the treatment of hate crime in the criminal justice process in Ireland. This research draws on qualitative interviews with members of the national police force conducted for both studies. In both cases, we formally applied to the national police service, An Garda Síochána, to interview police officers, and received ethical approval for the research from our institution, the University of Limerick. The first period of fieldwork in 2015 resulted in interviews with 12 police officers, primarily members tasked with addressing the needs of ethnic and LGBT minorities, referred to as Ethnic Liaison Officers and LGBT Liaison Officers respectively. The second period of fieldwork in 2017 included interviews with 18 police officers. During the course of the second research project we also had the opportunity to interview five employees of the national Garda Information Services Centre (GISC) who accept, log, and review police generated crime incident reports.

What is a Hate Crime?

Given the absence of an agreed EU definition of hate crime, we acknowledge differences among Member States in the manner in which "hate crime" is interpreted. Internationally, the most widely shared definition of a hate crime is an offence which is known to the criminal law and is committed in a context that includes identity-based hostility. The *Organisation for Security and Co-operation in Europe* (OSCE) describe a hate crime as:

> "... criminal acts committed with a bias motive. It is this motive that makes hate crimes different from other crimes. A hate crime is not one particular offence. It could be an act of intimidation, threats, property damage, assault, murder or any other criminal offence. The term "hate crime" or "bias crime", therefore, describes a type of crime, rather than a specific offence within a penal code. A person may commit a hate crime in a country where there is no specific criminal sanction on account of bias or prejudice." (OSCE/ODIHR 2009a)

This is the definition which we adopt in this article.

The Social Significance of Hate Crime

It is internationally accepted that hate crime has a more significant impact on its victims than ordinary crime (Iganski 2008). Direct impacts can range from physical injury to emotional and psychological harm.

> "I was working with a mother last year whose son was abused by [a] neighbour physically, verbally, they suffered property damage – spray paint on the house. The child tried to kill himself twice. He poured detergent over his skin because he thought it would make him white." (Employee of an Irish Civil Society Organisation) (Haynes et al. 2015).

Research increasingly supports the conclusion that there is a qualitative difference in the impact of hate crime as compared to non-hate motivated incidents. For instance, data from the Crime Survey for England and Wales (CSEW) showed that victims of hate crime were more likely than victims of crime overall to say they were emotionally affected by the incident (92 per cent and 81 per cent respectively) (Corcoran, et al 2015). Thirty six per cent of hate crime victims stated that they were "very much" affected compared with just 13 per cent of non-hate crime victims. The data also showed that twice as many hate crime victims suffer a loss of confidence or feelings of vulnerability after the incident compared with victims of non-hate crime (39 per cent and 17 per cent respectively). Hate crime victims were also more than "twice as likely to experience fear, difficultly sleeping, anxiety or panic attacks or de-

pression compared with victims of overall CSEW crime" (Corcoran et al. 2015; Herek et al. 1999).

Hate crime not only impacts on its direct victims: the targeting of victims on the basis of their membership of a particular community "communicates to all members of that group that they are equally at risk and do not belong" (Haynes et al 2017a). As such, the terrorizing effect of hate crime goes beyond the individual to generate fear and anxiety among the broader community of which the victim is part; what the EU Agency for Fundamental Rights (2014) refers to as the "resonating nature of hate crime", or what Perry and Alvi (2012) refer to as the "in terrorem" effect of hate crime. Hate crimes then can be perceived as "symbolic crimes" that operate as an exclusionary practice regulating marginalised groups in society (Perry 2003; Chakraborti & Garland 2015; Hall 2013; McDevitt et al. 2001).

The Importance of Hate Crime Statistics

In its implementation report on the EU Framework Decision on combating certain forms and expressions of racism and xenophobia by means of the criminal law, the European Commission specifically addressed the issue of data collection, asserting that States should produce "reliable, comparable and systematically collected data... in order to assess the level of prosecutions and sentences" (European Commission 2014). The publication of hate crime data benefits the wide range of non-state stakeholders who can use the data to inform their own interventions in respect to combating hate crime. More generally, the publication of hate crime statistics serves to raise public awareness of the reality of hate crime and of reporting and recording mechanisms. International organisations such as the European Commission against Racism and Intolerance (ECRI), the Committee on the Elimination of Racial Discrimination (CERD), the United Nations Human Rights Council (UN HRC) and the Organisation for Security and Co-operation in Europe (OSCE) look to data collection mechanisms as a means of promoting approximation of laws on hate crime (Perry 2015; Whine 2016):

> "The argument for evidencing the nature and volume of hate crime has been repeatedly made by the OSCE and FRA. The European Commission against Racism and Intolerance (ECRI) has similarly focused on the need to collect data on 'racist violence' and the UN Human Rights Council and Committee on the Elimination of Racial Discrimination (CERD) have made similar calls" (Perry 2015, p.72).

The official recording of hate crime at the point of first contact with the criminal justice system is important for three key reasons. First, it supports the appropriate investigation and prosecution of the hate element. Second, it ensures that victims are directed to appropriate support services. Finally, it allows police forces to develop informed policy responses. The Subgroup on methodologies for recording and collecting hate crime data of the EU High Level Group on combating racism, xenophobia and other forms of intolerance asserts that, given the importance of data on hate crime:

> "Appropriate mechanisms thus need to be in place to enable law enforcement officials to identify the potential bias motivation of an offence, and to record that information on file. Having such mechanisms in place would also help ensure that victims and witnesses can report hate crimes to law enforcement authorities with confidence." (EU High Level Group on combating racism, xenophobia and other forms of intolerance 2017, p.4).

Ireland's legislative and policing context

Ireland has a range of international obligations with respect to combating hate crime by means of the criminal law, but has not introduced any legislation designed for this express purpose. In particular, the 2008 EU Council Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law requires Member States, under Article 4, to "take the necessary measures to ensure that racist and xenophobic motivation is considered an aggravating circumstance or alternatively that such motivation may be taken into consideration by the courts in the determination of the penalties". In a 2012 publication on hate crime in the EU, EUFRA noted specifically that data on hate crime in Ireland is "limited because criminal law does not define racist or related hate offences as specific offences, nor does it expressly provide for the taking into account of racist motivation as an aggravating factor…the 2008 Irish Crime Classification System…does not cover offences with a suspected hate motivation" (European Union Agency for Fundamental Rights 2012a, p. 37).

The Production of Official Statistics on Hate Crime in Ireland

It has been noted that the Republic of Ireland does not have hate crime laws. Despite this, An Garda Síochána surpassed the limits of legislation with respect to recording over a decade ago and have been proactive in facilitating the recording of what they refer to not as hate crime, but as crimes with a discriminatory motive, since 2002. The recording of discriminatory motives occurs at the point of logging crimes onto PULSE - the computer-based national incident recording system. In the main, crimes are recorded onto PULSE via a telephone exchange between the police officer attending the scene or to whom the crime has been reported, and call takers at the Garda Information Services Centre (GISC) who take the police officer through the online reporting process and type in the details they provide.

GISC was rolled out nationally in October 2006 with the objective of reducing the administrative workload of An Garda Síochána. The purpose of the system was to centralize the collection of data relating to criminal offences, providing Garda management the platform to inform policies and practices in this regard (NCC 2004). According to the Central Statistics Office in a report published in June 2015, the most common variables for recording a criminal offence included: the date and time of incident occurrence; date of incident report; incident type; detection status; date of birth of victims and suspected offenders (where applicable); narrative of incidents; location of incident; and the modus operandi (MO) of the crime (Central Statistics Office 2017).

In recording details for this latter category, there were a range of approximately 40 MOs, or crime motivations, available to gardaí on the incident details screen, including corruption, domestic violence, extortion, jealousy and monetary gain. From this alphabetized list, five MOs related to hate motivations from 2002 to 2015: racism, xenophobia, antisemitism, homophobia and sectarian.

Recording methodology prior to 2015

The recording of discriminatory motivations commenced in 2002 as a result of Garda HQ Directive No 188/2002, which established that racist motivations were to be captured on PULSE. The 'perception test' was utilised in this Directive: that is, where the victim or any other person perceived the crime to be racist, it should be recorded as such (discussed in detail later in this article). Recording was later extended to include categories for homophobia, antisemitism, sectarianism and xenophobia. The category of xenophobia quickly became defunct and the Central Statistics Office reports (Central Statistics Office 2017) that by 2006, no data was being recorded for xenophobic motivations. The category was discontinued from 2007 (Central Statistics Office 2017). This same year the 2002 Directive was replaced with Directive 04/2007 which retained the perception test, but did not expand reference to any category beyond racism.

Discriminatory motivations were available to select within the database relating to criminal offences only. Within that database, the categories were included on the incident details screen as five among an alphabetised list of more than 40 motivations, including corruption, domestic violence, extortion, jealousy, and monetary gain. Taylor notes in a 2010 discussion of how PULSE works:

> "There is no mandatory field which must be completed at the recording stage to note whether an incident had a racist aspect. As a result a lot depends upon the victim's reporting and insistence on identifying the racist aspect, and furthermore a lot depends on Garda discretion as to what is written into the narrative section of the PULSE recording system" (Taylor 2011, p.18).

Until 2015, while a motivation for the offence had to be selected, there was no compulsion on PULSE users to specifically address the question of whether a crime might have had a discriminatory motive specifically.

Data 2006-2014

The table below presents Irish official statistics on the numbers of crimes recorded as having a discriminatory motivation for the period 2006-2014.

Table 1: Crimes recorded as associated with a discriminatory motivation 2006-2014

Discrimination type	2006	2007	2008	2009	2010	2011	2012	2013	2014
Anti-Semitism	1	1	2	5	12	3	4	2	4
Homophobia	21	11	9	32	13	21	17	17	13
Racism	171	210	165	122	111	132	93	93	93
Sectarian	6	11	1	2	3	4	3	6	œ4

As we can see, the number of crimes recorded as having a racist motivation peaked in 2007, with 210 such crimes reported, dropping to a low of 93 such crimes across 2012-2014. Crimes recorded with a homophobic motivation peaked in 2009 with 32 such crimes, falling to only 13 in 2014. The number of crimes recorded with an antisemitic motivation reached a high of 12 in 2010. Figures for sectarian crime peaked in 2007.

It has been widely acknowledged both by members of An Garda Síochána and by civil society organisations that the figures presented here were an underrepresentation of the number of crimes with discriminatory motives occurring in Ireland. Members of An Garda Síochána to whom we spoke in the course of our 2015 research fully accepted that police recorded data represents a significant undercount of hate crime occurring in Ireland (Haynes et al 2015). Gurchand Singh, the Head of Analysis, observed that the official figures:

> "… are not a reflection of the trends, extent, depth of hate crime in Ireland… [we cannot] assume that all incidents are reported to us. The challenge is knowing what [the] proportion of incidents reported to us are …." (Haynes et al 2015).

PULSE 6.8 and the 'Technical Solution"

The 2014 Garda Inspectorate Crime Investigation Report recommended that An Garda Síochána ensure that all crimes containing elements of hate or discrimination were flagged on PULSE, and advised for the creation of clear modus operandi features on PULSE that would allow the accurate recording of the nine strands of the Diversity Strategy. In November 2015, in anticipation of the Victims' Directive, a new way of recording crimes with a "discriminatory motive" was introduced, which made changes to both the recording categories and the recording process. As part of an update called PULSE 6.8, the five pre-existing recording categories were replaced. In November 2015, An Garda Síochána began recording eleven categories of discriminatory motives which were generated to reflect the police service's strands of diversity, in collaboration with the Garda Racial and Intercultural Diversity Office: Ageism, anti-disability, anti-Muslim, anti-Roma, antisemitism, anti-Traveller, gender related, homophobia, racism, sectarianism, and transphobia.

This was a significant change, providing for the recognition of hate motivations towards quite a comprehensive range of commonly targeted groups. On a critical note, neither religion, nor a lack of religion or belief, were included as discrete recording categories, therefore there is no marker to identify religiously aggravated crimes that are not antisemitic or anti-Muslim. Nonetheless, the expansion of the range of recording categories under PULSE 6.8 reflects Perry's (2001) assertion that we need to recognise the historically and culturally contingent character of hate crimes. Thus, the sectarian and anti-Traveller categories would not necessarily be as relevant in other jurisdictions, but allow for the recording of important local manifestations of hate in Ireland (see O'Connell 1997; see Carr 2015).

Possibly an equally significant methodological change is that made to the process of recording. PULSE 6.8 has altered the location of the discriminatory motive recording categories within the incident recording system for criminal offences. First, it has introduced a discrete question on discriminatory motives, rather than requiring that the user locate the eleven categories within a general motivations question. Second, the new discrete question on discriminatory motives is located in a dialogue box on the Victim Needs Assessment screen, which requires gardaí to indicate where the victim requires an individual needs assessment as a result of , for example, their status as a child, a person with a disability, a repeat victim,[1] a victim of domestic violence, or the presence of a discriminatory motive. The question on discriminatory motives offers the person logging the report a choice of the eleven discriminatory motives, plus an option which indicates that no discriminatory motive was present; one of these twelve options must be selected. Further, selecting an indica-

1 The Garda on the scene checks PULSE to ascertain whether the victim is a repeat victim.

tor of a discriminatory motive on the Incident Details screen automatically populates the discriminatory motives markers on the Victim Needs Assessment screen. Equally, selecting a discriminatory motive on the Victim Needs Assessment screen automatically populates the wider-ranging motives tab on the Incident Details screen.

This change suggests that information on discriminatory motives is sought for the purposes of victim support rather than investigation, a position which is supported by research interviewees who confirm that the selection of the marker shapes neither the investigation nor prosecution of a crime: however, the eleven discriminatory motives are ostensibly more visible under 6.8 than they were previously. The visibility of the question is copper fastened by its mandatory status: under PULSE 6.8 all users logging incidents by phone with GISC (the civilian service tasked with populating the crime incident database) are asked to complete the Victim Needs Assessment screen and must address the question of whether or not the crime had a discriminatory motive. Given that the 2017 *Report of the Expert Group on Crime Statistics* (Department of Justice 2017) asserts that every addition of mandatory data involves "legal, administrative and technical implications", the compulsory nature of the question on discriminatory motives indicates a commitment to fulfilling the State's obligations under the Victims' Directive to identify victims of hate crimes in order to provide them with access to appropriate supports.

The number of crimes recorded as having a discriminatory motive increased dramatically following the introduction of this technical innovation: from 114 in 2014 to 308 in 2016:

Table 3: Crimes recorded as associated with a discriminatory motivation 2016 [2].

Ageism	38
Anti-Disability	12
Anti-Muslim	13
Anti-Roma	*
Antisemitism	*
Anti-Traveller	25
Gender related	31
Homophobia	28
Racism	152
Sectarianism	*
Transphobia	*
Total	**308**

One of the challenges to the reliable recording of crimes with a discriminatory motive is police awareness of the recording categories. Having spoken to ELO/LGBT officers about their awareness of the pre-PULSE 6.8 recording categories in 2015 (see Haynes et al 2015), in 2017 we spoke both to members of An Garda Síochána and civilians working as call takers (Incident Creation Representatives) in the Garda Information Services Centre who log reports to PULSE on behalf of the police (see Haynes and Schweppe 2017).

In an earlier study, in interviews with gardaí conducted in 2012, Clarke (2013) found that officers differed in their understanding of recording procedures for racist crime – and that most did not know the definition of racism used by the service, or even that the service was required to record the numbers of racist crimes. Our 2015 research found that, pre-PULSE 6.8, police were broadly aware of the racist discriminatory motive.

However, while all of the interviewees in our research in 2015 were aware that it was possible to record a crime as racially motivated using the drop down motivations menu, there was less consistency in awareness of the other available prejudice-related categories (Haynes et al 2015). Few garda interviewees mentioned the category of antisemitic motivations. None mentioned sectarian motivations. While there were generally high levels of awareness of the potential for homophobic

2 * Indicates that there were between 1 and 3 crimes recorded in this category, but that the number of cases did not meet the Central Statistics Office's minimum frequency rules for the purposes of reporting. The CSO was not in a position to disaggregate by offence type.

crime, one ELO/LGBT officer was unaware that it was possible to record a homophobic motivation on PULSE.

> *"Interviewer: Do you know if you can record a homophobic motivation?"*
> *Interviewee: No. Definitely not.*
> *Interviewer: You can't?"*
> *Interviewee: Could you flag it as homophobic? … apart from the narrative? I don't think you can."*
> (Garda)

We raised the question of how bias-related motivations such as transphobia and disablism which are not available through the motivations menu on PULSE might be recorded. Responses varied; some interviewees suggested that they would use the menu entry for homophobia in flagging transphobic motivations:

> *"Interviewer: What about transphobic now?*
> *Interviewee: We have to record it under homophobic because there is no other place for it. The workaround at the moment … is to include transphobia in the narrative."* (Garda)

Others suggested that they would just note the motivation in the narrative section of the report. In one case the garda interviewee was unable to say how they might record either a transphobic or a homophobic motivation.

Although the Garda Inspectorate (2014) report *Crime Investigation* refers to the existence of an organisational definition of both racist and homophobic incidents, An Garda Síochána interviewees referred only to an organisational definition of racist incidents.

> *"Interviewer: Is there a definition of homophobic crime in An Garda Síochána? Interviewee: No."* (Garda)

While we saw earlier that some ELO/LGBT officers worked on ensuring that transphobic motivations were recorded, others had no understanding of the concept as we can see here from this participant.

> *"Interviewer: What about transphobic crimes?*
> *Interviewee: Transphobic crimes? Tell me what a transphobic crime is?"* (Garda)

Awareness of recording categories post-PULSE 6.8

Following the introduction of a discrete and mandatory question on discriminatory motives in November 2015 as part of the PULSE 6.8 update, GISC call takers interviewed in 2017 for this research unanimously agreed that they initially listed all eleven discriminatory motives available each time a report was made. Over time, however, this practice faded out they explained, with some call takers prompting officers where they perceived a particular discriminatory motive to be relevant to the incident details, and others asking an open question on whether any discriminatory motives were present in the case:

> *"I don't list it anymore. I just ask if there's any discriminatory motives."*
> (GISC Employee)

Gardaí interviewed in 2017 displayed little awareness of the recording categories when we asked them to recall the categories of discriminatory motive available:

> *"Interviewer: Do you recall what the categories are?*
> *Interviewee: I don't … I can't recall, no."* (Garda)

We then prompted participants by asking if they were aware of the presence of particular discriminatory motives available. Again, participants evidenced very low levels of awareness of specific categories:

> *"Interviewer: Is there an anti- Traveller motivation that's possible on PULSE? Interviewee: I'll have to check that and come back to you."* (Garda)
> *"Interviewer: Were you aware for example that anti-disability is listed as a discriminatory motive?*
> *Interviewee: No."* (Garda)

Indeed, the only individuals with a comprehensive knowledge of the available recording categories worked primarily with victims and in the Garda Racial and Intercultural Diversity Office.

Training and Policies

Awareness of a suitable range of recording categories is valuable but not enough by itself. Our 2015 research noted that, with the exception of the brief HQ Directives which govern the recording of discriminatory motives in Ireland, there was no other documentation detailing recording protocols, nor any training on the subject (Haynes et al 2015). An Garda Síochána began delivering diversity training to specialist officers since 2002 through the Garda and Racial Intercultural Office (GRIDO) with the assistance of representatives of minority groups (McInerney 2017), but this training is not mainstreamed nor, according to interviewees, does

it specifically address the recording of discriminatory motives.

In 2017, we found that training had been provided to alert members of the service to the introduction of new screens and questions in PULSE 6.8, although it appeared that not all members had had access to this training over a year following the rollout of the update (Haynes and Schweppe 2017):

> *"In theory they were supposed to know about all the changes that come through. But with all the cutbacks and everything a lot of them weren't getting their CPD [continuous professional development]."* (GISC employee)
> *"I can't think of any specific training."* (Garda)

Interviewees unanimously agreed that neither civilian call takers nor police officers had had access to either training or documentation on protocols for recording a discriminatory motive specifically, for example the circumstances under which a discriminatory motive should be recorded (see section below on the perception test) or the definitions of the various constructs referenced in the recording categories to be used.

> *"I went into [PULSE] recently, the tab for … an injured party for a person and I just went in and it was all these different tabs. I filled them out … you're asking me what they are, I don't know. … Like no doubt I was given an e-mail. But they get lost."* (Garda)

In the absence of institutional definitions, both police officers and call takers had to rely on common sense understandings and individualised interpretations of the constructs referenced.

> *"Interviewer: So you didn't get any training in terms of this is what transphobia is or?*
> *Interviewee: No. I think it's just taken you'd know yourself which sounds a bit weak really."* (Garda)

Consequently, both groups evidenced variation and uncertainty in interpreting recording categories. These issues are exemplified in the following excerpts from interviews with police officers in which they discuss their understanding of the recording category "gender-related":

> *"I don't know whether it comes down to transsexual?"* (Garda)
> *"I presume it's LGBT?"* (Garda)
> *"… if you have a female present and there is abuse hurled at her."* (Garda)
> *"A crime against someone because a suspected offender doesn't like a female or a male."* (Garda)

In discussing such challenges, a senior officer emphasized that:

> *"Training is more effective than guidelines"* (Garda)

Prior to any such training, however, detailed protocols for the recording of discriminatory motives are required, including agreed definitions of the eleven recording categories.

> *"Interviewer: Did you get any guidance on what the different discriminatory motives mean?*
> *Interviewee: Not really. They don't really. It's ageism and that's it. It's just one phrase. Doesn't give specifics as to what that is. Or it could be racially motivated but it doesn't specify anything else, it's just racial. D'you know?"* (GISC employee)

Operationalization of the perception test

The Garda HQ Directive No 04/2007 retained perception as the criterion for recording a racist discriminatory motive. This criterion was developed initially in England and Wales in the 1999 Macpherson Report, the product of an inquiry set up in the wake of the racist murder of Stephen Lawrence to examine the investigation of racially motivated crimes by London's Metropolitan Police Service (MPS). In the UK, the Macpherson Report "has been identified as the most significant driver for the recognition of targeted victimisation" (Mason et al 2017). England and Wales' College of Policing, in its 133 page long 2014 *Hate Crime Operational Guidance,* explains the perception test as follows:

> "For recording purposes, the perception of the victim, or any other person … is the defining factor in determining whether an incident is a hate incident, or in recognising the hostility element of a hate crime. The victim does not have to justify or provide evidence of their belief, and police officers or staff should not directly challenge this perception. Evidence of the hostility is not required for an incident or crime to be recorded as a hate crime or hate incident …If the facts do not identify any recordable crime but the victim perceived it to be a hate crime, the circumstances should be record-

ed as a non-crime hate incident and not a hate crime." (College of Policing 2014, p.6)

As noted above, the Macpherson definition of a hate crime or incident covers any incident which is perceived to be hate motivated *"by the victim or any other person"* (Macpherson 1999, 15-16). This is clearly a remarkably subjective definition – its purpose is to ensure effective and appropriate investigation. In Ireland, Garda HQ Directive No 04/2007 states that any incident which is perceived by "the victim or any other person" – for example the police officer, a witness, or a person acting on behalf of the victim – to have a racist motivation should be recorded as such.

Awareness of the perception test

In 2015 we had noted low levels of awareness of the relevance of the perception test to the recording of discriminatory motives in Ireland. In 2017, we found no evidence that awareness of the perception test had been mainstreamed. In this research, there were mixed understandings of the circumstances in which a discriminatory motive would be selected, with this garda stating that he would require evidence of a racist motive before the box would be ticked:

> *"Interviewee: So once you're satisfied that the incident … or that the statement complies with what you believe to be a racially motivated incident well then that's when you tick it.*
> *Interviewer: So the person will say I think it's racially motivated and then … do you need to verify that? Is that what you're saying to me?*
> *Interviewee: Yeah, it's like an allegation of an assault. You can't put someone down as being a suspected offender in an assault until you know the facts of the case. So that … that pretty much goes in line with that. Until you're 100 per cent certain or satisfied … you know it's your opinion as to what you're hearing from that person. You believe its bona fide allegation so you tick it."* (Garda)

Two gardaí described circumstances in which they would tick the box which approximated implementation of the perception test, but when we asked why they would take this approach, they responded that it was not because of any training, but rather, their own gut instinct.

Only those police officers who worked exclusively with victims and who had additional training on hate crime had any knowledge of the perception test. McInerney (2017) emphasises that full training for all officers in applying the Macpherson definition is essential. One individual who explicitly referred to the perception test had become aware of it through a course outside An Garda Síochána. A second, who undertook a training course delivered to all gardaí in the area, said to us that the trainer themselves was unaware of the circumstances in which an incident would be recorded as racist, and the garda had to instruct and correct the trainer on the perception test:

> *"Interviewer: So what was the trainer's perception of when you would tick the box for a racist motivation?*
> *Interviewee: If the guard believed it was racist then he'd tick the box … The lads delivering the course were great and everything … and said we didn't actually know that, you know. And that training was delivered to all the guards in [the District] and nobody knew what they were talking about."* (Garda)

Whatever methodology is adopted, the absence of clear protocols regarding the circumstances under which a discriminatory motive should be recorded impacts the reliability of the data collected. It is clear that at present members of An Garda Síochána differ in their belief as to whether it is the victim, or the police officer's perception, which determines recording, and more specifically, whether evidence is required. At present, victims cannot be certain of the protection proposed by the perception test against individual or institutional bias preventing the recording – and likely the investigation - of a hate element.

Conclusions

Ireland's police can be commended for taking a proactive, expansive, and inclusive approach to recording hate crime. By requiring members to answer the question of whether a crime they are recording had a discriminatory motivation, those seeking to record a crime are at least theoretically required to consider whether there was a hate motivation to the crime. The technical changes introduced via PULSE 6.8 evidence a progressive ethos with respect to:

- Recording the hate element of a crime beyond the limits of legislation
- Including a wide range of identities

- Making consideration of the presence of a hate element compulsory

The innovation has achieved a substantial increase in the number of recorded crimes with a discriminatory motive. However, in the absence of agreed definitions and training, the impact of this technical change will, we believe, be limited.

The quality of crime statistics is impacted both by methodological shortfalls and human error. Indeed, the EU Sub-group on Methodologies for Recording and Collecting Hate Crime has dedicated the first two years of its labours to improving police recording practices (EU FRA 2017). In Ireland, police recorded hate crime data do not attain the standards of quality required by those jurisdictions to be accorded the status of national statistics. The Irish State has not made official statistics on police recorded hate crime publically available since the end of 2016. The Central Statistics Office made the data cited in this article available to us on request to support our analysis. With specific reference to data on "discriminatory motivations" the Central Statistics Office in Ireland warns users:

> "It is important to note that the levels of crime with a discriminatory motive recorded in Ireland are very low in comparison with figures in other jurisdictions." (CSO 2017)

In the course of this research, we found significant shortfalls in police officers' awareness and comprehension of hate crime recording categories. The findings of our qualitative fieldwork with police officers and incident creation representatives places important context on the operational impact of the jurisdiction's "lists of bias indicators that police officers can use to identify the bias motivation underlying the reported offence" and "specific instructions, guidance or training on recording hate crime" recorded in the Subgroup on methodologies for recording and collecting hate crime data's *Improving the Recording of Hate Crime by Law Enforcement Authorities*. While we recognise the advancement which the list of eleven discriminatory motivations available to Irish police represented, we conclude that, by 2017, awareness of the new recording categories had not been mainstreamed among gardaí and little support had been provided to them in interpreting the meaning of the categorical labels. While technical training on the use of the recording system had begun to be rolled out, training on the substantive issues involved had not been mainstreamed and the training that was available did not specifically address the recording of discriminatory motivations.

We conclude that progress achieved via pulse 6.8 could be furthered with policy and training to address:

- Agreed definitions of recorded categories
- Applicability and meaning of the perception test
- Awareness of categories

Such training should be delivered across the force as a whole to ensure there is a collective and shared understanding of hate crime among all stakeholders - police, VSOs, call takers and reviewers.

The importance of such interventions cannot be overstated. Our 2015 research found that the point of recording is the first, and potentially the most significant, point at which a hate element can be disappeared from the criminal justice process (Haynes et al 2015). This 'filtering out' is significant in its impact on the visibility of the hate element of crimes to the criminal justice system: Where a hate element is not recorded at the point of reporting, it is unlikely that it will be investigated and prosecuted.

References

- Carr, J. (2015) *Experiences of Islamophobia: Living with racism in the neoliberal era,* Abingdon, Oxon: Routledge.
- Central Statistics Office (2015) *Review of the quality of crime statistics,* http://www.cso.ie/en/media/csoie/releasespublications/documents/crimejustice/2015/reviewofcrime.pdf, accessed 6 October 2017.
- Central Statistics Office (2017) *Crimes with a Discriminatory Motive: Information Note,* Cork: Central Statistics Office.
- Chakraborti, N. & Garland, J. (2015) *Hate Crime, Impact, Causes & Responses,* London: Sage.
- Clarke, H. (2013) *Recording Racism in Ireland*, Dublin: Integration Centre.
- College of Policing (2014) *Hate Crime Operational Guidance,* Coventry: College of Policing.
- Corcoran, H., Lader, D. & Smith, K. (2015) *Hate Crime, England and Wales 2014/2015*, London: Home Office.
- Department of Justice (2017) *Report of the Expert Group on Crime Statistics,* <http://justice.ie/en/JELR/Report_of_the_Expert_ Group_on_Crime_Statistics_2017.pdf/Files/Report_of_the_Expert_Group_on_Crime_Statistics_2017.pdf> accessed 8 November 2017.
- EU High Level Group on combating racism, xenophobia and other forms of intolerance: Subgroup on methodologies for recording and collecting hate crime data (2017) *Improving the Recording of Hate Crime by Law Enforcement Authorities: Key Guiding Principles,* Brussels: European Commission.
- European Commission (2014) *Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law COM/2014/027 final*, Brussels: European Commission.
- European Union Agency for Fundamental Rights (2012a) *Data in Focus Report: Minorities as Victims of Crime,* Vienna: European Union Agency for Fundamental Rights.
- European Union Agency for Fundamental Rights (2012b) *Making Hate Crime Visible in the European Union: Acknowledging Victims' Rights,* <http://fra.europa.eu/sites/default/files/fra-2012_hate-crime.pdf> accessed 1 July 2014.
- European Union Agency for Fundamental Rights (2017) *Subgroup on Methodologies for Recording and Collecting Hate Crime Data* <http://fra.europa.eu/en/project/2017/subgrsoup-methodologies-recording-and-collecting-data-hate-crime> accessed 26 February 2018.
- Garda Inspectorate (2014) Crime Investigation - Report of the Garda Síonchána Inspectorate. <http://www.gsinsp.ie/en/GSINSP/Crime%20Investigation%20-%20Full%20Report.pdf/Files/Crime%20Investigation%20-%20Full%20Report.pdf > accessed 19 June 2018.
- Hall, N. (2013) *Hate Crime,* 2nd ed., Abingdon, Ox.: Routledge.
- Haynes, A. & Schweppe, J. (2017a), 'LGB and T? The Specificity of Anti-Transgender Hate' in Haynes, A., Schweppe, J. & Taylor, S. (eds.), *Critical Perspectives on Hate Crime*, London: Palgrave Macmillan 2017 130, 111-136.
- Haynes, A. & Schweppe, J. (2017b) *Lifecycle of a Hate Crime – Country Report for Ireland*, Dublin: ICCL.
- Haynes, A., Schweppe, J., Carr, J.,Carmody, N., & Enright, S. (2015) *'Out of the Shadows' Legislating for Hate Crime in Ireland: Preliminary Findings,* Dublin: ICCL.
- Herek, G.M., Gillis, J.R. & Cogan, J.C. (1999) 'Psychological sequelae of hate-crime victimization among Lesbian, Gay and Bisexual adults', *Journal of Consulting and Clinical Psychology*,67(6), 945-51.
- Iganski, P. (2008) *Hate Crime and the City, Bristol:* Policy Press.
- Macpherson, J.C. (1991) *Macpherson Report on Tradition and Education, Towards a Vision of Our Future,* (Ottawa, Ca.: Department of Indian Affairs and Northern Development).
- Macpherson, J.C. (1991) *Macpherson Report on Tradition and Education, Towards a Vision of Our Future,* Ottawa, Ca.: Department of Indian Affairs and Northern Development.
- Macpherson, W. (1999) *Inquiry into the matters arising from the death of Stephen Lawrence,* London: UK Home Office.
- Mason, G. Maher, J.M., McCulloch, J., Pickering, S., Wickes, R. & McKay, C. (2017) *Policing Hate Crime: Understanding Communities and Prejudice*, Abingdon, Ox.: Routledge.
- McDevitt, J., Balboni, J., Garcia, L. & Gu, J. (2001) 'Consequences for Victims: A Comparison of Bias and Non-bias Motivated Assaults', *American Behavioural Scientist*, 45(4), 697-713.

- McInerney, D. (2017) 'Policing Racism on the Island of Ireland' in Haynes, A., Schweppe, J. and Taylor, S. (eds.), *Critical Perspectives on Hate Crime*, London: Palgrave Macmillan 2017, 419-422.
- National Crime Council (2004), *Report of the expert group on crime statistics*, Dublin: Department of Justice, http://www.justice.ie/en/JELR/ExpertGroupStats.pdf/Files/ExpertGroupStats.pdf
- National Focal Point (2002) *Analytical study on racist violence EUMC RAXEN3 report on Ireland*, http://fra.europa.eu/sites/default/files/fra_uploads/264-CS-RV-NR-IE.pdf.
- O'Connell, J. (1997) *Travellers in Ireland: an examination of discrimination and racism: a report from the Irish National Co-ordinating Committee for the European Year against Racism,* Dublin: Irish National Co-ordinating Committee for the European Year against Racism.
- Organization for Security and Co-operation in Europe/Office for Democratic Institutions and Human Rights, (2009) *Hate Crime Laws: A Practical Guide*, Warsaw: OSCE/ODIHR.
- Perry, B. (2001) *In the Name of Hate,* Abingdon, Ox.: Routledge.
- Perry, B. (2003) 'Where do we go from here? Researching Hate Crime', *Internet Journal of Criminology*, 9 http://www.internetjournalofcriminology.com/Where%20Do%20We%20Go%20From%20Here.%20Researching%20Hate%20Crime.pdf > accessed 1 July 2014.
- Perry, B. & Alvi, S. (2012) ''We are all Vulnerable': The In Terrorem Effects of Hate Crimes', *International Review of Victimology*, 18(1), 57-71.
- Perry, J. (2015) 'Evidencing the case for "hate crime"' in Chakraborti, N. and Garland, J., (eds.) *Responding to Hate Crime: The case for Connecting Policy and Research,* Bristol: Policy Press.
- Taylor, S. (2011) *Responding to Racist Incidents and Crime: An Issues Paper for the Equality Authority,* Dublin: Equality Authority.
- Whine, M. (2016) 'National Monitoring of Hate Crime in Europe: The Case for a European Level Policy' in Schweppe, J. and Walters, M. (eds.) *The Globalisation of Hate: Internationalising Hate Crime?,* Oxford: Oxford University Press, 213-232.

Croatian Model of Telecommunication Information Requests Management (TIRM)

Damir Osterman
National Police Office for Suppression of Corruption and Organised Crime, Ministry of the Interior

Damir Maračić
Police College Zagreb, Ministry of the Interior, Croatia[1]

Abstract
TIRM is an acronym for the Croatian model of Telecommunication Information Requests Management. It is an electronic application designed for the systematic requesting and issuing of electronic communication data, as well as the handling, processing, storage and use of data. TIRM application was developed and designed during the last three years of a process including the needs analysis, preparation, test, and implementation phases. It helps in the processes of authorisation and approval of requests, transferring and storage of data, and in the analytical processing. The paper presents and explains:
– Importance and values of the systematic requesting, issuing and managing of electronic communication information;
– Grounds for electronic communication information requests;
– Possible threats and possibilities of abuse;
– Advantages of using the electronic format of telecommunication information requests management.

Keywords: telecommunication information, electronic information, information requests management, electronic communication, data requesting

Introduction

The possession of electronic communication data by police officers and public prosecutors is a very powerful tool for combating crime. At the same time, it is a big responsibility to collect and keep the information properly, without any abuse in the context of human rights.

All police officers in the Republic of Croatia would agree with the conclusion that a police job is unimaginable without the usage of electronic information requests and analyses (Kralj, 2009).

1 Seconded National Expert at CEPOL in Budapest, Hungary. Corresponding author's email: damir.maracic@cepol.europa.eu

Public prosecutors would agree with the before mentioned conclusion as well, having in mind the value of evidence collected by special evidence collection actions.

Usage of a number of special evidence collection actions at the same time with requesting the telecommunication information is really important. In that sense, requesting the telecommunication information is the controlling and supporting action for all other actions (Maračić, 2015).

The term "electronic communication data" refers to data about the contact(s) between electronic addresses during a certain period (duration, frequency) or at the exact time, location of the device, the identification parameters of the device and the identification of the device user(s) location, excluding any information about the content of communication.

Technological improvements and development enable the public to communicate using various types of communication devices. Therefore, since criminals are using modern communication technology, law enforcement officials have to possess an adequate and efficient model of data collection that is in line with both technological requests and the legal framework.

Without going into details, the electronic communication data used for the intelligence purposes or in an evidentiary form helps to identify, locate and arrest the criminal offender(s) and also to investigate and prosecute criminal offences in numerous cases. Furthermore, it helps in situations when persons are lost or missing, when it is necessary to search for some objects or as an evidence collecting tool.

In general, numerous cases were solved thanks to a crucial evidence that originated from the electronic communication information.

On the other hand, a request for electronic communication information represents a temporary limitation of personal rights, protected by European Convention on Human Rights and its Protocols (Council of Europe 1950), national constitutions and other related laws, and it always comes under the scrutiny of the public eye.

Taking into consideration all the above reasons, law enforcement officers have to follow the very precisely prescribed procedure of: the requesting and issuing of electronic communication data, as well as the handling, processing, storage and use of data.

In terms of the use of electronic telecommunication tracing or interception, each EU member state has its own specific rules and regulations, but what all EU member states have in common is the need to act in accordance with the rules of European Convention on Human Rights and its Protocols. The information on different legal systems of the EU member states and details on the status of the implementation and ratification of regulations can be found on the European Judicial Network website (2018). This website, or, more specifically, the sections of Atlas, Compendium or/and Fiches Belges describe, among other things, all possibilities of electronic telecommunication tracing or interception in the EU member states. The European Judicial Network website thus gives an opportunity to explore and compare the possibilities and ways for a successful judicial cooperation (Maračić, 2016).

Croatian legal framework on electronic communication information requests

In accordance with the Croatian legislature, electronic communication data can be extracted in an intelligence or evidentiary form. The difference between the two forms depends on the used legal ground, since it can be used either in accordance with the Police Powers and Duties Act (Republic of Croatia, 2014) or with the Criminal Procedure Act (Republic of Croatia, 2017).

According to Article 68 of the Croatian Police Powers and Duties Act, electronic communication data verification is one of the police powers. It's allowed in the investigation and suppression of ex officio criminal offences; in the suppression of danger and violence; and also when searching for persons and objects.

Persons authorised for the electronic communication check approvals are the Head of Criminal Police Directorate, the Head of Police National Office for the Suppression of Corruption and Organised Crime and Heads of Police Districts. In the case of their absence, Deputy Heads are authorised for the mentioned approval.

Furthermore, the Croatian Regulation of the Police Proceedings (Republic of Croatia, 2015) regulates in more detail police powers and refers to the Croatian Police Powers and Duties Act. Article 103 of the Regu-

lation stipulates that electronic communication checks should be requested through Information Technology (IT) application of electronic communication information management.

On the other hand, the Croatian Criminal Procedure Act, Article 339a prescribes the verification of the establishment of telecommunication contact as an evidence collection action. It is allowed in the case of the investigation of criminal offences specified in the criminal offences catalogue for the special evidence collection actions and for the criminal offences with prescribed imprisonment of more than five years. The investigation judge is authorised to issue a warrant for requested telecommunication checks at the request of a public prosecutor, but in specific and very urgent cases, a warrant can be issued by a public prosecutor and later validated by a judge. If the registered owner or user of telecommunication devices gives his written approval, the warrant is not needed.

In both cases of requesting telecommunication information, either in a cognitive or evidentiary form, the operational technical procedure is almost the same. For the purpose of the coordination and control of all relevant bodies involved in requesting and conducting this process according to the Law on a Security Intelligence System (Republic of Croatia, 2006) and Criminal Procedure Act, the Operational Technical Centre has been established. The role of the Operational Technical Centre is to provide a flow of the requested telecommunication information between telecommunication providers and investigation authorities. The Operational Technical Centre provides a support to the Intelligence service as well.

The legal ground for requesting electronic information in the Republic of Croatia is regulated in accordance with the directions of the European Court, abiding by the rights of privacy and personal data protection (Juras & Vulas, 2016).

Monitoring of the implemented electronical communication information requests

When we speak about electronic information requests managed in accordance with the police powers, the Croatian Police Powers and Duties Act predicts possibilities for monitoring. For that purpose, in accordance with the Act, the Council for Civilian Supervision of police powers should be established. The Council is composed of 5 members and 5 deputy members. They can act after criminal investigation has been finalised and are authorised to ask for the relevant information from all bodies involved in the process. At the end of the supervision, the Council must submit a report to the President of the Croatian Parliament, the President of the Committees for Internal Politics and National Security, the Committee for Human Rights and Rights of National Minorities, the Minister of the Interior and the General Director of the General Police Directorate. At the same time, the applicant for monitoring should be informed.

When electronic data are collected in an evidentiary way in accordance with the Criminal Procedure Act, the monitoring and control mechanism is arranged through judicial system. A request for electronic (telecommunication) data could be initiated by the police toward the public prosecutor, or the public prosecutor himself can initiate a request. In both cases, the public prosecutor has to pass the request to the investigation judge who considers the request and makes a decision within 4 hours. If the investigation judge approves the request, he/she issues a warrant and sends it to the police authorities for action. As was mentioned earlier, in specific urgent cases the public prosecutor is authorised to approve and issue a warrant by himself but he/she has to inform the investigation judge within 24 hours and the judge has to decide whether to verify it or not. The described protocol is a guarantee for the protection of human rights, so the terms prescribed in the Criminal Procedure Act do not allow any abuse of this evidence action since otherwise all collected data is considered illegal and not usable in criminal proceedings.

It should also be mentioned that all the described actions regarding electronic telecommunication data requests and all results and reports of the requests are part of the chain of evidence used in the ensuing criminal proceeding. During that time, there is another way of monitoring conducted by trial judge or court council.

Statistics as a trigger for action

By adopting the amendments to the 2002 Criminal Procedure Act, the Republic of Croatia has for the first time clearly defined the possibility of access to retained data on electronic communications, or more specifically telephone calls and messages records, while the content of communication still remains in the domain of the gathering of evidence by using special evidence actions and depending on the possession of a court order.

In order to prevent uncontrolled access to retained data and to provide for the use of this power to be monitored, the prescribed way of accessing this information within the Ministry of the Interior implied a centralized approach to telecommunications operators. Such access is ensured through the Criminal Police Directorate, or the Special Investigation Service, which collects and verifies the technical validity of the request centrally and provides technical support to users, while the legality of requests to access the data is checked by the head officers of the criminal police line within the Police Directorates.

At the beginning, all the work was done by filling the forms manually and by delivering them physically to the Special Investigation Service, which recorded all the requests, collected the requested data and submitted them to the claimants.

The problems that dogged the work were the slowness of the entire process of data acquisition and analysis, insufficiently structured data and different data supplied by different telecommunication operators, insufficient explanations of service marks within the submitted records, the lack of data including the lack of infrastructure data for the transmission of communications etc.

Signs of additional problems emerged in 2003 when the first Law on the Liberalization of the Telecommunications Market was adopted, and the police began to notice these problems for the first time in 2005, when new telecommunications operators started providing services. All of this has led the police to face new data formats, new types of data, problems with communicating with operators, and a strong need for establishing new protocols. Rules of the game have been identified to prevent possible abuse without causing public safety erosion and inability to conduct criminal investigations.

The Ministry of the Interior launched an initiative to establish an independent agency that would represent a technical body between the law enforcement authorities and providers of telecommunication services in the field of legal interception of communications and access to retained data.

This initiative came to life in 2007, when the new Law on the Security Intelligence System of the Republic of Croatia entered into force, which was a major change considering that it foresaw the establishment of the Operational and Technical Center for Telecommunication Surveillance (hereinafter OTC). OTC gained an important role in the system when it comes to controlling lawful interception measures. OTC managed to arrange the standardization of procedures in accordance with the ETSI standards and the same format of call data, especially for mobile and landline telecommunications operators.

At the same time, the situation was out of control with the increased number of users of telecommunications services in the conditions of a growing economy in the pre-crisis period. At one point, the number of users exceeded 8 million in landline and mobile telephony services without users of Internet access.

Table 1. Indicators of the number of requests for access to retained data compared to the number of criminal offenses and the number of mobile and landline telephone network users without internet access users (Kralj 2009)

Year	Criminal offences (without traffic offences)	Requests	Phone numbers	Landline subscribers	Mobile subscribers
2001	75 730	1 182	2 466	No data	No data
2002	75 363	2 576	5 646	1 825 157	2 312 653
2003	77 653	4 099	8 867	1 871 347	2 537 332
2004	82 950	6 710	12 021	1 887 637	2 835 508
2005	77 587	11 790	18 648	1 882 500	3 649 700
2006	78 664	16 267	25 218	1 826 800	4 395 150
2007	73 319	18 823	28 915	No data	No data

According to the records of the Ministry of the Interior of the Republic of Croatia, during the years 2014 and 2015 a total of 48 460 requests for verification of telecommunication contacts were filed pursuant to Article 68 of the Police Powers and Duties Act (25 263 requests in 2014 and 23 197 requests in 2015), approved by authorized persons in accordance with the legal regulations, after which the requested information was verified by the telecommunications service provider (Juras & Vulas, 2016).

According to the "Annual comparative data of the electronic communications market in the Republic of Croatia" by the Croatian Regulatory Agency for Network Activities HAKOM, the number of users of services in the landline and mobile network for 2010, 2011, 2013, 2014 and 2015 was as follows:

Table 2. Indicators of the number of landline and mobile network subscribers

Year	Landline subscribers	Mobile subscribers	Sum of subscribers
2010	1 865 729	6 362 106	8 227 835
2011	1 606 090	5 115 140	6 721 230
2012	1 454 133	4 971 351	6 425 484
2013	1 430 644	4 912 134	6 342 778
2014	1 355 421	4 461 352	5 816 733
2015	1 315 654	4 415 660	5 731 314

By reviewing the above indicators, it is clear that the telecommunications market had an uncontrolled growth that stabilized by 2015 and returned roughly to the 2005 indicators.

As access to electronic communications is made available to all police officers working in criminal police lines from the smallest organizational units (police stations) to the units in the Police Directorate, the amount of work and time spent has reached a critical level in 2009. Encouraged by this development of the situation, the Police Directorate of the Ministry of the Interior has launched a comprehensive recording of the state, processes, procedures, data categories and the legislative and organizational framework in order to come up with concrete proposals in 2011 to change the model of work and to move to a solution based on the information and communication technology.

During 2014, an implemented solution based on Internet technology was completed, thus enabling the creation, approval, delivery, data visualization and process monitoring for the purpose of detecting potential misuse of data, called TIRM (Telecommunication Information Request Management hereinafter referred to as TIRM).

TIRM is available to every police officer in the line of criminal police work and is linked to the OTC, which enables a fully computerized process of accessing the retained telecommunication data and auditing them.

This solution has been recognized and accepted by police officers as easy, reliable and user-friendly since the very beginning of the application. The average time of the whole process compared to the previous state is reduced from 3 days to 2-6 hours, whereas in

urgent cases of rescue or search for persons, this process takes only a few minutes, with the level of protection of the data and the legality of using police powers duly secured.

Not less importantly, the whole process is practically paperless, with high savings in paper, ink, delivery costs and working hours. A significant number of police officers who worked on these jobs was returned to crime investigation jobs instead of being engaged with filling in and submitting requests and records and allowing managers to automate the creation of reports for their organizational units and to conduct a faster and more effective supervision over the use of the police powers.

Conclusions

In accordance with the previously explained facts, TIRM is a user-friendly application arranged by the needs of end users. It helps in daily work and is making the process faster. At the same time, the monitoring system is giving the best guarantees for the protection of citizens and their human rights.

As with any IT system, there is a constant need for improvement and upgrading TIRM, and this may be caused by external influences, such as changes in legal acts or new telecommunications services, and internal influences, such as organizational changes, additional requests from users etc. The TIRM system, due to its design, can easily be upgraded to new functionalities or adapted to new needs or additional protection measures.

References

- European Judicial Network website (2018).
  Available from: https://www.ejn-crimjust.europa.eu/ejn/ [Accessed 13th February 2018].
- Council of Europe (1950) European Convention on Human Rights and its protocols.
  Available from: http://www.echr.coe.int/Documents/Convention_ENG.pdf [Accessed 13th February 2018].
- Juras, D. & Vulas, A. (2016) Legal Framework for Checking of Telecommunication Contacts. Policija i sigurnost, Zagreb, Croatia, 1, 69-81.
- Kralj, T. (2009) Examination of the Identity of Telecommunication Addresses in Criminal Practice, Policija i sigurnost, Zagreb, Croatia, 2, 166-179.
- Maračić, D. (2015) Special Collection of Evidence, Simulated Sales: Assessment of Risks in Choice of Sale Objects and Impact of Sale Objects on the Start of Final Action. Proceedings of the 4th International Scientific and Professional Conference "Police College Research Days in Zagreb", Zagreb, Croatia, 620-628.
- Maračić, D., (2016) Webpage European Judicial Network (EJN) as Help for Establishing International Judicial Cooperation. Proceedings of the 5th International scientific and professional conference "The Police College Research Days, "New Technologies and Methods Used for Improvement of the Police Role in Security Matters", Zagreb, Croatia, 398-409.
- Republic of Croatia (2006) Law on a Security Intelligence System, Official Gazette of the Republic of Croatia "Narodne novine", 79/2006, 105/2006.
- Republic of Croatia (2014) Police Powers and Duties Act. Official Gazette of the Republic of Croatia "Narodne novine", 76/2009, 92/2014.
- Republic of Croatia (2015) Regulation of the Police Proceedings, Official Gazette of the Republic of Croatia "Narodne novine", 89/2010, 78/2014, 76/2015.
- Republic of Croatia (2017) Criminal Procedure Act. Official Gazette of the Republic of Croatia "Narodne novine". 152/2008, 76/2009, 80/2011, 121/2011, 91/2012, 143/2012, 56/2013, 145/2013, 152/2014, 70/2017.

New Technologies and the Need for New Law Enforcement Capabilities: Situational analysis in North Macedonia, Montenegro and Serbia

Kristina Doda
Aleksandar Vanchoski
Institute for Human Rights, Skopje, North Macedonia[1]

Abstract
Introduction of new IT hardware and software tools has a fearsome dynamic and is directly shaping the overall human interactions and patterns of economic and social development. All actors in the society, including decision makers, scientists, academia and civil society, must be aware that, when new technologies are developed, which are capable of opening new dimensions of communication, transport or development, there must be comprehensive evaluation not only of the positive effects but also of the potential negative side effects of these new kinds of products and services which very easily could be used by individuals or groups for jeopardizing citizens' security and overall public safety. Furthermore, the implementation of new technologies by law enforcement agencies raises the question of proper implementation of human rights standards and legal accountability. This analysis is also giving a short overview of the law enforcement capabilities regarding new technological developments in three EU candidate countries: North Macedonia, Montenegro and Serbia. These countries are into EU accession process and they need to harmonize their national legislations with EU acquis and achieve full interoperability with the EU agencies. Recommendations for improvement of the capabilities for adopting new technologies and innovation in the day-to-day operational functioning of the police forces and law enforcement agencies in these three EU candidate countries are also proposed at the end of this analysis.

Keywords: innovations, technology, law enforcement, North Macedonia, Serbia, Montenegro

Introduction

The police as the only legitimate state actor which can use force, conduct criminal investigation and at the same time restrict and protect human rights and liberties are facing tremendous challenges which are direct or indirect products of ICT revolution and process of digitalization.

Introduction of new ICT hardware and software is shaping the overall human interactions and patterns of economic and social development. Taking into consideration the complexity and the dynamics of ICT and digital innovations, law enforcement agencies (LEA) including the police organizations are put in unfavourable position because potential and existing trends that new technologies are bringing as own side effects

1 Corresponding author's e-mail: Kristina.doda@ihr.org.mk . Due to the official change of the name for the country, the reference to the Former Yugoslav Republic of Macedonia, used in the online-first version has been corrected, except for the references.

are numerous and are exceeding the police financial and human resources for prevention and investigation. However, from another side ICT presents a main medium for developing and introducing many innovations and new methods in LEA and police work.

Although the development of ICT has positive influence on many social and economic activities still there are many "grey zones" from legalistic, moral and social aspects in domains such as use of autonomous or semi-autonomous vehicles, use of various size of flying drones, developing of overall digital economic activities, new ways of production especially of the 3D printing and manufacturing, privacy data protection in internet domain and data mass storage practices. The use of autonomous or semi-autonomous vehicles are opening a lot of legal and practical police dilemmas over numerous situations as a traffic safety, traffic accidents, possibility who can use them etc. The flying drones are already one of the most challenging devices that police officers are facing regarding jeopardizing the security of some public buildings and security interesting individuals.

The digital economy is becoming driver of economic and social development of many countries including the EU which placed digital economy as one of its strategic goals and even have developed own digital single market strategy. Having in mind that through these kinds of processes the economic and financial activities are becoming faster and more dynamic, police officers must develop new skills and toolkits for ensuring implementing the law and providing security.

Furthermore, the stakeholders and especially LEA and police management officials should not underestimate and neglect the human rights-based approach which should be seriously taken into consideration when new technologies with potential for mass data storage, easily exceeding citizens' privacy and restricting many fundamental human rights are adopted by LEA and police organisations. Moreover, in the time of digital societies and rapid development of ICT there is also raising tendency of questioning the inviolability of the right to privacy.

This analysis highlights the importance of adopting and utilizing new technologies by LEA and police organisations with a special focus on the current developments in this particular domain in three EU candidate countries: North Macedonia, Montenegro and Serbia. The analysis is an initial stage for further research and is based on content and qualitative analysis of the National strategies for development of police forces in these three countries.

New technologies, what are the new challenges?

Beside the positive sides and new possibilities that new technologies are bringing, in the same time there are numerous challenges and threats that are appearing such as: digital frauds, different cyber-crimes, traffic safety issues, various legal and practical difficulties related to traffic accidents investigation and personal accountability, guaranteeing the security of particular public spaces and individuals from abuse of flying drones etc.

Ideally, LEA should strive for solutions before problems appear which means making assumptions and propose sustainable solutions for effective prevention. Developing a systematic infrastructure in policing for maximizing technology's potential will also require both police and researchers to make a commitment for a strong common research and development (R&D) agenda. "Researchers can assist practitioners by collaborating on evaluation studies assessing theories behind technology adoption. In addition, research is needed to clarify what organizational strategies as training, management and evaluation are most effective for achieving desired outcomes with technology and avoiding potentially negative unintended consequences" (Koper et al., 2015).

Police can facilitate R&D policies by making greater efforts for strategic and operational planning, sustainable medium and long-term funding for R&D activities and higher transparency and openness for cooperation with academia and civil society organizations (CSOs).

A very important issue which should be taken into consideration is the fact that any new developed technological toolkit or method before its adoption and implementation as a standardized police measure or authorization should be carefully tested and analyzed with regard to its impact on human rights limitations and police accountability. Advances in technology do not always produce obvious or straightforward improvements in communication, cooperation, productivity, job satisfaction, or officers' effectiveness in re-

ducing crime and serving citizens (Koper, Lum & Willis, 2014: 214).

Only inclusive and sustainable policies and strategies based on previous research on their effects upon society and law could lead towards higher levels of resilience to various forms of insecurity that ICT is bringing with its rapid development.

New technologies and the human rights perspective

Mostly when we think about technology we mainly focus on how technologies operate and not how and what is the impact of the technology on other police outputs such as police behaviour, effectiveness or relationships with citizens. Therefore, in order to increase the benefits of technology the new technologies in police need to be used with respect to the principles of accountability, transparency and data protection and privacy.

From a human rights perspective technology led policing (De Pauw et al., 2011), raises questions in relation to police accountability. As part of the development of the surveillance society (De Pauw et al., 2011) new police technologies including biometric databases, data collection and analysis, facilitate and hinder compliance with human rights. Although they are potentially useful ICT tools for law enforcement, the need for proper checks and balances is more than necessary when we speak about usage of new technologies by LEAs. This is especially important when LEAs are utilizing ICT tools whose capabilities enable collecting and storage of huge quantum of citizens' personal data, or easy access of surveillance over various forms of communication which requires setting a strict rules, procedures and ethical principles for protection and guaranteeing the right of privacy as a fundamental human right.

To gain the full potential benefits of technological innovations, police must also arguably address traditional and long-standing philosophical and cultural norms about the role of law enforcement. Training about proactive and evidence-based strategies—and how technology can be used in support of those strategies—is needed (Koper, et al., 2015:5).

Innovation and technologies in the EU candidate countries North Macedonia, Montenegro and Serbia

Regarding the innovation and new technologies in the area of law enforcement and more precisely in the police work we analysed the current strategic documents and approaches that are developed and present as guidelines for the political and professional police leadership in North Macedonia, Montenegro and Serbia. The purpose of this analysis is to emphasise how and to what extent North Macedonia, Montenegro and Serbia are prepared for the new security threats and challenges which are becoming more cyber space oriented and digitalized. Through the EU integration process these countries are committed to align their national legislation, strategic documents and goals with the EU values and acquis, including as well as the key EU strategic policy document and interests from the area of justice, security and freedom and area of common defence and security policy. Therefore, one of the most important benchmarks of the EU integration processes of the three countries is the EU based strategic planning and legislative alignment.

In situation when EU is facing more and more with technological driven security threats and criminal activities, there is a necessity for adopting new technology methods and instruments for prevention, detection and investigation of these phenomena as well as higher level of interoperability among law enforcement agencies of EU member and candidate states and EU institutions and agencies. The following chapters are focusing on national strategic goals and institutional capacities that North Macedonia, Montenegrin and Serbian law enforcement agencies are having, or more specifically the police forces, related to the adopting and developing new technology and technologies in conducting of its legislative duties and responsibilities. The analysis is done through analysing primarily the National strategies for development of police forces as a key strategic document that emphasises the main priorities and goals regarding the research and development capabilities of the police organisations in these three countries.

Also the paper gives a short overview whether the national police practices of utilizing new technologies are followed by proper privacy data protection standards which are in line with EU acquis as an important

precondition for safeguard of the fundamental human rights.

North Macedonia law enforcement capabilities regarding new technologies

The most important document which sets the strategic goals for enhancing the operational capabilities and organizational potentials of North Macedonia law enforcement agencies is the "Police Development Strategy 2016 - 2020". In accordance with the strategic objectives, this Strategy foresees that the development of North Macedonia police is based on "…4 (four) main pillars: resource management, police work with the community, successful dealing with crime, and learning and development." (Ministry of Interior [MoI] of R. Macedonia; 2016:7)

In certain parts of the Police Development Strategy directly are noted the existing organizational and operational capabilities of North Macedonia police in the domain of utilizing ICT technologies in carrying out day-to-day police activities and tasks as well as the necessity for implementing new technologies in improving the police capacities for guarantee of the safety and prevention efficiency of different forms of criminality.

For the past three decades, North Macedonia police and other law enforcement agencies have been constantly reforming and improving with different dynamics in accordance with the basic democratic principles stipulated in the Constitution and in accordance with the good practices of numerous European LEA. Also it should be noted that such reform processes and changes in a significant degree were supported and financed by certain international actors such as the Organization for Security and Cooperation in Europe (OSCE), the Council of Europe (CoE) and, in particular, the European Union (EU) through the pre-accession funds. More dynamical reforms related to the organizational setup and functioning of the Ministry of Interior (MoI) and North Macedonia police were conducted after 2001 and especially after obtaining the candidate status for an EU membership at the end of 2005. However, very often the positive effects of the implemented reforms were not very visible or the reforms were not always implemented in the right manner.

According to the data presented in the Strategy for the period 2016-2020, North Macedonia police is facing with low level of application of advanced ICT software and hardware tools which actually reflects upon its operational efficiency. Also, there are no sustainable and systematic programs and funds for developing innovative tools and solutions that in the medium and long-term run would enable police forces to obtain capabilities for proper respond to the dynamic technological needs of the society as well as to the risks that digitization brings with itself. Namely, the Strategy suggests that "the majority of the police workflows are not covered by ICT support tools, which substantially causes higher costs for material and human resources" (MoI of R.Macedonia, 2016:21) Additionally, part of the ICT applications that are currently used by the police "were developed with own resources, but they are not based on the same entity structure, which is a problem for integrating the overall police database" (MoI of R.Macedonia; 2016:22). The documentation and the exchange of documents within the police still is carried out in paper form which has a significant negative impact on the effectiveness of the police work (MoI of R.Macedonia; 2016:22)·There is no electronic centralized archive for storing all documents, thus preventing the possibility of effective monitoring, which is well known that is necessary in each segment of the police structure and work (MoI of R.Macedonia; 2016:21).

Another disadvantage that prevents North Macedonia police from having a more systematic approach for improving its operational functioning and establishing a sustainable system for development and application of new technologies is not existence of database and a checking mechanism for registering all police trainings, both nationally and internationally organized. Furthermore, related to the international cooperation, there is no common centralized record of projects that will enable management, monitoring, implementation, monitoring and supervision of these projects.

From an organizational and structural point of view, the police unit that has the authority and capacities to deal with the cutting edge forms of criminality closely related to ICT is the Department of Cybercrime and Digital Forensics of the MoI, which has the task of conducting investigations for the detection of serious and complex cases of cybercrime, such as malware analysis, internet fraud, social engineering, network attack, critical infrastructure attacks, child abuse via the Internet, "Darknet", etc. This department is a centralized police unit and it has own regional subunits. However these subunits are

not operational due to lack of human and financial resources (MoI of R.Macedonia; 2016:11).Therefore we can conclude that North Macedonia police is facing great challenges with regard to the implementation of innovative and advanced ICT software and hardware tools that inevitably imposes the need for drastic changes of the strategic approaches and operational concepts. It is also evident that certain basic preconditions firstly need to be established in order the officers from North Macedonia police to be able to respond to the challenges that the digital society imposes. One of these preconditions is certainly the ongoing process of development of a National Cyber Strategy which currently is in the process of drafting by various national stakeholders.

When it comes to the legal safeguards of fundamental human rights in situations when police officers are utilizing new high-tech ICT in conducting their duties and authorizations, unfortunately North Macedonia citizens have faced with serious challenges as a result of high volume of police misconducts. Just recently North Macedonia has experienced a mass wiretapping scandal because some police officers without court warrant or any other legally allowed security reasons made an illegal recordings of more than 20 000 citizens including politicians, businessmen, journalists and ordinary people. The recordings were acknowledged to have been made by the Administration for Security and Counterintelligence which is a structural part of the MoI. The content of many of the recordings provided numerous indications of unlawful activities and abuses of power which leaded to serious breaches of human rights and freedoms using advance ICT software and hardware technology illegally. These kind of unlawful practices have undermined the trust of the citizens in the organizational values and principles of the police.

The protection of privacy, the protection of personal data, and the protection of human rights related to freedom and dignity that were violated by this illegal recording of communication, are protected by the Constitution of the Republic of Macedonia and by number of laws, including the Law on Personal Data Protection, Law on Internal Affairs, Law on Police, while the Criminal Code sanctions unauthorized wiretapping. However, the European Commission Progress Report on the former Yugoslav Republic of Macedonia indicated that it is necessary to further adjust the sector-specific laws in order to fully comply with the European regulations on personal data protection (European Commission, 2018).

Montenegrin law enforcement capabilities regarding new technologies

The reforms in the police in Montenegro were implemented together with the overall post-conflict reconstruction process in Montenegrin society especially after the ending of Yugoslav secession wars. The pressure for democratic policing and police accountability of the Montenegrin police was dual. Firstly, the pressure was coming from Montenegrin citizens and secondly was imposed by the ongoing process of European Union accession process.

Montenegrin police and other law enforcement agencies as many other European LEA is feeling the pressure that process of digitalization and rapid breakthrough in the ICT is affecting its operational functioning and their capabilities for preventing and countering new forms of crime committed by various ICT tools.

According to the Montenegrin "Development strategy for police for the period 2016-2020" the speed of changes in the field of information and telecommunications technologies, imposed inevitable need for constant improvement of technologies and procedures, used by police officers (MoI of Montenegro, 2015:19). Furthermore, into the Strategy is noted that the "adoption of new technologies, new knowledge and skills should enable police conducts, police methods of work and achieved results to be constantly monitored, improved and evaluated in order to be achieved maximum efficiency and transparency of the police work process, and the needs of the citizens and the society as a whole to be fully meet" (MoI of Montenegro, 2015:34). As one of the priorities in the efforts for implementing specific innovations in the functioning of the Montenegrin police is "introduction of the electronic management of cases (Case Management), processing and intelligence analysis of the data (Entity management), introduction of system for electronic statistics and reporting in the police as well as development of a unique geographic information system for the needs of all segments of the police" (MoI of Montenegro, 2015:34).

This strategy also points out that as a result of an increased number of Internet users, new electronic services and in particular electronic payments via the Internet in Montenegro there is a rapid increase in the abuse of various forms of information technologies

with intention of committing various types of criminal offenses which on the end represent a special risk factor for the citizens and state security. Therefore, the strategy listed High-tech crime among the most serious security threats that Montenegrin police is facing currently or will face in the near future (MoI of Montenegro, 2015:19).

One of the steps for improving the operational capacities for preventing and countering high-tech crime is upgrading the ICT system of the financial intelligence unit of the Montenegrin police. However, shortcomings in the domain of the ICT and innovation implementing capabilities of the Montenegrin police include the lack of a secured data exchange link between prosecution office and law enforcement agencies as well as the need for increasing the administrative and ICT capabilities of the officers (MoI of Montenegro, 2015:35:40). Also, within the Ministry of Interior there is no special organizational unit that would deal exclusively with the planning and organization of training for the needs of police officers and there is no strategic multi-annual training planning (e.g. a five-year training plan).

Additionally, the Development strategy of the Montenegrin police regarding the innovations and new technologies is emphasising that there is a need for strengthening of the educational and training programs at the Police Academy and establishing a more proactive role of the Ministry of Interior - Police Directorate in creating study/ training curricula that meet the needs of modern policing (MoI of Montenegro, 2015:40-41). Also, the study curricula need to be revised and aligned with modern standards of police education, human rights protection and technological innovations.

In 2017 Montenegro has adopted amendments related to video surveillance of the Law on Data Protection. However, according to the most recent European Commission report the implementation of the data protection legal framework remains weak. Work has not yet started on aligning the broader legal framework with the new EU data protection acquis in the field (European Commission, 2018). Furthermore, as the only one among the analyzed countries, Montenegro has developed and adopted a special Cyber Security Strategy for the period 2013 – 2017. This actually shows the existence of awareness among the Montenegrin security stakeholders for the security threats that ICT and their everyday usage in all domains of the society could cause to the citizens' and the state security.

Serbian law enforcement capabilities regarding new technologies

Establishing a democratic and accountable police in Serbia was and still is a challenging step for the Serbian society. For a long period "the Ministry of Interior of the Republic of Serbia was an alienated force, deeply criminalized, politicized, centralized and with the absence of external democratic control, as well as a lack of efficient internal control. Since the democratic changes in 2000, the situation has slowly changed" (Paunovic, 2005:80). Numerous legislative and organizational reforms were undertaken for restructuring Serbian police forces in the notion of democratic and citizen oriented state organization. Furthermore as a result of the raising tendencies of more sophisticated forms of crime there is an evident pressure for reshaping of operational functioning of the Serbian police and other law enforcement agencies in accordance to the new social and technological realities.

In the case of Serbia for the purposes of this analysis firstly the "Development Strategy of the Ministry of Interior 2011 - 2016" was considered because in the time of writing this paper the new Strategy for the period 2018-2023 is under development at Serbian Ministry of Interior. This strategy still has the status of a draft version and process of public debates with academia and experts are ongoing. As a result of these developments the focus was mainly on the Development Strategy for the period 2011 – 2016 with taking in consideration eventual differences stated in the draft version of the new Development Strategy for the period 2018 – 2023.

A strategic approach to the development of the Ministry has been recognized as one of the key priorities in the scope of an overall reform of the public administration. In addition to this strategy, as other strategic and legal documents which are specifically related to the development of the Serbian police capacities for utilizing new technological and other innovations in day–to-day functioning are also: the"Strategic document - introducing e-learning as a support for the development of the training system in the Ministry of Interior" and the "Development Strategy for Information - Telecommunications Technologies of the MoI for the period 2016 – 2020".

According to the Development Strategy 2011-2016 as work areas that have strategic importance for the future development of the Serbian police are:

— Organization and management,
— Safety of the individual, the community and the state,
— Partnerships at national, regional and international level,
— Internal and external oversight systems and operational transparency (MoI of the Republic of Serbia, 2010:14).

In the "Organisation and management" section there is a sub-section "D) Developed Information and Communication Technologies (ICTs)" in which the necessity for development of the ICT capabilities of the MoI and police is acknowledged. Also, in the Development Strategy 2011-2016 several challenges which Serbian police are currently facing are detected. For example, it is noted that there is no secure platform for electronic data exchange or communication between law enforcement agencies (the prosecution service, the police, tax and other authorities (MoI of the Republic of Serbia, 2010:7:11).

In the Draft version of the new Development Strategy for the period 2018 – 2023 is stated that "Key challenges for MoI have been identified in the area of: Information and communication technologies; Cooperation at the national, regional and international level; Human resources; The availability of international development funds" (MoI of the Republic of Serbia, 2017:14).

Furthermore in the Development Strategy 2011-2016 is stated that "…substantial investments in Information and Communication Technologies (ICTs), material and human resources are needed" (MoI of the Republic of Serbia, 2010:9). Also, the Strategy unambiguously is acknowledging that "the use of ICTs is the prerequisite for:

— for having a functional organization based on the contemporary principles of a service-oriented institution, where the tasks are standardized and automated to the highest degree;
— for enabling the constant monitoring, improvement and appraisement of the organization, the work methods and the performance;
— Long-term planning regarding supplying of all levels of the organization with the proper knowledge, experience and equipment, while at the same time allowing their constant upgrading."(MoI of the Republic of Serbia, 2010:17).

The necessity for improvement of the ICT capabilities of MoI and police are also emphasized again in the Draft version of the new Development Strategy 2018 – 2023.

The Development Strategy 2011-2016 also refers to the need for improving the computer and communication infrastructure by replacing analog communication with new installations in order to: enable faster data flow to police departments and Ministry facilities both through the Intranet and Internet communication infrastructure; Further improve and introduce new technological concepts and information systems for providing support to the Ministry's work activities.

Similar objectives are stated in the Draft version of the new Development Strategy 2018 – 2023.

From the human resources point of view, there is a necessity to be improved the training and professional development system especially in the domain of providing specialized training, management training and continuous professional development. It is also necessary to develop new strategic and action plans as well as research and development projects.

Regarding the threats that ICT brings with their dynamic development, should be highlighted the fact that Serbia does not have a long-term strategy on how to address cybercrime.

Additionally the European Commission progress report for Serbia highlights "... a new law on personal data protection in line with EU standards needs to be urgently adopted. Processing and protection of sensitive personal data, biometrics and video surveillance, security of data on the Internet and direct marketing remain inadequately regulated, leaving a significant scope for abuse" (European Commission, 2016:61).

Regulation of the use of sensitive health data by public and private actors became an issue in Serbia following media coverage of a request made by a local police authority to a local hospital. The reason given by the local police authority was to "update relevant dossiers". (Journalism Development Network, 2015) The Serbian Data Protection Agency initiated the supervisory con-

trol over the implementation of the Law on protection of personal data (Official Gazette of the Republic of Serbia, nos. 97/2008, 104/2009, 68/2012, 107/2012) by the Ministry of internal affairs.

The Serbian government started working on a new law on personal data protection to harmonise the legislation with the new EU acquis entering into effect on 25 May 2018. The LEA have access to the personal data of the customers of Internet Service Providers and telecommunication companies in Serbia who according to relevant laws need to have a court decision to gain access to these data of online users. However there are no transparent information of how many requests for private information have been requested by LEA in Serbia.

From the above-mentioned, we can conclude that is necessary the Serbian police to undertake fundamental changes regarding the approach of adoption and utilizing new ICTs and innovations in its day-to-day operational functioning in order to deal more efficiently with the new forms of crime, to improve data protection and to ensure citizens' right to privacy as well as to improve interoperability with the other regional and European LEAs.

Conclusion

After the analysis conducted on the situation in North Macedonia, Montenegro and Serbia we can conclude that more comprehensive and sustainable efforts and solutions should be considered in order to utilize ICTs for improvement of LEA and police capabilities and performances. In all three countries is evident that police organisations are facing with significant challenges related to adoption and development of innovative and technological advanced methods and tools. Furthermore can be notice that even some basic preconditions are non-existent (organisational and personal) for utilizing basic ICT infrastructures for enhancement of the operational functioning and mutual communication between LEAs and other local, national and international institutions. Taking into consideration the accessibility of advanced ICTs to the crime networks and their trans-nationality these shortcomings need to be addressed systematically by LEA management and other relevant stakeholders. It is also evident that there is a necessity for more inclusive processes of cooperation with academia, ICT industry, civil society and citizens in the process of development innovative and technologically advanced solutions which can significantly help for day-to-day operational functioning of LEAs.

The privacy protection aspect during utilization of the advance ICT tools by LEAs in the observed countries is often weak due to the poor implementation of legislation and weak regulatory control practices. Socio-economic transformation and usage of ICT have radically changed the way of life in these countries as well. Therefore the LEAs and especially the police need to pay special attention both in building its own capacities for preventing the new sophisticated types of crime and also in providing accountable procedures and mechanisms to guarantee the fundamental rights when police officers used new ICT technological tools in providing public safety and crime prevention activities.

Recommendations

- Establishing productive cooperation and partnerships of the LEA and police organisations with private sector, academia and civil society organisations in order to be established more efficient process of following of the technological processes and minimizing the technological gap in the police workflow;
- Increasing the awareness of stakeholders, LEA management structures and police leadership for establishing special and sufficient funds for research and development in the law enforcement area and establishing a practice of conducting regular analysis of the current threats coming from abuses of the new technologies by criminals;
- Adopting and utilizing new ICT hardware and software for improving the analytical capacities of LEA and police, for reducing their response time in criminal investigation and crises management as well as for establishing secure channels of communication and data exchange at national, regional and European level;
- Conducting periodic awareness raising activities among the LEA and police officers on all organisational levels, nationally and at EU level about the new technologies possibilities and potential treats;
- Developing educational and training programs for LEA and police officers which will correspond

to the new digital realities and citizens' needs and will be focused both on the positive and negative sides of the new technologies over the safeguard of the fundamental human rights and over the outcomes of the police work activities and duties;

— Encouraging practices which allows bottom - top approach in developing new initiatives and innovation which actually means that any police officer beside his/her rank and position could propose and initiated development and adoption of new technologies and skills which will make police work more efficient and effective;

— Establishing formal and informal channels for initiatives, projects and recommendations by the state, non-state or international partners devoted for innovating the policing and maintaining the public security;

— Setting the protection of privacy as a priority when using the new technologies by LEA

— Strengthening the capacities of North Macedonia, Montenegrin and Serbian LEA and police for participation in EU funded projects (especially through Horizon 2020 programme) in order enhancing its organisational and human resources for adoption high –tech methods and toolkits in their day-to day work and for better interoperability with EU law enforcement and security systems for crime investigation and data exchange.

References

- Böhmelt, T. & Freyburg, T. (2017) Forecasting candidate states' compliance with EU accession rules 2017–2050. *Journal of European Public Policy*, 1-19.
- De Pauw, E., Ponsaers, P., Van Der Vijver, K., Bruggeman, W., & Deelman, P. (Eds.). (2011) Technological led policing. *CAHIERS POLITIESTUDIES (CPS)*. Antwerpen, Belgie ; Apeldoorn, Nederland: Maklu.
- European Commission. (2017) Horizon 2020 - Security,
  Available at: https://ec.europa.eu/programmes/horizon2020/en/area/security. Accessed on 15 October 2018.
- European Commission. (2015) "Priebe report"' - The former Yugoslav Republic of Macedonia: Recommendations of the Senior Experts' Group on systemic Rule of Law issues relating to the communications.
- European Commission. (2018) A credible enlargement perspective for and enhanced EU engagement with the Western Balkans.
- European Commission. (2016) European Commissions country report Serbia 2016, 61.
- European Commissions' country reports for the former Yugoslav Republic of Macedonia, Serbia and Montenegro.(2018)
  Retrieved from: https://ec.europa.eu/neighbourhood-enlargement/countries/package, Accessed on 7 May 2018.
- Journalism Development Network (OCCRP), Rise Project and the European Actors Association (EAA) (2015). Who are the Gatekeepers of the Internet? Internet ownership project, Serbia: It's Hard to Tell Who Owns Some of Country's biggest internet service providers (ISPs).
  Retrieved from https://www.reportingproject.net/internetownership/?p=116, Accessed on 08 January 2018.
- Koper, S., Lum, C. & Willis, J. (2014) Optimizing the Use of Technology in Policing: Results and Implications from a Multi-Site Study of the Social, Organizational, and Behavioural Aspects of Implementing Police Technologies. *Policing: A Journal of Policy and Practice*, 8-2, *Oxford University Press*, 214.
- Koper, S., Lum, C., Willis, J., Woods, J. & Hibdon, J. (2015) *Realizing the Potential of Technology in Policing* (December edition). George Mason University.
- *Law on protection of personal data*, „Official Gazette of the Republic of Serbia" nos. 97/2008, 104/2009, 68/2012, 107/2012.
- Ministry of Interior of Montenegro. (2015) *Development strategy for police for the period 2016-2020.*
  Retrieved from http://www.mup.gov.me/rubrike/strategija_razvoja_uprave_policije/.Accessed on 02 Jun 2017
- Ministry of Interior of Republic of Macedonia. (2016) *Police Development Strategy 2016 – 2020.*
  Retrieved from http://www.mvr.gov.mk.Accessed on 01 Jun 2017.
- Ministry of Interior of the Republic of Serbia. (2010) *Development Strategy of the Ministry of Interior of Republic of Serbia 2011- 2016.*
  Retrieved from http://mup.gov.rs/wps/portal/sr/dokumenti/Strategije/. Accessed on 02 Jun 2017.

- Ministry of Interior of the Republic of Serbia. (2017) *Development Strategy for the period 2018 – 2023*. Retrieved from http://mup.gov.rs/wps/portal/sr/reforme/.accessed on Jan 2018.
- Paunovic, D. (2005) Police Reform in Serbia. *Friedenskonsolidierung auf dem Balkan: Probleme und Perspektiven. Forschungen im Akademischen Netzwerk Südosteuropa 2003/2004*.

Interoperability: Diagnosing a novel assessment model

Sérgio Felgueiras
Lúcia G. Pais
Sónia M. A. Morgado
Major Events Laboratory, Research Centre (ICPOL), Instituto Superior de Ciências Policiais e Segurança Interna, Lisbon, Portugal[1]

Abstract

Today, uncertainty is what is most certain in our daily living. In the domain of security and protection, uncertainty becomes a critical condition for the decision-making process. Crowd's protection is a complex and arduous problem in what concerns to guarantee security and safety during mass gatherings. In Europe, after several terrorist attacks targeting crowded places, the first responders had to cooperate to mitigate the terrible effects of a terrorist attack, violence or an accident. The promotion of a better cooperation amongst first responders should be based on a multilevel interoperability model to solve potential and real coordination problems during rescue operations. It is clear that an interoperable system will respond in a better and integrated way to save lives. Preparedness is the key element. We all know that there are some traditional barriers for the interoperability implementation, such as technological, cultural, organisational and individual. The presentation of a general reflexion about the critical aspects of interoperability governance (plan, decision-making and training) tackles key issues such as innovation, harmonisation of safety and security culture, articulation of top-down and bottom-up approaches, operational procedures, technological support and general training. The discussion of a diagnosis model to assess the European interoperability continuum will give some food for thoughts to draft a roadmap to enhance the potential of each organisation and the overall interoperability system.

Keywords: diagnosis model, first responders, governance, innovation, interoperability

Introduction

´The two biggest challenges for police are interoperability and security between the information systems´ (Scarborough & Rogers, 2007: 666). In the domain of security and protection, uncertainty becomes a critical condition for the decision-making process. Crowd's protection is a complex and arduous problem in what concerns to guaranty security and safety during mass gatherings. In Europe, after the several terrorist attacks targeting crowded places, the first responders had to cooperate to mitigate the terrible effects of a terrorist attack, violence or an accident. But due to their diversity and the diverse multicultural approaches between European countries, and within the organisations, the response to critical incidents differs among them.

1 Corresponding author's email: sfelgueiras@psp.pt

Building trust between the different organisations involved in the first response activities is essential. Though, it may take too long to achieve regardless the urgency of the interventions, namely considering the jurisdictional disputes and the closeness of the organisations, their competitiveness, and the contemporary security demands. Sharing, integrating and managing of the information coming from the different stakeholders seems to be an impossible mission to accomplish.

This paper aims to contribute to the comprehension of the interoperability process, which considers different factors, dimensions, events and values of stakeholders, and helps to better understand how they can or interact in order to accomplish the interoperability potential. We propose to design a model for data collection and analysis that will allow the characterisation of the standard procedures as well as the malfunctions in each of the organisations studied. A survey will be conducted using this model and as a result it will help us to build a dynamic map where links and disruptions amongst them can be identified, thus enlightening us about current best practices and points of attention.

The usual focus for interoperability is information sharing (Allen, Karanasios & Norman, 2014; Chen et al., 2008; Desourdis, 2009; Miller et al., 2005; Thatcher, Vasconcelos & Ellis, 2015). However, working collaboratively implies achieving coordination between multi-team agencies at various levels. Therefore, the concept exceeds and goes beyond the strict sense of interoperability as information flows. For instance, the technological dimension is frequently approached on the basis of communications' equipment (Miller et al., 2005). Nevertheless, governance, usage, training and operations (Department of Homeland Security [DHS], 2005) are also elements for and of intervention with high levels of complexity that needs to be acknowledged.

In the context of multi-agency cooperation, interoperability is ´the capability of organisations or discrete parts of the same organisation to exchange operational information and to use it to inform their decision making´ (ACPO NPIA, 2009: 14).

The promotion of a better cooperation amongst first responders should be based on a multilevel interoperability model to solve potential and real coordination problems during rescue operations. It is clear that an interoperable system will respond in a better and integrated way to save lives.

Preparedness is the primary element. In fact, assuring readiness must rely not only on an adaptive response (Jenkins, 2006), but on a projected roadmap for first responders to deal with soft or hard incidents, in traditional or emergency missions, despite their unpredictability due to their dynamic nature.

This implies that police managers have to consider money expenditure, logistics, and opportunity-cost evaluation. In the end, the outputs of the organisations have to be questioned, and the whole missions will have to be reconfigured. A dilemma emerges: being focused on emergencies, routine activities are left aside... Regarding economic management, money expenditure in units that have to be stationed most of the time in a standby position is immediately questioned and put under criticism. Furthermore, it can be asked if this dilemma is pondered the same way by different organisations and in different countries, mainly if we bear in mind that the political climate may have a clear influence on these matters.

On the other hand, having a taxonomy and unifying procedures between first responders would ensure and improve the compatibility of approaches and interventions in critical incidents. As stated by Timmons (2007: p.3) 'it is imperative to devote resources to developing and implementing new procedures for responders during emergencies'.

And so, code sharing is essential for people to talk and understand each other. The human factor must be properly recognised, so the learning and training process is fundamental to raise awareness and thus improve the communication skills of everyone involved. This seems to be another item for proper consideration – the integration of these specific issues in the academies' curricula.

In this sense, not only the communication improves but also the decision-making process.

> ´More than a simple patch between two adjoining radio networks or a few officers talking on interoperability channels at a crisis, shared digital networks give all officers the ability to communicate with the right people to acquire the right information to accomplish their mission and solve problems whenever and wherever they need it.´ (Cowper, 2007: 1249-1250).

Some well-known traditional barriers for the interoperability implementation are technological, cultural, organisational and individual. Different organisations in the same country and in various countries as well, may be in different stages of development, acting based on different concepts of governance which are also differently operationalised.

Also, the constant technological development is another factor that separates countries, placing them apart from each other and thus compromising cooperation. The financial limitations police organisations are facing puts them in different levels of maturity in technological intervention. Therefore, they usually have a diverse perception of the same incident, and so engage in different activities to respond according to the organisational diversity.

In fact, some of the characteristics of the modern policing information technology systems, mentioned by Manning (2005: 230-231), such as the existence of ´nonlinked databases that are locally sourced, numerous software systems, the secrecy and nonlinked access points (multiple and incompatible channels of communication between the public and the police within the police department), the inconsistent user and backside technology interfaces, the tendency to use mapping information for short-term tactical interventions absent "problem solving"', must be overcome by coordinating with interoperability.

This fragmented approach may actually put people´s lives at risk. It seems imperative the first responders design a common language and method to boost the whole interventions. One of the best-known laws of Gestalt tells us that "the whole is other than the sum of the parts", so it seems mandatory to find a minimum common denominator. To accomplish this goal, different parties have to trust each other, understand the added value of interoperability, in order to pool and share resources, information, etc.

Building trust between stakeholders involves aggregating diverse information, models of intervention, eliminate isolated systems to manage and process information. The integrative and sharing mode would enable evocative information usage and boost operation, decision-making and security of crowds. The major problem here seems to be the time and length of the trust-building process because of the usual secrecy of police organisations culture. Thus, interoperability is the solution to facilitate data processing, management and decision-making.

A major question has to be answered: How to diagnose a model to assess the European interoperability continuum?

Method

General remarks

Building up a questionnaire demands to adequately address the issues that we want to learn about. First, we have to find out the proper dimensions to be addressed. Second, some linguistic precautions have to be taken, namely regarding the idiomatic expressions and some specific discourse technicalities, to maximise clarity. This issue directly links with the different professional specialities and organisations that will be under analysis. Also, the way the questionnaire has to be delivered must be taken into account – in this case, by mail.

Participants

The main idea is to apply this instrument in several European cities, in a multilevel approach (inter- and intra-organisation).

Procedure

The core dimensions were highlighted during the literature review and some (more or less) informal talks with operatives and experts in the knowledge domain. Also, they were based on the JESIP Multi Agency De-Brief Template[2] and the Homeland Security Interoperability Continuum (U. S. Department of Homeland Security, 2015). As far as the U.S. Department of Homeland Security (2015: 1) aims 'to assist emergency response agencies and policy makers to plan and implement interoperability solutions for data and voice communications', the JESIP template was designed to have a common approach for the post event assessment. Some examples of the dimensions are: context/framework, standard operational procedures, communication, and technology, amongst others.

2 www.jesip.org.uk/upload/media/pdf/JESIP_Interoperability_De_brief_.4.pdf

Results

Based on the specific goals established, some close-ended and open-ended questions were designed to collect different kinds of data. According to these different types of questions, statistical tests will be made. The questions will be ordered so that they follow each other logically and the diverse topics were organised clearly in between them. Demographic data is to appear at the beginning of the questionnaire, as usual. The questionnaire will be tested in different professional groups to ask for some feedback. The need for rewording or rephrasing, the order of the questions along the questionnaire, and/or the necessity of deleting or presenting new items, will be cleared in this phase.

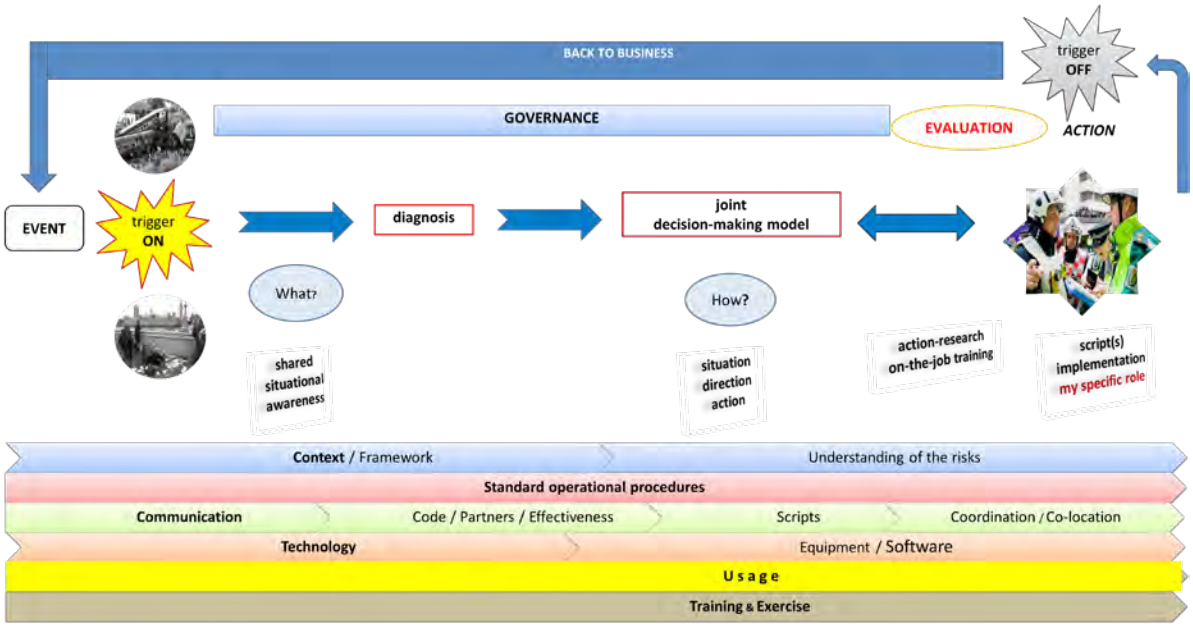
The meaning of interoperability in first responders is both intrinsically complex and dynamic and tends to fluctuate with context, type of event and time of occurrence. We intend to gather information about networking, processes involved, and technologies applied to improve interoperability, reliability and security.

We intend that interoperability involves a chain of processes (see Figure 1) starting from the event characterisation which according with its nature, context, etc. may or may not demand an interoperable approach. So, the first decision to make is to classify the event and, consequently, involve the necessary types of first responders. The proper identification of the concrete problem (or problems) at stake imply the existence of a shared situational awareness, and must consider the context features and the diverse institutional frameworks. This will permit to answer the main question in the first moment: What is happening? This is the phase in which the diagnosis is performed. At this stage, the conditions for the emergence of a common vision about the event should be met.

For this to happen, communication is crucial. It will allow to establish the necessary common-code to promote the effectiveness of the whole response. A common-code as well as a shared understanding of the standard operational procedures, supported by the technologies, may answer the second major question: How to deal and solve the problem? In this moment, it is possible to envisage a joint decision-making model and define the action course to manage the risks and implement the agreed scripts where each partner knows his role within the event operational coordination.

The after-event phase should let everybody go back to business. By then, it is possible to evaluate the whole operation, mainly in what concerns governance, data and information sharing, use of technology and the effectiveness of communication. In a word: Interoperability.

Figure 1 – Conceptual model of intervention



Therefore, the results of the survey to be conducted, that is the first stage of the process, will allow for a close picture of the interoperability situation in several European cities, according with the conceptual model of intervention. Actually, systemising the issues related to interoperability, acknowledges services, information and processes features, being the core and leverage for building a model that can be used to good governance in action. Considering the questionnaire also as a methodological tool for collecting data concerning the entire intervention, it is an action-research tool, and its results provide elements to conduct on-the-job training for all first responders' organisations.

Discussion

As stated by Allen et al. (2014), interoperability should be managed in organisational and informational aspects, developing systems that work in either routine or anomalous situations, within a common framework and taxonomy concerning procedures, working practices and harmonisation of first responders.

Building a cohesive interoperability platform would ensure that end-users can combine strategies and interact in order to serve a common purpose, regardless the differences between the services.

As so,

— the harmonisation of the different organisations regarding its subcultures, and in terms of the safety and security culture,
— the articulation of top-down and bottom-up approaches, operational procedures, technological support and general training,

will demand for a new and innovative decision-making model, that will withstand the reflexion about the critical aspects of interoperability governance and compose solutions highly optimised towards the needs of the first responders.

House, Power and Alison (2014) also argue that in the actual conceptualisation decision-making is at risk, considering that a non-hierarchical and decentralised network would benefit interoperability.

The diagnosis model as a roadmap for first responders can be considered a win-win situation. Its benefits for the intervention in different kinds of events seems obvious. It would increase the trust between partners, enhance collaborative processes, improve the homogeneity of process and information systems, and decrease disruption in data integrity that affects the collaborative processes, thus decreasing the responsibility and accountability gap.

References

- ACPO NPIA (2009) *Guidance on Multi-Agency Interoperability.* Available from: http: http://library.college.police.uk/docs/acpo/Multi-agency-Interoperability-130609.pdf [Accessed 10th January 2018].
- Allen, D. K., Karanasios, S. & Norman, A. (2014) Information sharing and interoperability: The case of major incident management. *European Journal of Information Systems*. 23 (4), 418-432. doi:10.1057/ejis.2013.8
- Chen, R., Sharman, R., Chakravarti, N., Rao, H. R. & Upadhyaya, S. J. (2008) Emergency response information system interoperability: Development of chemical incident response data model. *Journal of the Association for Information Systems*. 9 (3), 1-8.
- Cowper, T. (2007) Technology and the police. In: Greene, J. (ed.), *The Encyclopedia of Police Science*. 3rd ed. New York, Routledge, pp.1249-1250.
- Desourdis, R. I. (2009) *Achieving Interoperability in Critical IT and Communication Systems*. London, Artech House.
- House, A., Power, N. & Alison, L. (2014) A systematic review of the potential hurdles of interoperability to the emergency services in major incidents: Recommendations for solutions and alternatives. *Cognition, Technology & Work*. 16 (3), 319-335. doi:10.1007/s10111-013-0259-6
- Jenkins, W. O. (2006) Collaboration over adaptation: The case for interoperable communications in Homeland Security. *Public Administration Review*. 66 (3), 319-321. doi:10.1111/j.1540-6210.2006.00588.x
- JESIP (2015) *JESIP Interoperability De-Brief.* Available from: http: www.jesip.org.uk/upload/media/pdf/JESIP_Interoperability_De_brief_.4.pdf [Accessed 2nd November 2017].
- Manning, P. K. (2005) *Environment, Technology, and Organizational Change.* In: Pattavina, A. (ed.), *Information Technology and the Criminal Justice System*. Thousand Oaks, CA, SAGE Publications, pp. 221-239.
- Miller, H. G., Granato, R. P., Feuerstein, J. W. & Ruffino, L. (2005) Toward interoperable first response. *IT professional*. 7 (1), 13-20.
- Scarborough, K. E. & Rogers, M. K. (2007). *Information security*. In: Greene, J. (ed.), *The Encyclopedia of Police Science*. 3rd ed. New York, Routledge, pp.664-669.
- Thatcher, A., Vasconcelos, A. C. & Ellis, D. (2015) An investigation into the impact of information behaviour on information failure: The Fukushima Daiichi nuclear power disaster. *International Journal of Information Management*. 35 (1), 57-63.
- Timmons, R. (2007) Interoperability: Stop blaming the radio. *Homeland Security Affairs*. 3 (1), 1-17.
- U. S. Department of Homeland Security (2015) *Interoperability Continuum: A Tool for Improving Emergency Communications and Interoperability*. Washington, DC, Department of Homeland Security.

MOLECULA: The Tax, Economic and Financial Investigation of Transnational Organised Crime in European Union

Nelson Macedo da Cruz
Tax Action Unit, Republican National Guard, Portugal[1]

Abstract
In a European environment marked by the growing influence of transnational criminal organizations, boosted by the globalisation of markets and accelerated developments in information, knowledge and, specially, communication technology, it is recognised that the detection, immobilisation and recovery of illicit proceeds and instruments generated represent the key to its neutralisation. In this context, the MOLECULA PT Project materializes the use of the same technology, with the strict respect for the rights, freedoms and guarantees of European citizens, in order to highlight all the unjustified assets hidden from the authorities in the EU territory. At the same time, the MOLECULA PT Project represents the opportunity to adjust the interaction environment between the actors involved on tax, economic and financial investigations to a unified European architecture, enabling synergies, that renders transnational criminal organisations dysfunctional and their illicit assets exposed to the authorities' action.

Keywords: Transnational Organised Crime, Tax, Financial and Economic Investigation, MOLECULA.

Introduction

In the gradual legal and political *Judiciary and Police Cooperation in Criminal Matters* framework, within the scope of the *Area of Freedom, Security and Justice*, the tax, economic and financial investigation of transnational organised crime[2] needs to become a global, coordinated, innovative and, eventually, a unified response of EU.

As a way of feeding this differentiated response, understood as a pressing need to neutralize this growing threat, the present article presents the MOLECULA PT Project as a platform that, automatic and intelligently, exposes sufficient evidence on tax, economic and financial crime practices by individuals and companies in Portugal and potentially on EU territory, by confronting two global data groups:

— *the assets declared as licit for each natural person or company during a given time period*;
— *the assets actual and effectively held by the same person or company in that same time period.*

We will conclude by exploring the potential future development in European Law framework, based on the

1 Corresponding author's email: cruz.nm@gnr.pt

2 Threats materialised in "*(…) risks and dangers, some of them news, some old, which have only risen in the hierarchy of Member States concerns*" (Garcia, 2006, p. 1), which severely restrict the exercise of rights, freedoms and guarantees by its citizens.

texts approved by the Lisbon Treaty on 2009, of the legal and institutional architecture in which MOLECULA PT Project could grow, in parallel with its projected functioning in Portuguese institutional and legal framework.

Transnational Organised Crime

We start from a conceptual reference of organised crime, which is substantially different from *criminal association*. We rely instead on the definition formulated by the United Nations Assembly in 2000: *"a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes*[3] *or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit"* (UN, 2000). This definition has been supplemented by Sousa *et al* (2014): *"(…) a complex phenomenon, always ready in the name of easy and unlawful profit, tending to jeopardize the rule of law and corrupting societies"*. These transnational and organised criminal groups are fostered by recent social phenomena[4] (Alves, 2013), obtaining then "*organizational rationality*" Bravo, 2013, p. 14), *polymorphism*[5] and a global action capacity through national legislations (Natarrajan, 2011)[6].

Having defined the concept of a criminal organisation, it is necessary to apply it to the tax, economic, financial and transnational or cross-border approach involved in the international financial transactions linked to trafficking, drugs and arms smuggling, corruption and fraud financial market[7]*."(…) They are all linked by the mother crime – Money laundering. Without it, the crime economy wouldn't be global neither higly profitable."* (Hassemer, 1998: 313f)[8].

In this sequence, the 11th United Nations Congress on Crime Prevention and Criminal Justice established that *"(...) all forms of non-violent crime that results in a financial loss (...) a wide range of illegal activities, such as fraud, tax evasion and money laundering"*[9] (UNODC, 2005: 1) and, simultaneously, *"(…) violate, directly or indirectly, the norms that regulate the economic order and the financial or economic assets or interests of the State"* (Hassemer, 1998).

In order to systematise and operationalise the concept of transnational organised crime, we present the following Figure 1:

3 That means a "*conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.*"

4 In January 2013, the EU recognised that the Internet "(...) is opening up new possibilities at a remarkable pace and at a low cost (...)" (Pereira, 2013, page 13) and allows the distribution of new psychoactive substances, not controlled by international drug law (European Comission, 2013, p. 13).

5 According to Wright (2006:192) "*currently, countries that detain offenders or extradite them from places where they have sought refuge, must apply criminal proceedings against organized crime groups to which they belong, according to their own jurisdictions*".

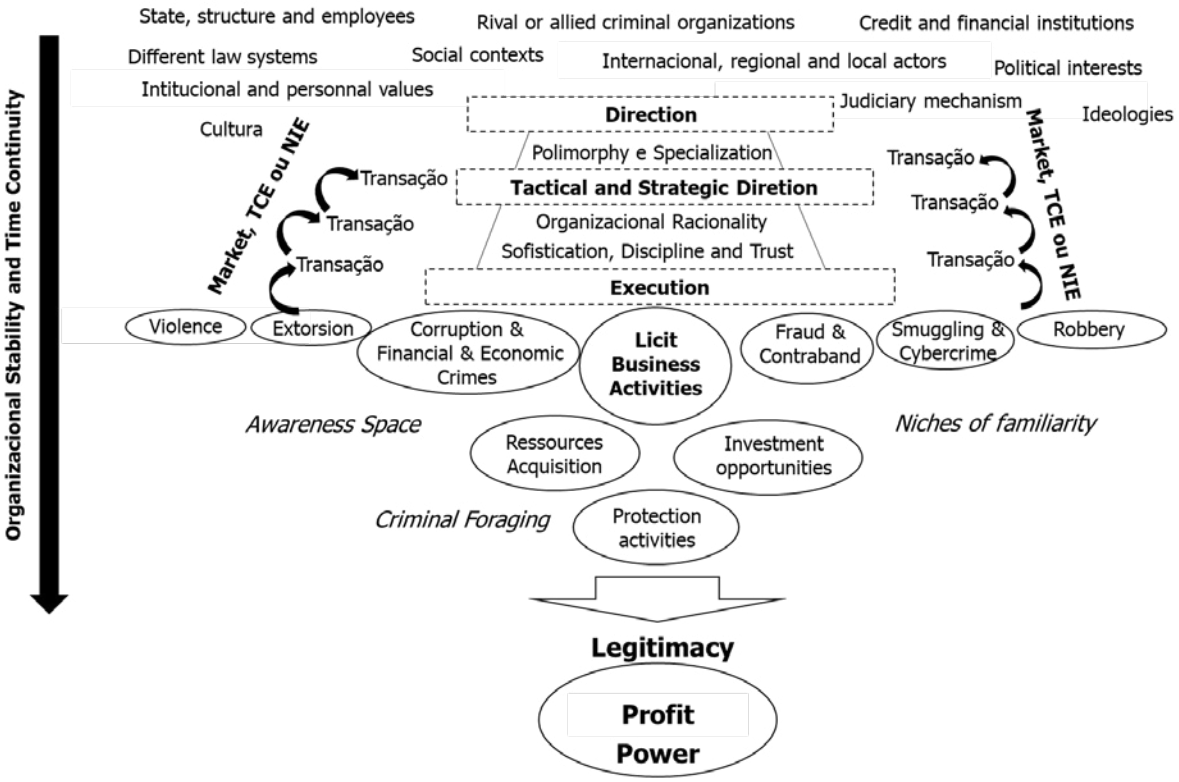
6 As it stays on the Council of Europe's 1998 Communication, which argued that each Member State had a key role to play in preventing and combating organised crime. On the other hand, Silva (2001) emphasises the European legal problems with regard to the liability of legal persons, authorship, establishment of causal link and to the intent and negligence evidences that encroach the capacity to punish the enumerated criminal conducts.

7 According to Bravo (2013: 10): *"(…) the impregnation by organized and economic crime of extensive sectors of activity, attractive as a means of recycling and washing the enormous revenues produced by criminal activities such as trafficking in persons,arms, drugs, metals and precious stones, corruption and fraud".*

8 Following W. Hassemer (1998: 313f) *"(…) all types of trafficking are practiced by this" shadow system "whose power is extended throughout the world: weapons, technology, radioactive materials, art, human beings, human organs, murderers on the pay and smuggling of the most diverse products to and from any part of the world (…)".*

9 The existence or mere speculation about the existence of this type of crime undermines the legitimacy of government and the sustained development of any state. Specifically, money laudering represents the guarantee of liquidity and reinvestment of criminal organisations and causes international financial and credit institutions and capital markets manipulations, as well as, discourages foreign direct investment (UNODC, 2005).

Figure 1 – Transnational Organised Crime



Tax, Economic and Financial Investigation

In this European framework, in order to find the illicit profits of transnational organised crime we need to focus investigation on the detection and evidence gathering for tax, economic and financial crimes - *"Given the increasing risk of penetration of the licit economy by serious and organised crime, financial investigation is an essential tool of a modern and effective response to criminal threats including terrorism financing."* (UE, 2016). This approach is set out in FATF (2012: 5), as *"(…) an enquiry into the financial affairs related to criminal conduct (…) identify and document the movement of money during the course of criminal activity (…) link between the origins of the money, beneficiaries, when the money is received and where it is stored or deposited (…) identifying the extent of criminal networks, the scale of criminality, by tracing proceeds of crime, terrorist funds (…)".*

The EU's capacity to effectively investigate and prosecute organised criminals about their tax, economic and financial crimes requires a process of institutional and legal change (Trauner & Servent, 2015), or, according to Boer (2016), an evolutionary process. Given that EU actors act in accordance with a procedures framework (treaties and other legislation that forms the EU Law) and a specific problem definition (in this case the economic-financial and tax fight against organised crime)[10], there is a need for institutional change [11] understood as *"(…) a change in the structural environment in which actors interact."* (Trauner & Servent, 2015: 19), which fundamentally comprises as an interface the EU institutions.

A process of institutional change in the Area of Freedom, Security and Justice should ideally involve agencies and institutions, whether national or European, with a central role in the tax, economic and financial fight against organised crime. These include police and law enforcement magistrates, tax and customs admin-

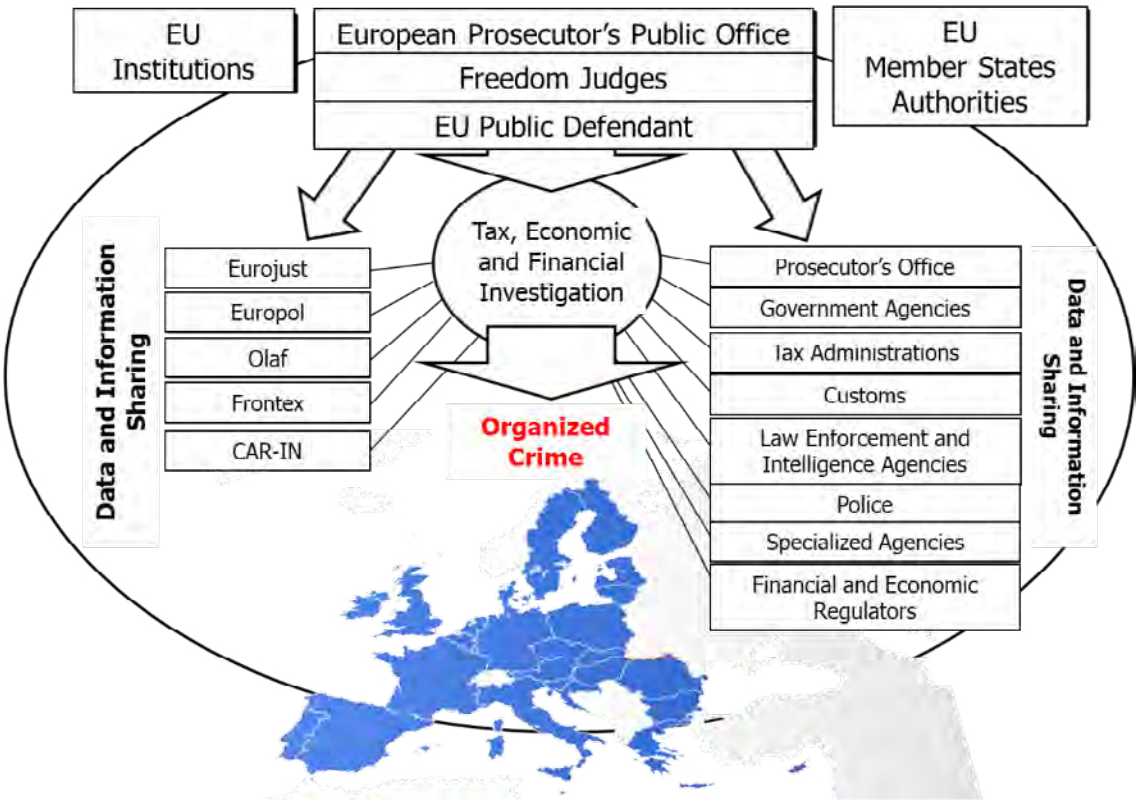
10 Its impact on the EU is evidenced in the 2003 European Security Strategy by recognizing that its space is the primary target of organised crime, and that *"Revenues from drugs have fuelled the weakening of state structures in several drug-producing countries. Revenies from trade in gemstones, timber and small arms, fuel conflict in other parts of the world"*, and in the 2008 Report on the Implementation of the European Security Strategy, *"organized crime continues to threaten our societies by the practice of trafficking in drugs, human beings and weapons, as well as international fraud and money laundering"* (UE, 2008: 4).

11 The shift or change can occur in a formal or informal way. The formal change involves the reform of treaties or the legal production by competent institutions of European bodies. On the other hand, the informal shift involves the process of exchange and sharing between the Member States, leading to new interinstitutional practices and a renewed understanding of the existing rules.

istrations, financial regulators, sources of operational and strategic information, as well as the European Parliament, the European Council, the Council of the EU, the European Commission, the European Commission, and the Court of Justice. There is also an enhanced role for the Area of Freedom, Security and Justice, the EU Court of Auditors, the European Central Bank and the Consultative Bodies.

In order to demonstrate the legal and institutional architecture, as Bayer (2010) says *"(…) a giant blue spider-web across the world, full of intricate entanglements and fine embroidery"*, where MOLECULA PT should ideally work, we present the Figure 2:

Figure 2 – The EU Legal and Institutional Architecture for Tax, Economic and Financial Investigation



MOLECULA PT Project

The MOLECULA PT Project was inspired by the 6th 1999 Tampere Conclusions:

"*- people have the right to expect the Union to address the threat to their freedom and legal rights posed by serious crime. To counter these threats a common effort is needed to prevent and fight crime and criminal organisations throughout the Union. The joint mobilisation of police and judicial resources is needed to guarantee that there is no hiding place for criminals or the proceeds of crime within the Union*"[12].

Within a Portuguese and EU society that increasingly realizes that its rights, freedoms and guarantees are restricted by criminal activities, propelled by the latest revolutions in the field of information, communication and knowledge technologies, as well as the globalisation of markets, it remains essential to provide to the State and regulatory authorities the effective capacity,

12 In a contrasting sense, Boer considers that *"The European Comission has been a strong propagator of public-private partnerships in the field of security, and the technology industry definitely has a foot in the door when it concerns the development of technology for police information and surveillance purposes."* (Boer, 2016: 129).

competence and power to apply the law, to verify its compliance and to punish conduct that jeopardizes its survival and the complete fulfillment of its mission. MOLECULA, in the 21st century, allows the Portuguese State and EU to bring together isolated and poorly exploited data held and managed by several legally competent public authorities[13] in order to tackle effective, efficient and economically organised crime with transnational relations.

Organised, group or even individually committed criminality is likely to produce a gain which is inconsistent with the funds legally declared to the tax authorities. Profit is the main aim of the great majority of committed crimes. Therefore, it is considered that the best way to neutralize and repress these illegal capital flows is based on the detection, immobilisation and recovery of the illicit revenues generated by the crime directly to State and EU Finances. Thus economic, financial and tax investigation assumes a central role.

In this context, MOLECULA PT Project, through automated and intelligent processing based on a permanently self-learning algorithm, aims at the clear and accurate detection of individuals or companies that have unjustified assets associated with suspicion of committed crimes. The Disproportions Report (DR), the final product of MOLECULA, represents a disclosure report, attached with a link chart[14], which is transmitted directly, in an encrypted and secure way, to the competent Portuguese Prosecutor's Office. In this point of view, MOLECULA provides to the economic, financial and tax investigation advanced intelligence, effectiveness, efficiency and economy[15].

MOLECULA PT scans, in a continuous, systematic and consistent way, the official databases of each of the Member State authorities [16] for every portuguese or european citizen[17], targeting previously selected data categories, coding them in coefficients, and then carrying them through an encryption process.

The last procedure is performed by *Fully Homomorphic Encryption* (FHE)[18], allowing computations over encrypted data, without the need of decryption (Zhang et al. 2016). Moreover, there is a warranty that neither the blocks nor the function result are exposed throughout the process[19].

The codified data that is extracted by the algorithm is in three main groups: the revenues, transactions and other fiscally relevant transactions legally declared in the last 5 years[20], the actual and effective taxable income, transactions and other transactions obtained in the same last 5 years[21], as well as judicial and police information for each of the same citizens or companies[22]. Disclosable events are detected by comparing the first two categories, complemented by the third category.

The three categories will be continuously processed by a predefined algorithm. The criminals' identification (and creation of the consequent Disproportion Report)

13 With the main purpose of detecting and investigating economic, financial and tax crimes on a efficient, parsimonious and efficient way, we consider as essential the rethinking, exploring and enhancing of the set of isolated or poorly related data which actually are managed by several competent authorities on Portugal.

14 The links chart, developed by *Analyst's Notebook* tools, represent a mirror of the criminal organisations elements connections, their influence on the territory and the localisation of their activities, composed by both predicated crimes and tax, economic and financial crimes.

15 If we think in all Portuguese authority work that would be necessary to obtain a Disproportion Report (DR), the quantity of information requests sent to other national or international authorities, the time lost on the data obtaining and analysis, we can safely say that MOLECULA PT Project brings the mentioned characteristics.

16 The data come from the civil registry, kinship relations, relations with individuals and legal persons, police and judicial precedents, information on assets, financial data or even use of telecommunications and internet.

17 Each citizen will see their identity coded based on their respective tax ID number, or, in case of non-existence, of civil identification.

18 As expected, Fully (FHE) is the most complete, having no limits about the type of operations (Partial) or the number of times that the operations can be applied (Somewhat).

19 In 2009, Gentry (Gentry 2009) provided the first FHE scheme as well as a generic method that was used as a basis for future encryption systems.

20 These data segments provide the legality reference and the basis for any inconsistency with the remaining data categories. In this category, there are the global registers held by the tax and customs authorities and the social system authorities, namely, among others, the registration information, declared income, transactions and sales of declared goods and services, declared assets additions, records of intracommunity transactions, or inheritances transmitted to the citizen or society in question.

21 This category includes information dispersed by a wide range of sources of information that englobes information from the national central bank, financial and credit institutions, registries and notaries, casinos, security forces and services (databases operations) or judicial databases.

22 The latter category includes information collected by police and security services, intelligence agencies, judiciary authorities and criminal records.

depends on a disproportion alarm value[23]. These *legality line* is then associated to each category and globally. That procedure is guaranteed by *Secure Multi-Party Computation* (MPC), based on *Boolean circuit evaluation*[24] and *arithmetic circuit evaluation*[25] protocols[26].

Whenever the preset criteria are met, The MOLECULA PT platform issues a Disproportion Report (DR) and associated links chart, which are anchored in disproportion coefficients resulting from comparison of the Declared Assets, Possessed Assets and Crime-Evidences categories. The DR is structured to identify behaviour which would amount to a tax, financial or economic crime, punishable by imprisonment, within the Portuguese legal system.

The DR and charts will be presented exclusively to the prosecutor's office which is competent to direct and conduct the investigation[27], in compliance with the rules and procedures of the criminal law[28]. The DR and Links Chart presented will result, after the prosecutor has assessed whether there is sufficient evidence of one or more criminal offences, in a direction to the investigative agencies[29]to obtain further evidence with the intention to secure the prosecution of the criminal organisation. In other hand, if the prosecutor determines that may be a lawful explanation for the DR or Links Chart or there are reasonable doubts about the evidence brought to light, both will be filled on MOLECULA PT archive or monitored by the platform[30].

In summary, MOLECULA PT project is not intended to be a centralised database but rather a platform that in a systematic, continuous and intelligent way is able to interrelate the data of the ATOMs[31] involved, and guarantee the following basic principles[32]:

23 Defined value based on the amount of 15,000.00 Euros of tax due, that, in the Portuguese criminal fiscal system separates a conduct classified as a misdemeanor and, therefore, punished with a fine, or a crime punished by imprisonment (Cfr. Art.os 92, 96 e 103, of Portuguese Tax Infractions General Law.

24 The mentioned protocol are also called "*garbled circuits*" and started with Yao work (Yao 1982).

25 The later protocol are normally "*secret sharing*" based (Shamir 1979) and often use the pattern Sharing - Computation – Output.

26 In these protocols, besides the parties we can also consider adversaries and according to the adversary type (active, passive or covert) we also have different types of security. Bogdanov (2007) describes the arithmetic circuit evaluation in a passive security scenario and Damgård et al. (2013) proposed the SPDZ protocol for an active configuration.

27 It will be firts and final entity that will have the possibility of consult the DR and Links Chart, as well as, the decision-maker about their destination (investigation, filling or special supervision). On EU application of MOLECULA PT Project, we consider that the Portuguese prosecutor's office will be replaced by the Eurojust. According to article 86, n.º 1, TFEU, the Eurojust have the power to assure the initiation of criminal investigations, as well as proposing the initiation of prosecutions, particularly those relating to offences against the financial interests of the Union, the coordination of investigations and prosecutions before referred and strengthening the judicial cooperation. The ideal conditions will be reached with the accomplishment of the possibility laid down by the same article above mentioned: the establishment by the Council, through means of regulations adopted in accordance with a special legislative procedure, of a European Public Prosecutor's Office from Eurojust.This same structure would be the leader andu nique user of MOLECULA, exercising the functions of prosecutor in the competent courts of the Member States in relation to such offences. The European Prosecutor's Office could become the starting point for the creation of a European body, composed by the national authorities of the Member States with the tasks of investigating, prosecuting and bringing to judgement offences against the Union's financial interests and serious crime having a cross-border dimension.

28 In order to applicate MOLECULA PT Project in EU, it will be crucial the European Criminal Law strengthening. In the procedure domain, as it stays on art.º 82, n.º 2, a) and d), TFEU, i tis fundamental to harmonize the mutual admissibility of evidences, the rights of individuals in criminal procedure, the rights of victims of crime and others aspects of criminal procedure. Regarding the substantive domain and according to article 83, n.º 1 and 2, of TFEU, the key reamins on the complete establishment of minimum rules concerning the definition of criminal offences and sanctions in the áreas of particularly serious crime with a cross-border dimension resulting from the nature or impacto f such offences or from a special need to combat them on a common basis – namely: terrorismo, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, money laundering, corruption, couterfeiting of means of payment, computer crime and organised crime.

29 In the case of transnational links detection, the prosecutor will consult Eurojust in order to potentially constitute a Joint Investigation Team (JIT). In any case and to apply MOLECULA PT Project on EU, it would be importante to create conditions for a common tax, economic and financial investigation by all EU Member States authorities. Appointed to this goal and attending to article 87, n.º 1 and 2, a) and c), of TFEU, it assumes a great importance to enhance the collection, storage, processing, analysis and exchange of relevant information, and to implement common investigative techniques in relation to the detection of serious forms of organised crime.

30 If the prosecutor foresees reasonnables doubts about the DR facts, he have the possibility to order the priority supervision on MOLECUL PT Platform of the individual sor companies signalised in order to facilitate a future alarm based on updated ou aditional data.

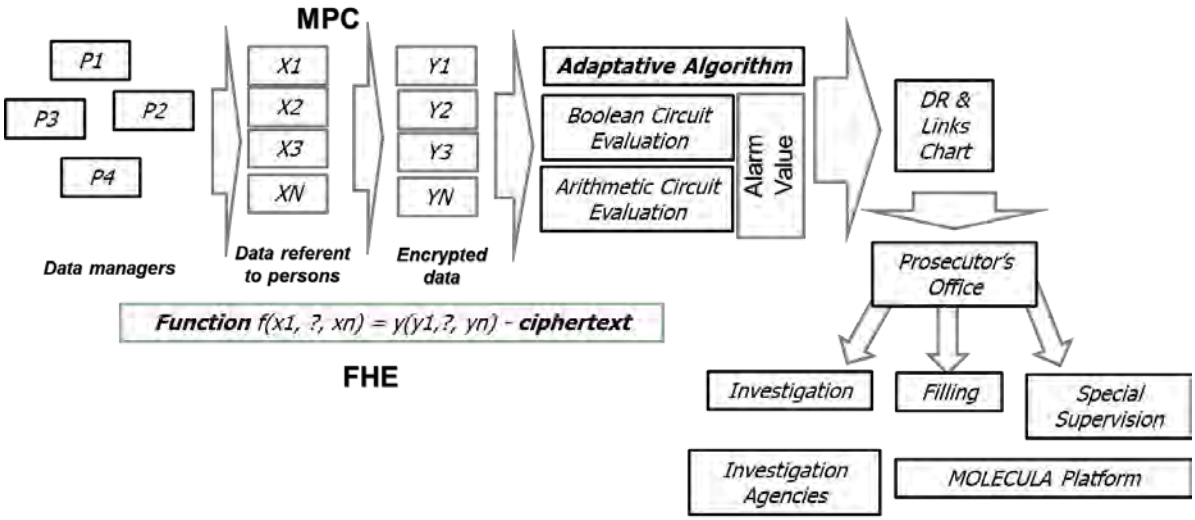
31 Concept used to name the range of entities, bodies and services in the national territory and EU that manage the data used by MOLECULA PT Platform for calculation.

32 Besides the following structural principles: security - only the ATOMs will have access to the platform; privacy - the data of each ATOM will be used only for the calculation and will not be accessible in any other way; equality - each ATOM will be treated equally; integrity - data is not vulnerable to tampering or accidental modification; and no repudiation - participation in a calculation by an ATOM can not be denied later.

— **legal and legitimate collection requirement**[33];
— **accuracy, update and quality requirement**;
— **objective and proportionality requirement**;
— **treatment legality and legitimacy requirement**;
— **storage time requirement**;
— **data security principle**;
— **advertising and accessibility requirment**;
— **participation requirement**;
— **control, supervision and appeal requirement**.

Figure 3 describes the Project architecture for MOLECULA PT:

Figure 3 – MOLECULA PT Project Architecture



Conclusions

In conclusion, MOLECULA PT Project is based on the recognition that the success on the tax, economic and financial crime depends on the automatic and intelligent interrelation of the vast data amount spreaded by several different national authorities and data managers, in order to detect, investigate, prosecute and bring to trial the highly owners of ilegal assets and members of transnational criminal organisations, as well as trace, freeze and confiscate these illicit profits and instruments.

The overall MOLECULA aim is to enable the creation of *"(…) a giant blue spider-web across the world, full of intricate entanglements and fine embroidery"* (Bayer, 2010), composed by EU agencies as Europol, OLAF, Frontex or CAR-IN, with national Member States authorities such as prosecutors, judges, and the vast range of authorities before referred, headed by Eurojust or even European Public Prosecutor's Office, to commonly conduct tax, economic and financial investigations and make transnational organised crime a easy prey before this new european architecture, oiled by MOLECULA, instead the nowadays serious threat to european citizens freedoms, rights and guarantees.

33 That congregates the following principles: Collection Limitation Principle (Guidelines for the Protection of Privacy and Cross-border Flows of Personal Data from the OECD – 1980); Principle of fair and lawful origin (art.º 5, a), of CPDCP, art.º 5, of 95/46/CE Directive and art.º 26, of 2008/615/JAI Decision); Principle of Data Collection (Recomendation n.º R (87) 15 of Ministers Committee, 17th de September 1987); Principle of Collection for Certain, Explicit and Legitimate Purposes (art.º 4 of n.º 45/2001 European Parliament and Council Regulation n.º 45/2001).

References

- Ackers, D. (2005) The Negotiations on the Asylum Procedures Directive, *European Journal of Migration and Law*, Volume 7 (1), 1-34.
- Alves, J (2013) *Criminalidade Transnacional. Jornal de Defesa e Relações Internacionais*. Internet: http://database.jornaldefesa.pt/ameacas/assimetricas/JDRI%20 016%20060113%20criminalidade%20transnacional.pdf, conulted in 3rd November 2015 (17H33).
- Argomaniz, J. (2013) *The EU and Counter-Terrorism: Politics, Polity and Policies after 9/11*. Routledge, Londres.
- Bayer, M. (2010) *The Blue Planet: Informal International Police Networks and National Intelligence*. NDIC Press, Washington DC.
- Béland, D. (2005) Ideas and Social Policy: An Institutional Perspective, *Social Policy & Administration*, Volume 39 (1), 238-239.
- Bigo, D. & Guild, E. (2005) *Controlling Frontiers: Free Movement into and Within Europe*. Aldershot. Ashgate.
- Bogdanov, D. (2007) *Foundations and properties of Shamir's secret sharing scheme*. Research Seminar in Cryptography.
- Bossong, R. (2012) *The Evolution of EU Counter-Terrorism Policy: European Security After 9/11*. Routledge, Milton Keynes.
- Bravo, J. (2013) Para um modelo de segurança e controlo da criminalidade económico-financeira – um contributo judiciário, in Vários, *Working Papers,* n.º 18. Observatório da Economia e Gestão de Fraude (OBEGEF).
- Clemens, E. S. & Cook, J. M. (1999) Politics and Institutionalism: Explaining Durability and Change, *Annual Review of Sociology,* Vol 25, 441-466.
- Couto, A. (1988) *Elementos de Estratégia - Apontamentos para um curso*. Volume 1. Lisboa: IAEM.
- Damgard, I., Keller, M. Larraia, E., Pastro, V. Scholl, P., & Smart, N. (2013) *Practical Covertly Secure MPC for Dishonest Majority or Breaking the SPDZ Limits*. Berlin: Heidelberg.
- Dias, F. (2001) *O Direito Penal na Sociedade do Risco. Temas Básicos da Doutrina Penal – Sobre os Fundamentos da Doutrina Penal.* Sobre a Doutrina Geral do Crime, Coimbra.
- De Kerchove, G. & Weyembergh, A. (2002) *L'espace penal européen: enjeux et perspectives.* Éditions de l'Université de Bruxelles, Bruxelas.
- EUR-LEX Acess to European Union Law. Internet: http://eur-lex.europa.eu/homepage.html, consulted in 13rd May 2015 (20H15).
- Gammeltoft-Hansen, H. (2013) *Access to Asylum: International Refugee Law and the Globalisation of Migration Control*. Cambridge: Cambridge University Press.
- Garcia, F. (2006) *As Ameaças Transnacionais e a Segurança dos Estados. Subsídios para o seu Estudo*. Negócios Estrangeiros, March 2006, Lisbon.
- Guild, E. (2009) Merging Security from the Two-Level Game: Inserting the Treaty of Prum into EU Law? *CEPS Policy Brief*, n.º 124, Centre for European Policy Studies, Bruxelles.
- Hassemer, W. (1998) Limites del Estado de Derecho para el Combate contra La Criminalidad Organizada, in *Ciências Criminais*, Vol. 23, (6), 25-30.
- Huysmans, J. (2000) The European Union and the Securitization of Migration, in *Journal of Common Market Studies*, Vol. 38 (5), 751-777.
- Kaunert, C. (2010) *European Internal Security: Towards Supranantional Governance in the Area of Freedom, Security and Justice*. Manchester University Press, Manchester.
- Lavenex, S. (2009) *Transgovernmentalism in the European Area of Freedom, Security and Justice.* Lynne Rienner Publishers, Boulder. CO.
- Menz, G. (2009) *The Political Economy of Managed Migration: Nonstate Actors, Europeanization; and the Politics of Designing Migration Policies*. Oxford University Press, Oxford.
- Monar, J. & Dahmani, A. (2007) *Specific Factors and Development Trends of Modes of Governance in EU Justice and Home Affairs*. New Gov. Policy Brief Summer.
- Natarajan, M. (2011) *International Crime and Justice*. Cambridge University Press, Cambridge.
- Neal, A. (2009) Securitization and Risk at the EU Border: The Origins of FRONTEX, *Journal of Common Market Studies*, Vol. 47 (2), 333-356.

- OCDE (2013) (2.ª Ed.). *Effective Inter-Agency Co-operation in Fighting Tax Crimes and Other Financial Crimes. OECD – Better policies for better lives*.
  Internet: http://www.oecd.org/tax/crime/effective-inter-agency-co-operation-in-fighting-tax-crimes-second-edition.pdf, consulted in 20th November 2015.
- Pereira, A. (2013) Novas tecnologias estão a mudar tráfico de droga, *Público*, 1 de fevereiro, XXIII (8332), 13.
- Ripoll, A. (2013) Holding the European Parlament Responsible: Policy Shift in the Data Retention Directive from Consulation to Codecision, *Journal of European Public Policy*, Vol. 20 (7), 972-987.
- Roos, C. (2013) *The EU and Immigration Policies: Cracks in the Walls of Fortress Europe?*, Palgrave, Houndmills.
- Santos, C. (2001) O Crime de Colarinho Branco (Da origem do conceito e sua relevância criminológica à questão da desigualdade na administração da justiça penal), *Boletim da Faculdade de Direito*. Studia Ivridica 56. Coimbra Edições, Coimbra.
- Shamir, A. (1979). How to share a secret, *Commun*, ACM, Vol. 22, (11), 612-613.
- Sousa, F.; Ferreira, J. & Agostinho, N. (2014) A Ameaça do Crime Organizado Transnacional em Portugal, in *Revista de Ciências Militares*, Vol. II (1), 13-39.
- Trauner, F. & Servent, A. (2015). *Policy Change in the Area of Freedom, Security and Justice*. Routledge, Studies on Government and the European Union, Londres.
- Triunfante, L. (2012) *Cooperação Judicial em Matéria Penal: Objectivos, Dificuldades e o Modelo Português*. Julgar, Coimbra Editora, Coimbra.
- Wallace, N. (2004) *An Institutional Anatomy and Five Policy Modes*. Oxford University Press, Oxford.
- Wright, A. (2006) *Organized Crime*. Willan Publishing, Portland.
- Yao, A. (1982) *Protocols for secure computations*. 23rd Annual Symposium Computational Science, pp. 160-164.
- Zhang, L. Zheng, Y., Kantoa, R. (2016) *A Review of Homomorphic Encryption and its Applications,* in Proceedings of the 9th EAI International Conference on Mobile Multimedia.

EUROPEAN LAW ENFORCEMENT RESEARCH BULLETIN

Special Conference Edition Nr. 4

CEPOL
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT TRAINING

CEPOL — EDUCATE, INNOVATE, MOTIVATE

European Union Agency for Law Enforcement Training
Offices: H-1066 Budapest, Ó utca 27., Hungary
Correspondence: H-1903 Budapest, Pf. 314, Hungary
Telephone: +36 1 803 8030 • Fax: +36 1 803 8032
E-mail: info@cepol.europa.eu • www.cepol.europa.eu