Tampereen yliopisto
Tampere University

Sirpa Virta, Professor, TAU & Adjunct Professor, Defence University.

Digital Meets Political

Strategic preparedness of the police for AI and Hybrid Threats

CEPOL Research and Science Conference 9.6.2022

Digital : AI

Political : Hybrid Threats

Main fields or perspectives of research on digitalization and hybrid threats

Policing Digital Crime (Bryant & Bryant eds. 2014, Ashgate): digital crimes, cyber crimes – quite a lot of criminological research and policing studies

Digital Policing (Marcinick 2021) ”*Adoption of advanced digital technology is one of the most controversial and fundamental transformations in contemporary police practice. Despite its significance, empirical enquiry of these technologies, and the way they shape and are shaped by policing environments are rare”.*

Research on **hybrid threats** is mainly from military research (hybrid warfare) and International relations (hybrid influencing, interference, operations). The European centre of excellence for countering hybrid threats (HybridCoE) produces a lot of good analysis.

Digital policing (ILP, EBP, Predictive policing)

Algorithmic governance (Katzenbach & Ulbricht 2019): is multiple, contingent and contested. The police employ algorithmic governance by combining and analysing various data sources in order to assess crime risk and prevent crime.

- The degree of automation / police is still accountable for decisions

Marcinick, D. (2021): **Data-driven policing**: How digital technologies transform the practice and governance of policing. (PhD thesis, University of Essex).

Do the radically changing policing environment, transformation and societal security context require re-thinking and analysis of the role and possibilities of future policing?

Hybrid threats (see HybridCoE)

The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means.

The European Centre of Excellence for Countering Hybrid Threats building 31 participants' capabilities to counter hybrid threats. Closely cooperating with the EU and NATO.:

- The Community of Interest on Hybrid Influence looks at how state and non-state actors conduct influence activities.
- The Community of Interest on Strategy and Defence focuses on hybrid warfare, related strategies and implications for security policy.
- The Community of Interest on Vulnerabilities and Resilience focuses on uncovering and understanding the Participating States' and organizations' vulnerabilities, and on improving their resilience.

Research and analysis, training and exercises

Undermine or harm a target?
Overt and covert military and non-military means?

A target can be another state, cohesion of society, political order /democracy, public order, police and trust towards authorities in general, critical infrastructure … anything

Undermine or harm -> hostile operations

Military and non-military means: disinformation, influencing, interference (for instance elections, GPS or other navigation signals interference, …) *what are the criteria*? *Why not criminal means mentioned?*

Action or operations are intentional = political

Strategic Preparedness of the Police?

in rapidly changing security environment

How (well) the police in Finland is prepared for digitalization, especially developing AI capabilities?

How (well) the police in Finland is prepared for countering hybrid threats (consequences of hybrid operations like disinformation, infuencing and interference; elections, GPS spoofing, signal jamming et c)?

”***Digitalization*** *represents a process of intensified interconnection between systems. This hyperconnectivity may lead to vulnerabilities that can be exploited by state and non-state actors. -> There is a need to focus on the implications for countering* ***hybrid threats***.” (HybridCoE, April 2022)

The contigencies (uncertainties) of security -> strategic ambiguity (Virta & Branders 2016)

GOOD GOVERNANCE CRITERIA:

Openess, transparency

Responsiveness

Citizen engagement and participation

Democracy

Accountability

Communication, interaction

Administrative operability

Political viability

Human rights, citizen's rights

Ethics, Legitimacy (Weber)

SECURITY AND ORDER:

Secrecy, closure, confidentiality

Politics

Political, social, moral and existential paradoxes

Really wicked problems, complexity

New securities (e.g. digital security, data security)

Limits of knowledge: *knowing the unknowable, thinking the unthinkable*

Emergency, disaster, crisis, catastrophe –contexts, urgency

Asymmetric power relations

The Other: enemy or threat, crime

Exception, state of emergency

Digitalization and hybrid threats -> vulnerabilities for European security (European or/and national issue?)

The Versailles Declaration of European leaders (10-11 March 2022): ”The need to prepare for fast-emerging challenges, including by protecting ourselves against ever-growing hybrid warfare, strenghtening our cyber-resilience, protecting our critical infrastructure and fighting disinformation.

- Coordinated EU support to Member States on hybrid threats.
- Preparedness is more essential than ever.”

The EU Security Union strategy, The European Democracy Action Plan follow-up, The Digital Services Act proposal… there is a lot going on in digital preparedness in order to strenghten preparedness for hybrid threats and to counter them.

Two sides of the coin: the police should be prepared for both

Being able to employ AI could enhance the police's ability to ensure security, prevent crimes and public order disturbances

- However, there are EU regulation and restrictions in use of AI (biometric regocnition, mass surveillance technologies); the EU AI Act / the French Presidency plans to loosen controls on law enforcement use of AI (7.4.2022) -> requires trust towards the police

On the other hand, digitalization is leading to a widening of the hybrid attack surface.

- The police, society as a whole, political order /democracy, public order can be targets of hybrid operations (of another state, criminal organisation, unknown global network, hostile actor) -> may be serious and harmful for trust towards the police

Hybrid threats: *Is there a crime? Who /what is the actor? Motivation*?

Hybrid threats ”emerged” and police management discourse changed from military and war-terminology to societal (civil) security and policing a couple of years ago.

Prediction, preparedness, protection, prevention (ILP, EBP, Predictive policing) are based on reliable intelligence, information and quality of knowledge. AI can help the police to recognize disinformation, deepfake videos, exceptions et c.

Hybrid operations are not crimes to be investigated or prevented; they have not been defined as war crimes, state crimes, political crimes, intelligence crimes (they can be cyber crimes though); who is responsible?

Motivation is hostile, political, criminal (what?)

Criminal justice systems and the police have to find solutions – strategic preparedness is needed: impact analysis of the possible consequences, risk management, forecast

Strategic preparedness of the police in Finland?

There are some digitalization initiatives of the National Police Board, Analysis Unit (to use AI in traffic control for instance)

- Machine vision (not so called second level identification)
- Drones

The police is represented in the Emergency Powers Act –process of the Ministry of Justice (rapid process, in order to have means to react to hybrid operations through border control)

The police is involved in the EU Horizon and other research and development projects

National Criminal Investigation Bureau has tested face recognition technology (Clearview) for criminal investigation purposes

Police training and education

Police University College:

Introduction of AI –lecture for Master's level students, prof of AI from Helsinki University (2 hours)

New cyber crime prevention and investigation –specialization studies 35 ECTS, starts in September 2022

Master's level studies (leadership and management) include 7 ECTS digitalization-related studies

"*We teach analogous skills for police officers in digital world*" (teacher)

Conclusion: Preparedness is fragmented, strategy is needed urgently

Old-fashioned and old, not very advanced, ICT-systems and organisation /structure of the ICT-services (outsourced to national ICT service organisation) – structures do not support development and innovations in police

Each police department have their own development projects, some buy cheapest systems … very dependent on outside technological expertise

There are good initiatives to develop digitalization and the use of AI especially, but the police do not get needed resources for implementation of the plans (National Police Board)

The annual budget plans of the police do not demand funding for digitalization, innovation and development (but increased nr of policemen, for criminal investigation, crime prevention et c)

”AI is too difficult”
”There are no resources for digitalization”

There is no strategy or plan regarding the digitalization and use of AI in policing

AI is seen useful mainly for investigation (afterwards), not prevention

There is no clear vision of what is to be done with hybrid threats (they are seen as political and national security issues, issues of border control or security services); nor what would be the consequences for public order and other police tasks.

There are many interesting and innovative initiatives but the ”situation picture” is very fragmented; some police departments and experts are enthusiastic but there are no national level steering, resources, outlines, policy

Hybrid operations' possible consequences are local

Hybrid operations like influencing, interference, et c are not crimes as such but their possible consequences need attention and strategic (as well as tactical and operational) preparedness

Common situation picture and awareness with other authorities (systematic organised situation picture system or network does not exist, not national nor local)

Hybrid operations' targets are peoples minds, ways of thinking, trust and societies' coherence and order -> chaos, disorder, suspiciousness, hate, polarization…

Concrete: critical infrastructure attacks (electricity, banks, transportation) -> public order, violence, domestic violence, crimes …

ILP and Predictive policing are good platforms for preparedness (using AI for countering hybrid operations' consequences): more innovation management and risk management

New Public Order?

Covid19-case analysis: new kinds of police tasks (control of curfew, movement, obedience to restrictions et c)

Demonstrations and public protests of a new nature: refusal and uncivil disobedience rather that resistance and threat of violence

-> threat also to policemens' occupational health in situations

Politicization of public order, "national securitization" and polarization -> new and even more challenging threat landscape

Drugs, alcohol, violence and other conventional crimes and public order tasks have not vanished, on the contrary!

Ice-Hockey world championship 2022 in Tampere -case

SURE (EU Urban innovative actions –funded project) in Tampere -> developing innovative ways to use AI for crowd control, movement of masses of people

Cameras, lightning, IoT-platforms, traffic … all are built and based on Nokia company's AI applications and structures

Authorities together, organisers and the police had a common situation picture during the championships

No biometric data was collected, the system just alarmed of exceptional behaviour and movement of people

The police can use the data for plans for the 2023 Ice-Hockey world championship in Tampere! (allocation of resources, crime prevention, public order policing)

Global, European, national or local

AI and hybrid threats are not national nor local issues

But: State sovereignty? / EU borders (Finland has over 1000 km EU's eastern border)

The police in Finland should be better prepared: follow the EU strategies and decisions on using AI and on countering hybrid threats, develop national applications, solutions and skills accordingly

- **Cooperation is the key in strategic preparedness (too)**
- **High level strategies and decisions should be made in cooperation with advanced technology experts (and social scientists)**

Superintelligence (Nick Bostrom 2014): “should be developed only for the benefit of all of humanity and in the service of widely shared ethical ideals”