Special Conference Edition Nr. 6

EUROPEAN LAW ENFORCEMENT RESEARCH BULLETIN

Preparing Law enforcement for the Digital Age

Conference in cooperation with Mykolas Romeris University,
8-10 June 2022, Vilnius, Lithuania

Editor:
Detlef Nogala

Co-Editors:
Annika Talmar
Aurelija Pūraitė
Bence Mészáros
Markianos Kokkinos
Roberto Narciso Andrade Fernandes
Salla Huikuri

EUROPEAN LAW ENFORCEMENT RESEARCH BULLETIN

Special Conference Edition Nr. 6

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 Agency for Law Enforcement Training (CEPOL) (Executive Director: Montserrat Marín López)

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

Printed by Bietlot in Belgium

Luxembourg: Publications Office of the European Union, 2023

Print	ISSN 2599-5863	QR-AG-22-001-EN-C
PDF	ISSN 2599-5863	QR-AG-22-001-EN-N

Publications Office of the European Union

SPECIAL CONFERENCE
EDITION Nr. 6

Preparing Law Enforcement for the Digital Age

Conference in cooperation with Mykolas Romeris University,
8-10 June 2022, Vilnius, Lithuania

Editor:
Detlef Nogala

Co-Editors:
Annika Talmar
Aurelija Pūraitė
Bence Mészáros
Markianos Kokkinos
Roberto Narciso Andrade Fernandes
Salla Huikuri

Content

Countering Crimes of the Digital

Borders, Identity & Interoperability

Towards AI-backed Digital Investigation

Authors

Editorial

Preparing Law Enforcement for the Digital Age – editor's reflection

Detlef Nogala
CEPOL

The work of the police and other law enforcement agencies is rarely viewed through the lens of ages, where an age is understood to be a distinct period in history characterised by particular circumstances or events. There are various ways of dividing human history into 'ages', and one of the more familiar is to refer to the characteristic material used to make tools or weapons at the time, such as the Stone, Bronze and Iron Ages. Fast forward to modern history, and the defining forces of production come to mind, such as the 'steam age', the 'oil age' or the 'nuclear age'. In this sense, the 21st century has certainly seen the full arrival of what is called '*the digital age*'[1].

The rapid spread of electronic computers and globalised information networks over the last seventy years are certainly main ingredients of this particular period, which in turn has had a significant impact on the way policing and law enforcement is conducted, when we look at communications, access to numerous databases and digital devices such as video cameras, fingerprint or automatic number plate readers, body-worn cameras, drones, gunshot detection systems (see Nogala 1995, Egbert & Leese 2020).

The distinct characteristics of the digital age affect law enforcement organisations no less than any other functional system in society, as it defines, shapes, enhances and constraints their operations in their environment to a large extent.

About the digital in the Digital Age

In order to approach the digital age conceptually, it is expedient to consider not only its effects, but above all with its basic prerequisites: what is the essential quality of 'the digital' – is it a tool, a weapon, a force of production?

The first thing to note is the essential distinction between the terms ***digitisation*** and ***digitalisation,*** which are sometimes used interchangeably but denote separate processes.

digitisation	digitalisation
Process of transforming information from a physical format to a digital version (sound, picture, texts, movement)	Using digital data to change or improve processes of perception, communication, working and interaction.

According to Brennen & Kreiss (2014) ***digitisation*** can be defined "…as the material process of converting

1 The curious thing about the descriptive periodisation into ages is that there are no really strictly consecutive time periods, but that they merge into each other with short or long transition periods. If one wanted to describe the development of human civilisation over large periods of time by its dominant communication structure, the periodisation by Albert D'Haenens (1983) in 'orality, scribality, electronality' is perhaps the most comprehensive.

individual analogue streams of information into digital bits." In other words, we have to think of a mere act of technical transformation to achieve a very similar effect. An illustrative example is recording music as acoustical signal on vinyl (analogue) or Compact Disc (digital).

In contrast, ***digitalisation*** "… has come to refer to the structuring of many and diverse domains of social life around digital communication and media infrastructures" (ibid.) and is indispensably anchored in the rise and development of networked computer technology in relevant core areas of society such as production, education or entertainment.

Both terms have been widely used in conjunction with the progressive computerisation of all areas of society in advanced societies since the last third of the twentieth century, and "digitalisation" has become a winged word in the political and public debate of our time.

However, since digitisation is a necessary precursor and therefore a necessary condition for the more consequential progression of digitalisation in different areas of society, it is worth taking a closer look at digitisation and its development, which goes back a long way in history and is surprisingly closely linked to the physicality of Homo sapiens.

Fingering the digital

First, there is Benjamin Peters (2016), who is not quite happy with the "…conventional sense — in which digital is synonymous with discrete electronic computing techniques" and leads us in his enlightening essay back to the Latin origin of the term digit – which literally means 'index finger'. His point is to emphasise the crucial role of the index finger as part of the human body in the evolution of the digital realm:

"Ever since we evolved extensor digitorum muscles, ours has literally been what media theorist (…) calls a 'digital condition': digital media do what fingers do (p. 94). (…) The work of digital media can be said to rest at our fingertips. The work of digital computing is similar to counting on our fingers: we think counting is abstract and without obvious real-world unit, and yet counting takes place on the very handy extensions of ourselves — digits, media, and their combination — that permit our bodies to interact with and to manipulate a material world. The human species has always already been born digital: building tools that count, index, and manipulate the world is almost unique to the anthropoid species — those higher primates with digital tools built right into their hands" (Peters 2016, p. 104).

This unusual approach has something to it in that children develop their first counting skills using their own fingers. Counting together with the help of the fingers is one thing, but in an anthropological sense, pointing and indicating with one's index finger seems to be more important and momentous for the human race. Every index begins with pointing, indicating and counting – and computing is just another word for a lot of complex counting. With this in mind, Peters is able to reveal the almost ironic connection between our primitive-looking physical tool, the index finger, and our hypermodern number-crunching machines:

"All these media, among many others, are digital in the simple sense that humans interface with them digitally, or with our fingers via manual manipulation and push buttons. Fingers and digital media alike flip, handle, leave prints, press, scan, sign, type. The touchscreens we pet and caress today continue the age-old work of counting, pointing out, and manipulating the literate lines animating every modern media age, including our own. Digital media, such as these, point and refer to real-world objects outside of themselves, and this transducing from the symbolic to the real limits both the computing and the indexing power of digital media" (Peters 2016, p. 98).

Without wanting to go deeper into a discussion of semiotics here[2], Peter's reflections are instructive in order to underline the difference in principle between the virtual and the real on the one hand, but also to understand the anthropological link between analogue corporeality and digital representation on the other.

To be or not to be – the value of zero

Who would have thought that the line "to be or not to be", famously uttered first around 1600 by the title character Hamlet in Shakespeare's play, held a hidden key to understanding the rise of the contemporary dig-

2 Fundamental to Peters' explanations is obviously the sign theory of Charles Sander Peirce, pragmatist and one of the founders of semiotics, who distinguished between three basic types of signs: „ (…) the icon, which like a portrait resembles the thing it points to; the symbol, which, like the word couch, means a place to sit only because convention has taught us to recognize the arbitrary name as meaningful (or as Shakespeare put it, "a rose by any other name would smell as sweet"); and the index, which has a natural connection to the thing it points to but it not that thing itself, such as how a symptom points to a disease while not being the disease, or an anthill points to ants without resembling ants" (Peters 2016, p. 98).

ital age? Not to be equals nothing, and giving nothing a number turned out to be a big challenge for early European thinkers (see Kaplan 2000; Seife 2000).

The first traces of the idea of 0 go back thousands of years to Mesopotamia and ancient Egypt, and the Mayans independently invented it around the time of Christ. The Mayans independently invented it. The number zero in its modern form was later developed in India in the middle of the fifth century, spread to Cambodia at the end of the seventh century, to China and further on to the Islamic countries at the end of the eighth century. Surprisingly, the great Greek philosophers and mathematicians, contrary to their other ingenuity, did not care much for the zero, and a certain rejection probably continued into the early Christian phase in the West (Joseph 2008).

It took a long time, until the early 13th century, for the number 0 to gain a foothold in Europe, thanks to Leonardo Fibonacci, who, as the young son of a merchant from Pisa, had travelled to the shores of North Africa and the Middle East and had been introduced to Indian-Arabic mathematics by local Muslim masters. Back in Europe, he wrote his Liber abaci (1202; 'Book of the Abacus'), which became the first work to introduce Indian and Arabic numerals to Europe – the number zero finally had come to stay.

It took more than another four centuries before zero became firmly established in Europe and some great minds of the Enlightenment were able to come up with new, ground-breaking mathematical ideas. Inspired by the time-honoured Chinese I Ching system, scholars in Europe in the 17th century dabbled in new, more efficient number systems. Regardless of who is ultimately to be considered the true intellectual originator, the publication of the article "Explication de l'Arithmétique Binaire," by the German philosopher and mathematician Wolfgang Friedrich Leibniz in 1703 can be considered the first successful roll-out of the modern-day binary number system[3].

Leibniz's system made it possible to represent any integer, both positive and negative, simply by using the digits 0 and 1. Any number in the decimal system could be converted into a corresponding binary number by breaking it down into powers of two, which he argued would make calculations faster and more efficient.

Today we are well aware that computers and other electronic devices use the binary number system because their electronics can only distinguish between two states: "off" or "on", which are represented by the digits "0" and "1".

Digitisation – Computerisation – Digitalisation

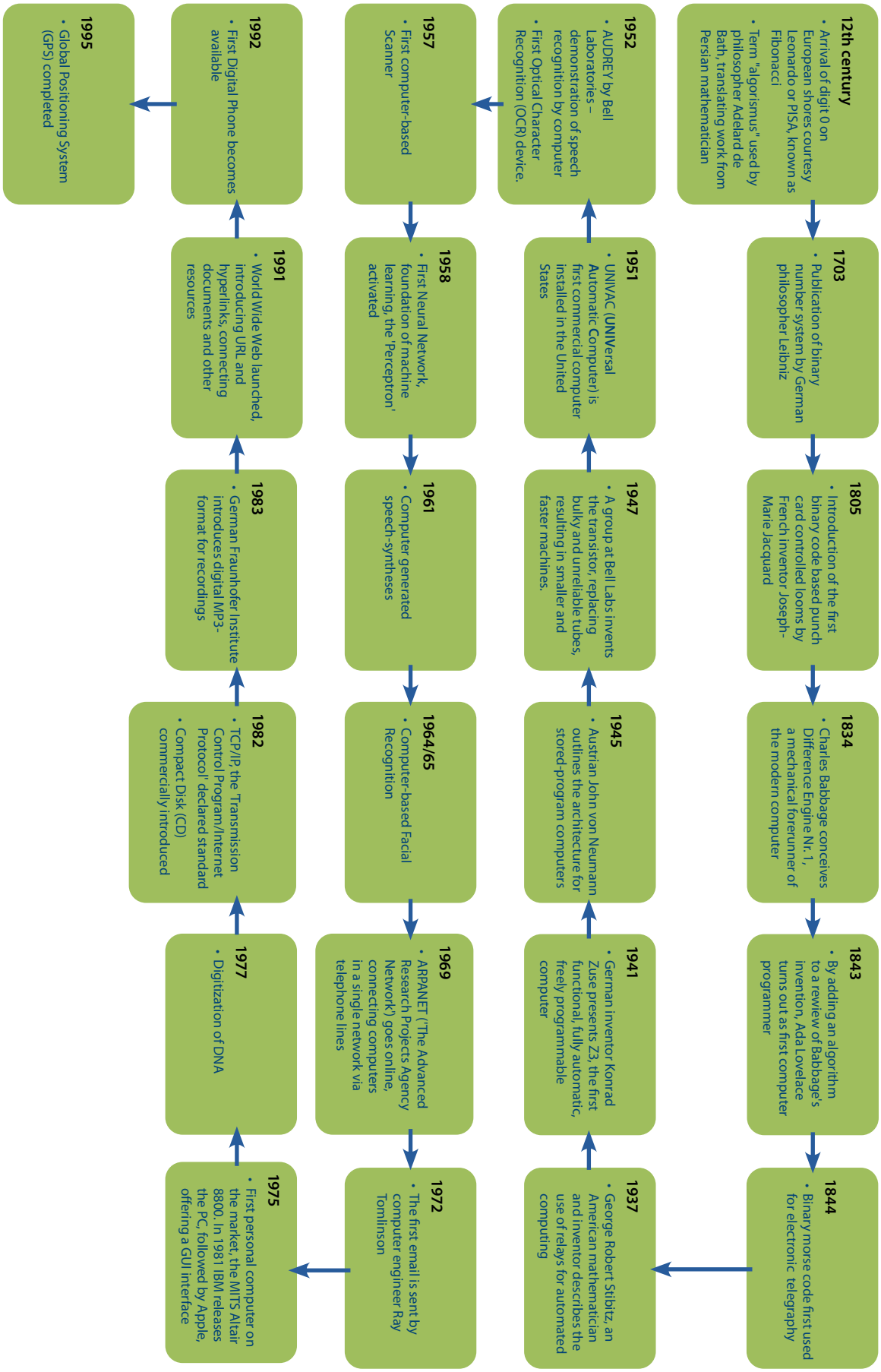
With reference to the timeline of the most important stages of ***digitisation*** *(Figure 1),* we should also realise how long it took – at least eight centuries from a European viewpoint – to set up the technical digital infrastructure to which we are accustomed today and on which the process of digitalisation of the global society is based. It took a long line-up of mathematicians, philosophers, inventors, research teams, entrepreneurial innovators and coders to prepare and realise the digital age.

It is important to remember that the digital age is at once a *computer, information and network age* in a globalised context. Only the combination of technological discoveries and interventions with the hyperlinking of new production and business models on a global scale has led to the distinct realities of the present. The computers we know today (based on digital technologies) are an intermediate product of a gradual sequence of technical inventions and improvements – essentially all digitisations. At the same time, as a complex and networked machine tool capable of processing previously unimaginable amounts of data, they have provided the technical basis for profound changes in social practices and customs since they became massively available.

Initiated, as shown, by the long historical run-up to digitalisation, the actual period of digitalisation in the dawn of computerisation of production kicked-off in the 1970-80s, and then immensely changed the reality of life in particular in terms of commerce and information exchange in the advanced industrial societies from around the turn of the millennium onwards. Scholars such as Alvin Toffler (1970) and Manuel Castells (1996) have analysed and commented early on the impact that digital technology will have on the social fabric.

3 As historical research has shown in many cases, it is rarely the lone but towering geniuses who suddenly come up with fundamental innovations. Often it is much more the case that an outstanding idea owes its existence to a preceding professional and scientific exchange with other researchers and intellectual minds - see Robert Merton's (1965/1993) treatment of Isaac Newton's famous remark about standing „on the shoulder of giants".
In the case of the development of the binary number system we know today, Englishman Thomas Harriot and Spaniard Juan Caramuel de Lobkowitz appear no less worthy of due credit (Ares et al. 2018).

Figure 1: Timeline of the most important stages of *digitisation*



If the use, creation, distribution, manipulation and integration of information can be defined as the typical signifier of an information society, then a digital society would be one in which the appropriation and integration of advanced technologies into social and cultural processes are characteristic.

While the internet would be unthinkable without computerisation and global network technology, as well as the digitalisations that underlie them, a look at the list of digital services that permeate our lives shows how far the digitalisation of social contexts has already progressed.

Table 1: Timeline of major digitalised services and products

Year of launch	Network Services or Social Media[4]
1994	**Amazon**
1995	**eBay**
1997	Netflix, AOL Instant Messenger
1998	**Google**
2000	Unrestricted commercial use of **GPS**
2003	**Skype**, LinkedIn, MySpace
2004	**Facebook**, Flickr
2005	**Youtube**
2006	**Twitter**
2007	**iPhone**
2008	AirBnB
2010	Instagram
2012	**Zoom**, Tinder
2013	Slack
2017	TikTok
2022	**ChatGPT**

4 Services with the highest social impact in bold.

By 2022, it is estimated that 90% of all European households will have access to the internet, mostly via a broadband connection. The continent's smartphone penetration rate among its 485 million inhabitants is around 78%, with a high of 97% in countries such as Sweden and the Netherlands. This means that the vast majority of the population has easy and instant access to a flood of information – welcome in the digitalised society![5]

The nasty and troublesome side of digitalisation

There is no doubt that many routines of life have changed profoundly in the digital age, taking place in a new informational ecosystem with many benefits for the individual and society. For those who can afford access, digitalisation means a world that has become more connected and globalised, where individuals can find articles, videos and tutorials on almost about anything they want to learn and stay informed about the world around them. Visual communication is possible across continents in real-time and one can virtually visit remote and exotic places. However, the digital age also brings its own and specific problems: just as with the invention of the railway the railway accident was co-invented, so new types of misery, harm, and life disasters have entered the world: digital crimes[6]. 'Computer virus', 'cyberbullying', 'DDoS attacks', 'hackers', 'malware', 'online fraud', 'ransomware', 'phishing', 'spam', 'spoofing', are the most familiar terms of digital unpleasantness that have either entered the dictionary of criminology or taken on a new meaning (see Marion & Twede 2020, including an instructive global chronology). As is well known, there is not such a thing as a

5 According to Katzenbach & Bächle (2019), algorithmic governance, platformisation, datafication, filter bubble and (diminishing) privacy can be understood as the defining concepts of the digital society.

6 Digital crime and cybercrime are related but distinct concepts. Digital crime refers to any crime that is committed using digital technology, such as using a computer to commit fraud or theft. Cybercrime, on the other hand, refers specifically to criminal activities that target a computer or network for damage or infiltration.

'free lunch' in life – in the digital age, novel threats and crime options in the form of digital and cybercrimes are the price to pay for its conveniences and benefits. However, society and its institutions are not helpless in the face of this negative side of digitalisation – the first responses were not long in coming.

Policing and Law Enforcement in the Digital Age

Tools and procedures have been needed to do the job since policing became organised and a profession. Handcuffs, batons, registers, telegraphs and telephones may have been sufficient as basic equipment in the 19th century (SEASKATE INC. 1998; Deflem & Chicoine 2014). However, scientific discoveries in combination with industrial-scale production soon opened up new possibilities for effectiveness. Berlin saw the first installed police radio system in 1920, but the first computer systems in police work for the purpose of data processing appeared only in the second half of the 20th century – USA (1965), Germany (1967) – and became effectively operational on a national scale only from the seventies onwards in the most developed countries (see Bergien 2017). At that time, the digital age with its information processing and analytical capabilities was already peeking around the corner, but the real potential of the computer revolution (and the equally rapid development of sensor technology) for policing unfolded in the decades that followed:

Table 2: Major digital innovation in policing and law enforcement

- 1974: First Automated Fingerprint Identification System (AFIS) created by the Federal Bureau of Investigation (FBI).
- 1979: German Federal Criminal Police Office uses computer dragnet.
- 1981: The first licence plate recognition system, invented a few years earlier, goes into operation in the UK.
- 1994: New York Police Department introduces COMPSTAT, a real-time computerised crime mapping system.
- 1995: England and Wales create the first national forensic DNA database
- 1999: Authorities in Minnesota (US) incorporate facial recognition into a booking system that allows police, judges and court officials to track criminals across the state.
- 2003: US police forces begin using GPS tracking to investigate crimes
- 2005: Devon and Cornwall Police (UK) trial body-worn cameras
- 2008: Los Angeles Police Department adopts predictive analytics software and is credited with inventing 'predictive policing'
- 2014: US Immigration and Customs Enforcement contracts Palantir's Gotham platform, an AI-enabled system that can ingest and sift through millions of digital records across multiple jurisdictions, discovering links and sharing data.

What we can see from this brief chronology of innovation is that individual police forces in the Western world have not been slow to embrace the potential of digital tools for law enforcement purposes. The need to adapt to the criminal underbelly of the digital age has set in motion a longstanding and ongoing process of innovation in the police and other law enforcement agencies, which in turn has a strong impact on their operational approach, actual effectiveness and overall impact within a conflictual societal context[7]. This is undoubtedly a very dynamic process, which is constantly creating new challenges and problems for trying to deal with criminal threats – whether they are traditional or digital in nature, and thus raises the question: how do you prepare members of the police and other law enforcement agencies for the rapidly changing technological situation?

Preparing Law Enforcement for the Digital Age: The Conference

Not least, the recent global pandemic crisis has highlighted the importance of digital tools, processes and instruments to our economies and daily lives, and how this has and will change and shape the challenges and opportunities for law enforcement in the coming decades.

For the CEPOL conference in Vilnius, which was organised once again in cooperation with Mykolas Romeris University[8], contributions were called for that would

7 Innovation was the dedicated theme of the CEPOL Research and Science Conference 2017 in Budapest - see Nogala & Schröder (2019) and various articles in Special Conference Edition No. 4.

8 In May 2021, the planned CEPOL Research and Science Conference could only be held in an online version and inevitably had the impact of the Corona crisis as its current topic (see Nogala et al. 2022). The originally planned conference was then to take place in December of the same year, but had to be postponed again, this time to June 2022, because of too high virus incidences.

address issues of education and training, inter-agency and cross-border cooperation, the emergence of artificial intelligence and public expectations with reference to the digital age. The Programme Committee finally accepted 75 of the diverse paper proposals submitted, which were presented over two and a half days in plenary and parallel sessions to a mixed audience of academic experts and law enforcement practitioners from across Europe and beyond. Most of the plenary sessions were broadcast live and can be viewed on the CEPOL website. All speakers were encouraged to submit a full paper of their presentation and this 6th Special Conference Edition of the European Law Enforcement Research Bulletin presents all the papers received by the editors in time.

The papers in this Edition

Plenary Presentations

The spirit and institutional context of the event is aptly introduced by the ***Opening Speech*** of CEPOL's Executive Director, *Ms Montserrat Marín López*, and the video-linked ***Opening Address*** of EU Commissioner for Home Affairs, *Ms. Ylva Johansson*. After an interruption of five years caused by various adverse circumstances, this was the first time that the young tradition of the CEPOL Research and Science Conferences, which goes back to 2003, could be continued again in the usual on-site format. Both speakers emphasised the role of the CEPOL for providing law enforcement training in the European context as well as the importance of a constructive dialogue between law enforcement practitioners, trainers and researching scientists.

Under the heading ***"Policing in a Digital Age: Balance between community-based strategies and technological intelligence"***, *Luis Elias* opens the round of papers in this volume and, with his theoretically guided reflections, immediately outlines the challenge of finding a pragmatic synthesis between technically effective police strategies and necessary citizen orientation. From a police practitioner's point of view, he is concerned about the security trends in today's societies, which invest more in hard policing and technological policing and less in community-based strategies. Instead, looking to scientific research and innovation, he advocates a comprehensive approach between HUMINT and TECHINT to better understand the peculiarities of communities and to improve the relationship between the police and vulnerable communities, as well as to prevent threats and risks to our collective security.

Biometric identification and matching, automated surveillance capabilities, short-term situation prediction, AI-assisted analysis of large amounts of data, and interoperability of large databases and platforms for data exchange and investigation are the applications that *Matthias Leese* looks at in his paper "***Digital Data and Algorithms in Law Enforcement***". The author argues that these tools can help increase the effectiveness and efficiency of law enforcement operations at the strategic, tactical and operational levels, but that they also raise a number of concerns that need to be recognised and addressed in order to realise their potential and avoid unintended side-effects and societal frictions, such as data limitations, automation bias or social implications.

The Project "***AP4AI: Accountability Principles for Artificial Intelligence in the Internal Security Domain***" seems to be a direct response to some of the concerns raised in the debate: In a joint effort the authors from Sheffield Hallam University (*Babak Akhgar & Petra Saskia Bayerl*) and Europol (*Grégory Mounier, Ruth Linden & Ben Waites*) address the challenge of how to harness the power of artificial intelligence (AI) and machine learning to improve the way investigators, prosecutors, judges or border guards carry out their mission to protect citizens and deliver justice, while ensuring and demonstrating true accountability to society for the use of AI. The approach adopted by the project is the expert-driven development of twelve core accountability principles (legality, universality, pluralism, etc.), which, once applied in the context of so-called *AI Accountability Agreements,* can support law enforcement practitioners in the deployment of any new AI application in the security domain, taking into account the position of citizens. However, such a preventive approach, in order to avoid possible damage to the trust and credibility of the authorities in the face of a sceptical public, requires a functioning legal policy setting, for which democratic societies may still have the best chances.

Maria Haberfeld's contribution provides a revealing contrast to the organisational-strategic and legal-ethical aspects presented so far, confronting us with the practical realities of "***North American policing in the Digital Age***". The author believes that society might be already in the post-digital age, in which the digital

has become an everyday, almost unrecognisable fact of life, while many police departments begin to realise, that the "game started over a decade ago". Using concrete empirical examples, the author illustrates how attitudes and preparation for the dangers and crime of the digital age vary according to the size and resources of police agencies in the US – there is awareness, but not always the implementation. Although policing in the US is currently facing a variety of serious non-digital problems (197 mass shootings in 2022, police use of deadly force in a racial context), the article concludes with some concrete recommendations for police practitioners and agencies regarding digital challenges.

Learning, Training, Knowledge

When we talk about readiness and preparation, we need to think about learning, training and, ultimately, education, as these categories determine how much or how far the potential of a given set of opportunities can be exploited. Of course, this also applies to the possibility of digitalisation. A distinction must be made here between the demands on the organisation and the demands on the individual, in our case the police and law enforcement officers. Learning is a process that (so far) takes place primarily at the individual level: Problems in combination with information lead to insights which, supported and reinforced by practice and repetition, mature into (basic) skills. Most people have figured out more or less over time by themselves, how to operate a computer, a smartphone or how to 'google'. It is a little different with training: an organisation or institution sets and prescribes a certain level of skill to be achieved. So how can the various police organisations and law enforcement agencies, which are themselves subject to an often gradual process of digitalisation, prepare their staff for the demands of practice in the digital age? Six articles in this issue are dealing specifically with this aspect.

From an organisational-institutional perspective, Training Needs Assessment is the crucial keyword. *Iulian Coman & Noemi Alexa*, in their paper ***'EU Law Enforcement Training Needs on Digital Skills and the Use of New Technologies***', detail how CEPOL, the European Agency for Law Enforcement Training, seeks to identify at the European level the specific training needs of the respective national law enforcement agencies in the area of digital skills of their employees and how training programmes in cooperation with other institutions would need to be designed and implemented. The first-cycle report of the EU Strategic Training Needs Assessment (EU-STNA) revealed that "digital skills and use of new technologies" were considered the highest challenge in terms of capability gaps. In the follow-up Operational Training Needs Assessment, digital investigation, use of new technologies and digital forensics were the top three on the subsequent training agenda.

Training needs assessment is also a concern in the paper by *Michael Whelan & Ray Genoe* entitled "***Law Enforcement Agency Capacity Building as a Driver for the Adoption of European Research***", here in the context of the EU-funded INSPECTr-project, a venture aimed at the development of a shared intelligent platform for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime, including big data analytics, cognitive machine learning and blockchain approaches. It is a good example, how training for staff can be planned ahead for a technical platform, which is still under development.

Planning ahead is certainly a good administrative idea, but what happens when "the practice" is reluctant or hesitant to adapt teaching and training methods to the demands of the digital age – and its younger cohorts of cadets and officers – as quickly as possible? This is the subject of *Cedric Carre's* article on "***The Challenges of E-Learning in the French Police Nationale***". Highlighting the role of interactivity as a critical element of e-learning, the author describes how the COVID-pandemic proved to be a game changer in the field of e-learning for the French National Police and provides a useful list of challenges in the process for both trainers and trainees.

But even the type of digital device can make a difference to the learning process. This, at least, is the conclusion that can be drawn from the paper "***The Influence of Digital Devices on Learning Interest, Engagement and Academic Performance in Basic Police Training***" authored by *Micha Fuchs & Kristina Ott*. They report on how the Bavarian police are taking an integrated approach to the digitalisation of their force, from training to operational practice, by equipping police trainees with convertibles and smartphones from the outset. However, a promising digitalisation already in the training phase required more than just the distribution of devices; it involved an appropriately set up learning platform, but also an adapted didactic concept as well as the further qualification of the teachers. In an internal study, they wanted to figure out, how the

digital gadgets influence the actual learning of trainees: no big surprise that the new generation of police officers like digital devices and material. However, the authors have a few practical advices to share.

Over the course of their careers, law enforcement officers, such as investigators, gain experience and knowledge, an asset that any organisation wants to retain. 'Expert-systems' have been on the agenda of IT-engineers for a long time. Thinking ahead, *Héctor López Carral & Paul FMJ Verschure* present their concept of "***An Assistive System for Transferring Domain Knowledge to Novice Officers***" in the expectation that such a system will help to harvest the knowledge of experienced investigators more effectively.

A more traditional approach is taken by *Nicoleta Apolozan & Andreea Jantea*, who sought to identify the main risks and vulnerabilities faced by young students aged 10-18 in the digital universe by interviewing police officers who investigate cybercrime in this age group. In their paper "***Children on the Internet – Law Enforcement Challenges***", they report on the variety of offences encountered and the specific risks and vulnerabilities of underage victims identified by investigators. The results of their study were used as part of a wider project to train crime prevention officers in Romania.

Countering Crimes of the Digital

Three contributions take a closer look at specific forms of crime whose manifestation owes much to the increasingly complex intertwining of capital and commodity flows across globally stretched networks.

Since the collapse of the Soviet empire and the global economy's decision to go fully capitalist, the citizens of the world have been hit by a series of financial crises and major scandals: Banking crisis (2008), Silicon Six tax avoidance (2010-2019), Panama Papers (2016), Paradise Papers (2017), Wirecard (2020), FTX (2022). Financial crime is usually not far from organised crime and the global interconnectedness of capital often has far-reaching negative impacts on broad sections of the population in the age of digital trade flows.

Not just for this reason, the contribution by *Antonio Bosisio & Maria Jofre* "***Investigating High-Risk Firms: A Machine Learning-based Approach to Cross-Border Ownership Data"*** deserves particular attention. Based on the observation that legitimate companies are often instrumentalised for money laundering and corruption, the EU-funded DATACROS project has been set up to try to shed light on opaque ownership relations of branched business conglomerates with the help of search algorithms. Complexity, secrecy and occasional unavailability of ownership data appear to be good indicators of the likelihood that companies are involved in illicit activities. The prototype aims in detecting anomalies in firm's ownership structure that can flag high risk of illegality. Apart from revealing some interesting risk rankings for the EU states, the article also reports on the first successful test runs of the new digital tool for financial investigations.

In a related area, though not at the same level of technical sophistication and maturity, the paper by *Rufian Fernandes & Constante Orrios* addresses the issue of "***Open Source Intelligence and Cultural Property Crimes***" and points to freely available digital tools which could be useful for investigations of illegal trafficking of antiquities on Internet platforms like Facebook.

While most people have always had a solid imagination of smuggling with antiquities or cultural goods, *Dimitrios Kafteranis' & Umut Turksen's* paper ***„Art of Money Laundering with Non-Fungible Tokens: A myth or reality?"*** highlights a phenomenon that only made headlines during the time of the pandemic and might not yet be familiar to everyone as subject to criminal suspicion. The article explains what NTFs are and how they are used for money laundering, hinting to gaps in law and training needs of law enforcement officers.

Borders, Identity & Interoperability

In the age of hyper-fast and seemingly unrestrained global flows of finance and information, it is easy to overlook the fact that borders and thus border controls still play a significant role – this is essentially about the verification of identities, as identity usually controls access to territories, resources and opportunities. On the other hand, national borders and jurisdictions still pose a hurdle to smooth cooperation between law enforcement agencies, even in a Europe that is growing together. Under the rubric of borders, identity and interoperability, the following papers deal with new opportunities and possible departures of digital options. The reliable clarification of an unknown or doubtful identity has been a core element of every police activity from the beginning. As described above, digitalised

fingerprint systems, DNA databases and computer-assisted facial recognition have been milestones in forensic biometrics. This aspect is of particular importance in the control of identities at border crossings.

The paper "***Technology Foresight on Biometrics for the Future of Travel***" by a team of authors from Frontex (*Luigi Raffaele, Darek Saunders, Magda Wojcikowska, Dragos Voicu, Claudiu Chiriac, Javier Quesada*) provides in this regard a clear and illustrative view of the present and future of digital identity verification techniques. They introduce the reader to a plausible taxonomy of familiar and less familiar biometric technologies, distinguishing between biomolecular, morphological and behavioural types, and present, with the help of scenarios, which of the possible digital biometric technologies could probably be the most promising for the future. Showing one's face and a raised index finger (sic!) could then at some point of the digital age open the barrier instead of a pass.

While the Frontex paper takes almost a purely engineering and managerial view and assessment, *Andras L. Pap & Eszter Kovács Szitkay* point out in their contribution "***Race, Ethnicity, Biotechnology and the Law: Potentiality and challenges for law enforcement in the digital age***" the more delicate and politically sensitive aspects of technology-based identity verification and assignment. They rightly insist on the differentiation between the notions of race and ethnicity, as well as the necessary legal-practical distinction between national and ethnic minorities. To this end, the authors draw on the concept of "*datafication*", which is often used in the social sciences in the context of the digitalisation discussion and is defined as the process by which subjects, objects, and practices are transformed into digital data (Southerton 2020). This is exactly what biometric identification technologies do.

In contrast, the article by *Amr el Rahwan* on "***Artificial Intelligence and Interoperability for Solving Challenges of OSINT and Cross-Border Investigations***" deals with very practical problems of identity clarification in cases of investigating cross-border serious crime and terrorism and how to overcome them with the help of new digital procedures. In particular, the difficulty of multiple and fraudulent identities in the context of a lack of intercultural and linguistic competence is, in his view, often a massive hurdle to successful investigations, as he illustrates in detail by the example of variations of Arabic names written in Arabic script.

With a view to the Council Regulations which provide for interoperability of information systems within the EU in the field of police and judicial cooperation, asylum, and migration, the author addresses the technical and organisational barriers to investigative cross-border collaboration and outlines how OSINT tools and AI applications could contribute to a better solution, a "person-centric approach".

Interoperability is also a key concern for *Fabrizio Turchi & Gerardo Giardiello* who let the reader in on their efforts of ***„Developing a Judicial Cross-Check System for Case Searching and Correlation Using a Standard for the Evidence"***. For them, the harmonisation of the presentation and exchange of information relevant to cyber investigations is the most pressing need. As the exchange of electronic evidence for a wide range of forensic information is increasing and will continue to do so, the need for a standard is essential. For this purpose, the open-source Unified Cyber Ontology (UCO) and the Cyber-investigation Analysis Standard (CASE) are presented in technical detail.

Towards AI-backed digital investigation

The specific role of advanced digital technologies in different areas of police investigative work is addressed in a number of further contributions.

It is no great surprise that in a time when digital mobile devices (phones, tablets, GPS devices, PDAs) are deeply embedded in people's everyday lives and the smart phone has become a kind of indispensable mental prosthesis for many, they now also play a central role in police investigations. "***Mobile Forensics and Digital Solutions: Current status, challenges and future directions***" is the title of the contribution by *Nikolaos Papadoudis, Alexandros Vasilaras, Ilias Panagiotopoulos & Panagiotis Rizomiliotis*, which introduces the topic in a concise overview and does not shy away from addressing practical complications such as the growing volumes of data and the rapid evolution of device and data specifications. Acting as endpoints of computerised communication, these digital mobile devices hold a range of potentially revealing data about the activities and behaviour of their users, such as call logs, text messages, contacts, image and video files, geospatial data, notes, communication records, network activity and application-related data. However, all this data requires comprehensible evaluation by forensic specialists, who in turn are subject to time pressure due to procedural requirements and investi-

gative processes. The article discusses machine-learning and AI-applications as a possible solution for the investigator's issues of volume and time pressure.

Rui Sousa-Silva's paper on "***Forensic Linguistics: The potential of language for law enforcement in the digital age***" is also located in a similar investigative territory. The paper is primarily concerned with the problem of anonymity in cyberattacks which take place in the form of written communication (email, messages), especially in the wake of mass-based social media (Facebook, Twitter, etc.). Two cases are presented to demonstrate the potential of the applied study of human language for the purpose of forensic identification of cyber-criminals even in transnational settings.

"On the Internet, nobody knows you're a dog" used to be a famous catchphrase in its early phase, capturing the sense of anonymity and possibility that came with this new way of communicating and interacting with others. Lies, spin and disinformation are certainly not inventions of the digital age, but in 2016 'post-truth' was announced as "Oxford Dictionaries' international word of the year", and the rise of social media during the Corona-pandemic (Su 2022) has certainly raised the stakes when it comes to the cyber-public discussion of (in)validity of facts. Post-factual misinformation has become a political issue and a concern for law enforcement as well. "***The Identification of Invalid Information about the COVID-19 Coronavirus Pandemic on a Social Networking Platform***" is the aptly titled paper by *Georgios Lygeros* who describes his technical approach of using Natural Language Processing algorithms to tackle the problem through machine learning. But automatically labelling tweets as 'true', 'false' or 'irrelevant' seems far from being trivial, not just for a digital machine.

Three contributions from the Netherlands with different time perspectives deal with the question of what possibilities computer-assisted artificial intelligence opens up for police investigative work. The problem of an average of 125 unsolved homicides per year and a backlog of 1700 cases is tackled by *Tatjana Kuznecova, Dimitar Rangelov & Jaap Knotter* under the heading "***Cold Case – Solved & Unsolved: Use of digital tools and data science techniques to facilitate cold case investigation***". They report on their innovative research approach using automated collection and analysis of open newspaper sources on unsolved murder cases and the first partial successes they have achieved in classifying such articles through algorithms. However, the capabilities of AI appear in their case still well below those of humans, which means that the goal of accelerating the time- and resource-consuming processing of cold cases seems to be still in its infancy. Also taking a look into the archives of unstructured texts, but more interested in structural elements of contemporary criminal conduct, is the contribution *Ana Isabel Barros, Koen van der Zwet, Joris Westerveld & Wendy Schreurs*, which aims to explore the "***AI Potential to Uncover Criminal Modus Operandi Features***". Their idea is to tap into the large body of documented Dutch court judgements relating to specific crimes using computerised text-mining techniques to create a base for a variety of experimental steps applying AI-techniques, hoping to reveal specific elements of the modus operandi for certain offenses. Some examples and results of their proposed are presented. Again, the hope of faster, less biased and less erroneous results through machine intelligence seems to take some time to materialise.

The view of *Nienke de Groes, Willem-Jan van den Heuvel* and *Pieter Tops* on "***The Potential of AI and Data Science in Reducing the Vulnerability of Ports to Undermining Crime***" is also directed more towards the (near) future than already describing the reality of security in large seaports. In this context, the authors hope to reduce crime risks primarily by largely eliminating the human factor in logistical processes.

The last contribution in this conference volume is about the benefits of a digital law enforcement technology that was initially the cause of fierce controversy, but has since been integrated into social processes in many places and has become something of a landmark of securisation in the digital age: video surveillance. *Ksenija Butorac & Hrvoje Filipović* review the "***Evidential Validity of Video Surveillance Footage in Criminal Investigation and Court Proceedings***" in reference to their Croatian and European context and related court proceedings. The authors aim to "determine the probative value" of video surveillance in the face of judgements by the European Court of Human Rights and Croatian high courts by looking at areas of application like public areas, workplaces, residential buildings, shopping malls – and most interesting in the context of training and education – faculty lecture halls.

The missing bits

Regrettably, it was not possible to acquire written versions of all the very interesting conference presentations. Nevertheless, in addition to the papers presented here, a number of presentation slides are available on the Vilnius 2022 conference page on the CEPOL website at https://www.cepol.europa.eu/scientific-knowledge-research/2022-cepol-research-science-conference-vilnius. Some late submissions may also appear in the next regular issues of the European Law Enforcement Research Bulletin. In addition, reference can be made to the websites of some EU-funded H2020 projects[9] whose research approaches and (interim) results were presented at the CEPOL conference.

Going all digital?

The choice of conference title may strike some readers as somewhat anachronistic, given that the digital age began many years ago, and may even have passed its zenith, according to others (e.g., Peters 2016). Why are we only now thinking about how police and other law enforcement and prevention agencies should be prepared for the digitalised world, when its expansion is already in full swing? Sure, the digital age has been long coming. At least that is what members of the post-World War II boomer generation can say when they consider the list of digital innovations that have fundamentally changed the way production, distribution and leisure work is done in the first quarter of the 21st century. One answer to this question lies in the reference to the enormous speed of the digital evolution, which goes hand in hand with rapid technological innovation cycles and equally rapid declarations of obsolescence[10]. The resulting need to adapt poses major financial, organisational and human resource challenges for every organisation – police and other law enforcement agencies are no exception. Now, it is the case that courageous reformers within these authorities have repeatedly faced up to the increasingly digitalising environment and introduced new methods and tools into policing. National police institutions in particular have proven to be digital pioneers, e.g., with the establishment and operation of central databases, and the need for cross-border cooperation has also driven the digital modernisation and cross-connection of law enforcement agencies, bearing in mind the many digital projects and tools set up by Interpol and – in the European context – by Europol, eu-LISA, and Frontex. In this context, one should not lose sight of the fact that these systems have their origins in the field of "high policing", to recall a helpful analytical distinction made by Jean Paul Brodeur (1983)[11], and only slowly have trickled down to the everyday, street-level "low policing" field in recent years. Necessary but expensive investments in the digitalisation of technical systems, devices and equipment can usually consume scarce resources, which are then no longer available to a sufficient extent for more local and preventive approaches, such as community-oriented policing, especially with regard to the orientation of the general police security strategy. This dilemma of real limited (financial as well as staffing) possibilities must be taken into account with all enthusiasm for the new digital options – this is also the tenor of Elias' contribution in this volume.

In a similar direction, a scholarly critique refers to the change in police culture and the resulting relationship with citizens that is associated with digitalisation. In field observations in local police stations, Dutch police researcher Jan Terpstra has identified certain phenomena of alienation both between different hierarchical police levels and in contact with citizens, which he attributes to the emergence of an 'abstract police':

"The increasing dependence of police services on digital devices and systems has resulted in important changes in relations, work processes and practices of the police. One of these changes has been the shift from street-level bureaucracy to, first, screen-level bureaucracy and, next, to system-level bureaucracy (…). These developments have

9 CC-Driver (https://www.ccdriver-h2020.com/)
DARLENE (https://www.darleneproject.eu/)
DATACROS (https://www.transcrime.it/datacros/)
e-CODEX (https://www.e-codex.eu/)
FORMOBILE (https://formobile-project.eu/events)
INSPECTr (https://inspectr-project.eu/)
RESPOND-A (https://respond-a-project.eu/)
ROXANNE (https://roxanne-euproject.org/)

10 Didn't video kill the radio star? Isn't the Compact Disc the fax machine of the streaming generation? Who still recalls the sound of the 14.4 k modem, connecting Netscape Navigator to the Internet?

11 Brodeur claimed, the policing task can be divided between 'high policing' and 'low policing.' 'High policing' is associated with the work of the intelligence community and is concerned with gathering intelligence to ensure the stability and security of the state. On the other hand, 'low policing' is the domain of everyday (often uniformed) officers and consists of providing emergency assistance, reacting to calls from the public, controlling traffic, nightlife, and events, and providing crowd control. In the meantime, the incidents of globalised terrorism and the associated general tendency towards intelligence policing have softened this original analytical demarcation (Brodeur 2007; Manning 2012).

had important consequences for relationships with citizens, which are now mediated by a computer screen or replaced by a computer system, reducing the room for direct and personal communication (…). The process of digitalisation has also contributed to a loss in the discretion of individual officers, who have become more dependent on system information. This implies that police work is now more bound to the frames and categories of computer systems and that personal knowledge has become less important" (Terpstra et al. 2022, p. 3-4).

It would be too convenient to dismiss this sceptical view as nostalgia and a sentimental reference to a pre-digital 'happier era' of policing and police organisation. Instead, it should be recognised that, as with most things in life, there is a downside to everything, and: be careful what you wish for. As the digitisation respectively the digitalisation of police tools and systems has brought significant gains in power for prevention, investigation and repression, there has also been a long academic trail of critical or sceptical academic commentary. Although law-abiding citizens generally want their police forces to be accessible, efficient and trustworthy, the digital-driven growth of surveillance power has raised fears of an all-seeing, all-knowing Orwellian police state[12], which is hardly compatible with the European vision of an "Area of Freedom, Security and Justice" and in particular Art. Article 8 of the European Convention on Human Rights, protecting human rights and fundamental freedoms. Gratifyingly, this was a reference point in many of the papers presented at the conference. Particularly at a time when news of questionable police behaviour and dubious surveillance policies is spreading rapidly digitally around the world and directly or indirectly influencing national debates, the legitimate expectations (and hopes) of the public cannot be ignored under the concept of 'democratic policing'. For a start, democratic policing means policing in a democratically governed society, adhering to the principles of the rule of law, being publicly accountable and protecting the human rights of all people, including suspects and victims (for all the details, see Manning 2010).

At the same time, police forces are expected to be efficient, effective and agile – able to adapt and respond to whatever comes their way. Taking these two requirements for modern police forces together, the concept of 'smart policing' may be a logical consequence in line with the digital age, if conceptualised as "the effective use of data and analytics, as well as improved analysis; performance measurement and evaluation research; improving efficiency, encouraging innovation and improving the evidence base for policing by promoting partnerships between police agencies and the research community", paraphrasing Coldren et al. (2013, p 275).

But eventually, what does all this mean for prospective and practising police officers and other law enforcement officials? How should they be prepared, or prepare themselves? There is probably no simple answer to this question because there are several levels and dimensions to distinguish. On the one hand, this is also a generational question, which is different for the outgoing analogue generation than for the proverbial 'digital natives'. Then it makes a difference whether one is thinking about education and training requirements for officers who are or should be active at the local, central or cross-border international level. Finally, the subtle but relevant difference between training and education for police officers cannot be pointed out often enough (see Project Group 2009, p. 157ff). It's pretty obvious that policing in the digital age has moved from being a craft to becoming a 'knowledge-based' job, without the need for street- and communitywise skills having diminished. Almost all of the approaches and systems presented in the lectures of the conference require not only in-depth (technical) operational training, but comprehensive analytical and contextual knowledge, which is supported by so-called 'artificial intelligence', but as long as this does not get beyond the status of a stochastic parrot (Bender et al, 2021), it cannot be replaced or digitally compensated for.

The idea of the "thinking police officer" is not new, if one thinks of August Vollmer, for example, who already at the beginning of the 20th century in California advocated the extensive, even higher academic education of his 'coppers'. And one hundred years later, this attitude is still as relevant as it is 'smart' for the challenges of the 21st century. As has been emphasised in variations over the many years of CEPOL Research and Science Conferences, comprehensive education and training, based on scientific research and democratic values, and open to innovation, is bound to be a solid foundation for 'good policing'. It is hoped that conferences such as Vilnius 2022, which brought together diverse perspectives and expertise from police practice, training and research, as well as this publication, will contribute substantially to this ongoing process.

12 For a supreme sociological analysis see Marx (2016).

Acknowledgements

After a pandemic period in which scientific exchange was suddenly largely confined to digital channels of communication, a conference in a lively real-world format once again vividly demonstrates the qualitative difference between reality and virtuality. Participation literally becomes more tangible, not least because it also involves collective movement and direct encounters at the venue.

Special thanks are due to a number of individuals and organisations for making this opportunity possible. First of all, Mykolas Romeris University, whose rector *Inga Žalėnienė* provided the venue and whose organising team under the guidance of Prof. *Aurelija Pūraitė* ensured a pleasant stay and smooth running.

The manifold support in the preparation and implementation on site by CEPOL staff and colleagues was also decisive for the success of the event.

This is the 6th Special Conference Edition of the European Law Enforcement Bulletin. Thanks are due not only to the authors but also to the members of the Programme Board (*Annika Talmar* (EE), *Aurelija Pūraitė* (LT), *Bence Mészarós* (HU), *Markianos Kokkinos* (MT), *Roberto Fernandes* (PT) and *Salla Huikuri* (FI)) who, as-co-editors received additional reviewing support from members of the Bulletin Editorial Board (*Vesa Huotari* (FI), *Jozef Medelský* (SK), *José Francisco Pavia* (PT), *Ioana Lucia Bordeianu* (RO) and *Ksenija Butorac* (HR)).

References

Bing, Google, Perplexity.AI and Wikipedia were used for fact-checking, in addition to the following references:

- Ares, J. et al. (2018) 'Who Discovered the Binary System and Arithmetic? Did Leibniz Plagiarize Caramuel?', *Science and Engineering Ethics,* 24(1), pp. 173–188. https://doi.org/10.1007/s11948-017-9890-6.
- Bender, E.M. et al. (2021) 'On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?', in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency.* New York, NY, USA: Association for Computing Machinery (FAccT '21), pp. 610–623. https://doi.org/10.1145/3442188.3445922.
- Bergien, R. (2017) '»Big Data« als Vision. Computereinführung und Organisationswandel in BKA und Staatssicherheit (1967–1989)', *Zeithistorische Forschungen/Studies in Contemporary History,* 14, pp. 258–285. https://doi.org/10.14765/ZZF.DOK.4.969.
- Brennen, J.S. & Kreiss, D. (2016) 'Digitalization', in K.B. Jensen et al. (eds) *The International Encyclopedia of Communication Theory and Philosophy.* New York: John Wiley & Sons, https://doi.org/10.1002/9781118766804.wbiect111.
- Brodeur, J.-P. (1983) 'High Policing and Low Policing: Remarks About the Policing of Political Activities', *Social Problems,* 30(5), pp. 507–520. https://doi.org/10.2307/800268.
- Brodeur, J.-P. (2007) 'High and Low Policing in Post-9/11 Times', *Policing,* 1(1), pp. 25–37.
- Castells, M. (1996) *The Rise of the Network Society.* Blackwell.
- Coldren, J.R., Huntoon, A. & Medaris, M. (2013) 'Introducing Smart Policing: Foundations, Principles, and Practice', *Police Quarterly,* 16(3), pp. 275–286, https://doi.org/10.1177/1098611113497042.
- Deflem, M. & Chicoine, S. (2014) 'History of Technology in Policing', in G. Bruinsma and D. Weisburd (eds) *Encyclopedia of Criminology and Criminal Justice.* New York, NY: Springer, pp. 2269–2277.
- D'Haenens, A. (1983) Oralité, *Scribalité, Electronalité. La scribalité occidental depuis le moyen âge.* Louvain-la-Neuve.
- Egbert, S. & Leese, M. (2021) *Criminal Futures: Predictive Policing and Everyday Police Work.* Taylor & Francis.
- Joseph, G. (2008) 'A Brief History of Zero', *Iranian Journal for the History of Science,* 6, pp. 37–48.
- Kaplan, R. (2000) *Nothing That Is: A Natural History of Zero.* Oxford: Oxford University Press.

- Katzenbach, C. & Bächle, T.C. (2019) 'Defining concepts of the digital society', *Internet Policy Review,* 8(4). Available at: https://policyreview.info/concepts/defining-concepts-digital-society
- Manning, P.K. (2010) *Democratic Policing in a Changing World.* New York: Routledge.
- Manning, P.K. (2012) 'Jean-Paul Brodeur on High and Low Policing', *Champ pénal/Penal field [Preprint],* (Vol. IX). Available at: https://doi.org/10.4000/champpenal.8285
- Marion, N. & Twede, J. (2020) *Cybercrime: An Encyclopedia of Digital Crime.* Santa Barbara, California Denver, Colorado: ABC-CLIO.
- Marx, G.T. (2016) *Windows into the Soul: Surveillance and Society in an Age of High Technology.* Chicago; London: University of Chicago Press.
- Merton, R.K. (1993) *On the Shoulders of Giants: A Shandean Postscript.* Reprinted edition. Chicago: University of Chicago Press.
- Nogala, D. (1995) 'The future role of technology in policing', in J.-P. Brodeur (ed.) *Comparison in policing: an international perspective.* Avebury, pp. 191–210.
- Nogala, D. & et al. (eds) (2022) Pandemic Effects on Law Enforcement Training & Practice: Taking early stock from a research perspective. Luxembourg: Publications Office of the European Union *(Special Conference Edition European Law Enforcement Research Bulletin).* Available at: https://bulletin.cepol.europa.eu/index.php/bulletin/issue/view/30.
- Nogala, D. & Schröder, D. (2019) 'Innovations in Law Enforcement – Introduction to the Special Conference Edition', in D. Nogala et al. (eds) *Innovations in Law Enforcement – Implications for practice, education and civil society.* Luxembourg: Publications Office of the European Union (European Law Enforcement Research Bulletin, Nr. 4), pp. 7–17.
- Peters, B. (2016) 'Digital', in B. Peters (ed.) *Digital Keywords – A Vocabulary of Information Society and Culture.* Princeton, N.J. and Oxford: Princeton University Press, pp. 93–107.
- Project Group on European Approach to Police Science (2009) *Police Science Perspectives: Towards a European Approach : Extended Expert Report.* Frankfurt am Main: Verlag für Polizeiwissenschaft.
- SEASKATE INC. (1998) *The Evolution and Development of Police Technology – A Technical Report prepared for The National Committee on Criminal Justice Technology,* National Institute of Justice. Washington D.C. Available at: https://www.ojp.gov/pdffiles1/Digitization/173179NCJRS.pdf.
- Seife, C. (2000) Zero: The Biography of a Dangerous Idea. New Ed edition. London: Souvenir Press Ltd.
- Southerton, C. (2020) 'Datafication', in L.A. Schintler and C.L. McNeely (eds) *Encyclopedia of Big Data.* Cham: Springer International Publishing, pp. 1–4.
- Su, Y. (2022) 'The Study of the Influence of Social Media on Post- Truth Era', Advances in *Social Science, Education and Humanities Research,* 664. https://doi.org/10.2991/assehr.k.220504.100.
- Terpstra, J., Fyfe, N.R. & Salet, R. (2022) 'Introduction: Abstract Police, the Concept and Some Main Questions', in J. Terpstra, et al. (eds) *The Abstract Police – Critical reflections on contemporary change in police organisations.* The Hague: Eleven, pp. 1–14.
- Toffler, A. (1970) *Future Shock.* Random House.

Plenary Presentations

Welcome Speech

Montserrat Marín López
CEPOL Executive Director

Dear ladies and gentlemen,
Let me begin this welcome address with our sincerest appreciation to the Rector and staff of Mykolas Romeris University for hosting the CEPOL 2022 Research and Science Conference and for all the efforts that have been invested in the organisation of this event.

This is the first major CEPOL activity bringing together so many participants for the exchange of knowledge and scientific insights in a traditional networking format since the last one in Budapest in 2017. As a true networking event, the conference has been organised in various venues and across many countries. In fact, this is the second time it is organised in partnership with Mykolas Romeris University, following the first online edition of the event during the pandemic in May 2021. Today, we are happy and lucky to see and meet so many of you in such a close social encounter.

The concept of systematically organising a constructive and critical dialogue between law enforcement and scientific scholarship has become an integral part of our vision of educating and training police and other law enforcement officials in Europe.

But knowledge and transfer of learning have no value if they are not shared. We will be better law enforcement officials if we improve our training with academic findings and methodologies. We will be more effective if we get to know our peers. The idea is to innovate, improve, educate and combine knowledge with scientific methods. We need a more competent, predictive, agile and secure law enforcement that can adapt to new social changes and knows how to respond in their fight against crime.

The role of higher education will be fundamental in CEPOL's new strategy. One of our objectives will be to increase the number of accredited training actions at various levels of specialisation with European universities of reference in topics such as EMPACT and the EU Strategic Training Needs Assessment. With this event, we aspire to make the work of law enforcement more transparent, to generate relationships of trust and, above all, to look to the future from a perspective of efficiency and professionalism.

The general theme of the conference, 'Preparing Law Enforcement for the Digital Age', reflects one of the most challenging trends in our society: the digitalisation of ever more areas of our public and private lives. During these 3 days, participants will hear about the many related topics that law enforcement agencies have to deal with:

digitalisation of crime, digitalisation of working patterns and tools for law enforcement officials, digitalisation of organisational structures and new ways of teaching and learning. Furthermore, the promises and pitfalls for law enforcement and civil society will take a prominent place in the presentations, along with demonstrations of specialist topics and some of the outcomes and products of the Horizon-Europe-funded projects.

I hope and trust that the presenters and participants will leave the conference informed, inspired and even a bit wiser about how to prepare law enforcement for the digital age.

Thank you for your attention.

Welcome Address

Ylva Johansson
European Commission

Good morning!
First, congratulations to CEPOL and to Executive Director Montserrat Marín for your appointment. New leadership brings new energy and new vision.

CEPOL has an important task. All of our crime-fighting efforts across Europe, across borders, depend on police officers having the skills they need. I thank you especially for your training programmes.

Trafficking is a terrible crime and CEPOL plays a vital role in this fight. You alert police to the dangers of trafficking in human beings. Thanks to your training activities, police can fight and prevent trafficking by learning to spot the danger signs. A trafficker can sell a weapon only once, but can sell a woman's body again and again and again. Older men offering shelter only to young women. Children travelling with people who are not their parents. On the first day after Russia attacked Ukraine, I immediately placed the fight against trafficking on top of the European agenda. When millions of people are on the move, traffickers target vulnerable people.

Our joint European fight is having results and that is how a small agency can make a big difference. The fight against crime is often local but in order to succeed, we must think and work continental.

This is certainly true for your topic today, the fight against crime in a digital age. CEPOL provides a crucial link between security research and everyday policing, by working in the EU innovation HUB for internal security and by teaching police officers to use digital tools.

CEPOL also makes a big difference by shaping a European culture of law enforcement. You train the leaders, you train the trainers, and you bring crime fighters and experts, practitioners and educators together. Like today at this conference.

The Research and Science Conference is very important; the first one in 5 years, during which time our world – particularly online – has changed. It is now your turn to change the world.

In the coming 3 days you will discuss an impressive number of issues with one goal in common: to keep Europe safe.

Your work will shape police work on the ground and inspire many policies.

In turn, I wish you a very inspiring conference.

Policing in a Digital Age: Balance between community-based strategies and technological intelligence

Luís Manuel André Elias

Higher Institute of Police Sciences and Internal Security (ISCPSI), Research Center (ICPOL), Lisbon

Abstract

Digital networks are a "new" environment for organized crime, radicalization, recruitment, terrorism, and disinformation. There is a deterritorialization of threats and risks, making digital networks a new dimension for the expansion of criminal networks and for justice and police.

Nowadays, democratic societies, human rights and internal/external security are challenged by artificial intelligence and other emerging technologies. This "brave new world" has created an illusion within Police and intelligence communities that prioritizing technological intelligence they will obtain immediate and better results.

The central aim of this article is to reflect on security trends in nowadays societies of investing more in hard policing and technological policing and less in community-based strategies.

Artificial intelligence, big data, machine learning, analytical software, predictive techniques based on algorithms are increasingly used by law enforcement. This resulted in a gradual devaluing of community policing and human intelligence and raises a set of ethical, deontological, fundamental rights protection, privacy, and, most likely, the systematic reproduction of biases.

We propose to analyze the benefits for Police to promote a comprehensive approach between HUMINT and TECHINT to allow a better understanding of communities' idiosyncrasies and to improve the relationship between Police and fragile communities, as well as to prevent threats and risks to our collective security.

We seek to prove the advantages of scientific research and innovation in the digital age, and of a comprehensive approach between soft and hard policing, between community policing and intelligence-led policing, promoting at the same time a permanent dialogue between Police and citizens.

Keywords: Security, emergent technologies, community policing, intelligence, human rights.

Introduction

Globalised contemporary society is increasingly complex due to disruptive technologies (Bower, Christensen, 1995; Immelt, Govindarajan & Trimble, 2009). These emergent technologies are likely to bring many benefits, from increased productivity and economic growth to greater success in tackling global threats, including terrorism and transnational organized crime. But may also impact in civil rights and data protection.

Buzzwords and acronyms, like VUCA and BANI (Cascio, 2020) try to illustrate in a fancy/comprehensive way nowadays volatile, uncertain, complex, and ambiguous (VUCA) world. And with covid-19 pandemic, a brittle, anxious, nonlinear and incomprehensive (BANI) society.

Law enforcement is about crime prevention, crime investigation, public order, police intelligence and international police cooperation (Elias, 2018) and there should be a straight coordination between these five pillars of policing. Checks and balances between prevention and repression strategies are crucial.

Our investigation will seek to answer the following starting question: Will it be possible to build-up a comprehensive approach between community policing, intelligence led-policing, technological policing and robust policing?

The methodology to be used will be of a composite nature, as we will draw on knowledge in the fields of Police Sciences, International Relations, Political Science and Sociology, as well as the intersection of theories and scientific methods. We will choose to carry out a descriptive-theoretical study, based on the bibliographic analysis, legislation, and official documents from different types of sources, both national and international.

We are going to present the results from the report on "Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain" coordinated by Europol Innovation Lab and the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC) published in February 2022, as well as a national survey carried out in 2021 in Portugal by the Research Center (ICPOL) of the Higher Institute of Police Sciences and Internal Security and the company SPIRITUC (a market research company specialized in the medical field) on public perception about Police Service.

This article is a theoretical study, and the structure obeys an introduction, state of the art, perspectives (guidelines) and conclusion (practical or theoretical implications).

State of the Art

As of the start of 2022, there are 4.95 billion active internet users (DataReportal, 2022).

Considering there is a global population of 7.91 billion people and that global internet users have climbed to 4.95 billion at the start of 2022, internet penetration now stands at 62.5 percent of the world's total population.

There are 4.62 billion social media users around the world in January 2022.

And what about crime and world security? According to the *Global Organized Crime Index 2021* "the vast majority of the world's population (79.2 %) live in countries with high levels of criminality, and in countries with low resilience (79.4 %)". The same document underlines the following:

- human trafficking is the most prevalent type of crime. In 2020, there were an estimated 281 million international migrants globally.
- the second most pervasive criminal market globally is the cannabis trade, which is a worldwide phenomenon.
- firearms trafficking is also worrying at international level.

The organized crime landscape "is characterized by a networked environment where cooperation between criminals is fluid, systematic and driven by a profit-oriented focus" (EU SOCTA, 2021, 10).

Europol underlines that:

- Close to 40 % of the criminal networks active in the EU are involved in the trade in illegal drugs;

- 40 % have a hierarchical structure and 60 % are fluid structures;
- 79 % are composed by six or more members and 21 % have up to five members;
- 80 % use legal business structures for their criminal activities;
- 68 % use basic money laundering methods such as investing in property or high-value goods;
- 60 % use violence as part of their criminal businesses and 60 % engage in corruption;
- The use of corruption and the abuse of legal business structures are key features of serious and organised crime in Europe. Two thirds of criminals use corruption on a regular basis (EU SOCTA, 2021, 18).

Criminals are "growing their operational security by hiding their online activity, using more secure communication channels and obfuscating the movement of illicit funds" (IOCTA, 2021, 16). And crime is more and more "crime as a service", providing goods and services to worldwide (online) consumers.

In the last 40 years, literature and academic studies proposed several policing models to better cope with changing reality and the liquid times (Bauman, 2007). Community policing (Trojanowicz & Bucqueroux, 1990; Monjardet, 1996; Normandeau, 1998), zero tolerance (Kelling & Colles, 1996; Kelling & Bratton, 1998; Kelling & Sousa, 2001), hot spots policing (Clarke, 1986, 1998), broken windows theory (Wilson & Kelling, 1982), evidence based policing (Sherman, 1998), problem oriented policing (Goldstein, 2003), intelligence led-policing (Ratcliffe, 2008) and predictive policing (Selbst, 2017; McDaniel, J. & Pease K., 2021) are paradigms that hold important implications for policing. Several times were combined between each other and there were good practices that had an excellent impact in local communities, but as well badly implemented programs, have not been evaluated and several others got poor results.

These paradigms, despite having a strong rhetorical component (Klockars, 2005, 442), are intended to generate willingness to reform Police organizations and performances.

Indeed, there are contradictory security trends in several western and non-western countries. On the one hand, several governments implement the militarization of policing, others maintain community based-policing strategies and others increase the privatization of several security areas. On the other hand, law enforcement agencies prioritize more and more technological intelligence, which may bring risks for civil rights, data protection and privacy in nowadays hi-tech brave new world (Huxley, 1932).

TechPol and TechInt in the Digital Age

The development of new technologies is faster than ever and it's intensifying social relations on a global scale (Giddens, 2005, 45). Life in the digital age is truly information-driven, with data becoming more valuable than oil (The Economist, 2017). For example, companies will lash out to know what drives customers' interests. Insights gained from refining data will allow companies to spend money where it should be spent and also increase profits.

Governments and Police state that they seek to improve efficiency and effectiveness in the fight against violent and organized crime. However, budget cuts made governments and municipalities to replace police officers to algorithms in several police departments (Heaven, 2020). Another reason for the increased use of algorithms is the widespread belief that they are more objective than humans (Reiss & Sprenger, 2020; Daston & Galison, 1992, 81): they were first introduced in United States for a fairer decision-making in criminal justice system and now machine learning is being implemented in several courts in other western countries (Heaven, 2020).

HUMINT requires a great deal of time and resources to gather assets and analyze information, rendering it one of the most difficult types of intelligence to produce and implement. The training alone is time consuming. Police officers need to learn

> *"(...) foreign languages; conducting, detecting, or evading surveillance; recruiting skills and other aspects of HUMINT tradecraft; the ability to handle various types of communications equipment, information systems, weapons, and so on"* (Margolis, 2013, 45).

Training of these intelligence officers is costly and can take several years to complete. But it's worth to mention that HUMINT is far less expensive than the various technical intelligence resources, although it still involves costs for training, special equipment, and the accoutrements clandestine officers need to build successful cover stories. The end goal of obtaining ad-

equate, accurate, and actionable information is best attained when HUMINT and TECHINT capabilities are combined (Crosston & Valli, 2017, 76).

An infatuation with technological methods of intelligence gathering

> *"(. . .) has developed within many organizations. As a result of the focus on technical methods, some of the worst intelligence failures of the 20th century can be attributed to an absence of human intelligence"* (Margolis, 2013, 43).

If Police (as well as intelligence services and even armed forces) only support their operations on TECHINT (SIGINT, GEOINT, IMINT, MASINT, CYBINT) they will get just part of the intelligence picture. Thus, it´s very important for Police "to put the boots on the ground" to gather HUMINT through crime investigation, intelligence analysts and community policing officers and to compare it with other sources obtained through TECHINT.

The (minority report) dream of predicting crimes almost came true. But at what price? Algorithms may carry biases (Miller, 2019) and stereotypes that may impact in citizens' rights in our democratic societies, such as the erosion of privacy and other human rights (Noble, 2018, 24). The fashion for data analytics and intelligence-led policing evidence the 'uberization' of security control (Sanders & Sheptycki, 2017).

Big Data often presents a façade of apparently rigorous, systematized, mathematical and neutral logic (Sanders & Sheptycki, 2017). Advances in emerging technologies raise a set of ethical, deontological, fundamental rights protection, privacy, legitimacy, public recognition and, most likely, the systematic reproduction of biases (Hunkenschroer & Luetge, 2022).

Emerging technologies and dataveillance (Esposti, 2014; Büchi, Festic & Latzer, 2022) will change policing in the future. Giving some examples about the extraordinary impact of technologies in policing in the present and in the future:

- CCTV systems with alarmist software and patterns that may identify crimes being committed or suspects and objects that may be a risk to public security;
- the use of augmented reality glasses to give criminal context to police officers;
- small autonomous drones programmed to follow police officers, scout locations, and provide video streams so that no officer ever must go into any situation truly alone;
- artificial intelligence and machine learning are key to identify hate speech online, child sexual abuse, recruitment, and radicalization campaigns in social media;
- location-based algorithms, crime patterns and identification of suspects;
- sensors for bomb detection in public spaces;
- IoT connected devices, AI and deep learning to improve connectivity and capacity to process information;
- threat screening for major events (AI and facial recognition software);
- police engagement with the community through social media (sensitization and prevention campaigns, public information, etc.) is also a new form of cyber community policing.

Besides this, the creation of national taskforces on cybercrime (composed of law enforcement authorities, representatives of the judiciary, AI technology developers, criminologists, and global service providers) may serve as a relevant vehicle to coordinate and tackle illicit conducts concerning the misuse and abuse of AI technologies (Velasco, 2022).

Europol Innovation Lab and the Centre of Excellence in Terrorism, Resilience, Intelligence and Organized Crime Research (CENTRIC) published the report "Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain. AP4AI Framework Blueprint" in February 2022.

After 5.239 answers about the AI use by Police forces citizens see great potential in AI use for safeguarding vulnerable groups and society, including the prevention of future crimes:

- 89,7 % agreed or strongly agreed that AI should be used for the protection of children and vulnerable groups,
- 87,1 % agreed that AI should be used to detect criminals and criminal organizations

- 78,6 % agreed that AI is used to predict crimes before they happen
- 90 % of participants expect Police to be held accountable for the way the use AI and for the consequences of their AI use.

AI may be fundamental to prevent and to counter-terrorism (namely online terrorist generated contents), child sexual exploitation (identifying the individuals sharing the material as well as their locations) and serious and organized crime. Yet, although AI and accountability in policing have become a central point of discussion across the law enforcement and internal security sector, they are often discussed in isolation and not as a targeted approach to ensuring accountability for AI deployments. This means that there remains a significant gap in addressing AI accountability within the fields of security and policing (AP4AI, 2022).

Europol supports that:

- law enforcement undercover capabilities are becoming increasingly important in cybercrime investigations. Nevertheless, legal barriers around the retention and sharing of data persist. Data is often not retained for long enough with ISPs, which can lead to a loss of potential evidence. Investigations would benefit from longer data retention. In addition, there is a need for clearer rules for registering IP addresses and domains could increase this data quality. Increased international cooperation is also crucial;

- there is a need for more technically skilled officers, training, and technical solutions to adequately address cybercrime, because of the increased technical sophistication;

- there is a need to establish a broader cooperative focus between public and private sectors to prevent and fight the new digital threats: bulletproof holsters, criminal VPNs, illicit cryptocurrency exchangers, and money laundering platforms.

- law enforcement agencies should be firmly embedded and enhanced within the national cybersecurity crisis management frameworks and clear roles and responsibilities should be assigned to the different competent authorities (AP4AI, 2022), namely defense, intelligence services, police, justice.

Community policing – policing by consent

There isn´t an academic consensus about Community Policing concept. According to a literature review, community policing implies consent, an agreement between the police and the community – policing by consent (Waddington & Wright, 2008).

For several scholars community policing *"is not a technique, it is not public relations, it is not a 'soft' strategy against crime, it is not paternalistic, it is not an independent entity within the police, it is not cosmetic, it is not just another designation for social work, it is not elitist, it is not intended to favor the rich and powerful in the community, it is not a panacea, as if poorly adopted it could have disastrous effects on the community"* (Trojanowicz, Kappeler, Gaines, Bucqueroux & Sluder, 1998, 22).

Community policing is crucial to create trust and co-operation between the Police, local communities, and citizens (Goldstein, 1990; Trojanowicz & Carter, 1988) and to produce HUMINT.

One of the fundamental conditions for the sustainability of policing models is their scientific evaluation. Community policing programs, as well as other policing models, must be regularly assessed to check their impact in citizens' perceptions. Besides that, these surveys may be important to know better what community needs are, to improve policing practices and to increase interactions with local communities.

In Portugal, the Higher Institute of Police Sciences and Internal Security coordinated a national scientific survey in 2021 to evaluate citizens' degree of satisfaction with Public Security Police (PSP) work/performance, as well as their (subjective) perception of security in urban areas. A total of 2561 complete/validated answers were collected. Concerning performance evaluation of PSP the following results were obtained:

- 93,1 % positively evaluated the attitude of the PSP police officers;

- 69,6 % considered it good or very good;

- 83,9 % positively evaluated the ability of PSP officers to deal with security problems;

- 52,2 % considered it good or very good;

- 72.2 % positively evaluated the presence of PSP police officers at public areas;
- 43.0 % considered it good or very good;
- 81.4 % positively evaluated the police response in urgent situations;
- 51.3 % considered it good or very good;
- 80.9 % reported being familiar with the Safety in School program;
- 77.5 % reported being familiar with the Support Program for Victims of Domestic Violence;
- 55.6 % reported being familiar with the Support to Elderly People.

These results express a very good opinion about PSP performance in Portugal, excellent perception about communities' safety, as well, it shows an important impact of community policing in Portuguese society, namely the Safety in School Program and the Support to Victims of Domestic Violence.

There isn't academic consensus that Intelligence Led-Policing is compatible with Community Policing (Carter & Fox, 2018). The literature articulates the relationship between COP and ILP along a continuum that ranges from closely related (Carter & Carter, 2009; Clarke, 2006; McGarrell, Freilich & Chermak, 2007; Bullock, 2013), sharing minimal similarity (Tilley, 2003; Innes *et al*., 2009; LeCates, 2018), and distinctly different (Deukmedjian & de Lint, 2007; Ratcliffe, 2016).

However, both community policing and intelligence led-policing appear to share many core elements, such as an emphasis on proactive versus reactive policing, and two-way sharing of information with the community. Both have a broad and flexible framework to allow these strategies to be utilized as long-term solutions and be customized to the individual needs and strengths of each agency (Carter & Fox, 2018, 15). Both emphasize a more active role of local policing in assisting in issues as counter-terrorism (McGarrell *et al*., 2007), gang intervention (Charles, 2018), social harm (Mohler *et al*., 2018; Ratcliffe, 2016), border security and immigration (Lewandowski *et al*., 2017), about policing the internet to detect organized crime and terrorism, as well to promote sensitization campaigns in social media in several areas: domestic violence, bullying, drugs consumption, diversity, animals' rights.

Intelligence-led policing has commonalities with problem-oriented policing and targeted, proactive policing (Ratcliffe, 2016, 4). Intelligence-driven policing requires a comprehensive interpretation of all information collected by the police trough: surveillance, interrogations, informants, analysis of criminal patterns, sociodemographic information, and other data from non-police sources.

Militarization and Privatisation of Policing

The shift from community policing work to the crime control militarization didn't start with the 'war on terror' (Rivas, 2013). The change started with the "war on drugs" and the "war on crime" (Meeks 2006).

When we mention militarization, we are not referring exactly to the change from civilian to military status of the police forces, but predominantly to the adoption of hard policing strategies and tactics, as well as SWAT teams (Cox S., Marchionna S., Fitch B., 2017, 86), assault rifles and more ostensive equipment (armored vehicles, ballistic vests and helmets, drones and others).

Many scholars and practitioners express their concern that the "war on terror" is contributing that several police agencies "replace community policing programs with traditional hardline models that give priority to hierarchy at the expense of autonomy, to rules and norms in place of some degree of discretion in police decision and action" (Murray, 2005; Greene, 2011; Mijares & Jamieson, 2011).

Militarization may exert even a stronger influence on what the regular police decide on for uniforms (e.g. military battle dress uniforms – BDUs), how they think, the weaponry and technology they employ, the organizational models they adopt, and the crime control solutions they devise. Community policing call for democratization may be increasingly drowned out by the drumbeats of high-technology militarization (Kraska, 2007, 12). It is assumed that hard policing increases effectiveness and influences public´s subjective feelings of insecurity, with an investment in the security apparatus, overestimating a supposed effectiveness, even at the expense of efficiency. Consequently, in

several countries TECHINT and robust policing are step by step replacing HUMINT, community policing and partnerships between the Police and the communities.

Academic studies mention several risks but also advantages of privatizing policing. On the one hand, private security lack accountability, may bring threats to civil liberties, concerns about loss of public-interest, greater inequality in protection, reputational concerns, threats to police jobs. On the other hand, it may bring increased effectiveness through public/private partnerships, alignment with the ideals of community policing, police may concentrate their efforts in more vulnerable sectors of community, access to specialized skills and technical resources and efficiencies through contracting out (Sparrow, 2014).

The proliferation of private security has both involved the spread of technologies, such as closed-circuit television together with artificial intelligence and the incursion of the private sector into forms of work, or areas of activity, more usually associated with public policing (Newburn, 2008, 826). Recent examples include private security being responsible for airport security, major sports events, cultural or political events, traffic and parking regulation, the transport and guarding of prisoners and, most important of all at a symbolic level, the patrolling of public streets, public buildings, and of the army and the police facilities. In addition, the notion of self-policing within communities and greater use of volunteers to assist public policing may generate a confusing landscape of plural policing in the future (Rogers, 2018, 400-401), mixing and melting traditional missions of Police with new private security tasks in a less accountable and equal way.

There are challenges inherent in the use of plural policing approaches which may affect the very nature of the democratic policing model. Despite criticisms to 'pluralised' policing, it would appear that privatization of security is low-cost, it's a strategy of frontline preventive presence, it may increment the deployment of experts for specific or specialized tasks, and it may also boost research and development of emerging technologies.

Discussion/Conclusion

Technological development has created an illusion within law enforcement and intelligence communities that prioritizing technological intelligence they would obtain immediate and better results. Artificial intelligence, analytical software, big data, predictive techniques based on algorithms are increasingly used by law enforcement. This will be a challenge for law enforcement but may also result in a gradual devaluing of community policing, human intelligence, and the understanding of community idiosyncrasies.

The results of the national survey coordinated by the Higher Institute for Police Sciences in Portugal show how important is scientific assessment to evaluate policing models and police performance. It shows as well that citizens understand the advantages of community policing-based strategies.

The results of Europol study underline that citizens see great potential in AI and emerging technologies use for safeguarding vulnerable groups and society, including the prevention of future crimes.

Policing has changed, as has the society being policed. The digital age will bring even more challenges. In this context, in the academia and law enforcement community it's necessary to reflect on future policing models that may better prevent and detect new threats and risks in nowadays complex world (Beck, 1992).

Answering to our initial question: despite lack of consensus at academia, an integrated approach between community policing strategy, intelligence led-policing, TECHINT and HUMINT, may be crucial to prevent and fight crime, to maintain a straight relationship with local communities and to improve the quality of police service.

Nowadays emerging technologies bring several challenges for law enforcement community, like the ones mentioned by Europol:

- data is often not retained for long enough with ISPs, which can lead to a loss of potential evidence. Investigations would benefit from longer data retention;

- law enforcement agencies need more officers, tools and training to fight cybercrime;

- there is a need for a broader cooperation between public and private sectors to address new digital threats;

- law enforcement agencies should be firmly embedded within the cybersecurity crisis management frameworks.

The fight against violent and organized crime must be robust, but above all must use analytical capabilities, crime investigation, intelligence and information systems, acknowledging socio-cultural problems, and respecting human rights.

The collaboration between the Police and a myriad of public and private entities is essential to maintain sustainable partnerships, to build bridges with minority communities and to discourage some of its members from embarking on the path of radicalization, terrorism (Forst, 2014, 634) and organized crime.

Militarization of law enforcement has the potential to undermine citizen's reliance in justice and police, because exceptionalism conveys to the community that if you transgress, you may encounter extreme, possibly deadly violence. Such perception of deterrence is unacceptable in a rule of law society.

Police must have special units to deal with serious crime: SWAT teams, public order units, bomb squads, canine units. However, robust policing strategies and militarization of Police departments shouldn't be "the solution". Police must know and understand the community and to analyze crimes that impact in local security to take preventive and repressive measures. Police need to recruit data scientists, financial experts, digital forensics, digital patrollers to face the cyber organised crime.

The disinvestment in human sources and the prioritization of technological solutions can create an aseptic perspective of reality, the inability to detect underground criminal phenomena and increase bias in police intelligence analyses.

New technologies may also pose significant challenges related to their questionable reliability and accuracy that lead to multiple risks to civil rights, discrimination, data protection, privacy, and unlawful profiling.

However, these emergent technologies have already an important role in modern policing, helping investigators, analysts, and regular policing to analyze large amounts of data, helping to detect suspects in video surveillance systems, facilitating the collection of (online) evidence in complex investigations, and detecting criminal networks and operations on the internet. But, at its core, law enforcement requires partnerships with communities, the same sense of duty and sacrifice, and the same integrity and respect for fundamental rights it always has.

References

- Bauman, Z. (2007) Liquid Times: Living in an Age of Uncertainty. Cambridge, Polity.
- Beck, U. (1992) Risk Society. Towards a New Society. 2nd edition. London: Sage Publications.
- Bower, J. L., & C. M. Christensen (1995) Disruptive Technologies: Catching the Wave. *Harvard Business Review* 73, no. 1, January–February, pp. 43–53.
- Bullock, K. (2013) Community, intelligence-led policing and crime control. Policing and Society, 23(2), 125-144.
- Büchi, M., Festic, N. & Latzer, M. (2022) The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical. *Big Data & Society*, January–June, pp. 1–14
- Carter, J. G., & Fox, B. H. (2018) Community policing and intelligence-led policing: An examination of convergent or discriminant validity. *Policing: An International Journal*, Vol. 42 (1), pp. 43-58.
- Carter, D. L., & Carter, J. G. (2009) Intelligence-led policing: Conceptual and functional considerations for public policy. *Criminal Justice Policy Review*, 20(3), 310-325.
- Cascio, J. (2020) Facing the Age of Chaos.
  Available from: https://medium.com/@cascio/facing-the-age-of-chaos-b00687b1f51d [Accessed 16th April 2022].
- Charles, J. B. (2018) How Police in One City Are Using Tech to Fight Gangs. Governing, March 02.
  Available from: https://www.governing.com/archive/gov-gang-violence-predictive-policing-high-point-lc.html

- Clarke, C. (2006) Proactive policing: Standing on the shoulders of community-based policing. *Police Practice and Research*, 7(1), 3-17.
- Clarke, R. V. (1998) Defining Police Strategies: Problem Solving. Problem Oriented-Policing and Community-Oriented Policing. In: Problem-Oriented Policing: Crime-Specific Problems, Critical Issues and Making POP Work, ed. O'Connor, Tara & Grant, Anna C., Washington DC: Police Research Executive Forum, pp. 315-330.
- Clarke, R. V. & Cornish, D. (1986) *The Reasoning Criminal.* New York: Springer-Verlag.
- Cox, S., Marchionna, S. & Fitch, B. (2017) Introduction to Policing. Interactive eBook Student Version Third Edition. New York, Sage Publications.
- Crosston, M & Valli, F. (2017) An Intelligence Civil War: "HUMINT" vs. "TECHINT". *Cyber, Intelligence and Security.* Volume 1, number 1, 67-82.
- Daston, L. & Peter, G. (1992) The Image of Objectivity. Representations, no. 40 (October), pp. 81–128.
- DataReportal (2022) Digital 2022: Global Overview Report.
  Available from: https://datareportal.com/reports/digital-2022-global-overview-report[Accessed 10th March 2022].
- Deukmedjian, J. E., & de Lint, W. (2007) Community into intelligence: Resolving information uptake in the RCMP. *Policing and Society*, 17(3), 239-256.
- Elias, L. (2018) Ciências Policiais e Segurança Interna. Lisboa, ISCPSI.
- Esposti, S. D. (2014) When big data meets dataveillance: the hidden side of analytics. *Surveillance & Society*, Vol. 12 N. 2.
  Available from: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/analytics. [Accessed 16th April 2022].
- Europol Innovation Lab & CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research) (2022) Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain AP4AI.
  Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/Accountability_Principles_for_Artificial_Intelligence_AP4AI_in_the_Internet_Security_Domain.pdf [Accessed 25th February 2022].
- Europol (2021) The EU Serious and Organised Crime Threat Assessment (SOCTA).
  Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf [Accessed 25th April 2022].
- Europol (2021) Internet Organised Crime Threat Assessment (IOCTA).
  Available from: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021[Accessed 25th April 2022].
- Giddens A. (1990) The Consequences of Modernity. Stanford, Stanford University Press.
- Global Initiative Against Transnational Organized Crime (2021) *Global Organized Crime Index.*
  Available from: https://globalinitiative.net/wp-content/uploads/2021/09/GITOC-Global-Organized-Crime-Index-2021.pdf [Accessed 25th February 2022].
- Goldstein, H. (1990) Problem-Oriented Policing. Philadelphia, Temple University Press.
- Goldstein, H. (2003) On Further Developing Problem-Oriented Policing: The Most Critical Need, the Major Impediments, and a Proposal. In: *Crime Prevention Studies*, vol. 15, pp. 13-47.
- Greene, J. (2011) Community Policing and Terrorism: problems and prospects for local community security. In: Criminologists on terrorism and homeland security. Cambridge: Cambridge University Press, pp. 208-244.
- Heaven, W.D. (2020) Predictive policing algorithms are racist. They need to be dismantled. MIT Technology Review.
  Available from: https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/. [Accessed 16th April 2022].
- Higher Institute of Police Sciences, Internal Security Research Center (ICPOL) & Spirituc – Investigação Aplicada (2021) Public Perception about Police Service. Lisboa, ISCPSI.
- Hunkenschroer & Luetge, C. (2022) Ethics of AI-Enabled Recruiting and Selection: A Review and Research Agenda. *Journal of Business Ethics*, volume 178, pp. 977–1007.
- Huxley, Aldous (1932). Brave New World. New York, Harper & Brothers.
- Immelt, J., Govindarajan, V. & Trimble, C. (2009) How GE Is Disrupting Itself. *Harvard Business Review*. October, pp. 1-11.
- Innes, M., Abbot, L., Lowe, T., & Roberts, C. (2009) Seeing like a Citizen: Field Experiments in 'Community Intelligence-Led Policing.' *Police Practice and Research*, 10(2), 99-114.
- Kelling, George L. & Sousa, William J. (2001) Do Police Matter? An Analysis of the Impact of New York City's Police Reforms. New York, Manhattan Institute Center for Civic Innovation.

- Kelling, G. L. & Bratton, W. (1998) Declining Crime Rates: Insiders' Views of the New York City Story. In *Journal of Criminal Law and Criminology,* 88 (4), 1217-1232.
- Kelling, G. L. & Coles, K. M. (1996) Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities. New York, Free Press.
- Klockars, C. B. (2005) The Rhetoric of Community Policing in Policing Key Readings. Portland, Willan Publishing.
- Kraska, P. (2007) Militarization and Policing. Its Relevance to 21st Century Police. In: Policing: A Journal of Policy and Practice, Volume 1, Issue 4, 501–513.
- LeCates, R. (2018) Share Intelligence-led Policing: Changing the Face of Crime Prevention. Police Chief Magazine. IACP. Available from: https://www.policechiefmagazine.org/changing-the-face-crime-prevention/ [Accessed 29th April 2022]
- Lewandowski, C., Carter, J. G., & Campbell, W. L. (2017) The utility of fusion centres to enhance intelligence-led policing: an exploration of end-users. *Policing: A Journal of Policy and Practice,* 12(2), 177-193.
- Margolis, G. (2013) The Lack of HUMINT: A Recurring Intelligence Problem. *Global Security Studies*, Spring, Volume 4, Issue 2, pp. 43-40.
- McDaniel, J. L. & Pease K. (2021) Predictive Policing and Artificial Intelligence. New York, Routledge-Taylor & Francis Group.
- McGarrell, E. F., Freilich, J. D. & Cherma, S. (2007) Intelligence-Led Policing As a Framework for Responding to Terrorism. *Journal of Contemporary Criminal Justice*, 23(2), 142-158.
- Meeks, D. (2006) Police Militarization in Urban Areas: The Obscure War Against the Underclass. *The Black Scholar*, 35(4), 33-41.
- Mijares, T. & Jamieson, J. (2011) Soldiers and Spies, Police and Detectives. In Criminologists on Terrorism and Homeland Security, edited by Forst, Greene & Lynch. New York, Oxford University Press, pp. 183-207.
- Miller, T. (2019) Explanation in artificial intelligence: Insights from the social sciences. *Artificial Intelligence*, volume 267, February, pp 1-38.
- Mohler, G., Porter, M. & LaFree, G. (2020) Learning to Rank Spatio-Temporal Event Hotspots. *Crime Science,* volume 9, Article number: 3.
- Monjardet, D. (1996) Ce que Fait la Police. Sociologie de la Force Publique. Paris, Éditions de la Découverte.
- Murray, J. (2005) Policing Terrorism: A Threat to Community Policing or Just a Shift in Priorities? In *Police Practice and Research* 6 (4), 347-361.
- Newburn, T. (2008) The Future of Policing. Handbook of Policing. Portland: Willan Publishing
- Noble, S. (2018) Algorithms of Oppression: How Search Engines Reinforce Racism. New York, New York University Press.
- Normandeau, A. (1998) Une Police Profissionnelle de Type Communautaire. Montréal, Éditions du Méridien.
- Ratcliffe, J. H. (2016) Intelligence-led policing. Second Edition. New York: Routledge.
- Ratcliffe, J. (2003) Intelligence-Led Policing, in Trends & Issues in Crime and Criminal Justice, n.º 248. Camberra: Australian Institute of Criminology.
- Reiss, J. & Sprenger, J. (2020, Winter Edition). Scientific objectivity. In: Zalta, E.N. (Ed.) The Stanford Encyclopedia of Philosophy. Available from: https://plato.stanford.edu/archives/win2020/entries/scientific-objectivity/. [Accessed 30th April 2022]
- Rivas, J. (2013) Militarization of the Police Force: Causes and the Alternative. The Faculty of the Sociology Department. California Polytechnic State University, San Luis Obispo.
- Rogers C. (2018) Plural Policing in England and Wales: Thoughts and Discussion. *Forensic Research & Criminology International Journal*, 6(5): 397-401.
- Sanders, C & Sheptycki (2017) Policing, crime and 'big data'; towards a critique of the moral economy of stochastic governance. *Crime, Law and Social Change*, volume 68, pp. 1–15
- Sherman, L. (1998) Evidence-Based Policing. In: Ideas in American Policing. Washington, *Police Foundation*, July 1998, pp. 1-16.
- Selbst, A. (2017) Disparate Impact in Big Data Policing. *Georgia Law Review*, 109, Available from: https://ssrn.com/abstract=2819182 [Accessed 10th November 2021]

- Sparrow, M. K. (2014) Managing the Boundary Between Public and Private Policing. New Perspectives of Policing, September. Harvard Kennedy School. National Institute of Justice.
- The Economist (2017) The World's Most Valuable Resource is No Longer Oil, But Data. May 11th.
  Available from: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [Accessed 15th January 2022]
- Tilley, N. (2003) Community policing, problem-oriented policing and intelligence-led policing. In T. Newburn (Ed.), Handbook of Policing, 311-339. Cullompton: Willan Publishing.
- Trojanowicz Robert C., Kappeler V.E., Gaines L. K., Bucqueroux B. & Sluder R. (1998) Community Policing: A Contemporary Perspective, Second Edition. Cincinnati, Anderson Publishing.
- Trojanowicz, R. C. & Bucqueroux, B. (1990) Community Policing: a contemporary perspective. Cincinnati, OH: Andersen.
- Trojanowicz, R. C. & Carter, D. (1988) The Philosophy and Role of Community Policing. In National Neighbourhood Foot Patrol Centre, Community Policing Series, No. 13, pp. 1-26.
- Velasco, C. (2022) Cybercrime and Artificial Intelligence. An Overview of the Work of International Organizations on Criminal Justice and the International Applicable Instruments. *ERA Forum volume*, 23, pp. 109–126.
  Available from: https://link.springer.com/article/10.1007/s12027-022-00702-z [Accessed 30th April 2022].
- Waddington, P. A. & Wright, M. (2008) Police Use of Force, Firearms and Riot Control. In: Newburn, T. (eds.) 'Handbook of Policing', Second Edition, Portland, Oregon, Willan Publishing.
- Wilson, J. Q. & Kelling, G. L. (1982) Broken Windows: The Police and Neighborhood Safety. *Atlantic Monthly*,249 (March), pp. 29-38.

Digital Data and Algorithms in Law Enforcement:
Some pointers for responsible implementation and use

Matthias Leese
Department of Humanities, Political and Social Sciences
ETH Zurich[1]

Abstract
Digital data and algorithms have over the past years increasingly found their way into law enforcement contexts, including modes of biometric identification and matching, automated surveillance capacities, short-term situational predictions, AI-supported analysis for large amounts of data, and the interoperability of large-scale databases and platforms for data exchange and investigation. These tools can help to increase the effectiveness and efficiency of law enforcement operations on the strategic, tactical, and operational level. They do, however, also come with a number of concerns that must be acknowledged and addressed in order to realize their potential and avoid unintended side-effects and societal frictions. Based on a multi-year research project on predictive policing in Germany and Switzerland, this paper provides a perspective on some of the challenges involved in implementing new and emerging technologies in law enforcement contexts. Specifically, it addresses (1) the nature of data, i.e. how data are socially constructed and present a particular account of the world, inevitably leading to "biased" results; (2) transparency in algorithms and AI, i.e. how "black boxes" undercut human capacities to understand and retrace processes and create problems for public accountability; (3) automation and human control, i.e. the question how human operators can retain meaningful influence over analytical processes; (4) decision-making processes and automation bias, i.e. how humans can be empowered to critically question and override system recommendations; and (5) strategic and societal implications, i.e. the fact that digital tools should not be misused to displace larger programs that address the root causes of crime.

Keywords: digitization; data; algorithms; implementation; civil liberties; accountability; police

Introduction

Digital data and algorithmic tools for their processing have over the past decade found their way into law enforcement contexts in multiple ways, including modes of biometric identification and matching, enhanced surveillance capacities, short-term situational predictions, AI-supported analysis for large amounts of data, and the interoperability of large-scale databases and platforms for data exchange and investigation. These tools can help to increase the effectiveness and efficiency of law enforcement operations on the strategic,

1 Author's email: mleese@ethz.ch

tactical, and operational level. They do, however, also come with a number of concerns that must be acknowledged and addressed in order to realize their potential and avoid unintended side-effects and societal frictions. Civil society organizations have for example warned of chilling effects of surveillance technologies, increased or new forms of data-driven discrimination, and the lack of transparency and democratic control in algorithmic decision-making (Ferguson, 2017; Robinson & Koepke, 2016; Susser, 2021).

Vis-à-vis these concerns, the challenge for law enforcement organizations is to find responsible ways of implementing and using digital data and algorithms, such that they enable enhanced strategic, tactical, and operational capacities while at the same time protecting democratic rules, civil liberties, and human rights. Law enforcement occupies a key role in society due to its mandate to produce and maintain public order. Needless to say, policing is therefore accompanied by considerable legal and moral responsibilities towards society. Crucially, the ways in which police agencies carry out their mandate undergo profound transformations when knowledge and action are based on data and pre-configured by algorithmic forms of data analysis. To think about responsible forms of digitization in law enforcement, this paper proposes five key pointers that should be given attention when implementing and using data-driven and algorithmically mediated technologies. These pointers concern (1) the nature of data themselves, as well as questions of (2) transparency, (3) automation and human control, (4) decision-making, and finally (5) strategic implications.

While these themes generally pertain to any form of the use of data and algorithms in law enforcement, they will be throughout this paper illustrated with examples from a multi-year study on the implementation and use of predictive policing software in Germany and Switzerland (Egbert & Leese 2021). During the research, empirical data on new, algorithmically mediated forms of crime data analysis for crime prevention were gathered through interviews with involved officers and analysts, field observations, as well as extensive document analysis. In total, research covered 12 police departments at the local and state level. Throughout the research period, most of the involved departments used the commercial predictive policing software PRECOBS by German manufacturer IfmPt.[1] PRECOBS specifically focuses on residential burglary and professionalized serial burglary activities, aiming to identify patterns of ongoing criminal behavior through continuous analysis of current crime data and producing risk estimates for particularly vulnerable areas or neighborhoods. In this way, it seeks to provide police departments with timely and flexible response capacities, most notably the opportunity to adjust crime prevention schemes and reallocate otherwise randomized patrols and other resources to identified risk areas in a targeted fashion. The optimal outcome of predictive policing would in this sense be to instill situational awareness that leads to the deterrence of crime (Balogh 2016; Schweer 2015).

Overall, the research project explored how predictive policing software was implemented into everyday crime analysis and crime prevention/patrolling contexts. Questions informing the research pertained to, among other things, technologically mediated knowledge production and communication within police organizations, the visualization and actionability of crime forecasts in patrolling and crime prevention, and the normative implications of policing based on data-driven risk estimates. The findings presented in this paper are based on a set of practical recommendations for the responsible use of data and algorithms in law enforcement that have been derived from the analysis of the empirical data (Egbert & Leese, 2021; Leese, 2020). They should be understood as points to consider when thinking about what data and algorithms (can) do and how they can be implemented and used in ways that speak to the particular mandate and responsibilities of law enforcement within society.

(1) Data

Predictive policing, as most other new technological tools for the purpose of intelligence and decision-making in law enforcement, is predicated upon data. The production and use of data about crime and crime fighting in law enforcement is, needless to say, not a new phenomenon (Maguire, 2012). However, with the increasingly easy production and availability of large amounts of digital data, novel insights about crime and its social contexts can be crafted from those data and inform law enforcement activities in new and more efficient ways. From an operational point of view, predictive policing rests on the assumption that crime

1 Some involved police departments did, during the research period, use different predictive policing tools that they had developed in-house. Those were, however, similar to PRECOBS with regard to the operational focus on residential burglary, theoretical and conceptual assumptions, as well as data input.

analysis – hitherto carried out manually by specialized analysts – can be algorithmically enhanced in terms of both scale and speed, enabling police departments to discover patterns of criminal activity in time to intervene into still ongoing offenses or serial crime. As a consequence, the timely availability of high-quality data as an input for pattern-detection algorithms is considered a key prerequisite for the estimation of – and intervention into – potential future crime.

Crime data are, however, rather notorious when it comes to accuracy, completeness, and timeliness (Maguire & McVie, 2017). Per definition, there is usually some lack of information about the characteristics of criminal offenses. In the case of residential burglary, initial data created from the crime scene might not yet contain complete information about stolen goods, the ways in which perpetrators gained access to a dwelling, or the time of the offense. Additionally, data creation is prone to error. Evidence at the crime scene might be overlooked, data might be entered sloppily into the database in the late hours of a night shift, or they might accidentally end up in the wrong category (Huey et al., 2021). These variables are, however, important for algorithmic pattern detection that screens for indications of professional serial burglary behavior that would make follow-up offenses likely (Townsley et al., 2003). To amend shortcomings in crime data and render them fit for analysis, there are usually multiple layers of quality control in place that check for inconsistencies such as syntactic errors or missing values (Leese, 2022). Moreover, the availability of information about criminal offences is likely to change throughout an investigation, which is why data need to be updated regularly. In summary, considerable efforts are required to render crime data trustworthy in the first place.

But apart from these practical considerations about the informational value of crime data, there are also some more fundamental concerns about the nature of data that need to be kept in mind when implementing data-driven tools for law enforcement. Data are often believed to be a true and objective representation of the world (Kitchin, 2014). As a consequence from this assumption, it is furthermore believed that if only enough data points were available, new insights about the world could be gained and the future could be modified according to specific preferences (Anderson, 2008). Data do, however, not exist independent of their creation contexts and the technical tools and practices used to produce them (Bowker & Star, 1999). When police officers produce burglary data from a crime scene, for example, they look for specific things that will allow them to describe their findings and fit them into the classification systems that structure police databases. Classification systems are relevant for the statistical processing of data, and as such a key consideration for predictive policing and other forms of crime analysis. As they already pre-structure how crime is recorded, other observations will be discarded and will not end up as analyzable crime data (Harper, 1991). Data must thus always be understood as a partial and filtered account of the world that has been constructed within a particular context and for a particular purpose (Gitelman, 2013).

This means that there is selection bias at work when data about crime and society are created. Such bias is a natural and inevitable part of any dataset and can by definition never fully be removed (Barocas & Selbst, 2016). While this means that bias must to a certain extent simply be accepted, it also means that the limitations of data must be acknowledged and interventions based on data analysis must be put into context. Law enforcement organizations should be mindful that every dataset contains over- and/or underrepresentations of certain empirical phenomena and is in its structure and informational value determined by various technical and social aspects. Importantly, as data are used as input for analytical tools such as predictive policing software, there is a danger that data bias will be perpetuated throughout the analysis and live on in the form of, for example, biased risk estimates (Kaufmann et al., 2019). Data can be a valuable resource for effective and efficient law enforcement in complex and fast-paced environments. However, their social constructedness must be kept in mind when evaluating the 'truthfulness' of data and their representative value. A healthy degree of skepticism toward their objectivity and truthfulness is appropriate, especially when they are acquired from external sources and little is known about the ways in which they were brought into being.

(2) Transparency

Algorithms range on a scale from simple and easily understandable to inherently complex and irretraceable – even for experts and programmers. Usually, the more complex variants are also the more powerful ones, as they are capable of handling large and heterogeneous datasets or even of 'learning' and adapting to new pat-

terns in the analyzed data. But even in comparatively simple and straightforward cases such as predictive policing focused on residential burglary, it can be difficult to understand how exactly crime risk has been computed and how a particular recommendation for action (e.g., "preferentially patrol this specific neighborhood within the next 48 hours") comes into being. The inner workings of complex algorithms are often called 'black boxes', meaning that humans can see the data input and the analytical output, but they can no longer understand the processes that took place in between (Latour, 1999). The likelihood of algorithms becoming black boxes further increases when commercial tools are used, as their design and analytical models are usually considered trade secrets (Pasquale, 2015). In the context of law enforcement, black boxes can have two fundamental implications.

First, they undermine institutional accountability capacities towards the public. Accountability depends on the ability to explain how decisions were made and why specific actions were carried out (Bovens, 2005). When the ways in which data are analyzed are incomprehensible for decision makers, this ability is essentially lost (Bennett Moses & Chan, 2018). A lack of accountability capacities is problematic due to the role of the police in the production and maintenance of social order. Police forces have several exceptional competencies, including the use of force and the interference with individual privacy and intimacy. Such interventions must be carefully justified in terms of their necessity and proportionate nature, which in turn requires the ability to explicate on which knowledge base they have been carried out. In fact, research indicates that police departments are increasingly turning away from the use of commercial predictive policing software and instead focus on the in-house development of predictive policing capacities – with understandability and transparency being cited as major reasons for this development (Leese, forthcoming).

Secondly, black boxes make internal resistance against data-driven analytics more likely. Research has shown that police officers and the larger organizational cultures within which they work are often skeptical towards new technologies in the first place (Manning, 1992). Such skepticism can easily turn into outright resistance when officers come under the impression that their own expertise and professional experience are threatened to be overruled by a technological tool that they cannot understand (Chan et al., 2022). As a consequence, there is a chance that recommendations for action will not be implemented on the ground (Sandhu and Fussey, 2021). In the case of predictive policing, patrol officers have, for example, shown reluctance to actually prioritize risk areas that have been identified through algorithmic crime data analysis. Such reluctance was based on the assertion that they would have better knowledge of their city/neighborhood and the crime risks associated with it than a machine.

In order to align technological capacities with external and internal transparency requirements, law enforcement organizations should thus be mindful that digital tools should always remain as transparent and comprehensible as possible, independent of whether they are commercial products or in-house developments. This will strengthen both the capacity for external accountability and the likelihood of internal compliance.

(3) Automation and control

Predictive policing software and other data-driven analytical tools automate many of the analytical tasks that previously were carried out manually by a human analyst (Perry et al., 2013). In this way, so the general idea, intelligence can be produced much quicker, on a larger scale, and without random error. Automation is thus fundamental for the advantages that data-driven analytics bring for police work. Automation does, however, come with a number of challenges. While the initial hypothesis in engineering and design for human-computer interaction was to implement as much automation as possible to free up human capacities for other, more meaningful tasks, research has over the years shown that too much automation can be detrimental for human capacities and for effective human control of activities outsourced to machines or computer systems (Parasuraman & Manzey, 2010). Moreover, it has been argued that in domain contexts where errors can have wide-ranging consequences, such as for instance nuclear safety or public security provision, automation should by default be delimited (Jones, 2017). Especially this latter point is relevant for law enforcement contexts, as high levels of automation in algorithmic data analysis effectively can entirely remove the human from the process of knowledge production and leave little or no possibility for human intervention in crime analysis, for example to double-check the plausibility of system recommendations or to correct malfunctions or other errors.

In predictive policing, the automation of crime analysis processes through algorithmic means has been shown to facilitate the work of crime analysts due to its potential to relieve humans of repetitive and monotonous tasks. At the same time, police departments have emphasized the need to subject automation to rigid human control in the form of an operator who is set up to be "in the loop". Keeping a human in the loop requires a system to interrupt automated processes at pre-defined points and only to continue when active approval is given by the user. In this way, human awareness of analytical functions carried out by the software is ensured and a possibility to double-check input data and the plausibility of output is granted. This is important in regard to the potential lack of trustworthiness in crime data, but also in regard to issues of bias and accountability discussed above (Cummings, 2006).

Research has shown that police departments ensure control over automated data analysis processes in several ways. Most notably, predictive policing software is exclusively executed by human operators, who in most cases are trained and experienced crime analysts. While fully automated analyses would in theory be possible, an operator is considered a necessary safeguard against faulty data input, system malfunctions, and implausible outputs. Importantly, a human operator is expected to be able to put estimates about crime risks into a larger situational picture and available resources. Other forms of safeguards consist of a four-eyes principle during the review of system output, or checklists that instruct human officers to cross off potential error sources in a systematic fashion before confirming system outputs and forwarding them to local stations for front line implementation.

Given the implications of data-driven knowledge for the ways in which society becomes policed and how resources in public security provision are re-distributed, law enforcement organizations should be mindful that, in principle, full automation of analytical processes by means of technological tools should be ruled out. It is important to carefully configure automation and human oversight in ways that ensure meaningful control at all times. To do so, human analysts must always remain in the loop and have meaningful control over system functions. That means that algorithmic systems must not withhold information from the user or proceed at critical junctions without user approval. Only then will law enforcement agencies be able to benefit from novel analytical insights while at the same time firmly remaining in the driver's seat.

(4) Decision-making

The main implication of data and algorithms in law enforcement is to aid decision-making and planning. The general idea in this context is that more effectiveness and efficiency can be accomplished if the strategic, tactical, and operational level are informed by data-driven knowledge. There is, however, a risk that algorithmically produced recommendations are uncritically followed (Cummings, 2004). The reason for this 'automation bias' is that humans consider technical systems to be objective, neutral, and immune to error. Given the potential error sources in data-driven analytics discussed above, it is, however, key that decisions about the allocation of security provision are not exclusively determined by technological tools.

In predictive policing, initial decisions about the suitability of data-driven crime risk estimates are, as discussed above, made by a human operator who is tasked with plausibility checks of system input and output. Only after human review do forecasts become part of concrete crime prevention schemes. Human review is particularly important in those cases where plausibility conditions are not fully met, for example when input data are incomplete or when identified risk areas do not align with the larger situational picture or the professional experience of operators. In such cases, it is key that humans are encouraged to overrule system recommendations in order not to implement misleading risk forecasts into crime prevention operations and waste resources instead of using them in a targeted fashion. Research has, however, shown that it can be challenging to argue against allegedly neutral and objective system outputs, particularly when counter-arguments are based on non-systematized evidence such as personal experience or a "gut feeling". Moreover, in the domain of security provision, a foundational principle is to rather err on the side of caution than to miss out on the prevention of harm. Consequently, operators tend to approve system outputs even in cases where they do not fully agree.

In order not to go against the rationale of data-driven knowledge, that is, to put resources to use in more effective and efficient ways, law enforcement organizations should thus ensure that operators are put in

a position where they can make informed and responsible decisions. To do so, they should actively be encouraged to engage with all aspects of the analytical process, including the explicit right to overturn algorithmically produced intelligence and recommendations for action. As blind trust in algorithmically produced intelligence and recommendations for action might lead to faulty operational decisions that can undercut the effectiveness of police work and deteriorate the relationship between law enforcement and the public, critical engagement with algorithmic recommendations should be encouraged and the right to override them should be facilitated and institutionally enshrined. More generally speaking, law enforcement organizations should also be mindful that human decision-making is a key assumption in both legal and moral terms, and that automated decision-making would have negative implications for questions of accountability as discussed earlier.

(5) Strategic implications

Whereas the previous themes have mostly highlighted operational quandaries in the use of data and algorithms for law enforcement purposes, there are also important strategic implications that must be considered vis-à-vis such technologies. In light of political discourse, media attention, as well as financial commitments made through procurement and implementation, there is often a perceived need to maximize the utility of predictive policing and other data-driven analytical tools (Egbert & Leese, 2021). This perceived need leads to overemployment, demonstrating to policy-makers and the general public that financial commitments are being put to good use. This can, however, in turn lead to one-dimensional problem perception and corresponding treatment.

Predictive policing tools, for example, have been designed largely on assumptions from environmental criminology and situational crime prevention. Implicitly, these approaches contend that crime is a natural part of human behavior/societal forms of organization and that it can thus be expected that crime will happen by default if not prevented or otherwise intervened into. Operationally, they therefore favor policing approaches built on deterrence by means of increased police presence, environmental modifications, and (technological) means of target hardening. This means that they aim to suppress rather than evaluate why crimes happen and how incentives for criminal behavior could be addressed in the first place (Wilson, 2018). Such a focus rules out questions concerning the root causes of crime and their possible resolution through social reform, as for example found in community policing approaches.

Admittedly, the reasons for the occurrence of crime might often be outside the scope of law enforcement activities. Nonetheless, it is important to keep in mind that technological tools can reinforce particular strategic approaches to crime control while marginalizing others. Data and algorithms should, in this sense, not be used to replace programs of community engagement and larger debates about social reform. For law enforcement organizations, this means that the capacities and limitations of new and emerging technologies must be carefully assessed. Predictive policing software can, for example, be a powerful tool for the efficient use of resources and targeted and effective crime prevention – but outside of these narrow boundaries, it offers little insight into the larger dynamics of crime and society. It should thus remain a complementary tool in the overall toolkit of the police and not be used to suppress or replace long-term strategic programs that address the root causes of crime. Law enforcement agencies should be careful not to overemphasize the role that data-driven analytics can and should play in their work.

Conclusions

This contribution has given a brief, cursory overview of some of the issues that are at stake as law enforcement agencies increasingly integrate data and algorithms into their daily work practices. As has been shown, data-driven knowledge and action reconfigure how the police go about their business and in doing so also affect the role of the police in the production and maintenance of public order and the interface between law enforcement and the general public. The pointers presented here speak to some of the most pressing questions that need to be reflected when integrating new technological tools into security work. The issues discussed here should not be regarded as exhaustive, but rather as representative of some of the most pertinent challenges that police departments faced when dealing with predictive policing software.

The pointers for the responsible use of data and algorithms can both be used as a form of reflection and as a practical guideline. Clearly, the message here is not to not use new technologies at all. On the contrary, it can hardly be denied that law enforcement agencies require updated tools to cope with new challenges in complex and fast-paced environments. The implementation and use of new tools can, however, be understood as a welcome opportunity to further align operational requirements and the protection of democratic rules, civil liberties, and human rights. In this sense, every prototype, every trial run, and every implementation process of a new technology can be seen as a chance to ensure that the use of data and algorithms will not create (unforeseen) detrimental societal effects. Paying attention to the pointers laid out throughout this contribution can serve as a starting point that puts law enforcement organizations in a position to critically assess and reflect how new and emerging technologies can be implemented and used in a responsible fashion. In the end, it should be in the interest of society not to undercut the capacities of law enforcement. But just as well, law enforcement organizations should have a strong interest to respect democratic rules, civil liberties, and human rights.

References

- Anderson, C. (2008) The End of Theory: The Data Deluge Makes the Scientific Method Obsolete. *Wired* (16.07).
- Balogh, D. A. (2016) Near Repeat-Prediction mit PRECOBS bei der Stadtpolizei Zürich. *Kriminalistik* (5):335-341.
- Barocas, S. & Selbst, A. D. (2016) Big Data's Disparate Impact. *California Law Review* 104 (3):671-732.
- Bennett Moses, L. & Chan, J. (2018) Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability. *Policing and Society* 28(7): 806-822.
- Bovens, M, (2005) Public Accountability. In Ferlie E, Lynn L E J & Pollitt C (eds.) *The Oxford Handbook of Public Management.* Oxford: Oxford University Press, 182-208.
- Bowker, G. C. & Star, S. L. (1999) *Sorting Things Out: Classification and Its Consequences.* Cambridge: MIT Press.
- Chan, J., Sanders, C., Bennett Moses, L. & Blackmore, H. (2022) Datafication and the Practice of Intelligence Production. *Big Data & Society* 9(1): 1-13.
- Cummings, M. L. (2004) Automation Bias in Intelligent Time Critical Decision Support Systems. AIAA 1st Intelligent Systems Technical Conference. Chicago, Illinois.
- Cummings, M. L. (2006) Automation and Accountability in Decision Support System Interface Design. *Journal of Technology Studies* 32(1): 23-31.
- Egbert, S. & Leese, M. (2021) *Criminal Futures: Predictive Policing and Everyday Police Work.* London/New York: Routledge.
- Ferguson, A. G. (2017) Policing Predictive Policing. *Washington University Law Review* 94(5): 1115-1194.
- Gitelman. L. (ed.) 2013. *"Raw Data" is an Oxymoron,* Cambridge: MIT Press.
- Harper, R. R. (1991) The Computer Game: Detectives, Suspects, and Technology. *British Journal of Criminology* 31(3): 292-307.
- Huey, L., Ferguson, L. & Koziarski, J. (2021) The Irrationalities of Rationality in Police Data Processes. *Policing and Society* online first: 10.1080/10439463.2021.2007245.
- Jones, M. L. (2017) The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood. *Social Studies of Science* 47(2): 216-239.
- Kaufmann, M., Egbert, S. & Leese, M. (2019) Predictive Policing and the Politics of Patterns. *British Journal of Criminology* 59(3): 674-692.
- Kitchin, R. (2014) Big Data, New Epistemologies and Paradigm Shifts. *Big Data & Society* 1(April-June): 1-12.
- Latour, B. (1999) *Pandora's Hope: Essays on the Reality of Science Studies.* Cambridge: Harvard University Press.
- Leese, M. (2020) Predictive Policing: Proceed, but with Care. *CSS Policy Perspectives* 8 (14).
- Leese, M. (2022) Enacting Criminal Futures: Data Practices and Crime Prevention. *Policing and Society* online first: 10.1080/10439463.2022.2112192.

- Leese, M. (forthcoming) Predictive Policing and Human Rights: The Swiss Case. Amsterdam: Amnesty International.
- Maguire, M. (2012) Criminal Statistics and the Construction of Crime. In Maguire M., Morgen R. & Reiner R. (eds.) *The Oxford Handbook of Criminology*, Oxford: Oxford University Press: 206-244.
- Maguire, M. & McVie, S. (2017) Crime Data and Criminal Statistics: A Critical Reflection. In Maguire, M., Morgan, R. & Reiner, R. (eds.) *The Oxford Handbook of Criminology.* Oxford: Oxford University Press, 163-189.
- Manning, P. K. (1992) Technological Dramas and the Police: Statement and Counterstatement in Organizational Analysis. *Criminology* 30(3): 327-346.
- Parasuraman, R. & Manzey, D. H. (2010) Complacency and Bias in Human Use of Automation: An Attentional Integration. *Human Factors* 52(3): 381-410.
- Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms that Control Money and Information.* Cambridge: Harvard University Press.
- 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: RAND Corporation.
- Robinson, D. & Koepke, L. (2016) Stuck in a Pattern: Early Evidence on "Predictive Policing" and Civil Rights. Upturn.
- Sandhu, A. & Fussey, P. (2021) The 'Uberization of Policing'? How Police Negotiate and Operationalise Predictive Policing Technology. *Policing and Society* 31(1): 66-81.
- Schweer, T. (2015) „Vor dem Täter am Tatort" - Musterbasierte Tatortvorhersagen am Beispiel des Wohnungseinbruchs. *Die Kriminalpolizei* 32 (1):13-16.
- Susser, D. (2021) Predictive Policing and the Ethics of Preemption. In Jones B. & Mendieta E. (eds.) *The Ethics of Policing: New Perspectives on Law Enforcement.* New York: New York University Press, 268-292.
- Townsley, M., Homel R. & Chaseling J. (2003) Infectious Burglaries: A Test of the Near Repeat Hypothesis. *British Journal of Criminology* 43 (3):615-633.
- Wilson, D. (2018) Algorithmic Patrol: The Futures of Predictive Policing. In Završnik A. (ed.) *Big Data, Crime and Social Control.* London/New York: Routledge, 108-127.

AP4AI: Accountability Principles for Artificial Intelligence in the Internal Security Domain

Babak Akhgar
Petra Saskia Bayerl
Centre of Excellence in Terrorism, Resilience, Intelligence and Organized Crime Research (CENTRIC), Sheffield Hallam University, Sheffield[1]

Grégory Mounier
Ruth Linden
Ben Waites
Europol Innovation Lab, The Hague

Abstract
The challenge for internal security practitioners including law enforcement and the justice sector is to determine how to capitalise on the opportunities offered by Artificial Intelligence (AI) and Machine Learning to improve the way investigators, prosecutors, judges or border guards carry out their mission of keeping citizens safe and rendering justice while, at the same time, safeguarding and demonstrating true accountability of AI use towards society. The AP4AI (Accountability Principles for Artificial Intelligence) Project addresses this challenge by offering a global *Framework for AI Accountability for Policing, Security and Justice*. The AP4AI Framework is grounded in empirically verified Accountability Principles for AI as carefully researched and accessible standard, which supports internal security practitioners in implementing AI and Machine Learning tools in an accountable and transparent manner and in line with EU values and fundamental rights. The principles are universal and jurisdiction-neutral to offer guidance for internal security and justice practitioners globally in support of existing governance and accountability mechanisms through self-audit, monitoring and review. This paper presents the project approach as well as current results of the project and their relevance for the internal security domain..

Keywords: Artificial Intelligence, Accountability, Accountability Principles, Internal Security, AP4AI

1 Corresponding author's email: p.s.bayerl@shu.ac.uk.

Introduction

Artificial Intelligence (AI) has become a versatile tool in the arsenal of internal security actors such as law enforcement agencies (LEAs) as it can offer effective means to protect society and save lives, e.g., by improving police performance and efficiencies. It finds application in a wide range of fields such as the pre-processing of unstructured data, machine translation, named entity extraction, image classification, the early detection of unusual patterns (e.g., in the context of cybercrime, child sexual exploitation or counter terrorism challenges), the fast identification of potential threats amongst massive amounts of data points (such as faces in a crowd or the assessments of insider threats) or the deployment of smart autonomous vehicles to secure events or borders. AI can further support strategic forecasting of crime trends. AI capabilities may thus provide crucial support for LEAs across core functions of their work.

At the same time, AI use in the internal security sector also give rise to concerns and fears in some parts of society. Negative societal reactions are often based on a perceived lack of transparency of AI technologies and their usage, as well as fears of biased decision making (e.g., around gender or ethnicity) which may disproportionally affect certain groups in society. Also, a perceived mis- or over-use of AI can threaten the legitimacy of law enforcement efforts. Examples are campaigns such as 'Reclaim Your Face', 'Campaign Against Advanced AI' or even 'Stop Killer Robots'.[2] From a fundamental rights standpoint, scholars and policymakers (EU Commission, 2020) point to potential additional risks of AI use by LEAs, especially to the rights to privacy and data protection, freedom of expression and association, non-discrimination and the rights to an effective remedy and fair trial.

Important legislative processes are ongoing.[3] Yet, practical guidance for internal security practitioners on the best ways to apply evolving norms is still lacking. Also, the question of establishing legitimacy is not made easier by a dearth of governance models focused on AI deployments by internal security practitioners (Babuta et al., 2018).

The solution cannot be to reject AI. Rather solutions are needed which ensure that societal, legal, ethical and operational requirements equally inform and support the potential of AI to enhance LEA and judicial missions and actions. For this to happen, ***a*** *reproducible but adaptive mechanism* is needed to accomplish and sustain this ambition.

The Accountability for AI (AP4AI) Project develops solutions to help internal security practitioners across the full AI lifecycle, i.e., research, design, assessment, review and revision of AI-led applications as well as the evidencing of appropriate AI usage in case of challenges. The solutions aim to be both internally consistent and externally compatible with the respective jurisdictions of widely differing organisations in the internal security domain, while safeguarding AI accountability in line with EU values and fundamental rights. To this end, AP4AI offers a Framework for security and justice practitioners which integrates central indefeasible tenets that, if adopted, will provide practitioners, legal and ethical experts as well as citizens with a high degree of reassurance and redress. In this way, the AP4AI Framework will allow practitioners to capitalise on available AI capabilities, whilst demonstrating meaningful accountability towards society and oversight bodies.

AP4AI objectives and products

AP4AI will deliver concrete products to support internal security practitioners in their deployment of AI:

- A robust set of agreed and validated Accountability Principles for AI, which integrate practitioners' as well as citizens' positions on AI;
- Implementation guidelines and toolkit including supporting software tool to give practitioners and oversight bodies practical, actionable compliance and assessment tools to assess and review AI capabilities from design to deployment;
- Training and policy briefings for the internal security community and oversight bodies on how to apply the AP4AI Framework, as well as broader insights from AP4AI research;

2 Reclaimyourface.eu; https://twitter.com/againstASI; https://www.stopkillerrobots.org

3 The European Commission launched a new 10-year economic strategy, called Europe 2020, to boost European economy and promote a smart, sustainable and inclusive growth, based on a greater coordination of national and European economic policy. One of the main priorities for the EU is to create "A Europe fit for digital age", where the development of trustworthy AI plays a crucial role.

- A set of reports and documentation as reference for the internal security and judiciary community, as well as oversight bodies and the public;

- Engagement with national and EU-funded projects to inform ongoing and future research efforts on AI with respect to AI Accountability needs and applications.

AP4AI partners

The AP4AI Project is jointly conducted by CENTRIC and Europol and supported by Eurojust, the EU Agency for Asylum (EUAA), the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) and the EU Agency for Police Training (CEPOL) and advised by the EU Agency for Fundamental Rights (FRA) in the framework of the EU Innovation Hub for Internal Security.

Why Accountability as guiding principle?

AP4AI focuses on accountability as a guiding standard under the premise that in the field of security and justice, functional AI Accountability is as important as the technology itself. Currently no known efforts exist that address accountability as a process that manages to integrate the complexities of AI applications in the law enforcement and justice sector. There is thus a profound *accountability gap* with respect to societal, organisational, legal and ethical aspects to understand and sustainably manage the complexities of AI in the internal security sector in a way that affords monitoring *and* enforcement towards human-centred AI.

We argue for the primacy of accountability as guiding framework for AI use in the internal security domain as it is the only concept that binds organisations to enforceable obligations and thus provides a foundation that has actionable procedures at its core. The notion of accountability therefore offers vital benefits compared to other instruments and frameworks.

Accountability comprises in itself the three aspects of monitoring, justification and enforcement (Schedler, 1999), and in a legal perspective is defined as the "acknowledgement and assumption of responsibility for actions, decisions, and their consequences" (Thomas Reuters Practical Law, 2021). It thus has at its very core the notion of negotiation across disparate legitimate interests, the observation of action and consequences and the possibility for redress, learning and improvement. The acknowledgement of disparate legitimate interests is of particular relevance for AI capabilities in the internal security domain, where safeguarding one section of society may potentially infringe on rights and freedoms of others.

Accountability is a practical mechanism as it is bound to enforceable obligations and thus actionable. Using AI Accountability as framework hence ensures that legitimate interests (as well as concerns, fears and hopes) of stakeholders are factored in and engaged with throughout the full decision-making process about AI capabilities in the internal security domain. Using accountability as primary lens reinforces an organisation's responsibility to act in accordance with the legitimate expectations of diverse stakeholders and the acceptance of the consequences – legal or otherwise – if they fail to do so. In this context liability, or rather 'answerability', is the basis for meaningful accountability as it creates a foundation for the creators and users of AI to ensure that their products are not only legally fit for the legitimate purpose(s) for which they are deployed but also invite scrutiny and challenge and accept the consequences of using AI in ways that communities may find morally or ethically unacceptable. There is further the responsibility to ensure the avoidance of misuse and malicious activity in whatever form by both the relevant security practitioners and their contractors, partners and agents.

AP4AI approach to accountability

AP4AI's approach to accountability is shaped by two tenets: firstly, *accountability as a process;* secondly, *accountability as a network of mutual obligations.*

1. ***Accountability as a process:*** Accountability can be defined as a responsibility for the fulfilment of obligations towards one or multiple stakeholders, in the understanding that not meeting these obligations will lead to consequences. To create accountability requires several steps from defining what someone (a person, organisation or group) is accountable for and to whom to setting clear parameters by which to measure fulfilment of obligations and linking them to consequences, monitoring progress, dis-

pensing consequences and redressing divergences. Any divergences need to be identified as early as possible, as scholars have rightly claimed that relying on "the big red button" as emergency stop is insufficient (Arnold & Scheutz, 2018). AP4AI, therefore, builds its AI-focused accountability process as procedure parallel to the AI system lifecycle starting from initial idea to the potential decisions for the system's retirement as well as the need to evidence appropriate use. This process perspective ensures that accountability is not a 'one-off exercise' but an ongoing effort of justification, monitoring and enforcement. In this way, accountability becomes solidly embedded into internal security applications of AI from start to end.

2. *Accountability as a network of mutual obligations:* Accountability is a relational concept in that obligations are directed towards particular stakeholders or groups. In a security context, discussions of accountability tend to be focused on police accountability towards citizens. This is insufficient given the complexity and the scale of effects security applications of AI have on individuals, communities, societies and organisations (LEAs and others) as well as on local, national and international levels. AP4AI acknowledges this complexity by extending accountability into a network of mutual obligations. For instance, the ethical and lawful development of AI will need to take into account not only a legitimate expectation that data will be provided by internal security actors as part of the latter's accountability towards civil society, but also situations whereby LEAs dependent upon citizens' data. The creation of such relationships may well carry a legitimate expectation on behalf of internal security actors that citizens will attract some degree of accountability for the data they contribute. Accountability obligations do therefore not only flow from internal security actors to citizens but also the other way around. In the same way, LEA organisations and their personnel have mutual obligations (for example, safeguarding officers' long-term employability on the one hand and adherence to fair procedures in decision-making on the other).

The primary challenge to the implementation of AI accountability in the internal security domain is that there is little clarity on what AI Accountability means in a societal, legal, ethical and operational sense. While organisational accountability in policing is a widely discussed concept (e.g., UNODC, 2011), at present no firm definition of accountability in the context of AI in the internal security domain exists. Also, currently no clear legal definition of 'accountability' in the EU jurisprudence (where it is rather a principle as evident in the GDPR) is available. Unsolved remains further how accountabilities interrelate throughout the process of an AI system's lifecycle including the development of disparate AI tools, applications and platforms for practitioners.

AP4AI offers a definition of AI Accountability by putting forward 12 constituting principles that together describe the scope and content of AI Accountability in the internal security domain.

Defining AI Accountability in the internal security domain: The AP4AI Principles

AP4AI puts forward 12 Accountability Principles which define the requirements that need to be fulfilled to assure Accountability for AI utilisation in the internal security domain. The 12 Principles are the foundation on which all other AP4AI activities and solutions are built. The following list provides the overview of the 12 Principles:

1. ***Legality:*** Legality means that all aspects of the use of AI should be lawful and governed by formal, promulgated rules. It extends to all those involved in building, developing and operating AI systems for use in a criminal justice context. Where any gaps in the law exist, the protection and promotion of fundamental rights and freedoms should prevail.

2. ***Universality:*** Universality provides that all relevant aspects of AI deployments within the internal security community are covered through the accountability process. This includes all processes, including design, development and supply, domains, aspects of police mission, AI systems, stages in the AI lifecycle or usage purposes.

3. ***Pluralism:*** Pluralism ensures that oversight involves all relevant stakeholders engaged in and affected by a specific AI deployment. Pluralism avoids homogeneity and thus a tendency or perception for the regulators to take a one-sided approach.

4. ***Transparency:*** Transparency involves making available clear, accurate and meaningful information about AI processes and specific deployment pertinent for assessing and enforcing accountability. This represents full and frank disclosure in the interests of promoting public trust and confidence by enabling those directly and indirectly affected, as well as the wider public, to make informed judgments and accurate risk assessments.

5. ***Independence:*** Independence refers to the status of competent authorities performing oversight functions in respect of achieving accountability. This applies in a personal, political, financial and functional way, with no conflict of interest in any sense.

6. ***Commitment to Robust Evidence:*** Evidence in this sense refers to documented records or other proof of compliance measures in respect of legal and other formal obligations pertaining to the use of AI in an internal security context. This principle demonstrates as well as facilitates accountability by way of requiring detailed, accurate and up to date record-keeping in respect of all aspects of AI use.

7. ***Enforceability and Redress:*** Enforceability and redress requires mechanisms to be established that facilitate independent and effective oversight in respect of the use of AI in the internal security community, as well as mechanisms to respond appropriately to instances of non-compliance with applicable obligations by those deploying AI in a criminal justice context.

8. ***Compellability:*** Compellability refers to the need for competent authorities and oversight bodies to compel those deploying or utilizing AI in the internal security community to provide access to necessary information, systems or individuals by creating formal obligations in this regard.

9. ***Explainability:*** Explainability requires those using AI to ensure that information about this use is provided in a meaningful way that is accessible and easily understood by the relevant participants/audiences.

10. ***Constructiveness:*** Constructiveness embraces the idea of participating in a constructive dialogue with relevant stakeholders involved in the use of AI and other interested parties, by engaging with and responding positively to various inputs. This may include considering different perspectives, discussing challenges and recognising that certain types of disagreements can lead to beneficial solutions for those involved.

11. ***Conduct:*** Conduct governs how individuals and organisations will conduct themselves in undertaking their respective tasks and relates to sector-specific principles, professional standards and expected behaviours relating to conduct within a role, which incorporate integrity and ethical considerations.

12. ***Learning Organisation:*** Learning Organisation promotes the willingness and ability of organisations and people to improve AI through the application of (new) knowledge and insights. It applies to people and organisations involved in the design, use and oversight of AI in the internal security domain and includes the modification and improvement of systems, structures, practices, processes, knowledge and resources, as well as the development of professional doctrine and agreed standards.

Together the above AP4AI Principles constitute a universal, empirically validated Framework for AI in the law enforcement and justice sector to fundamentally assess and enforce legitimate and acceptable usage of AI by the internal security community.

Development of the AP4AI Principles

The principles were developed in an exploratory 'bottom-up' manner. This means principles were identified and refined by engaging directly and intensely with the people who are either using, designing, regulating or are affected by AI in an internal security context, i.e., practitioners in the security, policing and justice domain, oversight bodies, law makers, industry, researchers and research institutions, as well as citizens.

The project is conducted in three cycles which are implemented as consecutive steps for the exploration, integration and validation of findings. The sequential approach was chosen to ensure the robust development and validation of the AP4AI Framework and products. The three cycles are:

- ***Cycle 1 – Development of the AP4AI Principles (completed):*** The first cycle consisted of two activities: (a) a review of existing frameworks aiming to guide or

regulate AI and (b) expert consultations with subject-matter experts from law enforcement, justice, legal, fundamental rights, ethical and technical fields identified by the AP4AI partners. Results of the expert consultations are reported in the *AP4AI Summary Report on Expert Consultations* (Akhgar et al., 2022a).

- ***Cycle 2 – Citizen consultation for validation and refinement of the Principles (completed):*** An online consultation was conducted in 30 countries (all 27 EU members states, UK, USA and Australia, resulting in answers from 6,774 participants) to collect citizen input on the AI Accountability Principles developed in Cycle 1, as well as insights into possible accountability mechanisms. A blueprint was published on the basis of the results, including preliminary results of the citizen consultation (Akhgar et al., 2022b).

- ***Cycle 3 – Expert consultation for validation and contextualisation of the AP4AI Framework (ongoing):*** The AP4AI Framework goes through continued validations by subject matter experts using structured feedback collection, hands-on implementation workshops, as well as case creation for the operationalisation of the Framework into practice.

AP4AI was from the start conceptualised with an international focus. The international focus is required as AI use in the internal security domain – whether at practitioner or citizen level – is strongly affected by the national contexts in which AI capabilities are deployed. The project has so far brought together expertise from experts and citizens across 32 countries.

The chosen methodology, which integrates security, legal, ethical as well as citizens' perspectives by design, allows AP4AI to develop a robust and application-focused Framework that offers a step-change in the application of AI by the internal security community.

High-level view on AP4AI implementation

From the outset, the AP4AI Project aimed at translating the Accountability Principles (as the conceptual representation of AI Accountability requirements) into actionable steps and processes in support of internal security practitioners. This translation step into guidance for practical application is the second core element of the AP4AI Framework. To this end, each of the 12 Principles has been contextualised for AI deployments within the internal security domain, providing legal and practical consideration, as well as examples (see section on *'Principle-specific guidance'*). The tangible realisation of the Principles is demonstrated through the provision of an implementation container – the *AI Accountability Agreement* – which will serve as a universal mechanism for the implementation of the principles. It further offers concrete accountability narratives that will permit flexibility for local implementations at the organisational level.

AI Accountability Agreement (AAA)

AP4AI advocates for an *AI Accountability Agreement (AAA)* that specifies formal and implementable processes for the implementation of the Accountability Principles for different applications of AI within the internal security domain.

An AI Accountability Agreement (AAA) should be viewed as a social contract underpinned by legal obligations between internal security organisations and its stakeholders including citizens, oversight bodies, suppliers, consumers of AI services (e.g., other agencies) and others, as applicable. The AAA should address all AP4AI Principles and their realisation in an operational setting for the specific application of AI. The AAA can thus be understood as an implementation container or reference architecture, which drives the implementation of the 12 Principles in a practical and operational setting within internal security organisations. It hence serves as a mechanism to bring the abstract nature of the Principles into the implementable environment of internal security organisations and their wider ecosystem (e.g., oversight bodies and government agencies).

Every AAA should clearly set out and formalise the following four steps:

1. The accountability must-haves (non-negotiables), should-haves and could-haves within the specific application of AI;

2. Definition of who will be Responsible, Accountable, Consulted and Informed (RACI index) in relation to each of the AP4AI Principles for each application of AI and who has been Consulted and Informed about the purpose and development of the AI application (with a summary of what they have said);

3. The materiality thresholds and tolerances to allow for practical variance (dates, changes in personnel, etc.), the range of acceptability and for assessing the proportionality of disclosure, consultation, and publishing of information;

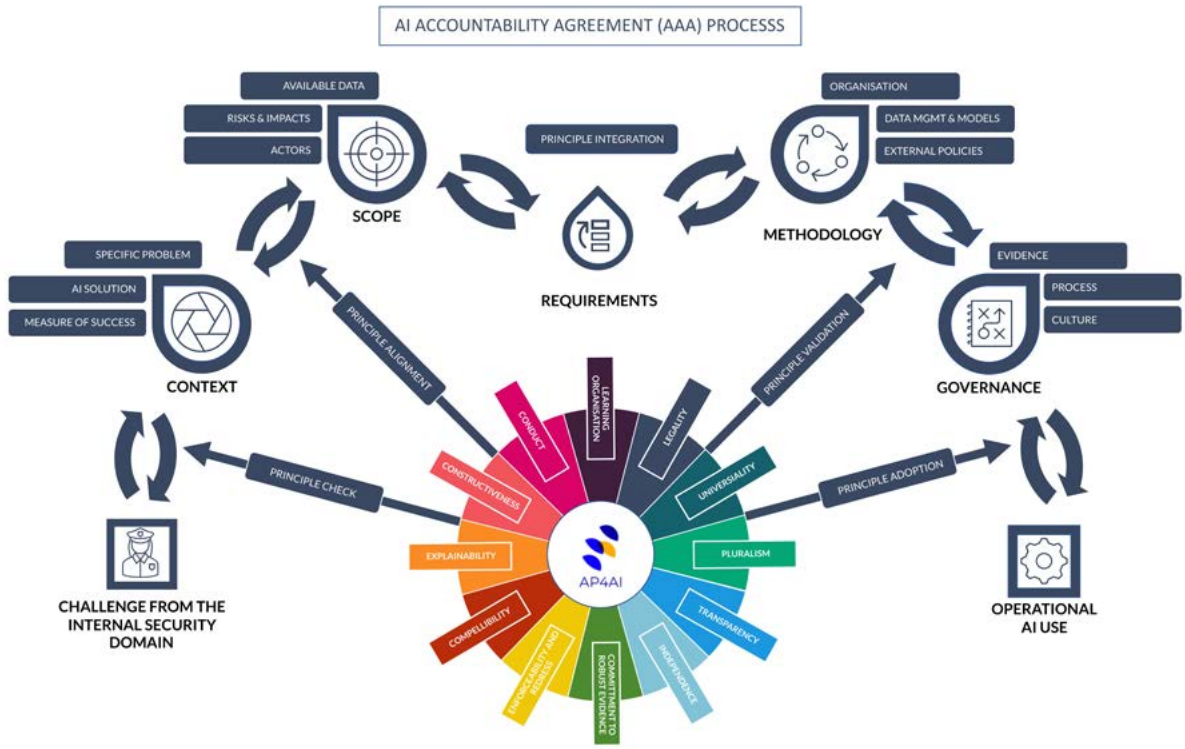
4. The process that must be followed before making any variation to the specific application of AI.

In order to pave the way for the implementation of the 12 Accountability Principles, AP4AI utilises the concept of Materiality. *Materiality* is an assessment of the relative impact that something may have on accountability within the context of an application of AI in the internal security ecosystem. Materiality allows to set *materiality thresholds,* i.e., impacts below which AI Accountability processes may be required only to a limited extend or not at all. Material thresholds acknowledge that the material importance and impact of a specific AI capability or application will very much depend on the nature of the AI project (e.g., automating the logistics of ordering police uniforms versus calculating potential re-offending of a person to inform a bail decision).

The AAA is designed to be created and validated prior to any programme of work that encompasses the application of AI. Each application of AI involves one or more stages of the AI lifecycle: scoping, planning, research, design, development, procurement, customisation, deployment, modification, maintenance and decommissioning. It can also be employed for evidencing the appropriate use of AI capabilities in case of challenges.

To achieve this, the AAA must include, as a baseline, the four components: *context, scope, methodology,* and *accountability governance*. Each phase in the AAA should adopt the application of all 12 Principles and use them as a milestone to progress to the next stage. Figure 1 gives an overview of the stages involved in the development of an AI Accountability Agreement.

Figure 1. Stages of development for an AI Accountability Agreement (source: Akhgar et al., 2022b)



Principle-specific guidance

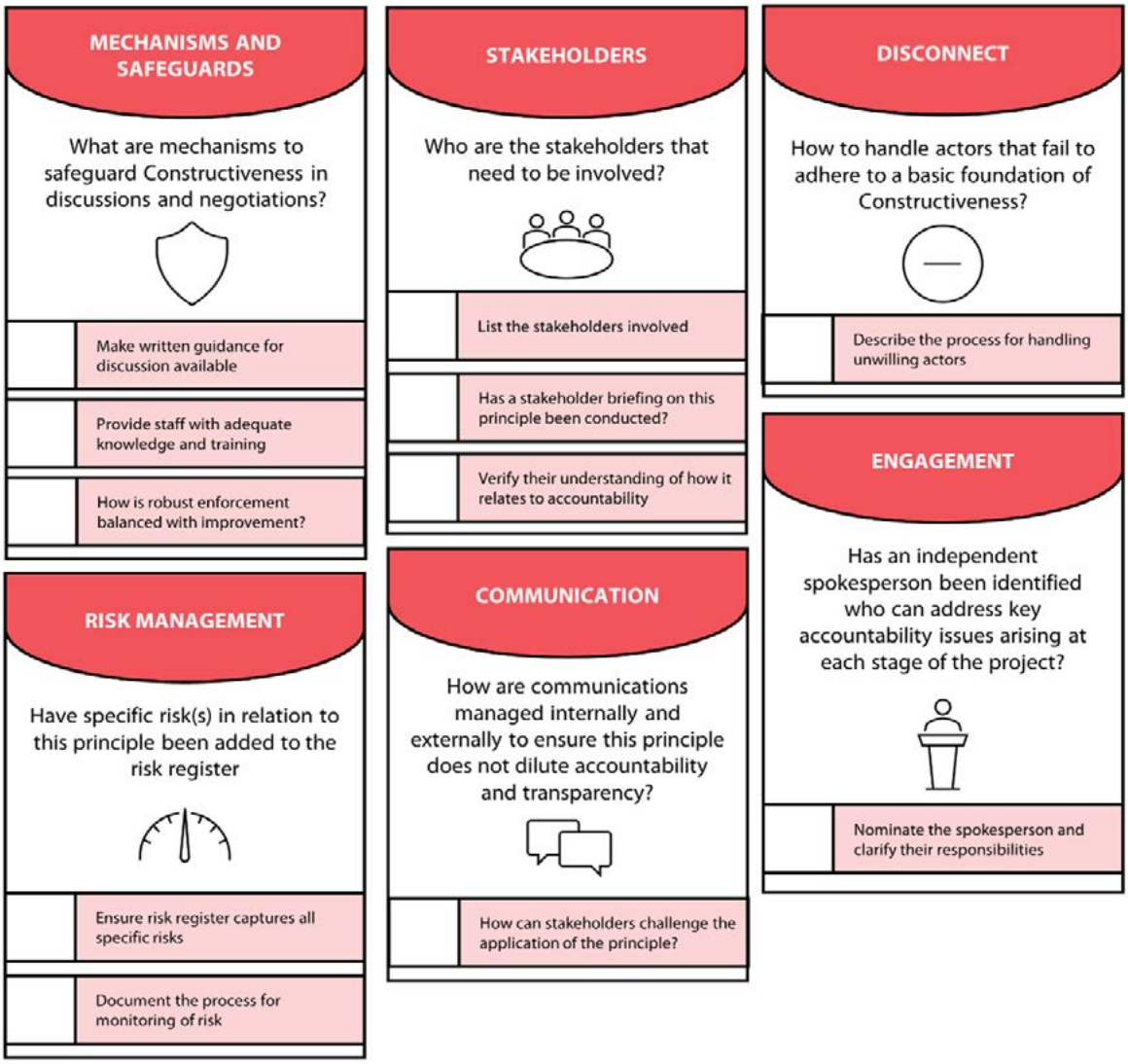
Next to the AAA as overarching mechanism, AP4AI further provides structured, semantic representation guidance on each of the individual Accountability Principles. The template used to present each principle consists of eight elements which collectively provide the core requirements for its implementation. The template is designed in a way that it can be extended and refined throughout the AP4AI Project yet maintain its conceptual foundation which is grounded in the evidence-based research conducted previously as well as the input from expert and citizen consultations described above. The granularity (e.g., set of purposeful questions) and visual representation of the 'implementation guide' for each principle supports the development of practical guidance and application mechanisms such as a dedicated software tool.

In detail, the guide consists of the following elements for each Principle:

- ***Name:*** principle name
- ***Meaning:*** provides the principle's definition contextualised for AI and the internal security domain
- ***Materiality threshold:*** offers an assessment of the relative impact that something may have on accountability within AI development or utilisation
- ***Examples of applicable law:*** lists examples of applicable law pertinent to AI Accountability in the internal security domain
- ***Note on Human Right Impact Assessment (HRIA)***: provides an initial direction for HRIAs and alerts the reader about the pivotal role of HRIAs in the context of AI Accountability Principles
- ***Note on Data Protection Impact Assessment (DPIA, where applicable)***: alerts the reader to legal and ethical requirements of conducting a DPIA and, where applicable, a Privacy Impact Assessment (PIA)
- ***Implementation guide:*** identifies the processes, activities, tasks, documentations, assessments, actions and communication needed for the realisation of the principle
- ***Operational considerations:*** provides clarification and further consideration about implementation of the principles for the operational environment

Figure 2 provides an example of the implementation guide and operational considerations for the principle "Constructiveness".

Figure 2. Illustration of the implementation guide and operational considerations for the Constructiveness principle (source: Akhgar et al., 2022b)



Operational considerations: It may be useful to pre-emptively document how particular issues will be dealt with, for example, who is accountable for fixing critical flaws in the AI system should they occur. Security practitioners and oversight bodies should have mechanisms and resources in place to ensure a constructive outcome is given in a reasonable time period.

Next steps and outlook

The main aim of the AP4AI Project is to offer concrete and practical tools that support LEAs and justice practitioners in assessing and evidencing the accountability of current and future AI capabilities as well as to enrich ongoing policy and legal discussions.

Our currently ongoing work focuses on:

- Further validation and instantiation of the AI Accountability Agreement using real examples and challenges of internal security practitioners;
- Extension of use cases and application scenarios for AI deployments (most critically CSE/CSEM, cyber-dependent crime, serious and organised crime activities including cross-border issues, harmful internet content such as terrorist generated internet content, protection of public spaces and communities, terrorism related offences, financial crime, procurement of AI solutions by internal security practitioners, research and development for AI either by the internal security actors or a third party intended to create the solution to be deployed for the internal security domain);

- Development of a software application as a supporting mechanism for the implementation of AP4AI;
- Input into ongoing policy and legal discussions.

Conclusions

The AP4AI Project is guided by an enabling philosophy. The fundamental premise which drives AP4AI and its outcomes is that AI is a critical and strategic asset for internal security practitioners. It thus aims to support internal security practitioners in the appropriate and legitimate management of AI capabilities, both before and during AI deployments.

The AP4AI Framework is specifically designed for security and justice practitioners, including LEAs, and offers validated AI Accountability Principles as a fundamental mechanism to assess and enforce legitimate and acceptable usage of AI. The AP4AI Project has the ambition to become a globally known standard of quality for the research, design, development and deployment of accountable AI use in the internal security domain.

The core foundation of the AP4AI Project is that of policing by consent whereby the burden of trust as a mutual obligation between police and society is enshrined within the notion of accountability. The challenge for internal security practitioners is how to capitalise on new technological capabilities that derive from AI in response to societal expectation and demands while, at the same time, demonstrating true accountability and compliance, assuaging societal concern at the use of advanced technology such as AI and automated processing. AP4AI aims to offer solutions to this complex issue for organisations within the security and justice sector.

Acknowledgements and funding

We are grateful to the experts and citizens, who have generously given their time and input to AP4AI. No specific funding from external funding agencies or funding bodies has been received for the project. The research outcomes, the opinions, critical reflections, conclusions and recommendations do not necessarily reflect the views of authors' organisations. The project received ethics approval by the university ethics board of Sheffield Hallam University, where CENTRIC is located as academic lead of the AP4AI Project.

References

- Akhgar, B., Bayerl, P.S., Bailey, K., Dennis, R., Heyes, S., Lyle, A., Raven, A., Sampson, F., & Gercke, M. (2022a) AP4AI Report on Expert Consultations.
  Available at: https://www.ap4ai.eu/node/6
- Akhgar, B., Bayerl, P.S., Bailey, K., Dennis, R., Gibson, H., Heyes, S., Lyle, A., Raven, A., & Sampson, F. (2022b) AP4AI Framework Blueprint.
  Available at: https://www.ap4ai.eu/node/14
- Arnold, T. & Scheutz, M. (2018) 'The "big red button" is too late: An alternative model for the ethical evaluation of AI systems', Ethics and Information Technology, 20, pp. 59–69. https://doi.org/10.1007/s10676-018-9447-7
- Babuta, A., Oswald, M. & Rinik, C. (2018) 'Machine Learning Algorithms and Police Decision-Making Legal, Ethical and Regulatory Challenges', Whitehall Report 3-18, RUSI.
- EU Commission. (2020) White Paper on Artificial Intelligence: A European Approach to Excellence and Trust.
  Available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf
- Schedler, A. (1999) 'Conceptualizing Accountability', in: Schedler et al. (eds), The Self-restraining State: Power and Accountability in New Democracies (pp. 13-28).
- Thomas Reuters Practical Law (2021) Accountability Principles.
  Available at: https://uk.practicallaw.thomsonreuters.com/w-014-8164
- United Nations Office on Drugs and Crime (UNODC). (2011) Handbook on Police Accountability, Oversight and Integrity. Criminal Justice Handbook Series. United Nations Publishing, New York.
- More information
  Project website: https://www.ap4ai.eu
  Twitter: @ap4ai_project

North American Policing in the Digital Age

Maria R. Haberfeld
John Jay College of Criminal Justice, New York, N.Y.

Abstract
This article addresses the varying levels of training preparedness and legal challenges facing the American local law enforcement agencies in the Digital Age. From the example of the New York City Police Departments' multiple units like: the SMART Unit (Social Media and Research Team), Real Crime Unit, Domain Awareness and Vehicle Recognition Unit to the overview of the majority of smaller police departments that have very limited, if any, type of preparedness. The majority of police departments in the United States are staffed with less than 50 sworn officers and the Digital Age policing challenges are numerous and addressed in a very uneven manner. However, the larger departments, like the N.Y.P.D., can provide a template for a more professional and effective response. Finally, in addition to the different modalities of numerous tactical responses embedded in the creation of the specialized units, there are challenges related to the legal aspects of these initiatives. Some of the legal challenges facing the specialized unit are discussed, focusing on the hurdles in obtaining legal subpoenas for the information posted on various social media platforms like the Instagram, Facebook and Snapchat. A template for proper proactive preparedness concludes this overview.

Keywords: Digital policing; North American policing; preparedness; digital interoperability; tactical response

Introduction

Policing in the 'Digital Age" is a somewhat obsolete concept in the year 2022. According to Goodwin (2016), the digital era, in all business like environments (which would include policing as well) commenced over a decade ago and right now we actually seem to be well immersed in the mid-digital environment. Goodwin further identifies three distinct stages of digital development:

- *Pre-digital age* – At first, the pre-digital age evolved slowly. Products became digitized. Photos became bits. Knowledge moved from encyclopedias to Wikipedia. The phone book became an online directory. Printed magazines became websites. This first age was all about physical products becoming digital. It led to creative destruction in retail, manufacturing and distribution, which is where we are now: the mid-digital age.
- *Mid-digital* – This is a period that straddles the age where digital is just becoming accepted into the mainstream, and the age where digital is fully immersed into our society.

- *Post-digital* – Like pre-digital, nobody will think of "digital" in this age. The concept of it will move into the background and, much like oxygen or electricity, we'll understand digital to be transformative yet irrelevant. There will be no more Chief Digital Officers in the same way that a Chief Electricity Officer doesn't exist today. In the post-digital age, digital technology will be a vast, quiet element forming the seamless backbone of life. The internet will be a background utility, noticeable only in its absence. Smart homes will work. Video will follow us around. Content will be paid for… all seamlessly and effortlessly (Goodwin, 2016).

Based on the fact that these developmental stages were identified by Goodwin over eight years ago, I would argue that we are past the mid-digital stage and well into post digital. Thus, looking at police organizations one needs to ponder if the departments themselves realize that they might be late into the game that started over a decade ago.

This article provides a brief insight into the level of preparedness of some of the 18,000 North American police departments, ranging from the largest, the New York City Police Department, to the smaller ones, with less than 50 sworn officers, while the latter truly represent the average size of a police department in the United States.

Research Questions

While looking at the concept of policing in the digital era, one needs to ponder what kind of research questions we need to answer to arrive at the conclusion regarding the level of preparedness of various law enforcement agencies. Lack of proper operationalization of complex phenomena goes back decades ago, when researchers started to look at cyber criminality and law enforcement ability to respond in a timely and proactive manner.

Going as far back as over four decades ago, Kupperman & Trent (1979) argued that the problem with technological terrorism has generally been ignored and that the United States government is woefully under-prepared to deal with a technological threat. Following their premonition into the year 2022, I posit that there are a number of vital research questions that need to be addressed, in order to arrive at a realistic picture of the level of proactive response of the American police forces.

These research questions are divided into two categories, one with a more general focus and the other centers on actual case studies. The case studies provide a perfect backdrop for understanding of the challenges facing American law enforcement.

- Digital age policing can be divided into crime challenges and, on the other end, preparedness and response - do these two align?
- Since January 2022 over 7000 shooting deaths with 197 mass shootings took place while at the same time 847,376 complaints of cyber-crime were recorded by American police forces, based on the latter, what are the local police departments' challenges/priorities?
- Case study 1: Hudson County, NJ: need versus response – do they align?
- Case study 2: New York State: size versus capabilities – do they align?

Understanding United States Law Enforcement Agencies

In 2016, there were about 100,000 full-time federal law enforcement officers in the United States and U.S. territories who primarily provided police protection. 701,000 full-time sworn officers served in general-purpose state and local law-enforcement agencies nationwide. However, in 2022, in the aftermath of over two years of some extremely negative coverage of the police profession (Haberfeld et al, 2022), less than 690,000 remained in state and local agencies, with some projections that these numbers will decline throughout the year, American law enforcement is struggling with recruitment of new officers while experiencing an unprecedented decline in the numbers of its sworn officers (Young & Sayers, 2022).

An insight into the Decentralized Nature of the American Police from NYPD to Chester, NJ from In-house to Outsourcing

A quick peak into the way digital crime is handled in American law enforcement. Depending on the jurisdiction and any of the 50 states, the following entities may be designated as the lead investigative agencies:

- Prosecutors Office
- FBI
- Attorney General
- Homeland Security

- Joint Terrorism Task Forces (JTTFs)
- Fusion Centers
- And so many more, including local police departments, the ones that have the capacity to investigate, which are primarily the larges agencies only, like the NYPD (LEMAS, 2016).

Increase in Digital/Cyber Crimes

- The majority of first response is still in hands of the municipal police departments – that outsource the investigations into state and federal agencies

YET

- As the number of cyber-crimes increase the federal and state agencies cannot handle the increase

According to the FBI's Internet Crime Report 2021, a record 847,376 complaints of cyber-crime were reported to the FBI by the public, a seven percent increase from 2020. The Federal Trade Commission's (FTC) Consumer Sentinel Network took in over 5.7 million reports in 2021 of which 49 percent were for fraud, and 25 percent for identity theft (Federal Bureau of Investigations, Internet Crime Complaint Center, 2022).

From Guttenberg Police Department to Jersey City Police Department: A Tale of Two Cities yet very similar approach

Guttenberg, New Jersey Police Department, is a local Police Department in the State of New Jersey, an independent entity, with 22 full time sworn officers, 8 full time civilians and 17 part time civilians (Guttenberg Police Department, 2022). In contrast to one of the largest police department in the State of New Jersey, Jersey City Police Department with its 975 uniformed officers 200 crossing guards, and 200+ civilian employees dedicated to the safety of Jersey City's residents and visitors (Jersey City Police Department, 2022). Despite clear difference in the size of the departments the way both handle digital crimes is identical – through outsourcing. Both departments reside in the New Jersey Hudson County, where the approach to digital crime is pretty much uniform through the outsourcing of the investigations to the Hudson's County Prosecutor's Office (Haberfeld, 2022).

I interviewed a detective from the Hudson County Prosecutor's Office to obtain a realistic insight into the way digital crimes are investigated in the field. The following bullet points summarize the information collected (Haberfeld, 2022).

- NJ county prosecutors oversee major crime investigations
- There are 22 Police Departments in Hudson County, New Jersey, serving a population of 679,756 people in an area of 47 square miles. There is one Police Department per 30,898 people, and one Police Department per two square miles (Police Departments in Hudson County, 2022).
- The Prosecutor's Office receives referrals from other police departments in the County. Following the information received detectives access, externally, suspects Instagram/Facebook accounts. The law enforcement officers open fake profile accounts, sometimes friend the suspect. Needless to say that these investigative tactics lead to legal challenges, when the cases end up being prepared for the prosecution.
- No warrants are needed to access the suspects account, similar to the American legal doctrine: 'in plain view' (Legal Information Institute, 2022).
- In the case of parallel investigations in a number of interrelated cases and when there is a probable cause to suspect a more intricate investigation, detectives petition the court for "communication data warrant " which allows them to extract all the information from suspect's profile like: chat messages, videos, photographs, etc., as well as all the data related to the IP addresses, where the illegal images come from. The challenges involved in obtaining these warrants are numerous (JD Supra, 2022).
- The next step involves the location of the alleged victims, providing that these actions reach a level of criminality, the challenges here are, primarily, related to the willingness of the alleged victims to cooperate to enable the detectives to apply for an arrest warrant.
- In case the alleged victims do not provide enough support to apply for an arrest warrant, the next step is to initiate a meeting with the suspect which, once again, can lead to legal challenges and accusations of entrapment (United States Department of Justice, 2022).
- An example of a complicated case included a pervasive distribution of sexual images, which according to the detective constitute a bulk of under reported crimes. These cases are investigated once or twice a month just in one unit. Subsequently, the victims are lured to unknown locations. One such case involved a 14 years old, who was developmentally challenged. The alleged perpetrator sent an Uber to bring him to his location, he befriended the victim through a contact on the Instagram. The family intercepted this communication, called the JCPD, which immediately referred the case to the Prosecutor's Office. According to the detective: "They (the Jersey

City Police Department) just don't have the tools. Assistant prosecutors have to handle it." (Haberfeld, 2022).

- Finally, the detective pointed out that in the last few years there is a huge learning curve facing the investigators, especially when it pertains to forensic crime training: "…they have to catch up on learning all about how to conduct the investigation and then the technical aspects... (Haberfeld, 2022).

From the NYPD to the Sodus Point Police Department

In the neighboring state, the New York State, the digital crime phenomena is handled slightly different depending, once again, on the size of the department. As unusual as it may sound, the Sodus Point Police Department, an independent and one of the almost 600 autonomous and independent police departments in New York State, is comprised of 1 full time police officer, 3 part time officers and a civilian (Sodus Point Police Department, 2022). On the other end of the spectrum, still within the same state of New York, the New York City Police Department (NYPD) is the largest and one of the oldest municipal police departments in the United States, with approximately 36,000 officers and 19,000 civilian employees (New York City Police Department, 2022).

The NYPD is divided into major bureaus for enforcement, investigations, and administration. It has 77 patrol precincts with patrol officers and detectives covering the entire city.

The department also has 12 transit districts to police the subway system and its nearly six-million daily riders, and nine police service areas (PSAs) to patrol the city's public housing developments, which are home to more than 400,000 residents.

Additionally, uniformed civilians serve as traffic safety agents on the city's busy streets and highways, and as school safety agents, protecting public schools and the over-a-million students who attend them (New York City Police Department, 2022).

Needless to mention that the Sodus Point Police Department does not handle its digital crime problems. However, the NYPD created a remarkable response to the ongoing and increasing rate of web related criminality.

The New York City Police Department in the Digital Age – a Template for Success

Real Time Crime Center and the S.M.A.R.T. UNIT

- Real Time Crime Center is a centralized, technology-driven support center which uses state-of-the-art technology, such as facial recognition and link-analysis software, to provide instant, vital information to detectives and other officers at the scene of a crime.
- T.A.R.U. – Tactical Response – technologically advanced support unit.
- The Social Media Analysis & Research Team (S.M.A.R.T.) analyzes social media for chatter, videos and relative information in regards to active investigations.
- The SMART unit also identifies patterns and trends on social media such as bullying, gang activity, and types of crimes and translates the information into useable intelligence for patrol officers in the field.
- SMART also collects and memorializes this information as evidence in police investigations. The unit also offers presentations to agencies and the public on the dangers and uses of social media (NYPD, 2022).

The S.M.A.R.T. Unit as a Tactical Template

Based on a thorough overview of the NYPD's tactical response to the digital crimes, it is recommended that other law enforcement departments adopt the S.M.A.R.T. units as their tactical template. The benefits of this approach are summarized below.

- Every shooting and/or gang related activity reported by detectives from each precinct is referred to S.M.A.R.T. This approach allows for a tactical alignment of, otherwise, dispersed criminal patterns.
- This approach allows for identification of digital footprints and the interrelated connections.
- In addition, this approach allows for alignment of information and proper connections between different investigative units.
- Further, it creates a mechanism of effective internal information dissemination to other units, that might otherwise be not informed.
- The above approaches lead to the elimination of the proverbial "linkage blindness" that plaques American law enforcement agencies, almost from their inception (Brown, 2018).

How is the knowledge disseminated?

One of the most critical issues that needs to be addressed in order to enhance law enforcement agencies' abilities to face, target, and effectively respond to digital crimes is directly related to the way knowledge about this phenomenon is disseminated to the smaller and less technology savvy and adapted agencies. A White Paper disseminated by Officer.com website, one of the American law enforcement publications (not peer reviewed but popular with law enforcement audience) identifies the following challenges facing policing in the era of digital criminality:

- Digital evidence has become an integral part of today's criminal investigations.
- As agencies struggle to adapt to growing volumes and complexity of digital data, a new paradigm for digital investigations is emerging – one that leverages a modernized approach to fuel greater collaboration at all levels. When agency teams are able to work together more effectively, the quality and speed of their investigations can be greatly improved.
- The digital evidence review process can be accelerated by empowering investigators and other stakeholders to collaborate on evidence review securely in real-time, regardless of their physical location, and with tools designed to help them easily find the evidence that matters across a variety of sources. (Officer.com, 2021.)

Police Chief Magazine 2022 – Awareness is there but not the Implementation

Police Chief Magazine, a widely disseminated official publication of the IACP (International Association of Chiefs of Police), is yet another example of awareness to the problem but, not necessarily a solution to the field implementation, as the membership in this association is voluntary and only a fraction of American police executives holds membership in this organization and is exposed to its recommendations (Haberfeld, 2018). Nonetheless, in its May 2022 issue the publication recommends the following steps to be taken by law enforcement agencies to better prepare them for the ongoing challenges of digital related crimes:

- Traditional Public Information Offices must evolve into aligned, strategic Communications Operations
- Agencies need to get in front of Facial Recognition
- Agencies need to make more use of remote Drone Dispatch
- Agencies need to address the opportunities and challenges of Intelligent Emergency Response (Police Chief Magazine, 2022).

Recommendation: In-house versus the Outsourcing Approach

Upon the review of the responses to digital policing challenges, I would recommend the following steps police practitioners and agencies should consider to enhance their proactive capabilities and capacities in the era of digital policing:

Interoperability – critical in the age of digital policing.

Interoperability became a buzz word in the aftermath of 9/11. Many practitioners and academics used in term to denote lack of proper cooperation between law enforcement agencies, especially in the field of technology. Prior to 9/11 law enforcement agencies in the US operated their radio communications, using different frequencies which, in turn, prevented them from communicating effectively during times of crises. The 9/11 Commission identified this problem as one of the failures of first responders (Falkenrath, 2004). Over twenty years later, the implementation of the 9/11 findings is still sporadic which, in turn, creates a larger challenge in the fight against web based crimes where speedy communication between agencies can make a real difference in the apprehension of criminal actors and disablement of their networks.

An in house unit – allows for proper sharing and connectivity

An in house digital crimes investigative unit, while part of the overall structure of any given department, can quickly and effectively share the information on the intranet of the organization and thus enable other internal units to make the connections between the investigated crime and other reported crimes that are currently not classified as internet related.

When you outsource you miss the connections to other serious crimes from Organized Crime to terrorism

Related to the above bullet point, the concept of outsourcing internet based crimes makes it much harder to identify the relevant connections to other serious crimes investigated by other units within the police organization like the Organized Crime and Counter Terrorism. These units are frequently stand- alone units

that suffer from what is referred to as organizational "linkage blindness" (Sheptycki, 2004).

An in house unit mandates better and ongoing training

As one of the detectives interviewed for this article mentioned, training for digital crime investigations is a huge curve and challenge for many police officers, especially the ones from the smaller police departments where in-service training is rare and usually related to some high profile organizational failure (Haberfeld, 2018). An in house unit would advance the concept of a more frequent and updated training, especially in the knowledge area that changes so frequently and rapidly.

The danger of leader technology illiteracy, and the importance of embracing new ideas in a more proactive rather than reactive manner

Related to the previous bullet, technological illiteracy, from the top of the organizational pyramid up to the specialized investigators, can only be addressed properly in an in house unit as the inability to effectively investigate serious crimes has a direct impact on the clearance rate of a given organization. In the era of laser focus on police effectiveness, the clearance rate becomes even more critical for police executives and the probability of approval of the more proactive and innovative ideas increases contemporaneously with the increase of internet based crimes.

Establish specialized units in larger police departments

Although the idea of having specialized units that are capable of effective investigations of digital crimes is a tempting one, in reality only the large police department can afford to establish them. However, "larger police department" term needs to be re-evaluated in terms of the actual staffing numbers. It is probably wise to recommend that each unit that exceeds 100 sworn officers should consider creating a specialized digital investigations bureau.

Digital crimes are no longer a domain to outsource

As the internet crimes increase in volume, in a manner that is highly disturbing, the idea of not been able to investigate these law violations within the police organization is no longer acceptable and appears to be obsolete. The times when internet related crimes were rare occurrences are long gone.

Need to adapt to crime patterns that are increasingly cyber related

Embracing the seriousness, intensity and scope of the new crime patterns is an obligation of any police executive who wants to be not just proactive in the response to crime patters but, first and foremost, up to speed with the daily reactive realities.

Change in recruitment and training need to be considered, it is possible that we need more technologically savvy officers than ones who can do a certain number of pushups in a minute.

While police training in the United States remains far behind many of its counterparts around the world, and while the calls for reduction of standards for recruitment, selection and training become more of an ongoing theme, the numerous police oversight bodies need to rethink the tactical and operational needs of the local police departments and their capabilities to respond effectively to the digital crimes phenomena.

Into the future

From the overview of the state of American Policing in the past few years, it appears as if police departments are focused more on Police Community relations rather than the digital age threats and challenges, this approach needs to change before it is too late.

It appears that moving into the proactive approach by tomorrow is a misguided approach that is probably already too late to be able to deliver any effective response. I would posit that, actually, even today might be too late! Although not all of the research questions posed at the beginning of this article were fully answered, the critically of a proper response has been established.

Borrowing from Goodwin's (2016) advice to businesses owners it appears that adapting his concept for law enforcement agencies is the savvy way to move into the future:

"*…as we move from the mid- to the post-digital era, the advice is simple. Prepare for eventualities. Ensure that your business is culturally prepared for what's to come. Consider extremities. Be aware of the bleeding edge. Leave nothing off the table ….*" (Goodwin, 2016.)

Figure 1. Introducing the P.E.C. approach to the era of Digital Policing

Time is of essence, this old adage cannot be more relevant than when it comes to the investigations of web related crimes. The legal challenges can be enormous, the need to *prepare* ahead of time cannot be overstates. A thorough familiarization with the local, state and federal laws and statues becomes a critical part of the preparedness. *Ensuring* the interoperability and law enforcement collaboration cannot be overstated. *Considering* and acting upon international cooperation and collaboration is the way forward.

References

- Brown, R. (2018) Understanding law enforcement information sharing for criminal intelligence purposes. *Trends and Issues in Crime and Criminal Justice [electronic resource]*, (566), 1-15.
- Falkenrath, R. A. (2004) The 9/11 Commission Report.
- Federal Bureau of Investigations (2022) Internet Crime Complaint Center.
  Retrieved on August 30, 2022 from https://www.fbi.gov/investigate/cyber
- Goodwin, T. (2016). The 3 Ages of Digital. Tech Crunch.com.
  Retrieved from: https://techcrunch.com/2016/06/23/the-three-ages-of-digital/ on June 1, 2022
- Guttenberg Police Department (2022)
  Retrieved from https://www.guttenbergnj.org/Departments/police-department
- Haberfeld, Maria R. *Critical issues in police training* (2018*)* NJ: Pearson Customs Publishing.
- Haberfeld, M.R. (2022) Field notes.
- Haberfeld, M.R., Cheloukhine, S., Herrmann & Schneider, J. (2022) Policing the Streets of New York City during the COVID Pandemic: with a Comparative Angle. Forthcoming (fall, 2022) *Journal of Policing*.
- J.D. Supra (2022). A Communication Data Warrant or Wiretap Order - Which is needed for Law Enforcement to Obtain ESI from Facebook.
  Retrieved from https://www.jdsupra.com/legalnews/a-communication-data-warrant-or-wiretap-6197099/
- Jersey City Police Department Official website (2022)
  Retrieved on August 30, 2022 from https://www.jerseycitynj.gov/cityhall/PublicSafety/Police
- Kupperman, R. H., & Trent, D. M. (1979) Terrorism: Threat, reality, response (pp. 48-74). Stanford, CA: Hoover Institution Press.

- Legal Information Institute (2022) Plain View Doctrine.
  Retrieved from https://www.law.cornell.edu/wex/plain_view_doctrine_0
- Law Enforcement Management and Administrative Statistics (LEMAS) 2016.
  Retrieved from https://bjs.ojp.gov/data-collection/law-enforcement-management-and-administrative-statistics-lemas
- New York City Police Department (2022) Official website
  Retrieved from https://www1.nyc.gov/site/nypd/index.page
- Officer.com (2021) White Paper on Digital Forensics.
  Retrieved from https://www.officer.com/whitepaper/whitepaper/21278776/magnet-forensics-digital-forensics-software-a-new-paradigm-in-digital-investigations
- Police Chief Magazine (2022) Policing in Digital Era.
  Retrieved from https://www.policechiefmagazine.org/
- Police Departments in Hudson County (2022)
  Retrieved from https://www.countyoffice.org/nj-hudson-county-police-department/
- Sheptycki, J. (2004). Organizational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence-led policing. *European Journal of Criminology*, *1*(3), 307-332.
- Sodus Point Police Department (2022) Official website.
  Retrieved from https://www.villageofsodus.org/police-department
- United States Department of Justice (2022) Entrapment Defense.
  Retrieved from https://www.ojp.gov/ncjrs/virtual-library/abstracts/entrapment-defense
- Young R. & D. S. Sayers (2022). Why police forces are struggling to recruit and keep officers, CNN.
  Retrieved from https://www.cnn.com/2022/02/02/us/police-departments-struggle-recruit-retain-officers/index.html

Learning, Training, Knowledge

EU Law Enforcement Training Needs on Digital Skills and the Use of New Technologies

Iulian Coman
Noemi Alexa
European Union Agency for Law Enforcement Training[1]

Abstract
Digitalisation, one of the key elements addressed by CEPOL in law enforcement training, is carried out based on the continuing and emerging technological innovations that needs to be given the highest priority across the European law enforcement community.
The new European Union Strategic Needs Assessment (EU-STNA), defines the strategic EU-level training priorities of law enforcement officials for the next 4-year cycle, 2022-2025, in line with the EMPACT priorities, emphasizing the importance of digital skills and use of new technologies, as one of the main horizontal aspects that should be addressed in all training activities.
Cyber-attacks, had the highest priority rank, as EU training need, within the Member States, indicating more than 7600 officials that would need to be trained. Law enforcement and judiciary authorities would need further awareness raising regarding cyber security, cyber-enabled and cyber-dependent crime, but also further improvement in dealing with e-evidence and international cooperation mechanisms.
Taking into consideration the deliverables of the EU-STNA process, CEPOL has further launched a structured training needs analysis in 2021, the OTNA on Digital skills and the use of new technologies, in order to define the training portfolio addressing digitalisation of law enforcement for 2023-2025. Amongst most relevant training topics of the responding countries, we can highlight the Digital investigations, use of new technologies and digital forensics, which would need to be included in law enforcement training activities.

Keywords: digitalisation, digital skills, new technologies, law enforcement training, EU priorities

Introduction

Technological innovations continue to change the law enforcement landscape and despite the investment already made in improving digital skills and the use of new technologies for law enforcement officials, further efforts in building professionals' capacity to use advanced technology and of deepening their understanding of how technology is utilized for criminal purposes, are still needed, as concluded by CEPOL's European Union Strategic Needs Assessment (EU-STNA) 2022-2025.

1 Authors' emails: iulian.coman@cepol.europa.eu; noemi.alexa@cepol.europa.eu

Recent studies demonstrate that the increased cyber-crime activities, reflects also on the preparedness of the law enforcement officials on responding and tackling such offenses (e.g. Harkin, and Whelan 2021, Bieber 2019). The use of technology remains an important feature for serious and organized crime, in a rapid evolving digitalised society (ENISA 2021; EUROPOL 2021) and the specialised training on digital skills is important for all police officers. Online criminality is so common, that all the law enforcement officials should be equipped with the knowledge and skills to understand and proactively fight cybercrime (HMIC, 2015).

Assessment and Analyses of Training Needs

Training needs assessments (TNAs) is a strategic and organizational process that collects and analyses data to support decision makers to improve individuals' performance through training and are considered powerful tools to support organizational change and development, while supporting adjustments for the external stakeholders (Reed & Vakola 2006). The strategic role of the TNAs provide clear gaps in professional skills, institutional needs and insufficient knowledge and involve different parties to participate, that are directly or indirectly interested or involved in the training process (Ferreira & Abbad, 2013).

At European level, the need for continuous training of law enforcement and identifying threats and risks, has led different EU Agencies and Institutions to develop and apply TNAs in line with their business needs, through complex processes with stakeholders.

EU-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, develops annually a Training Needs Assessment exercise that is part of the development and update of their training courses, methodologies, materials and tools.

Europol identifies the priorities in the fight against serious and organised crime through an annual Serious and Organized Crime Threat Assessment (SOCTA) that uses mixed method involving qualitative and quantitative analysis techniques. The methodology consists of two key steps, identification of all threats related to serious and organized crimes and secondly the identification of the key threats. The advantage of Europol in this process is that the preliminary analysis that identifies intelligence gaps, is conducted based on the data already available within the agency, combined with strategic reports from EU partners, EU Member States (MS) and other stakeholders. Further questionnaires for identifying descriptive data, are sent to the MS and other stakeholders. All data is evaluated by using the 4x4 system.

European Security and Defense College (ESDC) presented the methodology for its Training Requirements Analysis (TRA) in 2020, in line with the EU Global Strategy 2016, Civilian Compact 2018 and EU Policy on Training, that consisted of five phases: identifying requirements, research including EU policies/guidelines/frameworks, questionnaires and interviews, mapping of existing security sector reform (SSR) training, analysis and preparation of high-level training outcomes. The TRA concluded in a final report – ESDC Executive Academic Board (EAB) Security Sector Reform (SSR) Report on Training Requirements Analysis for Civilian Common Security and Defense Policy (CSDP) Missions that identified existing CSDP civilian training requirements and gaps.

In accordance with the Article 3 (2015 Regulation (EU) 2015/2219),CEPOL is mandated to support, develop, implement and coordinate training for law enforcement officials, while putting particular emphasis on the protection of human rights and fundamental freedoms in the context of law enforcement, in particular in the areas of prevention of and fight against serious crime affecting two or more Member States and terrorism, maintenance of public order, in particular international policing of major events, and planning and command of Union missions, which may also include training on law enforcement leadership and language skills.

Pursuant to the Article 4.1 of the Regulation 2015/2219, CEPOL is tasked to prepare multi-annual strategic training needs analyses and multi-annual learning programs.

Introduction of the European Union Strategic Needs Assessment (EU-STNA) and the Operational Training Needs Assessment (OTNA) is one of the performance indicators of CEPOL to ensure high quality, multidisciplinary, innovative and relevant training and learning options, accessible to its target group.

The EU-STNA aims at assessing strategic training needs and address EU priorities in the area of internal security and its external aspects, with a view to better coordinate training activities for law enforcement officials and avoid duplication of efforts.

As a follow up to this exercise, CEPOL regularly conducts training needs analyses on operational level, on the priority topics defined by the EU-STNA. The aim of these analyses is to get a detailed understanding of the number and profile of officials to be trained as well as on the proficiency and urgency level of training to be delivered.

EU-STNA Process and Methodology

EU level training activities refer to strands 3 and 4 of the Law Enforcement Training Scheme (LETS) as identified in Commission Communication COM (2013)172, and namely: strand 3 - thematic policing specialism; and strand 4 - European Union civilian missions and capacity building in third countries. EU-STNA only looks at EU level priorities, as national training (strand 1 of the above mentioned LETS) and bilateral/regional training cooperation (strand 2 of LETS) remains outside of the scope of the exercise. More specifically, the EU-STNA aims at identifying those EU level training priorities that can help close capability gaps for law enforcement officials.

It is a collective, EU-wide effort that requires participation from all stakeholders, so that training providers can deliver better, more targeted training to the European law enforcement community on the top priority topics.

The Council of the European Union, the European Parliament, together with the European Commission are the main addressee of the EU-STNA report, which provide background for the law enforcement training policy development for the upcoming years.

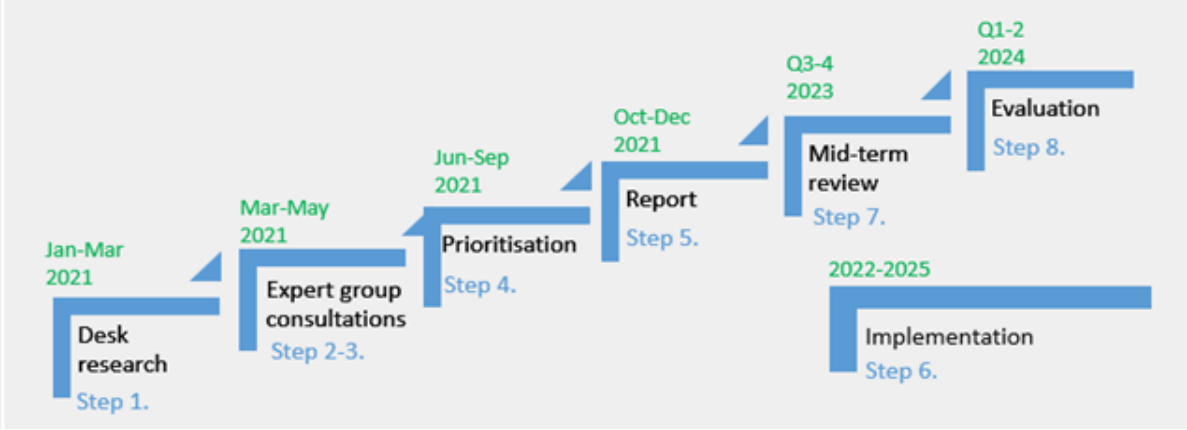
Member States are crucial in the EU-STNA process, as their experts assess capability challenges in law enforcement and corresponding training needs, and their policy makers prioritise those EU training needs. The successful implementation of the EU-STNA depends on the stakeholder (JHA agencies, EU networks) contributions, who are involved in the different steps of the EU-STNA process.

The process of the EU-STNA started with a desk research from key policy documents on EU internal security issues, followed by clustering on 17 thematic categories, one of the categories being Cyber-attacks. Further to the desk research, expert consultations were held on the available information and a gap analysis was conducted to define those areas where EU level intervention is required and to determine relevant training to address the capability challenges identified across Member States. EU Member States prioritized the final list of training needs, with the opinion of EU institutions and relevant agencies.

In October 2021, CEPOL initiated the drafting of the EU-STNA Report, which lists the key EU training needs and indicates potential training providers. The Report was finalised in November 2021, then shared with the Directorate-General for Migration and Home Affairs of the European Commission (DG HOME).

The mid-term review of possible new threats and training priorities will be conducted in 2023, more precisely during months 27–30 of the EU policy cycle. Finally, the evaluation focusing on assessing the impact of the second EU-STNA and identifying possible improvements for the next cycle, will be carried out by an external evaluator, contracted by CEPOL in 2023. Thus, the evaluation will be conducted during the first half of 2024 in order to allow sufficient time for possible methodology adjustments and for the alignment of the next EU-STNA with the future EMPACT cycle 2026–2029.

Figure 1: EU-STNA process structure



Findings

The EU-STNA process identified eight core capability gaps (Figure 2) constituting the main areas in which law enforcement officials need capacity building through training, with *digital skills and use of new technologies,* being the most identified in all expert group discussions for all thematic areas. Furthermore, 230 training needs were identified, clustered in 17 thematic areas as well as 9 other specific training needs included under a separate category. It has to be noted that the core capability gaps are relevant for all thematic areas of training.

Figure 2: Core capability gaps

Core capability gaps	Thematic training areas	
o **Digital skills and use of new technologies** o **High-risk criminal networks** o **Financial investigations** o **Cooperation, information exchange and interoperability** o **Crime prevention** o **Document fraud** o **Forensics** o **Fundamental rights and data protection**	1. Cyber-attacks 2. Criminal finances, money laundering and asset recovery 3. Counter-terrorism 4. Trafficking in human beings 5. Drug trafficking 6. Migrant smuggling 7. Child sexual exploitation 8. Online fraud schemes 9. Organised property crime	10. Border management and maritime security 11. Firearms trafficking 12. Missing trader intra-community fraud 13. Corruption 14. Excise fraud 15. Intellectual property crime, counterfeiting of goods and currencies 16. Environmental crime 17. External dimensions of European security 18. Other thematic areas

After a thorough desk research of EU policy documents and strategic reports and series of consultation with expert groups, networks and other stakeholders, the list of EU-level training needs of law enforcement officials was composed and it was sent to prioritisation to the MS authorities via a survey. Responders were asked to rank the EU level training needs by assigning a numerical value that corresponds to its priority (e.g. 1 means a training need of highest priority, 2 – second priority, etc.) by first ranking the main categories against each other and after that rank the training needs within each thematic category.

After submitting the priority order, in line with the EU-STNA methodology the ranking has been weighted (multiplied) by the coefficient equal to the proportion of the country's representation in the European Parliament. The final list of priorities is therefore reflecting the sum priority scores given by the Member States.

The highest priority has been given to the need for digital skills and the use of new technologies. Technological innovations continue to change the law enforcement landscape, and the related training needs have been revealed by the process of identifying the core capability challenges across the European law enforcement community.

Figure 3: List of training needs for digital skills core capability gap

Digital skills and use of new technologies
Cybersecurity fundamentals for EU officials' everyday use (cyber hygiene, cybersecurity guidelines, secure exchange of information, physical security).
Raising awareness of the most important cyber-threats (e-mail based attacks, web-based attacks, DDoS attacks, social media scams). Understanding the cybersecurity challenges from the modern technologies, like AI or 5G.
Better, modern and validated tools and training materials for tackling activities related to disinformation and fake news that are considered as crime or could lead to crime and are supported by advanced digital technologies.
Digital investigation: OSINT, dark net, cyber threat intelligence (CTI) knowledge management, decryption, use of AI, big data analysis, quantitative and qualitative analysis methods, internet of things, advanced use of camera systems, drones, exoskeletons and speech processors, big data analysis for prediction of criminal behaviour, cryptocurrencies
Digital forensics
Victims' protection
Fundamental rights and data protection

Member States have indicated that at present a total of 110 368 law enforcement officials would need EU-level training in the areas identified, with 7 659 officials in the area of cyber-attacks, for all training needs (Figure 4).

The key training priorities relate to the modi operandi and investigation techniques of cyber-attacks. Digital skills of law enforcement officials and the judiciary as well as their ability to deal with e-evidence need substantial improvement through training. Investigators should benefit from training on the operation of criminal networks and on national and international cooperation mechanisms. Besides investigators, cybercrime analysts should also be trained.

Figure 4: List of identified and prioritized training needs for cyber-attacks

	Cyber-attacks
1	Investigating cyber-attacks on information systems and modus operandi: analysing latest cyber-attacks and EU emergency response; developing alternative investigation techniques and EU tools, including their use
2	Latest challenges for dealing with encryption, anonymisation and bulletproof hosting services
3	Identifying, handling, securing, preserving, analysing and exchanging e-evidence
4	Combatting crime-as-a-service used by criminals and criminal groups in illegal activities
5	Effective international cooperation
6	Protocols to tackle large-scale cyber-attacks
7	Raising awareness of cyber-attacks for EU agencies, law enforcement agencies and the public, including a coordinated approach for prevention; cyber-enabled and cyber-dependent crime awareness, cyber threats and cybercrime investigation
8	Big data analysis
9	Blockchain analysis
10	Using artificial intelligence, machine learning and deep learning in cybercrime investigation
11	Cybercriminal profiling and motivation analysis
12	Fundamental rights such as human dignity, non-discrimination, gender equality, privacy and data protection

OTNA Process and Methodology

The CEPOL Regulation mandates the Agency to incorporate training needs assessments and analyses in its planning. CEPOL completed the second EU Strategic Training Needs Assessment (EU-STNA) in 2021, identifying strategic level training priorities for law enforcement officials across Europe for the next 4-year cycle 2022-2025 of the European Multidisciplinary Platform Against Criminal Threats (EMPACT). In order to analyse the particular training needs in more details, CEPOL is conducting the OTNAs.

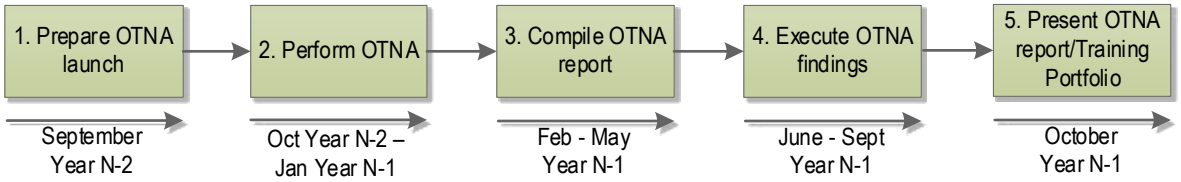
The OTNA methodology is a complex approach to operational level analysis aiming at getting a detailed picture of training needs of a given thematic priority from relevant experts in Member States. The OTNA method-

ology is applied to core capability gaps and thematic training priorities as defined in the EU-STNA. It collects data on:

- subtopics to be addressed by training;
- proficiency level of training needed;
- urgency level of training needed;
- number of participants who would need the training;
- profile of participants who would need training.

Outcomes of the OTNAs are valid for 3 years; a mid-term OTNA review as well as certain ad-hoc TNAs may be performed to address the emerging training needs and new developments.

Figure 5: OTNA process structure



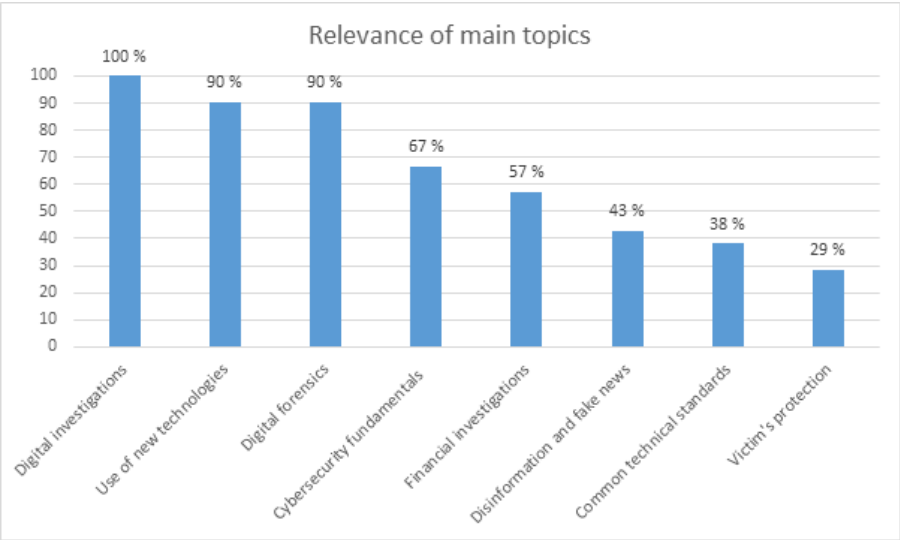
Findings

In December 2021, CEPOL launched an online survey built around the strategic training priorities defined in the EU-STNA. In order to collect relevant data, the survey was addressed to direct contact points of 26 Member States and EU structures dealing with the subject of the OTNA. Data was collected between 21 December 2021 and 2 February 2022, resulting in 45 individual answers from different law enforcement agencies and EU structures of 21 different MS, reportedly representing more than 15252 law enforcement officials. Considering the representativeness of the sample in terms of MS, 81 % response rate can be seen as a good level of responsiveness for a survey research, in this case, intended to represent the European law enforcement community (CEPOL 2022, *OTNA Report on digital skills and the use of new technologies*).

Based on the analysis of the collected data, the report describes training priorities in the area of Digital skills and the use of new technologies for 2023-2025.

All responses indicated clear relevance for the scope of activity, the most relevant main topics (out of the 12 individual topics) for law enforcement officials in this area were related to digital investigations, use of new technologies and digital forensics.

Figure 6: Relevance of main topics



Respondents indicated that 9607 officials would need training on the prioritized main topics in 2023. Based on the volume of trainees communicated by the respondents, notably highest need for training is at awareness level. Second highest number of potential participants divides almost equally between practitioner and advanced practitioner.

Figure 7: Proficiency levels and number of participants of all institutions

Proficiency level	Number of participants (median)	Number of participants (actual)
Awareness	3081	131780
Practitioner	2054	67104
Advanced practitioner	2080	28275
Expert	1469	10985
Train-the-trainer	923	2306
Total	**9607**	**240450**

Conclusions

Based on the analysis of the collected data, the report describes training priorities in the area of Digital skills and the use of new technologies for 2023-2025.

Future trainings should target practitioners and advanced practitioners (online modules or online courses) in the area of use of new technologies (artificial intelligence and big data analysis) and disinformation and fake news (deep fakes). For the awareness level, webinar and e-lessons should be developed, in the area of use of new technologies (illegal use of drones, use of cameras, 5G, automotive) and disinformation and fake news (detecting tampered evidence).

All the results indicate that the demand for training in terms of topics and volume of potential trainees is high and flexible learning solutions are needed for further preparing the law enforcement officials for the digital era.

References

- Anderson, J. E. (2000) Training needs assessment, evaluation, success, and organizational strategy and effectiveness (Doctoral dissertation). Utah State University, Logan, Utah.
- Ap, Z., (2019) Impulsivity and Risky Cybersecurity Behaviors: A Replication, 1-4.
  Available from: https://www.cepol.europa.eu/sites/default/files/EU-STNA-2022-CEPOL.pdf
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Establishing a European Law Enforcement Training Scheme, Brussels, 27.3.2013, COM (2013) 172 final.
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Agenda on Security (28.04.2015 COM(2015) 185 final).
- Decision 32/2017/MB (15/11/2017) of the Management Board of the European Union Agency for Law Enforcement Training On CEPOL Operational Training Needs Analysis Methodology.
- ESDC Executive Academic Board (EAB) Security Sector Reform (SSR) Report on Training Requirements Analysis for Civilian Common Security and Defense Policy (CSDP) Missions.
  Available from: https://issat.dcaf.ch/Learn/Resource-Library/Other-Documents/Civilian-Coordinator-for-training-in-Security-Sector-Reform-CCT-SSR-ESDC-EAB-SSR-Report-on-Training-Requirements-Analysis-for-Civilian-CSDP-Missions
- Ferreira, R. & Abbad, G. (2013) Training Needs Assessment: Where We Are and Where We Should Go, 1-6.
- Harkin, D. & Whelan, C. (2021) Perceptions of police training needs in cyber-crime. International Journal of Police Science & Management. Online First (forthcoming), 1-2.
  Available from: https://journals.sagepub.com/doi/10.1177/14613557211036565 https://www.researchgate.net/publication/334726198_Impulsivity_and_Risky_Cybersecurity_Behaviors_A_Replication

- Operational Training Needs Analysis on Digital Skills and the Use of New Technologies.
  Available from: https://www.cepol.europa.eu/sites/default/files/OTNA_Report_Digital_Skills.pdf
- Reed, J., & Vakola, M. (2006) What role can a training needs analysis play in organisational change? *Journal of Organizational Change Management*, 19, 393 – 400.
- Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL)
- Regulation (EU) 2015/2219 on the European Union Agency for Law Enforcement Training
- Serious and Organized Crime Threat Assessment (SOCTA) 2021.
  Available from: https://www.europol.europa.eu/publications-events/main-reports/socta-report
- The European Union Strategic Training Needs Assessment (EU-STNA) 2022 – 2025.
  Available from: https://www.cepol.europa.eu/sites/default/files/EU-STNA-2022-CEPOL.pdf
  Website: https://www.cepol.europa.eu

Law Enforcement Agency Capacity Building as a Driver for the Adoption of European Research

Michael Whelan
Ray Genoe
University College Dublin

Abstract

The INSPECTr project aims to produce a proof of concept that will demonstrate solutions to many of the issues faced by institutional procedures within law enforcement agencies (LEAs) for combating cybercrime. Unlike many other H2020 projects, the results of INSPECTr will be freely available to stakeholders at the end of the project, despite having a low technology readiness level. It is imperative that LEAs fully understand the legal, security and ethical requirements for using disruptive and advanced technologies, particularly with a platform that will provide AI assisted decision making, facilitate intelligence gathering from online data sources and redefine how evidential data is discovered in other jurisdictions and exchanged. However, INSPECTr will also require the support of stakeholders beyond the scope of the project, in order to drive further development and investment towards market-readiness. The development of a robust capacity building program has been included in the project to ensure that LEAs can confidently use the system and that they fully understand both the pitfalls and the potential of the platform. During our training needs analyses, various European instruments, standards and priorities are considered, such as CEPOL's EU Strategic Training Needs Assessment, the course development standards established by ECTEG and Europol's Training Competency Framework. With this research and through consultation with internal and external stakeholders, we define the pathways of training for the INSPECTr platform in which we aim to address the various roles in European LEAs and their requirements for the effective delivery and assessment of the course. In keeping with the project's ethics-by-design approach, the training program produced by INSPECTr will have a strong emphasis on security and the fundamental rights of citizens while addressing the gaps in capabilities and training within the EU LEA community. In this paper we describe the process we apply to curriculum design, based on the findings of our research and our continued engagement with LEA and technical partners throughout the life-cycle of the project.

Keywords: Law Enforcement Agency Capacity Building, Training Needs Analysis, Advanced Technologies

Introduction

According to the European Union Strategic Training Needs Assessment (EU-STNA) Report (CEPOL, 2019a)1 EU-level training should not only boost knowledge, but also allow an exchange of experiences and practices between the practitioners and contribute to building trust. The EU-STNA was developed to identify gaps in knowledge, skills and competencies and trai ning needs. It identifies training priorities and aims at coordinating available training to prevent overlaps and duplication. It also identifies emerging law enforcement trends, such as increasing synergies and overlaps between different crime areas, as well as larger demands for cooperation between disciplines.

The undertaking of training by law enforcement personnel will not only improve their knowledge of the latest laws and legislation but also help them remain cognisant of new police tactics and evolving trends in criminal activities. For example, the ever-evolving landscape of technology provides criminals with new opportunities to commit cybercrime. Criminals are exploiting new technologies with lightning speed, tailoring their attacks using new methods that are facilitated, enabled or amplified by the Internet (Europol, 2021)[2].

Likewise, new technologies are rapidly changing the field of law enforcement in the fight against cybercrime. New automated technologies, such as artificial intelligence and predictive analytics, are being used by law enforcement to both improve efficiency and enhance safety. As the development of these technologies continues to improve and evolve, their adoption and implementation by LEAs requires proper instruction on usage, through the provision of specialised training. For example, new technology such as AI assisted intelligence gathering would have many positive aspects for police investigators but improper use could have many negative impacts on society. In addition to technical and legal obstacles barriers to the misuse of such technology, instructional training courses should also sensitise participants to the consequences of misuse.

The EU's approach to the fight against cybercrime focuses on three main areas: adoption and update of appropriate legislation; cross-sectoral and international cooperation; as well as capacity building.

Legislation: EU rules on cybercrime correspond to and build on different provisions of the Council of Europe's Convention on Cybercrime (Council of Europe, 2001). The key measures for the EU's cybercrime legal framework include:

- 2022: Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber resilience Act (COM (22) 454 final, 2022)
- 2020: Proposal for Interim Regulation on the processing of personal and other data for the purpose of combating child sexual abuse (COM (20) 568 final, 2020)
- 2019: Directive on non-cash payment (Directive (EU) 2019/713, 2019)
- 2018: Proposals for Regulation (COM (18) 225 final, 2018) and Directive (COM (18) 226 final, 2018) facilitating cross-border access to electronic evidence for criminal investigations
- 2013: Directive on attacks against information systems (Directive 2013/40/EU, 2011)
- 2011: Directive on combating the sexual exploitation of children online and child pornography (Directive 2011/93/EU, 2011).

Using this legal framework as a foundation for an effective response to the fight against cybercrime, its measures and actions according to EU Migration and Home Affairs (2022) aim to:

- improve the prevention, investigation and prosecution of cybercrime and child sexual exploitation,
- build capacity in law enforcement and the judiciary,
- work with industry to empower and protect citizens.

Cooperation: The EU also supports cooperation frameworks amongst criminal justice actors and across sectors particularly with industry which controls a large part of information infrastructures.

Key cooperation mechanisms and structures supported by the EU include:

- European Cybercrime Centre[3] (EC3): set up by Europol in 2013, serves as a central hub for criminal information and intelligence and supports operations and investigations

1 European Union Agency for Law Enforcement Training; see https://www.cepol.europa.eu/.

2 European Union Agency for Law Enforcement Cooperation; see https://www.europol.europa.eu/.

3 The European Cybercrime Centre (EC3) was set up by Europol to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime; see https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

by EU Member States by offering operational analysis, coordination and technical expertise.

- EU Internet Forum[4]: established in 2015 with the aim to reach a joint, voluntary approach based on a public-private partnership with ISPs to detect and address harmful material shared online.
- European Judicial Cybercrime Network[5]: set up in 2016, facilitates sharing expertise, knowledge and best practice amongst experts from competent judicial authorities dealing with cybercrime, cyber-enabled crime and investigations in cyberspace.

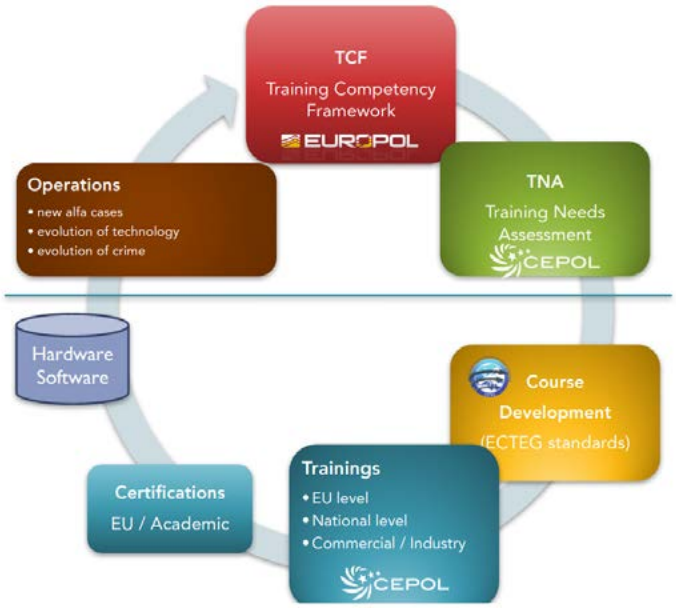
The main focus of this paper will centre around the third area, *capacity building*. In the next section, we will outline the recommendations from the training governance model that was developed by various EU institutions. The remainder of the paper will be structured as follows:

- The section "INSPECTr Training Needs Analysis", will describe the methodology of the training needs assessment and present a summary of our findings.
- The identified training pathways, course format and course curriculum will be discussed in the section, "INSPECTr Capacity Building Programme".
- The "Conclusion", will present our conclusion and future works.

Capacity Building and the Training Governance Model

In 2015, several EU agencies, namely the European Commission, Europol-EC3, ECTEG[6], CEPOL and Eurojust[7], agreed to develop a Training Governance Model (TGM) on cybercrime. The TGM was a deliverable under the EU priorities defined in the Internal Security Strategy and one of the operational actions specified for 2014 in the context of the EMPACT[8] policy cycle. The TGM intends to provide the foundations for a coordinated approach to training and education in the EU for law enforcement and the judiciary.

Figure 1: Training Governance Model on Cybercrime[9]



4 The EU Internet Forum (EUIF) launched by the Commission in December 2015, addresses the misuse of the internet for terrorist purposes; see https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en.

5 The European Judicial Network in criminal matters (EJN) is a Network of national Contact Points for the facilitation of judicial cooperation in criminal matters; see https://www.ejn-crimjust.europa.eu/ejn2021/Home/EN.

6 European Cybercrime Training and Education Group (ECTEG) is an International Non Profit Association, supported by EU funding. It is composed of participants from European Union and European Economic Area Member state law enforcement agencies, international bodies, academia and private industry; see https://www.ecteg.eu/.

7 Eurojust, the European Union Agency for Criminal Justice Cooperation, is a unique hub based in The Hague, the Netherlands, where national judicial authorities work closely together to fight serious organised cross-border crime; see https://www.eurojust.europa.eu/.

8 EMPACT (European Multidisciplinary Platform Against Criminal Threats) is a security initiative driven by EU Member States to identify, prioritise and address threats posed by organised and serious international crime (EU Migration and Home Affairs, 2021).

9 Image from ECTEG presentation to Council of Europe in 2018 (Sobusiak-Fischanaller, M. and Vandermeer, Y. 2018).

Cybercrime TGM: The Training Competency Framework

In Figure 1 the first step of the TGM is the Training Competency Framework (TCF). The aim of Europol's TCF is to identify and document the required knowledge, skills and in general the training needs of the key actors involved in combating cybercrime at EU level, focusing on both LE and the judiciary. The TCF is a living document, as the area of cybercrime is extremely dynamic, the TCF will be periodically reviewed and updated when necessary.

Figure 2: Training Competency Framework on Cybercrime Matrix

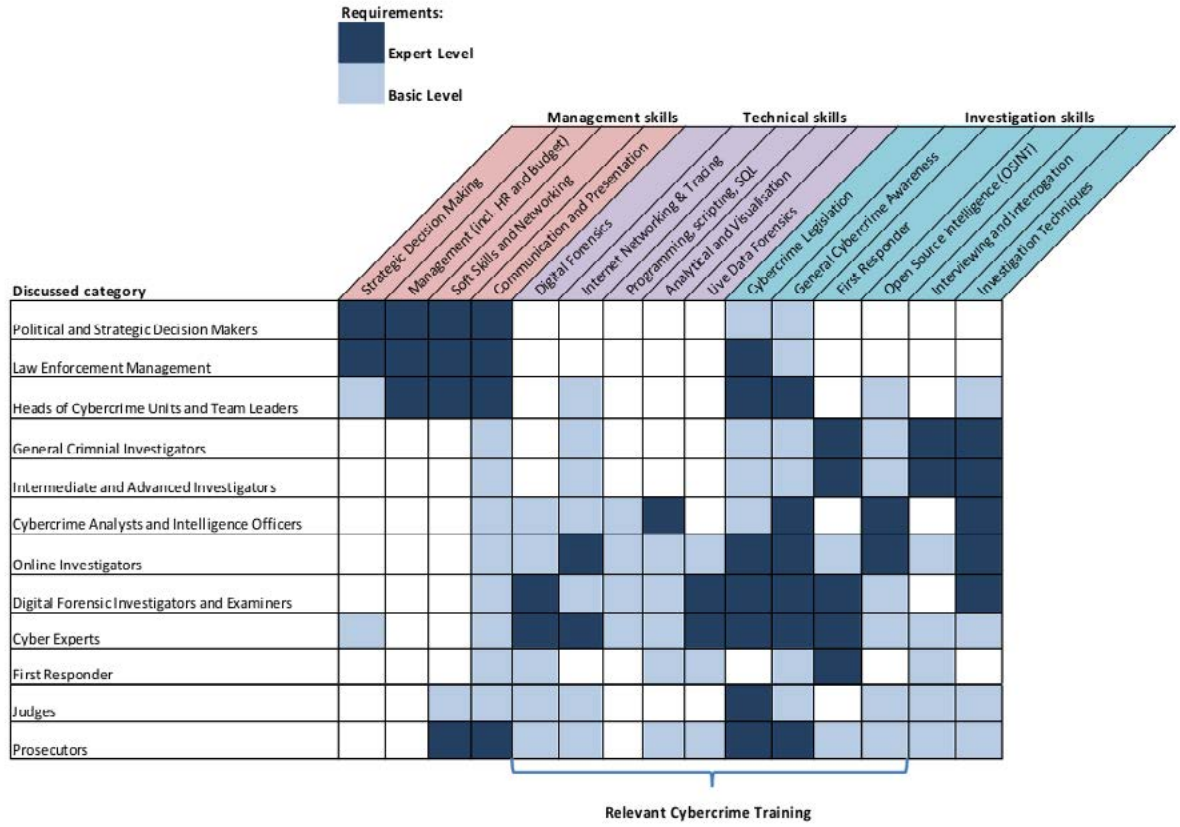


Figure 2 shows that TCF identifies ten key actors in law enforcement and two in the judiciary that are involved in the fight against cybercrime. The TCF establishes the required skills and expertise for each actor. The necessary competencies and skills described fall into three main categories – management skills, technical skills, and investigation skills. It is hoped that this standardised and harmonised description of each of the actors will ensure coherence and help avoid duplication of effort when developing training courses and educational programmes for law enforcement and the judiciary.

The strategic and operational value of the TCF can be very valuable in providing support for the coordination of organisations involved in cybercrime training and education, that will allow for a more sustainable and harmonised approach to capacity building at national and EU level. Benefits include:

- Development of a framework that specifies the skills and expertise required by the various actors involved in the fight against cybercrime
- Help minimise any overlap in the area of training and capacity building and to ensure the most effective use of budget and resources
- Define national training / education requirements
- Structure curriculum
- Help LEA to build national career paths
- Create/grow specialised units

Cybercrime TGM: Training Needs Assessment

The next step of the TGM (Figure 1) is to carry out a Training Need Analysis (TNA) based on the TCF. The analysis, as well as the consequent prioritisation of training needs and the design of the training portfolio, is a joint effort coordinated by CEPOL in cooperation the other members involved in the TGM. One such example is CEPOL's TNA for the area of cyber-attacks against information systems (CEPOL, 2019b). The research assessed training needs against the necessary competencies law enforcement officials should have in order to perform their duties. The level of necessary competencies was defined in the TCF. The analysis provided an understanding of training needs from two perspectives:

- comparing the current level of knowledge of law enforcement officials performing different roles in investigations of cyberattacks to the level of knowledge necessary to fulfil their obligations
- identifying where there is a need for training and the dimensions of training needed such as the level, form, urgency and number of participants who would need training.

After the analysis step in the TGM, the coordination and delivery of the identified training is the responsibility of training providers such as CEPOL and ECTEG.

Cybercrime TGM: Course Development Standards

ECTEG's course development standards (ECTEG, 2022) aim to provide experience and knowledge to further enhance the coordination and support for the development and delivery of cybercrime training courses for law enforcement personnel at various levels.

The decisions to develop or update the training material of a course, are made by ECTEG members and are assisted by an advisory group that has CEPOL and Europol-EC3 permanently represented. Each course training package must follow ECTEG's course development standards which involves the use of subject matter experts and requires the creation of trainer and student manuals, presentation slides and practical exercises with solutions. In addition, courses should be developed using Markdown syntax, for easy translation for an international audience and, should be run at least once as a pilot training course for feedback and refinement.

Cybercrime TGM: Course Delivery

Within the TGM, the delivery of training is mainly led by CEPOL - who are generally responsible for the implementation of training and learning activities for law enforcement at European level. CEPOL's approach to learning (CEPOL, 2022) includes offering up-to-date, innovative training courses, bringing together the latest expertise and developments in research and technology. CEPOL provides modern education methodologies such as e-learning or blended learning, which combines e-learning components with classroom or practical training.

INSPECTr Training Needs Analysis

In light of the TCF, we wish to define pathways of training for the INSPECTr platform, which will be designed to address the various roles in European LEAs and their requirements for the effective delivery and assessment of the course. To accomplish this we carried out our own TNA.

A TNA is one of the key steps in preparing a training plan. If a TNA is not carried out there is the risk of doing too much or too little training, or missing the point completely. Conducting a thorough TNA will improve the chances of a successful training program by making informed decisions on the training composition, based on concrete data and information.

An electronic survey was used to gather the training needs for LEA wishing to use the INSPECTr platform. The *first part* of the 3-part survey asked the respondents about the cyber-related roles in their organisation. The respondents were required to indicate if there was a person or persons assigned to a specific task or was it combined with other roles. The tasks referred to were:

- setting up and maintaining the IT-infrastructure of an organisation;
- performing detailed forensic examinations of computer based digital evidence;
- monitoring the digital world and proposing new topics and cases to investigate;
- strategic analysis, researching, analysing and presenting the latest threats and providing situational overviews;
- engaging in operational analyses to find patterns, trends, hotspots and create links between live cases.

The feedback will help to define optional training pathways through INSPECTr's training curricula, which LEA can easily map to specific roles.

In the *second part* of the survey, the respondents were asked to share details of their best previous training experience, which involved technologies or techniques for LEA cybercrime investigation, whilst referring to whether:

- the training was internal and developed internally, or developed by a third-party, such as ECTEG;
- the training was external and provided for free by a third-party, such as CEPOL;
- the training was provided by a commercial vendor.

Answers to these questions will allow researchers to follow-up on specific courses that compared favourably to others.

The *third and final part* of the survey asked the respondents about what their wishes were for the INSPECTr training course and to indicate their current understanding about specific features of the INSPECTr platform. The respondents were required to answer questions on:

- their preferred method of delivery;
- how detailed the platform's manuals need to be;
- their knowledge of various topics for INSPECTr.

The responses to these questions will determine the delivery of training and the level of detail required for providing instruction on the main features of the INSPECTr platform.

The group consisted of 15 participants from the LEA project partners. Each participant had to complete an informed consent before being allowed to access the survey. All responses were pseudonymised, so that none of the participants could be directly identified by their responses.

Training Needs Assessment Findings

This section lists the key findings from the TNA. They will have a considerable influence on the proposed outputs described in the next section.

Need for different pathways through proposed training curricula: Considering the feedback for part one of the survey on LEA roles, it is clear that different pathways will be required through the training curricula of the INSPECTr platform. The survey responses indicated that there are dedicated staff carrying out specific roles in LEA's cybercrime units:

- 85% of respondents indicating there is at least some presence of dedicated IT staff on their team;
- 92% of organisations have indicated there is the presence of a dedicated digital forensics member of staff on the team;
- 84% indicate there are some staff members who are dedicated to conducting online investigations;
- the majority of organisations have dedicated staff cybercrime analysis with 53% having dedicated staff only and 83% in total having at least one member of staff dedicated to the role;
- finally, an extra role of a Digital Forensic Supervisor was proposed.

The benefit for providing these pathways for the specific cyber-related roles, is that a training course can be tailored for a particular role by selecting a subset of the INSPECTr training topics that are related to knowledge and abilities needed for that role. More details on the pathways are found in next section.

Replicate positive aspects from previous training experiences: The outcome from the feedback for part two of the survey on positive previous training experiences was that the majority of responses indicated that the popular preference was for:

- training that was developed and delivered by external experts;
- training that focused on specialised tools rather than a general overview course;
- the delivery of the training was in-class;
- the purpose of the training was tool specific and had instructors who gave hands-on practical-based demonstrations.

The aim will be to replicate this in the proposed training courses. Further details of the approach taken can be seen in the next section on training format.

Focus on level of knowledge for each INSPECTr training topic, in-class training with hands-on instructor-led and practical scenario-based training: According to the feedback for part three of the survey on training format and topics for proposed training:

- the training format overwhelmingly preferred by the respondents would be in-class training with hands-on instructor-led and practical scenario-based training;
- the level of knowledge of most of the respondents is very low in relation to nearly all of the INSPECTr specific topics.

The preferred method of training delivery will be discussed in more detail in the next section on training format. The low level of knowledge on training topics is to be expected for any new product, so some basic levels of knowledge will need to be delivered, particularly with respect to the installation, configuration and usage of the platform. Further details on the contents of the training curriculum are discussed in the next section of training curriculum.

INSPECTr Capacity Building Programme

The training materials presented in this section are based on the findings of our TNA and the feedback from a number of Living Labs (European Commission, 2009) that were conducted during the execution of the project. Living Labs provide an opportunity for technical developers to discuss the direction of the product with LEA partners and receive iterative feedback through co-creation and testing cycles.

Also, another important consideration is the project's ethics-by-design and privacy-by-design approach to development of the platform from the ground up. A key part of this is sensitising the project partners to ethical and privacy issues that could arise during a project like INSPECTr, this needs to be reflected in the technical development and the training, to protect fundamental rights of citizens, and to avoid security errors, misuse, etc.

Training Curriculum

The following training curriculum, illustrates the recommendations from discussions held with the INSPECTr ethics and technical teams. It is considered to be a fluid curriculum, since it will be subject to change due to emerging technical developments, or issues encountered by LEA partners when they experiment with the system.

Including a curriculum of training during the ongoing process of project research and development is a difficult task, since the outcome of R&D tasks may require changes to be applied to the training material. However, it is important to define an early framework for the curriculum. The following is an outline of the topics we have initially proposed:

Introduction to the platform: A general overview of the issues that the platform tries to address; an introduction to the platform including screenshots of the interface; an outline of additional training and pathways.

Installation and maintenance: An explanation of hardware and networking requirements; an outline of installation steps, up to creating an admin user; an overview of system health monitoring, and updating and upgrading INSPECTr nodes; conclude with practical exercises on installation and maintenance.

Platform and user interface: A detailed tour and focus on User Interface; an outline of the main components of a node, storage layers, gadgets, analytics, pub/sub, Blockchain, e-CODEX[10], etc.

Platform administration and configuration: An introduction to admin user tasks, such as: legal configurations for discovery and sharing, user administration - creating users and groups, tool administration - adding/restricting capabilities to groups; conclude with practical exercises on platform configuration.

External data ingestion: An explanation of how to configure gadgets to communicate with external storage and how to transfer data to INSPECTr storage, such as: disk images, commercial tool reports, etc.; an introduction to federated access to data using SIREN[11] intro (as an alternative to ingestion); conclude with practical exercises on external data ingestion in INSPECTr.

Chain-of-evidence and Chain-of-custody: An introduction to CASE[12] ontology and standardisation of evidence; an outline of the use of Blockchain technology for logging and tracing evidence.

Digital forensic tools: An outline of the use of integrated digital forensic and parsing (to CASE) commercial tool

10 e-CODEX: e-Justice Communication via Online Data Exchange; see https://www.e-codex.eu/.

11 Search-based Investigative Intelligence; see https://siren.io/.

12 An international standard supporting automated combination, validation, and analysis of cyber-investigation information; see https://caseontology.org/.

reports; conclude with practical exercises on digital forensic and Blockchain.

Open source intelligence (OSINT) gathering tools: An outline of the use of integrated OSINT gadgets, an overview of data privacy and operational security issues including ethical aspects (on data privacy, minimisation, etc.); conclude with practical exercises on OSINT.

Data analytics and reporting: An overview of SIREN analytics including configuration of SIREN dashboards, and federated access to external data using SIREN; an overview of INSPECTr widgets for data enriched visualisations and INSPECTr reporting; conclude with practical exercises.

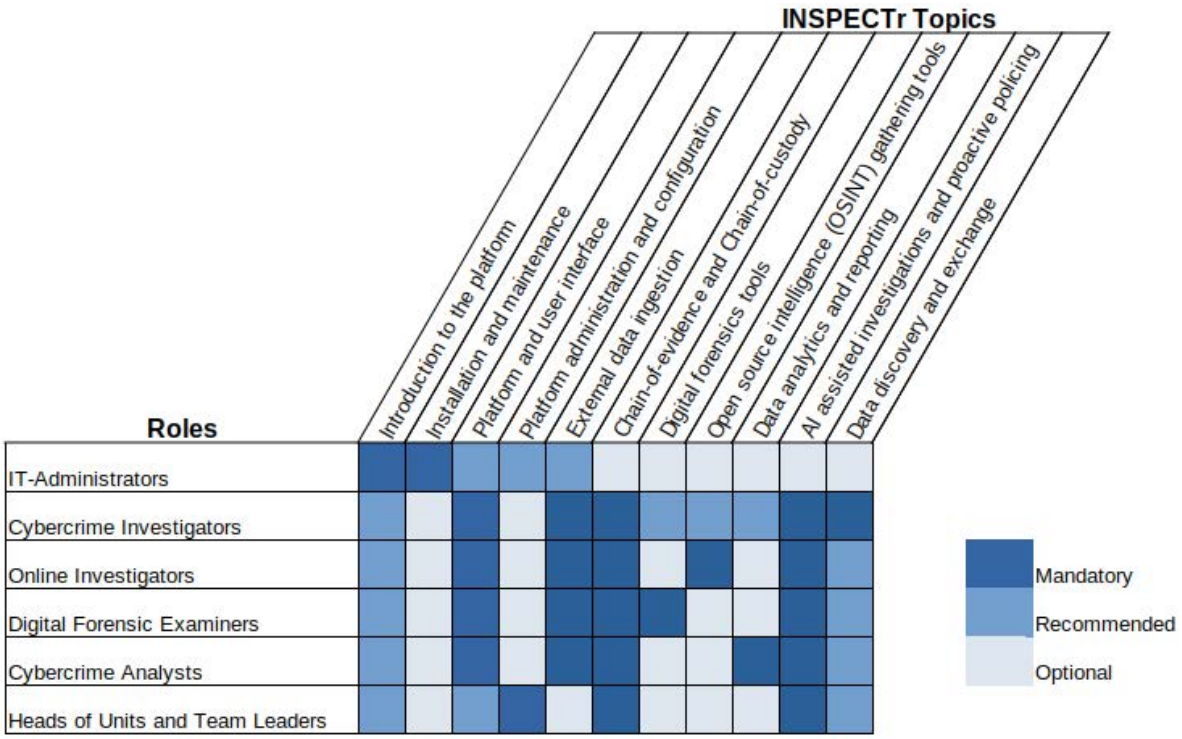
AI assisted investigations and proactive policing: An outline of the use of AI tools, such as: computer vision, natural language processing, cross-case linkage, detection of criminal networks, crime forecasting, machine learning framework; ethical considerations for each aspect; conclude with practical exercises on all AI tools.

Data discovery and exchange: An overview of configuring and using the pub/sub for evidence discovery, configuring and using e-CODEX for evidence exchange; conclude with a joint investigation exercise.

Training Pathways

Subsets of the topics outlined in the training curriculum section, will be chosen to define the learning pathways through the INSPECTr Training Curriculum for the specific roles in LEA's cybercrime units. The matrix in Figure 3 illustrates the proposed pathways for the chosen types of law enforcement personnel that will need to be trained to use the INSPECTr platform.

Figure 3: Pathways matrix



The proposed roles presented in Figure 3 were agreed upon after receiving the feedback from part one of the TNA survey and consulting the TCF on cybercrime seen in figure 2. Judicial training will be considered at a future stage, as the project matures (for TRL[13] 9 – System Proven in Operational Environment). Each INSPECTr topic is identified either as mandatory (blue), recommended (light blue) or optional (very light blue)

13 Technology Readiness Levels (TRLs) are a method for understanding the technical maturity of a technology during its acquisition phase; see https://en.wikipedia.org/wiki/Technology_readiness_level.

to define the chosen subset for each role. The selection process, regarding how each topic is assigned for each of the roles, was agreed upon after discussions with the INSPECTr technical team.

While the estimated duration of completing all training modules would be 41 hours, the estimated duration of training each of the pathways is shown in Table 1.

Table 1: Estimated training duration for each pathway

Pathways	Mandatory Hours of Training	Mandatory + Recommended Hours of Training
INSPECTr IT-Administrator	10	19
INSPECTr Investigators	17	29
INSPECTr Forensics	17	23
INSPECTr Intelligence	16	22
INSPECTr Analysts	16	22
INSPECTr Management	12	20

Training Format

The proposed training course format will follow closely the positive aspects identified in the TNA feedback received for the previous training experiences of the respondents.

- Delivery: in-class, instructor-led demonstrations
- Materials: slides handouts, mocked evidence, use-cases, platform user-guides
- Evaluation: practical exercises
- Duration: pathway dependent

Remote learning or the production of videos was not considered to be a requirement for the training at this stage. There are two reasons for this. The first, is that remote learning was not hugely preferred by the survey respondents, and the second is that the maturity of the platform means that videos are impractical, since the technology is subject to change. Therefore, the delivery of the training will target the standards set by ECTEG, which requires trainer and student manuals, and solutions to all exercises, to be included with the main content as presentation slides. This will make it easier to disseminate training materials for delivery by others, a core principle for ECTEG training delivery. For example, an LEA who wished to adopt the INSPECTr platform would request the training material for free and could then deliver, or seek assistance in delivering, the training. The latter may come at a cost, unless delivered by CEPOL. However, the trainer guides should assist that LEA should they wish to deliver it using in-house staff. These would also be invaluable when the platform matures and there becomes a greater need for the creation of remote learning material.

Course Evaluation

In terms of course evaluation, the maturity of the project also dictates that formal assessment cannot be considered at this time. However, after the pilot course has been completed and the final course packaged, this decision will be revisited. One approach may be to engage with ECTEG's Global Cybercrime Certification Project[14] to determine the suitability of establishing a globally recognised certificate for each of the INSPECTr pathways described above.

Conclusion

In this paper we have described how various instruments, standards and priorities for the development of European law enforcement training, can guide the development of a robust capacity building programme for understanding emerging technologies. For example, following the different steps of the TGM, developed by key EU stakeholders, we defined the training curriculum for the INSPECTr platform, the format of the training course to deliver the curriculum and the different pathways for training different law enforcement users of the platform. We feel this is vitally important to ensure the adoption of new LEA technologies, while safeguarding the end-users from various legal, ethical or regulatory issues.

14 The goal of the Global Cybercrime Certification Project (ECTEG-GCC, 2022) is to create an international certification framework based on the the TCF to enable Law Enforcement Agencies and Judicial authorities to develop their knowledge and skills.

Our analysis clearly indicates that:

- tailored pathways through the training material are needed due to the number of different cyber-related roles existing in LEA's cybercrime units;
- despite the current popularity of online training, the training format overwhelmingly preferred by the respondents is in-class training with hands-on instructor-led and practical scenario-based training;
- training focused on specialised tools is preferred over general overview course material.

It is important to note that the development of the training will be an ongoing process and needs will be reflected on throughout the project, particularly after each Living Lab experiment. After the final pilot course, the training material will be packaged at the end of the project for LEA adopters of the platform. With future developments of the technology likely, the training framework will ensure that updates can be easily reflected in the capacity building program.

References

- CEPOL (2019a) *European Union-Strategic Training Needs Assessment Report 2018-2021*. Luxembourg: Publications Office of the European Union.
  Available from: https://op.europa.eu/en/publication-detail/-/publication/e83f9a06-c3c0-11e9-9d01-01aa75ed71a1 [Accessed on: 08 May 2022]
- CEPOL (2019b) *Operational Training Needs Analysis Cybercrime – Attacks against Information Systems*. Luxembourg: Publications Office of the European Union.
  Available from: https://www.cepol.europa.eu/sites/default/files/OTNA_Cybercrime_Attacks_Against_Information_Systems_2019.pdf [Accessed on: 08 May 2022]
- CEPOL (2022) *Types of Learning*.
  Available from: https://www.cepol.europa.eu/education-training/our-approach/types-learning [Accessed on: 08 May 2022]
- COM (18) 225 final (2018) *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*.
  Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN [Accessed on: 08 May 2022]
- COM (18) 226 final (2018) *Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*.
  Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN [Accessed on: 08 May 2022]
- COM (20) 568 final (2020) *Proposal for a Regulation Of The European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online*.
  Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020PC0568 [Accessed on: 08 May 2022]
- COM (22) 454 final (2022) *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*.
  Available from: https://ec.europa.eu/newsroom/dae/redirection/document/89543 [Accessed on: 20 September 2022]
- Council of Europe (2001) *Convention on Cybercrime 2001 (ETS No. 185)*,
  Available from: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 [Accessed 1 June 2022]
- Directive 2011/93/EU (2011) *Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*. OJ L 335, p. 1–14.
  Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093 [Accessed on: 08 May 2022]
- Directive 2013/40/EU (2013) *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*. OJ L 218, p. 8–14.
  Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0040 [Accessed on: 08 May 2022]
- Directive (EU) 2019/713 (2019) *Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA*. OJ L 123, p. 18–29.
  Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG [Accessed on: 08 May 2022]
- ECTEG (2022) *Course Packages*.
  Available from: https://www.ecteg.eu/course-packages/ [Accessed on: 08 May 2022]

- ECTEG-GCC (2022) *Global Cybercrime Certification Project*.
  Available from: https://www.ecteg.eu/running/gcc/ [Accessed on: 08 May 2022]
- EU Migration and Home Affairs (2021) *EMPACT fighting crime together*.
  Available from: https://ec.europa.eu/home-affairs/policies/law-enforcement-cooperation/operational-cooperation/empact-fighting-crime-together_en
  [Accessed on: 08 May 2022]
- EU Migration and Home Affairs (2022) *Cybercrime*.
  Available from: https://ec.europa.eu/home-affairs/cybercrime_en [Accessed on: 08 May 2022]
- European Commission (2009). Living Labs for user-driven open innovation, an overview of the Living Labs methodology, activities and achievements. European Commission, Brussels.
  Available from: https://op.europa.eu/en/publication-detail/-/publication/3f36ebab-4aaf-4cb0-aada-fe315a935eed [Accessed on: 10 May 2022]
- Europol (2021) *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Luxembourg: Publications Office of the European Union.
  Available from: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021#downloads
  [Accessed on: 08 May 2022]
- Sobusiak-Fischanaller, M. & Vandermeer, Y. (2018) *Cybercrime Training Governance Model - Cybercrime Training Competency Framework* [online].
  Available from: https://rm.coe.int/3148-2-3-ecteg-16-cy-train-module/1680727f34 [Accessed on: 25 May 2022]

Challenges of E-Learning in the French Police Nationale

Cédric Carré
French Police Nationale Training and Recruitment Department (DCRFPN)

Abstract
This paper aims at studying the shortcomings and strengths of the French Law Enforcement administration in the use of E-learning with a focal point on the Police Nationale. The evolution of law enforcement knowledge, techniques, and materials, and even regulations and professional recommendations make continuing education for the Law enforcement professions more essential than ever. Despite the extraordinary rise in digital technology in the training and education field, the French Police Nationale refused for a long time to take the turn of digital progress in the training it offered to cadets but also to experienced officers on the grounds that it was inefficient and approximative in the completion of Police Training. Reputedly monolithic and hard to modernize, the Law Enforcement system in France was reluctant if not closed to the idea of using a tool they saw as unprofessional and unserious. The COVID-19 pandemic shattered their certainties. Unable to give in-person trainings but having to ensure the continuity of curriculums, the French Police Nationale training department had to think out of the box. Facing reluctance, mistrust and sometimes lack of skills from its agents, a cumbersome process ensued for the administration with the construction of a new online training structure, the hiring of new digital experts and education-specialised civilians and the funding for new digital tools to implement quality courses. New training ideas emerged with these new recruits and new tools. Soon, major e-learning projects were achieved, among which the cadet-training curriculum and the national language program are now the best examples.

Keywords: e-learning, innovation, pandemic, challenges, police training

Introduction

The evolution of law enforcement knowledge, techniques and materials, and even regulations and professional recommendations make continuing education for the Law enforcement professions more essential than ever. The extraordinary rise of digital technology in our societies has simultaneously changed the amount of information available, the forms of education and the means of accessing this knowledge. (Hubackova, 2015)

E-learning, which is the absolute emblem of this, has become indispensable because of all the advantages it makes available to learners but it is also because of the population it is or will be aimed at, generation Y (1980-1995) or Z (1996 and onwards), who are deeply rooted

in the digital world through their lifestyle and communication habits (Hargittai, 2010).

E-learning consists of "the use of new multimedia technologies of the Internet to improve the quality of learning by facilitating on the one hand access to resources and services, and on the other hand, the exchanges and collaboration at a distance (European Commission, 2001).

It adapts the training offer to demands that face-to-face training is struggling to meet, by these spatial and temporal, conceptual and also generational issues.

The aim of this paper is to assess the e-learning techniques and, to list their advantages and disadvantages, to verify if possible, the benefits in terms of knowledge acquisition and the evolution of practices regarding law enforcement training as a whole. The relevance and efficiency of e-learning in the training arsenal choice will also be discussed with regard to challenges encountered by trainers and trainees alike.

The methodology is a desk study analysing the figures and comparing practices in a pre- and post-pandemic context. It primarily focuses on cadet training and more specifically on language training within the Law Enforcement training program in the aftermath of the first Covid surge.

E-learning and the Police Nationale: context

The advent of digital technology in our daily lives, initiated at the end of the last century, has brought about major changes in all areas, and in particular in education and training systems. With the emergence of new teaching platforms, came enhanced strategies for the implementation of e-Learning projects and the adoption of ICT by new generations have contributed to its development.

The main advantage of e-learning is lower training costs and a massive distribution channel for companies and universities. A decisive opportunity to increase exchanges with foreign countries and to significantly their international influence. (Camilleri, M.A. & Camilleri, A.C, 2017)

Yet, despite the undeniable possibilities of e-learning, France like many countries, was reluctant to develop e-learning as a recognized method of learning whether in its national education system or at a university level. The Law Enforcement agencies followed the same path, preferring using the same face-to-face academic courses, unable to modernize their training system (Mailfait, 2002). The lack of trust in the technology itself and the perception that a distant trainee was a lazy student were unmovable hurdles to digital progress.

The Police Nationale in particular, before COVID, relied mainly on in-person courses. The idea that a police course could not be performed without physical presence was running deep in the decision-makers' minds within the administration. Curriculum builders and trainers were content with the activities they offered - and had always offered - to the learners and kept on preaching the same philosophy. E-learning was therefore perceived as unnecessary but also as a frivolity from the young generations. This monolithic perception of education first stemmed from the fact that for a very long time, the French Police administration had neglected the importance of training (Mailfait, 2002) disregarding the possible innovations that might have led to a faster and more efficient training of cadets and higher officers alike.

The effect of this inability to dynamise its training before Covid finds an echo in the DFD (Division de la Formation Digitale) survey, which counted only 30 online modules (DFD Survey, 2020) on the Police Learning Management System (LMS) platform by the end of 2019. A ridiculous amount of modules that clearly reflected the lack of interest from trainers who were repeatedly discouraged by the indifference of their decisions-makers. Likewise, considering the figures of learners' attendance on the LMS, the detachment from trainees was obvious, as they were not thrilled by the linear aspect of pdf-based courses uploaded on the platform. Only 10% of police officers, cadets, and higher officers had - by 2019 - attended a course on the LMS (Division de la Formation Digital: DFD Survey, 2020).

The pandemic as a game changer

As a result of the COVID-19 pandemic and containment in several countries around the world, education systems were severely disrupted. New e-learning resources had to be adopted to ensure continuity of educa-

tion and teaching. In this article, we will take a closer look at the new situation and how user-feedback can help you adapt to this sudden change.

This unprecedented shock disrupted the lives of nearly 1.6 billion pupils and students in more than 190 countries on all continents. School and other learning space closures affected 94% of the world's school-going population, and up to 99% in low- and lower-middle-income countries. (Himberg, K. 2021)

As a result, e-learning tools, like many digital tools, could serve different educational purposes:

- Connecting educators and learners in different locations
- Accessing information and environments not always available to individuals or institutions
- Supporting the continuing professional development of educators in an accommodating setting.

Many schools and learning spaces had to close in response to the global health crisis and education systems had to adapt quickly to ensure continuity of education.

Ensuring educational continuity during school closures became an international priority. Many turned to digital technology, which led to the development of the e-learning sector. Distance learning literally became the only efficient go-between during the pandemic (Vidal, 2020). As the figure above shows, countries favoured a variety of distance learning methods. In areas where Internet access was limited, learning was achieved through TV and radio broadcasting and the distribution of printed materials.

Police academies had to apply the same principles and give up their previous way of thinking. The change brought by the pandemic was short of an earthquake for Police Training. The necessity for a remote way of learning became paramount as police officer trainings could not be postponed and solutions for continuity had to be found overnight.

For many in the education and training sphere, E-learning was a logical and easy option because already effective. But for the *Police Nationale,* and because of the lack of anticipation, a quantity of challenges arose.

Challenges regarding e-learning

The study we carried on showed that challenges that emerged during the pandemic are still a hindrance today when implementing an online course but also when taking a course. They are described in subsequent sections.

Challenges for trainers

- Use of technology

  The technological challenges of e-learning can be considered as key technological and pedagogical research area. Trainers who are new to an LMS platform can be reluctant to implement courses on such a tool. The amount of work needed to create and implement such a course often acts as a deterrent for trainers who gave in-person classes all their lives.

- Lack of learner engagement and motivation

  Not every online learner is going to be 100% committed to the e-learning experience. They may be distracted, busy, or simply unmotivated. We live in an age where attention is at a premium and learners have access to more information than they can consume. All of these hurdles prevent them from actively engaging with online learning programs.

- Staying up-to-date with modern technology

  Every year welcomes new tech tools, gadgets, and software that you can use to improve e-learning delivery methods. But, with so much digital transformation, it can be hard to tell which new learning technology is worth the investment.

- Designing e-learning courses for different generations

  Learning content isn't one-size fits all. Our audience is now made up of four different generations — Baby Boomers, Gen X, Millennials, and Gen Z, which can make it challenging to create generic e-learning experiences for all, since each generation has its own traits and needs (Moore, Jones & Frazier, 2017).

- Balancing tight e-learning budgets

  E-learning projects always come with limited budgets. In fact, most will be restricted to limited financial resources, so being creative to work with what you've got becomes an obligation. Before starting any e-learning project, the trainer may have to draft

a detailed budget that includes all expenses and make sure to have a realistic estimate of what the project is going to require.

- Finding the perfect e-learning authoring tool or learning platform

  Choosing a new e-learning authoring tool or LMS can be a challenging process. There are so many e-learning authoring tools and learning platforms to choose from and so little time. The main difficulty resides in dedicating the right amount of time for the selection of the right tool.

Challenges for trainees

- Equipment

  The lack of proper equipment for trainers at home is the main reason why e-learning can be challenging. Some trainees do not have a computer or possess too old an equipment to make the platform work. Even from their workplace, French Police officers can be hindered by out outdated computers or machines limited by security protocols.

- Familiarity with digital tools

  Although new generations are generally very comfortable with computers, older officers are sometimes reluctant to work on PCs and find the process of studying on the internet cumbersome and unproductive. They easily give up in front of a tool they are not familiar with. The police administration quickly realises that

  "*the online environment presents challenges for many academic staff who increasingly require higher levels of technological competency and proficiency on top of their regular academic workload.*" (Gillett-Swan, 2017)

- Lack of in-person teaching

  Some people need classroom contact and only learn when in a real classroom with another human being. We are human beings and as such, socializing is paramount in our own psychological construction (Grundmann, 2018). After two years of COVID, the need for real life interactions became even more fundamental.

- Lack of motivation

  When working from home, learners are easily distracted from their computer. Whether their kids or their daily chores, they always find another activity if the online course is not captivating enough. Motivation has to be triggered through interactive activities and reachable learning outcomes. Whatever the learner's profile, game-based activities are often a good tool against boredom and lack of motivation

Evolution of Law enforcement training: a new strategy

The tsunami that was COVID created a shockwave in the training spheres of the Police forces in France and in Europe. Training departments faced the hard reality of the uselessness of their teaching method in that particular context.
Already before COVID, Police training departments had an LMS platform (Moodle) that they did not (or seldom) used. From the start of the pandemic, the realisation became clear. All courses had to be implemented and e-learning was the only way to convey knowledge and assess students. Fundamental questions were then raised:

- Was the existing platform powerful and efficient enough to hold future activities and courses?
- What software was available to implement attractive activities?
- What courses could be offered on the platform?
- And above all: which students would be targeted by these online courses?

Within the French Police Nationale, a Digital Training Division (DFD) was created within the "Sub directorate of training and exams (Sous-direction des Méthodes et de l'Appui) in order to monitor that new necessary aspect of Training. The necessity for civilian experts in the field of training and e-learning techniques became pressing.

Teachers from the French National Education system were hired as trainers to support the need for training specialists. In parallel, Online education and e-learning experts were also called upon to set up the organisation of an online Police curriculum on the national level. But this took time.

In the meantime, the first and most important issue was to resume the training of future cadets. It was then decided to create online classes on all the subjects that

were not operational proper regardless of the previously settled calendar. In-person operational courses (shooting practice, self-defence, anti-riot techniques etc.) would be left for later when COVID-19 would have subdued.

Whether from a lack of time, imagination, or skills, the first courses offered by trainers on the *Police Nationale* LMS platform (E-campus) were a list of copy-pasted typed lectures the student could only read and memorize, assessed by a quiz or two. Interactivity was not considered. Likewise, learning outcomes were not clear and the pedagogical progression absent.

Quickly though, with the help of newcomers and the will among trainers to improve trainees' experience, courses became more and more structured and aimed at meeting clearer outcomes designed in respect to a relevant taxonomy. A coherent learning process led to an obvious and efficient choice of activities. An issue remained however, how could the learner get fully involved in the process.

The answer seemed obvious. Courses needed more interactivity. With the pandemic and the dire need to develop online applications, new software became available to create a number of interactive activities. Along with authoring tools such as Storyline, Rise 360, H5P, useful websites (learningapps, genially, classflow etc.) but also game-based applications (mentimeter, slido, kahoot), learning activities became much more interactive, enabling the learners – here academy cadets - to get involved and be more active in the learning process.

The after-COVID period resumed in-person courses. It was indeed a relief for numerous trainers and trainees, from a social point of view as well as an educational one. However, the possibilities offered by e-learning during the pandemic opened a new way of teaching. The challenge then became to be more flexible and give the learners new opportunities to learn, whether from home or from the academy.

Blended Learning therefore became the best option in giving the learners a flexibility that did not exist before (Belur & Bentall, 2021). Being able to study self-paced lectures from home and get practical courses (or operational skills) during in-person sessions. Not only did it become obvious for trainers and trainees, but it also convinced a formerly reluctant Police administration.

Not only cadets but also experienced Police officers could now attend virtual classes when they had time, between shifts and from their workplace, allowing a more cost-effective and less time-consuming training program for the Police administration.

Conclusion

With the COVID-19 pandemic, the French Police administration reacted quickly with a new e-learning offer, bringing along experts and teachers with another view of what Police training should be. Modernizing its training process took some time but it clearly understood the necessity of such tools for the new generations of cadets arriving at the academy.

In the meantime, the administration realised the financial and organisational benefits of such online trainings for Police Officers who worked shift and could not, before, attend a training, except by taking some days off from work.

However, hard habits die hard, and the Police administration is still reluctant to fund e-learning material and useful (if overly expensive) web software that could improve trainers' creativity while enhancing the relevance of courses for trainees.

Because of the various and cumbersome challenges, the temptation was hard from the Police administration to resume all in-person classes, but the benefits of online classes prevailed. While operational skills still rely on practical in-person classes (self-defence classes/ shooting range drills and others) for obvious reasons and despite recent applications' interactivity, a growing number of online sessions are opened on the French E-campus every day, showing the way to a new way of teaching within the French Police.

Keeping in mind that Police work is a field job, the operational practical skills are a large part of the curriculum and cannot be transferred online unless virtual gaming is one day put into the equation. In any case, the French police adopted a new teaching balance. Blended Learning has become for the French Police what some authors would call the "new normal" in course delivery (Norberg, p. 207), thus enabling the learner to combine self-paced theoretical study and in person practical classes, probably achieving the most important modernization of training in the past 20 years.

References

- Alpert, G. P., Dunham, R. G. & Stroshine, M. S. (2015) Policing: Continuity and Change. Second Edition. Long Grove, IL: Waveland Press, Inc.
- Bartkowiak-Théron, I. (2019) Research in police education: current trends, Police Practice and Research. 20(3), 220-224. https://doi.org/10.1080/15614263.2019.1598064
- Beavis, C. (2017) Serious play: Literacy, learning and digital games. In C. Beavis, M. Dezuanni, & J. O'Mara (eds.) Serious Play. New York, NY, Routledge, pp. 17–34.
- Belur, J. & Bentall, C. (2021) Blended learning: The future of police education. CEPOL Online Research & Science Conference - Pandemic Effects on Law Enforcement Training and Practice, 5-7th May 2021.
- Camilleri, M.A. & Camilleri, A.C. (2017) Digital learning resources and ubiquitous technologies in education. Technology, Knowledge and Learning, 22(1), 65-82. https://doi.org/10.1007/s10758-016-9287-7
- Campbell, W. K., Campbell, S. M., Siedor, L. E. & Twenge, J. M. (2015) Generational Differences Are Real and Useful. Industrial and Organizational Psychology. 8(03), 324-331.
- Direction de la Formation Digitale SDMA PN Statistiques (2021) pour la plateforme E-campus
- European Commission 2001**.** The e-learning action plan : Designing tomorrow's *education*
- Gillette-Swann, Jenna (2017) The Challenges of Online Learning: Supporting and Engaging the Isolated Learner. Journal of Learning Design, [S.l.], v. 10, n. 1, p. 20-30. ISSN 1832-8342.
- Grundmann, Matthias (2018) Social constructions through socialization, In M. Pfadenhauer & H. Knoblauch (eds) : Social Constructivism as Paradigm ?. London: Routledge, pp.91-104.
- Hargittai, E. (2010) Digital na(t)ives? Variation in internet skills and uses among members of the net generation". Sociological Inquiry. 80(1), 92-113.
  Available from: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1475-682X.2009.00317.x
- Himberg, K. (2021) COVID-19: The legacy of the pandemic in police education. CEPOL Online Research & Science Conference - Pandemic Effects on Law Enforcement Training and Practice, 5-7th May 2021.
- Hubackova S**.** (2015) History and Perspectives of Elearning, Procedia - Social and Behavioral Sciences,Volume 191, pp. 1187-1190.
- Kirschner P. A. & De Bruyckere, P. (2017) The myths of the digital native and the multitasker. Teaching and Teacher Education. 67, 135-142. https://doi.org/10.1016/j.tate.2017.06.001
- Mailfait Pierre-Antoine. (2002) « La formation professionnelle des policiers. Promotion René Cassin », *Revue française d'administration publique*, vol. n°104, no. 4, pp. 625-638.
- Moore, K., Jones, C. & Frazier, R. S. (2017) Engineering education for Generation Z. American Journal of Engineering Education. 8(2), 111-126. https://doi.org/10.19030/ajee.v8i2.10067
- Norberg, A., Dziuban, C. D., & Moskal, P. D. (2011). A time-based blended learning model. *On the Horizon*, *19*(3), 207–216. https://doi.org/10.1108/10748121111163913
- Ransley, J. & Mazerolle, L. (2009) Policing in an era of uncertainty. Police Practice and Research. 10(4), 365-381. https://doi.org/10.1080/15614260802586335
- Seemiller, C. & Grace, M. (2017) Generation Z: Educating and engaging the next generation of students. About Campus: Enriching the Student Learning Experience. 22(3), 21 -26. https://doi.org/10.1002/abc.2129
- Vidal Martine (2020) « L'enseignement à distance, trait d'union en temps de pandémie », *Distances et médiations des savoirs* [En ligne], 32 | 2020.
  Available from : http://journals.openedition.org/dms/5721
- Wilson, K. A., Bedwell, W. L., Lazzara, E. H., Salas, E., Burke, C. S., Estock, J., Orvis, K. L. & Conkey, C. (2009) Relationships between game attributes and learning outcomes: Review and research proposals. *Simulation & Gaming*. Vol.40 (2), pp. 217-266.

The Influence of Digital Devices on Learning Interest, Engagement and Academic Performance in Basic Police Training – Experiences and Findings

Micha Fuchs
Kristina Ott
Department Police Training and Further Education,
Bavarian Riot Police, Bamberg[1]

Abstract
The Bavarian Police training aims to equip all 750 police teachers and 4.000 police officer trainees with officially approved police tablet PCs and smartphones by the end of 2025. Following a phased approach, teachers and trainees are being issued with tablet PCs (convertibles) and smartphones. Overall, there is no doubt that the use of digital devices is important and necessary in order a) to prepare the police trainees for their future work as police officers and b) to support their learning process. However, the question arises as to how exactly they benefit from those digital devices. For getting a first insight on the impact of digital devices on learning interest and engagement of police officer trainees in the classroom, as well as on their academic performance in general, the Bavarian Police conducted a digital pilot project with a single unit of 100 police officer trainees and 20 police teachers and trainers for 21 months from December 2019 to August 2021. The findings show that different digital devices have different impacts on the learning behaviour as well as on the academic performance of the police trainees. Above all, tablet PCs and interactive whiteboards have shown to improve learning behaviour. Furthermore, the findings show that digital devices, which are not used regularly, do not improve the classroom behaviour of the trainees or they may even worsen it slightly. The study puts forward several practical suggestions for the further implementation of digital devices at police training such as the necessity of training for the police personnel and the need to develop new didactic methods as well as new modes of teaching.

Keywords: police training, digitalisation, mobile devices, learning interest, academic performance

1 Author's email: micha.fuchs@polizei.bayern.de

Introduction[2]

The world and society are continuously changing and, especially the digital transformation has increased the speed of this change. Therefore, the police as an organisation, the fields of work and police training are also strongly affected by the digital transformation. While the research on digitalisation and its impacts on schools and higher education (e.g., Hwang & Tsai, 2011; Nikou & Economides, 2018) has led to a large number of empirical studies and projects, the number of publications on the impact of digitalisation on police education and training remains low. Research on police education tends to focus on topics such as the relationship between police training, higher education, and performance (Albarano, 2015; Henson et al., 2010), use of force (Paoline & Terrill, 2007), police behaviour (Rosenfeld, Johnson & Wright, 2020; Rydberg & Terrill, 2010) or the impact on simulation based training in police education and training (Beinicke & Muff, 2019; Sjöberg, Karp & Rantatalo, 2019). However, empirical research on the impact of digitalisation on police education and training (e.g., Chapparo, 2017; Holmgren, Holmgren & Sjöberg, 2019) is currently very limited.

In the following, we will show how Bavarian police training has responded to the digital transformation and what are the actual measures adopted by it. We shall present empirical findings on how the use of digital tools in police training has proven itself so far. Although empirical evaluations are still rare in the police context, the evaluation of the measures and actions taken is essential in finding out what works and what more needs to be done to achieve the desired success. Firstly, the Bavarian police training is briefly described to enlighten the context of our study.

The Bavarian Police approach to face digital transformation in police training

Already before the COVID-19 pandemic in spring 2020 the Bavarian police training had launched the process to renew and replace the classroom equipment in their police academies with digital devices (digital whiteboards). The COVID-19 in spring 2020 accelerated this on-going digitalisation process enormously. For example, a learning management system (LMS) (operated by the open source software ILIAS) was implemented and has since been used as a central component in teaching and learning at classroom as well as in self-study. In addition to the adoption of the LMS, teaching and learning materials were also changed accordingly or created anew.

Besides the immediate response to COVID-19 and its consequences for police training (e.g., locking down all police facilities), the Bavarian Police decided to equip its police students with digital devices by 2025 and formulated guidelines for managing this process (cf. Fuchs, 2022). Since September 2022, 3,040 police trainees (around 80% off all trainees) have received personally assigned convertibles.

The convertible is used in two ways. On the one hand, it provides a learning medium. Trainees can, for example, take notes on learning materials in class, prepare for tests or participate in video conferences. On the other hand, they can use the convertible as an operational tool. It can be used to make queries in the police systems or to create an accident sketch via the tablet function. By taking the convertible to the internships at the Police stations, the transition from the police training to the police practice can be made seamless.

Additionally, the Bavarian Police pursues the *Mobile Police* (mPolice) concept. The same equipment is available in the police stations as is used in training. The so-called *mPolice* smartphones enjoy a high level of acceptance among the police officers. The police trainees learn about the police applications of the smartphone in the class and in practical training. *mPolice* smartphones were distributed to police trainees.

To enable the smooth functioning of the new digital devices, the technical infrastructure in the police academies had to be upgraded. The Figure 1 points out the four central components. i.e. qualified teachers, didactics, learning platform, hard- and software, a successful digitalisation process in police training requires.

Method

Context of the study – Bavarian Police training

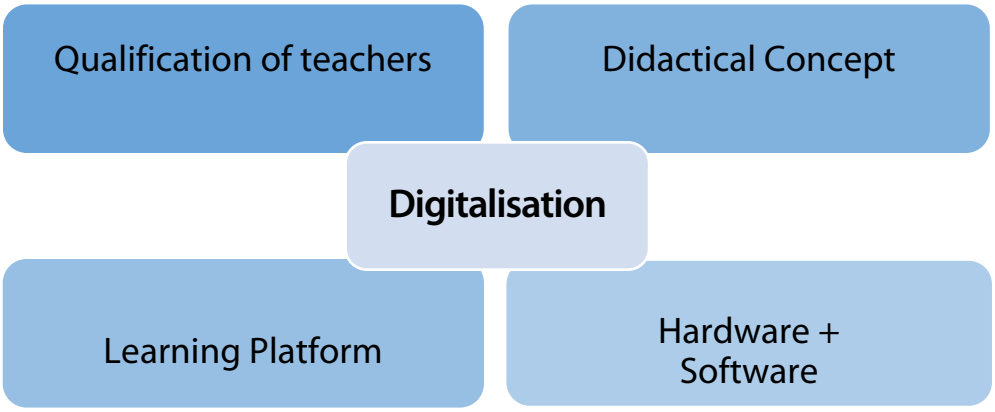
Our study evaluates the implementation of the digital pilot project in Bavarian Police training. Bavaria is a federal state in the south-east of Germany with a popu-

2 Acknowledgement: This paper is derived in part from an article published in Police Practice and Research: An international Journal, published 24 April 2022, available online: http://www.tandfonline.com/10.1080/15614263.2022.2067157

lation of 13.1 million. In 2022, the Bavarian Police has 44,000 employees, including around 3,800 police trainees. In total, the Bavarian Police comprises six police academies of different sizes in terms of the number of personnel and trainees.

Each police academy is divided in organisational units of 100 to 160 police officers. All the trainees complete their police training within their respective units. In the two and a half years of the police training (divided into five terms), each trainee completes 5,000 hours of classroom lessons and practical training.

Figure 1: Four central components for a successful digitalisation process in police training (own illustration)



The curriculum consists of two almost equally weighted parts. On the one hand, there are Legal Theory classes as well as studies in Politics, Professional Ethics and English. On the other hand, there are practical classes such as simulation-based training for typical work situations (e.g., traffic checks or domestic violence interventions), lessons in Driving and Communications as well as in Self-Defence and Physical fitness. Moreover, the curriculum includes two internships at a local police station for four weeks (during the third term of training) and again for twelve weeks (during the fourth term of training). After passing the final examination[3], police officer trainees can join a police station or the riot police or qualify for the higher education programme (diploma programme of the Bavarian Police).

Participants

Instead of equipping the whole police training personnel (700), all police officer trainees (3,800) and each classroom (160) at once with the new devices, it was decided to launch a pilot project in one organisational unit (project unit) with 25 teachers, 99 police officer trainees and 4 classrooms[4]. Initially the participants in the study comprised all 99 police officer trainees (29.0% female), but six police officer trainees left the unit during the training run. By the end of the police training, 21.5% of the participating 93 police officer trainees were between 19 and 21 years old, 49.5% between 22 and 24, 17.2% between 25 and 27, and 11.8% were 28 years or older. In addition, five organisational units (N = 629; 25.6% female) of the same cohort served as control group regarding the measurement of academic performance.

Research design

In the second term of their police training in December 2019, each classroom in the project unit was equipped with an interactive whiteboard (IWB). Previously the classrooms in the project unit had a data projector and a whiteboard, like the classrooms in the other organisational units.

In early March 2020, the teachers involved in the project attended a one-day workshop on the use of IWBs. The workshop consisted of two parts: a theoretical part on lesson structure and learning settings with digital devices and on the interactive possibilities regarding whiteboard and learning management system, as well

3 The final exam consists of two parts: a) the written exam including four different sub-exams regarding the topics patrol duty, traffic police work, crime prevention and working in a police station and b) a practical examination.

4 Due to the positive results during the evaluation period of the project unit, the Bavarian Police was encouraged to continue on the path of digitalising the entire police training and therefore equipped other organisational units with digital devices even before the end of the evaluation of the project unit.

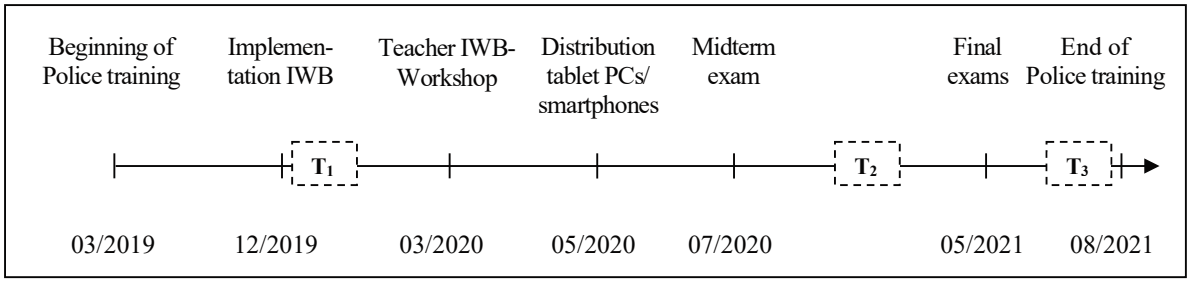
as a practical part where the participants would learn how to handle and use the IWB by trial and error.

In May 2020, each trainee received a personal tablet PC for their remaining time at the police training until August 2021 supported by a technical briefing in its use. Until the end of their training, the police officer trainees had the opportunity to use their tablet PCs as a fully-fledged learning medium during and after lessons (e.g., taking lecture notes, looking things up on the internet, preparing for exams).

In addition, all the trainees in the project unit received a personal smartphone and a technical introduction to it. The use of the smartphone in the class was at the discretion of the respective teacher (e.g., to look things up on the internet or to do police queries or quizzes).

Due to the unsteady course of the COVID-19 pandemic, different instructional settings had to be implemented from March 2020 to August 2021 in addition to the usual classroom teaching, e.g., learning and practising in smaller groups and/or online teaching. To measure the influence of the digital devices in the classroom, three surveys were conducted: January 2020 (T_1), November 2020 (T_2) and July 2021 (T_3) (cf. Figure 2).

Figure 2. Overview of the research design



Note: IWB = interactive whiteboard

Instrument/Measures

The survey items were developed based on a previous research by Gerrick and Eickelmann (2017) and Renz, Rayiet and Soltau (2012) on the use of digital devices in the classroom.

Student engagement: To measure the influence of digital devices on student engagement, three items were asked on a 5-point Likert scale ranging from 1 (*negative*) via 3 (*neutral*) to 5 (*positive*) for tablet PCs and smartphones, e.g., "Using my tablet PC during class has influenced my active participation".

Learning interest: The parameter learning interest was measured with two items "Using the digital device during class helps me to develop a greater interest in learning" and "Using the digital device motivates me and raised my interest" using the same Likert scale as mentioned above.

Frequency of usage behaviour: In order to find out how often and for what purpose the mobile devices were used, the two scales *classroom-related behaviour* and *field-related behaviour* (e.g., "How many times do you use your smartphone to check administrative-related applications?") were developed on a 5-point Likert scale (1 = never; 3 = several times a week; 5 = several times a day). The scale classroom-related behaviour comprised five items (e.g., "How many times do you use your tablet PC to take lecture notes?") and the scale field-related behaviour, also comprised five items (e.g., "This is how often I use my tablet PC to get information about my organisational unit.").

Visualisation of instructional content: To measure the influence of the interactive whiteboard on visualisation methods of instructional content, a visualisation scale was developed on a 5-point Likert scale from 1 (*negative*) to 5 (*positive*) with three items (e.g., "The use of the interactive whiteboard has changed the visualisation of the instructional content in class.").

Academic Performance: In order to measure the impact of digitalisation at the project unit, two objective performance measures were taken: the results of the written midterm exams in July 2020 and the results of the written final exam in May 2021. Both exams consisted of four sub-examinations on the topics patrol duty,

traffic police work, crime prevention, and working in a police station.

Mobile devices as operational tools: An important reason for the digitalisation of the Bavarian police training, apart from the intended improvement of the police training in general, is the concomitant improvement of user competence regarding tablet PCs and smartphones as operational tools. In order to find out whether the classroom implementation of those two mobile devices had improved the practical use of those devices in their future purpose as operational tools, the following item was used "The use of the tablet PC has improved my practical competence in using the tablet PC as an operational device". The item ranged on a 5-point Likert scale from 1 (negative) to 5 (positive).

Further measurements: Two additional questions were asked at the end of each survey. The first question asked the trainees to evaluate the project. Using a positive statement, the trainees rated their impression on a 5-point Likert scale from 1 (*strongly disagree*) to 5 (*strongly agree*). The second question aimed at how the police officer trainees rate the future importance of traditional (e.g., books, worksheets) and digital teaching and learning materials (e.g., tablet PC, videos, learning management systems) in the classroom on a 10-point scale from 1 (*very unimportant*) to 10 (*very important*).

Data collection and analysis

In order to assess the impact of the interactive whiteboards in the classroom, the trainees responded to the first survey in January 2020 (T_1). The second survey was conducted in November 2020 (T_2); half a year after the trainees had received their tablet computers and had started to use the smartphones during practical police training. After the trainees had passed their final exams, the third survey was conducted (T_3) in July 2021 (Fig. 1).

The surveys were conducted using the web-based open-source learning management system ILIAS (Integrated Learning, Information and Work Cooperation System) within the police internal network. All surveys consisted of a questionnaire with 65 items altogether and took approximately 15 minutes to complete.

As the police officer trainees received their tablet computers and smartphones in May 2020, these topics were only covered in the second and third surveys in November 2020 and July 2021 respectively. All analyses were computed in IBM SPSS Statistics 23. To facilitate interpretation, the effect size d for the t-tests (d = 0.20 ≙ small; d = 0.50 ≙ medium; d = 0.80 ≙ large), the effect size η^2 for the ANOVA (η^2 = 0.01 ≙ small; η^2 = 0.06 ≙ medium, η^2= 0.14 ≙ large) and the correlation coefficient r (r = 0.10 ≙ small; r = 0.30 ≙ medium; r = 0.50 ≙ large) were calculated (cf., Cohen, 1988).

Findings

Student Engagement: The trainees rated their use of tablet PCs as rather positive in terms of engagement after six months on a 5-point Likert scale (M = 3.69; SD = 0.69) and after eight more months of use (M = 3.75; SD = 0.76), $t(160) = 0.51$, $p = .79 > .05$, $d = 0.08$). In contrast, the trainees rated the use of smartphones in the classroom as ineffective or slightly negative in terms of their own engagement after six months of use (M = 2.86; SD = 0.60) and after another eight months of use (M = 2.85; SD = 0.76), $t(160) = -0.69$, $p = .95 > .05$, $d = -0.01$.

Learning interest: The results for the influence on learning interest showed an overall positive influence for the tablet PCs after six months (M = 3.72; SD = 0.68) and after eight more months of use (M = 3.76, SD = 0.77), $t(159) = 0.33$, $p = .75 > .05$, $d = 0.05$. Almost identically to the analysis of the influence on student engagement, the smartphones had no or a slight negative influence on learning interest after six months (M = 2.83; SD = 0.63) and also after eight further months of use (M = 2.86; SD = 0.77), $t(159) = 0.05$, $p = .96 > .05$, d = 0.01.

The strongest influence on the police officer trainees' interest resulted from the implementation of the interactive whiteboard (IWB). The conducted *ANOVA* analysis shows that after three weeks of using the interactive whiteboard, there was a slightly positive influence the trainees' interest (M = 3.41; SD = 0.66), which increased significantly after ten months of use (M = 3.88; SD = 0.79) and again marginally after 18 months of use (M = 3.94; SD = 0.88), $F(2,254) = 12.62$, $p < .001$, $\eta^2 = 0.09$. The subsequent *Tukey post-hoc* analysis revealed a significant difference between the first measurement and the second measurement (.47, 95%-CI[.20,.73]) and between the first and the third measurement (.53, 95%-CI[.25,.82]).

Frequency of use: As Table 1 shows, there is a difference in the frequency of use of tablet PCs and smart-

phones regardless of classroom use patterns or field-related behaviour. On average, the trainees reportedly used the tablet PCs between about once a day and several times a week with a slight preference towards classroom hours. In contrast, the use of smartphone during police training was sporadic throughout the sample period, with significant increases in frequency at low levels after the first survey in November 2020 for both usage patterns.

Table 1. Influence of mobile devices on learning interest and engagement as well as frequency of use of mobile devices in regard to different usage behaviour in the context of police training

		Nov. 20 (T_2) M_1 (SD)	July 21 (T_3) M_2 (SD)	t-value	Effect size *d*
Tablet PC					
Motivation	learning interest	3.72 (0.68)	3.76 (0.77)	0.33	0.05
	engagement/activation	3.69 (0.69)	3.75 (0.76)	0.51	0.08
Usage pattern	classroom-related	3.38 (0.93)	3.48 (1.00)	0.70	0.11
	Field-related	3.29 (0.90)	3.23 (1.07)	-0.36	-0.06
	overall use	3.33 (0.79)	3.36 (0.95)	0.18	0.03
Smartphone					
Motivation	learning interest	2.83 (0.63)	2.86 (0.77)	0.05	0.01
	engagement/activation	2.86 (0.60)	2.85 (0.76)	-0.69	0.01
Usage pattern	classroom-related	1.18 (0.31)	1.45 (0.61)	3.55**	0.56
	field-related	1.18 (0.41)	1.33 (0.62)	1.95*	0.31
	overall use	1.18 (0.30)	1.39 (0.59)	2.97*	0.47

Note: * = $p < 0.05$; ** = $p < 0.01$;

M_1 = 11/20 (six months after implementation); M_2 = 07/21 (fourteen months after implementation)

$Scale_{Motivation}$: 1 = *negative*, 3 = *neither negative nor positive*, 5 = *positive*

$Scale_{Usage\ pattern}$: 1 = *never*, 2 = *several times a month*, 3 = *several times a week*, 4 = *once a day*, 5 = *several times a day*

Furthermore, Table 2 shows that there are significant positive correlations between the frequency of tablet PC use – regardless of the usage behaviour – and the learning interest, respectively engagement, of the police officer trainees. In contrast, the frequency of smartphone use does not correlate significantly with learning interest and engagement.

Table 2: Relationship between frequency of use of mobile devices in relation to learning interest and engagement of police officer trainees in terms of different usage behaviour.

	(1)	(2)	(3)	(4)	(5)
Tablet PC					
(1) Overall frequency use	-	0.89**	0.89**	0.51**	0.44**
(2) Frequency classroom behaviour		-	0.58**	0.53**	0.49**
(3) Frequency field-related behaviour			-	0.37**	0.29**
(4) Learning interest				-	0.87**
(5) Engagement/activation					-
Smartphone					
(1) Overall frequency use	-	0.91**	0.92**	0.10	0.12
(2) Frequency classroom behaviour		-	0.68**	0.07	0.10
(3) Frequency field-related behaviour			-	0.10	0.12

(4) Learning interest	-	0.97**
(5) Engagement/activation		-

Note: ** = $p < 0.01$

Visualisation of teaching content

The police officer trainees stated a quite positive influence of the interactive whiteboard on the visualisation of instructional content in the classroom after one month of use ($M = 3.96$, $SD = 0.58$). After ten months ($M = 4.44$, $SD = 0.66$) as well as after eighteen months ($M = 4.54$, $SD = 0.52$) the influence of the interactive whiteboard on visualisation of the teaching content increased significantly, $F(2,254) = 23.31$, $p < .001$, $\eta^2 = 0.16$. The following *Tukey post-hoc* analysis revealed a significant difference between the first measurement and the second measurement (.48, 95%-CI[.26,.68]) and between the first and the third measurement as well (.58, 95%-CI[.35,.80]).

Academic performance

Table 3 shows mixed results on the academic performance of the project unit compared to the reference unit.

Table 3. Descriptive statistics between the project unit and its reference units in terms of grade points for the midterm examination and the final written examination.

		N	M (SD)	Median	Min	Max
Midterm exam	Project unit	93	9.23 (1.95)	9.50	5.50	12.75
	Reference units	629	9.09 (1.85)	9.00	4.25	13.50
Final written exam	Project unit	92	8.77 (1.67)	8.94	5.12	12.75
	Reference units	617	8.83 (1.83)	8.75	4.00	13.62

Note: Grading scale: 0.00-1.99 ≙ very poor (fail), 2.00-4.99 ≙ unsatisfactory (fail), 5.00-7.99 ≙ satisfactory, 8.0010.99 ≙ good, 11.00 -13.49 ≙ very good, 13.50-15.00 ≙ excellent

With regard to the midterm exam, the project unit achieved a slightly higher grade points average ($M = 9.23$, $SD = 1.95$) than the reference units ($M = 9.09$, $SD = 1.85$). However, the following *t-test* showed no significant difference between both groups $t(720) = 0.70$, $p = .48 > .05$, $d = 0.08$. The results of the final written exam also revealed no significance difference between the project unit ($M = 8.77$, $SD = 1.67$) and the reference units ($M = 8.33$, $SD = 1.83$), $t(707) = -0.29$, $p = .77 > .05$, $d = 0.03$.

Mobile devices as operational tools

In addition to the use of the digital devices as learning medium, there is a high expectation in the Bavarian Police that the implementation of tablet PCs and smartphones will improve the use and handling of both devices as operational tools for future police officers. The following analyses show that the police officer trainees consider the use of a tablet PC as a later operational tool to be helpful both after six months ($M = 4.43$, $SD = 0.69$) and after a further eight months ($M = 4.37$, $SD = 0.66$). The subsequent t-test showed no significant change over the course of the project, $t(159) = 0.53$, $p = .60 > .05$, $d = -0.09$. Despite the fact that the smartphone was only used sporadically during the pilot project (Table 1), the trainees rated the use of the smartphones as slightly positive after six months ($M = 3.38$, $SD = 0.83$) and after 14 months ($M = 3.33$, $SD = 1.05$) in terms of them handling it as a future operational tool. There was no significant time trend, ($t(159) = 0.38$, $p = .71 > .05$, $d = 0.06$).

Further measurements – evaluation of the digital pilot project and importance of the use of future teaching and learning material

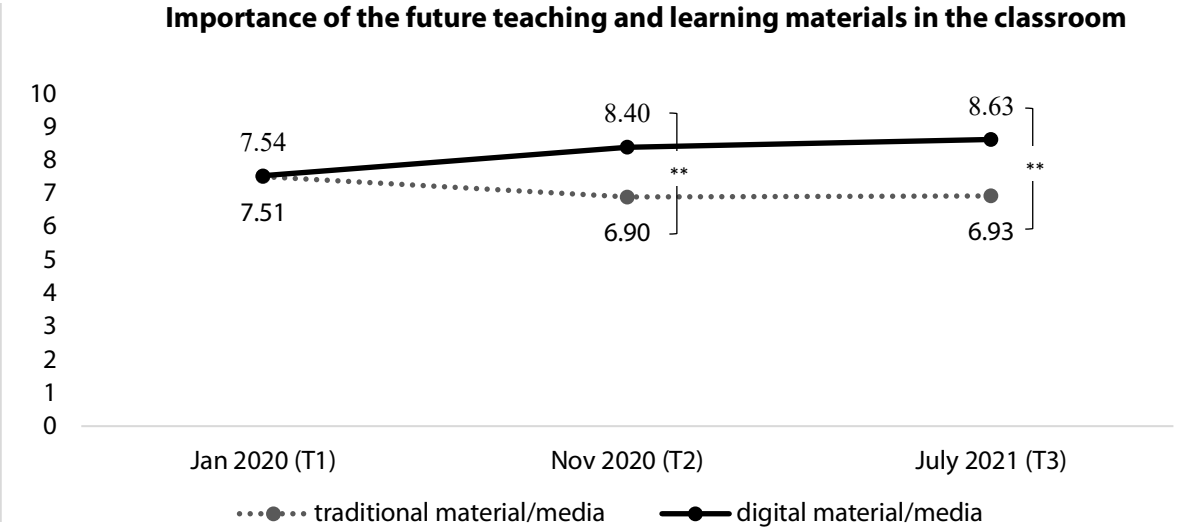
The results of the evaluation of the digital pilot project based on the project unit police officer trainees' perception show that the trainees rated the pilot project quite positively at the first measurement point - one month after the start (January 2020) ($M = 4.23$, $SD = 0.83$). In the course of the digital pilot project, the positive assessment on the pilot project increased at the second measurement point in November 2020 ($M = 4.44$, $SD = 0.73$) and at the end of the police training in July 2021 ($M = 4.56$, $SD = 0.53$). The following *ANOVA* analysis shows a small but significant effect

between the three individual measurement points, $F(2,254) = 4.52$, $p < .05$, $\eta^2 = 0.03$.

The analysis on the importance of the use of future teaching and learning materials on a scale of 0 to 10 shows at the first measurement point (January 2020) that both traditional ($M = 7.51$, $SD = 2.65$) and digital teaching and learning materials in the classroom ($M = 7.54$, $SD = 2.56$) are considered equally important by the trainees. In the course of the pilot project, both lines run in opposite directions, as figure 3 shows. The importance of digital teaching and learning materials in the classroom increases continuously in November 2020 ($M = 8.40$, $SD = 1.60$) and at the third measurement point in July 2021 ($M = 8.63$, $SD = 1.34$).

The following *ANOVA* analysis shows that the police officer trainees rated the importance of using future digital teaching and learning materials significantly higher over the course of the pilot project (January 2020 until July 2021), $F(2,257) = 7.58$, $p < .01$, $\eta^2 = 0.06$. On the other hand, the importance of traditional teaching and learning materials in the classroom decreased at the second measurement in November 2020 ($M = 6.90$, $SD = 2.57$) and levelled off at the third measurement in July 2021 ($M = 6.93$, $SD = 2.65$). However, the conducted ANOVA-analysis shows no significant decrease during the course of the pilot project, $F(2, 257) = 1.57$, $p = .21 > .05$, $\eta^2 = 0.01$.

Figure 3. Assessment of the importance of future teaching and learning materials in the classroom over the course of the digital pilot project.



Note: ** = $p < 0.01$

Scale: 0 = *very unimportant* to 10 = *very important*

Regarding the direct comparison between the future use of both forms of teaching and learning materials and media, the following *t-tests* show a significant difference at the second measurement date, $t(180) = 4.72$, $p < .001$, $d = 0.70$ and at the third measurement date, $t(138) = 4.80$, $p < .001$, $d = 0.81$ in the preference for the importance of using digital teaching and learning material.

Discussion

This study focused on the relation between the use of digital devices in the classroom and engagement, learning interest, and academic performance of police officer trainees in police training from December 2019 to August 2021. The study examined whether the use of interactive whiteboards improves teaching methods (visualisation) and whether the use of mobile devices (tablet PCs and smartphones) improves the handling of them as operational tools.

The results provide some new insights on the impact of digital devices on learning behaviour and academic performance in police training. Firstly, within a short time of their implementation, the use of the interactive whiteboards was related to a positive development in learning interest. The same trend was found in relation to personal tablet PCs. Secondly, digital devices that are not used regularly, interfere with the learning process and participation in the classroom. Thirdly, the use of digital devices in police training does not show a significant influence on academic performance at this stage of implementation. Fourthly, the regular practical use of tablet PCs during police training helps to prepare the trainees to use and handle their tablet PCs as operational tools. Finally, the new generation of police officer trainees tends to prefer to be taught via digital devices and digital teaching material.

Conclusion and practical implications

Digital devices will play a crucial part in teaching and learning at every future classroom setting including police education and training (Fuchs, 2022). Our pilot study has very important empirical results for further action and has encouraged the Bavarian police to continue on the chosen path in digitalising the police training. Therefore, the question for the future of police training – at least for the Bavarian police training – is not whether digitally supported teaching should take place, but with which digital tools, in which way and which administrative departments should be in charge and should work with which means.

The conducted pilot study showed that, above all, interactive whiteboards and personal tablet PCs can immediately improve teaching and learning settings in police training. Nevertheless, there are areas where the conventional approach to police training is more useful or a mix of both the old and the new achieves the best results. Hence, to reach the full potential of digital devices in educational settings, it is crucial that teachers and policy makers find strategies to integrate mobile devices into teaching concepts and curricula and find ways to use the unique features of mobile devices (e.g., mobile game-based learning) and to solve specific pedagogical challenges (e.g., distraction, superficial information processing) (cf. Sung, Chang & Liu, 2016).

Thus, what can police training learn from the findings of the pilot study? Firstly, qualification and training for teachers and instructors have a key role in the integration of technology into teaching and practical training. In addition, the training courses should have a high practical relevance, where the various digital devices can be actively tried out.

Secondly, both the faculty as well as the administration of police training have to embrace the digital transformation and the changes it entails. Therefore, an overall media-pedagogical concept is needed that explains the vision, the opportunities but also the challenges, and, above all, the necessary action and implementation steps of the digitalisation in police training.

Thirdly, hardware (digital devices) and software (e.g., learning management system (LMS)) as well as the technical infrastructure must function properly to ensure acceptance by police teachers and trainees. Furthermore, it is recommended to integrate the LMS into the police network so that all learning and teaching materials – both non-confidential as well as confidential – can be shared. Moreover, the integration of the LMS into the police network offers the possibility to provide the complete police training content via LMS for in-class teaching as well as distance and hybrid learning models.

Fourthly, the learning and teaching materials need to be adapted to the new learning and teaching context, therefore new forms of learning and teaching material need to be created e.g., interactive videos, quizzes, wikis, learning modules. Finally, in order to improve teaching and learning in combination with digital devices and to meet the requirements of the new generation of police officer trainees, *new* teaching forms such as Just-in-time teaching (Novak, 2011) and Flipping the classroom (Davies, Dean & Ball, 2013; McLean et al., 2016) should be tried out.

References

- Albarano, R. F. (2015) College education and officer performance: Do college educated police officers perform better than those without a college education? *International Journal of Education and Social Science*, 2(7), 41-48.
  Available from: https://web.archive.org/web/20180410143511id_/http://www.ijessnet.com/wp-content/uploads/2015/08/5.pdf [Accessed 6th July 2022].
- Beinicke, A., & Muff, A. (2019) Effectiveness of simulation-based training in basic police training. *European Law Enforcement Research Bulletin*, 4, 207-212.
  Available from: http://91.82.159.234/index.php/bulletin/article/view/330/273 [Accessed 6th July 2022].

- Chapparo, L. (2017) Digital learning: How to improve knowledge and skills for law enforcement managers. *European Law Enforcement Research Bulletin*, 3, 131-135.
  Available from: http://91.82.159.234/index.php/bulletin/article/view/303/233 [Accessed 6th July 2022].
- Cohen, J. (1988) *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum.
- Davies, R.S., Dean, D. L., & Ball, N. (2013) Flipping the classroom and instructional technology integration in a college-level information systems spreadsheet course. *Educational Technology Research and Development*, 61, 563-580.
  Available from: https://doi.org/10.1007/s11423-013-9305-6 [Accessed 6th July 2022].
- Fuchs, M. (2022) Challenges for police training after COVID-19. *European Law Enforcement Research Bulletin*, (SCE 5), 205-220.
  Available from: https://doi.org/https://doi.org/10.7725/eulerb.v0iSCE%205.480 [Accessed 6th July 2022].
- Gerick, J. & Eickelmann, B. (2017) Abschlussbericht im Rahmen der wissenschaftlichen Begleitung der Evaluation des Projekts „Lernen mit digitalen Medien" in Schleswig-Holstein. [Final report within the framework of the scientific monitoring of the evaluation of the project "Learning with Digital Media" in Schleswig-Holstein].
  Available from: https://kw.uni-paderborn.de/fileadmin/fakultaet/Institute/erziehungswissenschaft/Schulpaedagogik/PDF/Abschlussbericht_Evaluation_Modellschulen_Gerick_Eickelmann_Feb2017.pdf. [Accessed 6th July 2022].
- Henson, B., Reyns, B. W., Klahm IV, C. F., & Frank, J. (2010) Do good recruits make good cops? Problems predicting and measuring academy and street-level success. *Police Quarterly*, 13(1), 5-26.
  Available from: https://doi.org/10.1177/1098611109357320 [Accessed 6th July 2022].
- Holmgren, R., Holmgren, T., & Sjöberg, D. (2019) Teaching and learning in redesigned digitalized learning environments: A longitudinal study at the police education in Sweden. In 12th annual International Conference of Education, Research and Innovation, 11-13 November, 2019, Seville, Spain (pp. 1976-1985). Spain: IATED Academy.
  Available from: https://doi.org/ 10.21125/iceri.2019.0556 [Accessed 6th July 2022].
- Hwang, G. J., & Tsai, C. (2011) Research trends in mobile and ubiquitous learning: a review of publications in selected journals from 2001 to 2010. *British Journal of Educational Technology*, 42, 4, 65–70.
  Available from: https://doi.org/ 10.1111/j.1467-8535.2011.01183.x [Accessed 6th July 2022].
- McLean, S., Attardi, S. M., Faden, L., & Goldszmidt, M. (2016) Flipped classrooms and student learning: Not just surface gains. *Advances in Physiology Education*, 40(1), 47–55.
  Available from: https://doi.org/10.1152/advan.00098.2015 [Accessed 6th July 2022].
- Nikou, S. A., & Economides, A. A. (2018) Mobile-based assessment: A literature review of publications in major referred journals from 2009 to 2018. *Computer & Science*, 125, 101-109.
  Available from: https://doi.org/10.1016/j.compedu.2018.06.006 [Accessed 6th July 2022].
- Novak, G. M. (2011) Just-in-time teaching. Special issue: *Evidence-Based Training*, 2011(128), 63-73. DOI: 10.1002/tl.469.
- Paoline, E., & Terrill, W. (2007) Police education, experience and the use of force. *Criminal Justice and Behavior*, 34(2), 179-196
  Available from: https://doi.org/10.1177/0093854806290239 [Accessed 6th July 2022].
- Renz, M., Rayiet, O., & Soltau, A. (2012) Multiplikatorenschulungen zum Einsatz interaktiver Whiteboards.
  Available from: https://li.hamburg.de/contentblob/3466092/a5b1eae7458b00091eaae65c97d8bb64/data/download-evaluation-whiteboard.pdf. [Accessed 6th July 2022].
- Rosenfeld, R., Johnson, T. L., & Wright, R. (2020) Are college-educated police officers different? A study of stops, searches, and arrests. *Criminal Justice Policy Review*, 31, 206-236.
  Available from: https://doi.org/10.1177/0887403418817808 [Accessed 6th July 2022].
- Sjöberg, D., Karp, S., & Rantatalo, O. (2019) What students who perform in "secondary roles" can learn from scenario training in vocational education. *International Journal for Research in Vocational Education and Training*, 6(1), 46-67.
  Available from: https://doi.org/10.13152/IJRVET.6.1.3 [Accessed 6th July 2022].
- Sung, Y., Chang, K., & Liu, T. (2016) The effects of integrating mobile devices with teaching and learning on students' learning performance: A meta-analysis and research synthesis. *Computers & Education*, 94, 252–275.
  Available from: https://doi.org/10.1016/j.compedu.2015.11.008 [Accessed 6th July 2022].

An Assistive System for Transferring Domain Knowledge to Novice Officers

Héctor López-Carral

Laboratory of Synthetic, Perceptive, Emotive and Cognitive Systems (SPECS), Institute for Bioengineering of Catalonia (IBEC), The Barcelona Institute of Science and Technology (BIST), Barcelona[1]

Paul FMJ Verschure

Donders Institute for Brain, Cognition and Behaviour – Donders Centre of Neuroscience, Radboud University, Nijmegen[2]

Abstract:
Instructional strategies in many operative fields, including law enforcement, have reached a high level of complexity due to dynamically changing task environments and the introduction of different technologies to help users in their operational work. In the last decades, a transition has been observed from dedicated trainers to the adoption of automated technologies to support the trainees. Based on a review of state-of-the-art literature and direct feedback from law enforcement agencies, we have developed an assistive system to aid in the knowledge transfer from expert to novice officers and, consequently, improve the time necessary to train new police practitioners. This system is grounded on the most relevant instructional principles derived from cognitive and learning theories. The result is a system that can dynamically deliver suggestions based on previous successful actions from other users and the current performance and state of the user. To validate our system, we implemented a knowledge graph exploration task. The novel knowledge transfer system is introduced here by presenting the results from our literature review, explaining the architecture of the assistive system, and discussing our observations from the validation task. With this work, we aim to facilitate the transfer of domain knowledge, which could have a significant impact on the training and education of law enforcement officials in and for the Digital Age.

Keywords: assistive system; knowledge transfer; training; recommender system; crime investigation; knowledge graph.

1 Author's email: hlopez@ibecbarcelona.eu

2 Author's email: paul.verschure@donders.ru.nl

Introduction

Instructional strategies in many operative fields have reached a high level of complexity due to dynamically changing task environments and the introduction of different technologies to help users in their operational work. In the last decades, a transition has been observed from dedicated trainers to the adoption of automated technologies to support the trainees. This paradigm shift makes transferring precise knowledge to novice users a challenging problem, which becomes especially relevant when the user is dealing with large and complex datasets from which to extract relevant information.

Supportive technologies, such as recommendation systems, have attracted a lot of interest in the last decades, both in the industry and the academia. The goal of such systems is to help the users to reduce the burden imposed by the high information load that is intrinsic to the exploration of large and complex datasets by providing valuable suggestions in the form of specific items or possible actions to choose from. Despite clear technical advances witnessed in the field in improving the accuracy of the recommendations, several challenges and open issues remain, especially regarding the specific role of various human factors.

Among the functionalities that were identified to provide Law Enforcement Agencies (LEAs) with a set of automated tools and systems to boost the investigative work in the fight against illicit trafficking activities, one was the capability to provide adequate solutions facilitating the transfer of the acquired expertise among experienced users and, consequently, boost the take-up time necessary to train new users. In order to accomplish this task, we decided to build a novel assistive system, which, combining practical knowledge from classical recommender systems with theoretical knowledge from cognitive systems, is able to aid in the transfer of domain knowledge to novice officers.

We will discuss, firstly, the recommender systems in general before outlining the recommender system for assisting knowledge transfer that reflects the best practices, approaches, and directions in the respective law enforcement domain. Our recommender system is conceptually grounded in a cognitive architecture, learning from interactions to later assist novice users by suggesting key pieces of information that other users have selected. Then, we describe the case used for validating this system in a knowledge graph exploration task based on a novel interface for LEAs to present the collected information in a criminal investigation. Finally, we will put forward our conclusions and outline possible next steps.

Introduction to recommender systems

Recommender systems have been used extensively in research and industry since the mid-1990s (Goldberg et al., 1992). The most common domain for their use is electronic commerce (e-commerce), the entertainment and media industry, and services. Many online businesses employ dedicated algorithms to provide recommendations to their customers based on inputs such as their history of items visualised and purchased or their demographic data. Another popular area in which recommender systems are used is multimedia applications (Ge & Persia, 2017). For example, many online music platforms use them to recommend songs or artists based on what each individual listens to (Song, Dixon & Pearce, 2012). Similarly, recommendation systems are common in online video platforms to provide personalised suggestions for TV shows, movies, and other videos (Asabere, 2012).

Several types of recommender systems have been proposed that, depending on the techniques employed, can be classified into different categories (Park et al., 2012; Villegas et al., 2018; Ricci et al., 2011; Adomavicius et al., 2011). In content-based recommendation schemes, the system learns to propose items similar to those that were preferred in the past by the same user. In contrast, collaborative filtering approaches recommend items that other users with similar profiles have preferred in the past. Knowledge-based systems recommend options based on specific domain knowledge about how certain features meet users' needs and preferences. Finally, hybrid systems are based on the combination of the techniques mentioned above to improve performance (Burke, 2002).

Despite providing varying degrees of support, overall, recommender systems are not always tailored to specific user needs and situations. It has been suggested that adaptive recommender systems should be modelled in terms of situations rather than knowledge structures (Adomavicius & Tuzhilin, 2005; Richthammer & Pernul, 2018; Adomavicius et al., 2011). Such a system would be capable of delivering better results to the

user by taking into account contextual factors in the delivery of highly tailored information. Typically, these contextual factors include location, time, computing context, the activity of the user, or social relations (Verbert et al., 2012).

However, context can also refer to the motivational, cognitive, and emotional aspects that are inherent to the interaction between the user and the system. Most of the research on personalised recommender systems has been focused mainly on technical issues, neglecting the importance of the underlying psychological and implicit factors when exploring and analysing data (Buder & Schwind, 2012).

Thus, it is now considered relevant that for a recommender system to be effective, it should merge a variety of techniques and features in order to offer valuable support and reduce the demands imposed by information load. In this sense, systems have been developed that incorporate adaptive content presentation and adaptive navigation support (Brusilovsky, 2007). Content adaptation adjusts the presentation of the content to the user's goal, knowledge, and other information, which is stored in a model of the user to balance factors such as cognitive load, arousal, or learning style (Jin, Cardoso & Verbert, 2017).

Recommender system for domain knowledge transfer

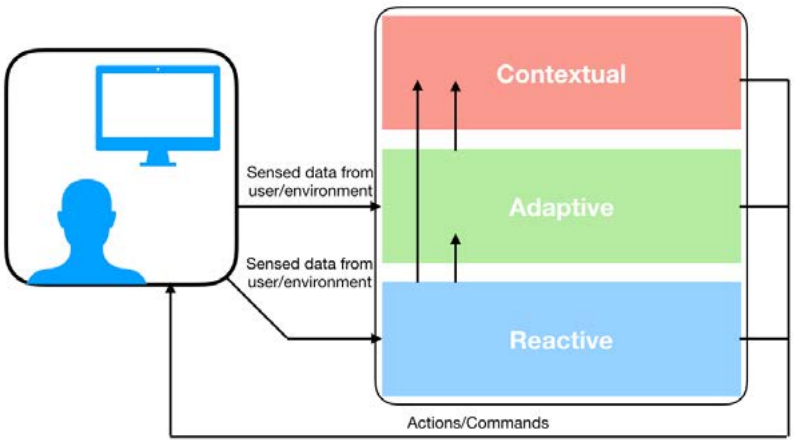
This literature review on knowledge transfer systems reveals a multifaceted and active field where a plethora of technological approaches have been proposed and developed. It also becomes apparent that individual differences (such as motivational and emotional ones) have not received proper consideration when defining effective recommender technologies. This is mainly because of a lack of coherent principles derived from learning and cognitive sciences to guide the development of such systems.

Instead of working from a pure computer science perspective, the proposed recommender system will be grounded on cognitive theories, specifically, the Distribute Adaptive Control (DAC) theory of mind and brain (Verschure, 2012). This theory will serve a dual role in the theoretical framing and the implementation of the core functionalities of the system.

DAC considers humans themselves as adaptive systems that react and adapt to the changing demands of the environment by applying self-regulation strategies in response to intrinsic goals and motivations. The same principles play a foundational role in the implementation of more effective cognitive artificial systems.

Conceptually, this recommender system can be realised as an artificial agent whose reasoning and memory components need to extract relevant knowledge from sequences of interactions in a coordinated way. The proposed system thus emerges as the interplay of the Reactive, Adaptive and Contextual layers as defined in the DAC architecture (see Figure 1).

Figure 1: Abstract conceptualisation of the cognitive architecture of the knowledge transfer system based on the DAC framework.



The recommender system emerges as the interplay between the three layers, which work at different timescales, with the fastest layer at the bottom and the slowest one at the top. In this architecture, the layer at the bottom (Reactive layer) provides the basic form of interaction, taking as input information from the environment and the user to facilitate the basic interaction.

Secondly, the Adaptive layer oversees adjusting the information given to the user, such as suggesting a specific piece of information or directing attention to a specific subset of information. Finally, the Contextual layer operates on longer timescales to learn from interactions from all the users, building profiles and detecting interaction strategies in order to create a knowledge base on which to optimise its behaviour to improve its capabilities in assisting the users. All in all, the system works hierarchically at different time scales, from the immediately reactive, to the medium to adapt to each user, to the long one across different interactions.

Next, one of the key aspects of a recommender system like this, which participates dynamically during an interactive task, is to decide when to provide a suggestion. There are many criteria that could be employed, depending on factors such as the specific task that the user is carrying out, how the interface has been implemented, or the number of user feedback sources available. Although we could include more complex features related to the user state (e.g., estimating stress, attention), here we present the interaction features that we have implemented in the current version of the system, to be used in an online task running on a web browser.

One of the interaction criteria is based on time. If the user has spent more than a specific amount of time without interacting with the system (by clicking somewhere), a suggestion is provided. This is done to stimulate interaction with the system, which is based on exploration to obtain information. This time threshold was fixed at 10 seconds.

Another criterion to provide a suggestion is based on the number of clicks that the user has performed without advancing in the given task. If the user has clicked a certain number of elements without getting closer to solving the task, a suggestion is provided with the goal of reorienting the user towards more relevant information.

If these criteria are not met, no suggestions are provided, as this would indicate that the user is carrying out the task successfully: with fluidity and accessing information that is relevant to solve the task at hand. This way, expert users, who already have successful strategies to accomplish the task, are not encumbered by unneeded recommendations, while novice users, who have not yet developed successful strategies, get the necessary guidance.

Another important aspect of the recommendation system is that not all the suggestions are equally revealing of the next action to take. Instead, there are different levels of recommendations, which are adapted dynamically based on the performance of the user. First, the system starts by providing general recommendations based on the content that just some users interacted with, but not most of them. As the users keep interacting with the system, if they have already received several suggestions at the current level, the recommendation level gets upgraded, and, consequently, the system recommends content of increasing popularity among the previous expert users who successfully solved the task.

To bootstrap the recommender system, some initial interaction data was needed. To achieve this, a custom synthetic data generator was developed. For a given task, the algorithm that was developed generates a random solution resembling one that an expert user would perform. This synthetic interaction data arrives at a solution by following a series of steps that are close to the optimal ones, by following some natural strategies that most users would develop after familiarising themselves enough with the system (i.e., becoming expert users).

The algorithm creates this synthetic data by working backwards from the solution of the task (i.e., starting at the end of the interaction). Then, it generates data corresponding to clicks of random pieces of information at different levels of separation from the solution. The result is a data file almost indistinguishable from the one obtained from actual interaction data.

Finally, the last step in the process is generating the recommendations from the interaction data collected or generated. To achieve this, a custom algorithm was implemented. It gathers all the existing interaction data for a given task and lists all the existing pieces of information. Then, it counts how many times each

piece of information was selected by the users. The result is a data file that will later be processed by the main application to create a ranking of possible recommendations based on this information.

Use Case: Investigation knowledge graph exploration

As the initial use case of this recommender system, we chose the exploration of different knowledge graphs. These knowledge graphs represent, conceptually, one investigation. Each knowledge graph is composed of a number of interconnected nodes. The nodes represent a piece of evidence which is related to others. This is indicated by lines (edges) connecting the nodes bidirectional.

Thus, a knowledge graph here is an abstract graphical representation of all the information collected in an investigation. This modality of information presentation and exploration was designed in collaboration with Law Enforcement Agencies as part of a bigger system of state-of-the-art tools to assist officers in their investigative work by exploiting the latest digital technologies.

In this context, to validate the resulting recommender system that we implemented, we developed a simplified knowledge graph tool that does not use real investigation data, but a gamified and goal-oriented version of crime investigations. The users are asked to put themselves in the position of an investigator who must solve a series of investigations using a new visual interface. For this, they are invited to interact with the knowledge graphs, interacting with the nodes (again, each representing a piece of evidence) in search of a target node. This target node is the solution for each of the cases, representing the piece of evidence required to solve the investigation. Nodes around this target provide hints that allow participants to find out the solution.

Although this task uses the analogy of solving a case, it is important to emphasise that this is just the conceptual idea. As explained, the task is a simplified version, being closer to a game than an actual job of an officer investigating a real case. The way to solve each of the tasks is based on solving a series of logic puzzles, as explained below.

Figure 2 depicts the user interface that we implemented to present the task. The knowledge graph itself occupies the central part of the screen. Users can interact with the graph by clicking on the different nodes to obtain information about them (name and possible relationship to the target node). The name of the node also appears when hovering the mouse cursor over it. It is also possible to move the nodes by clicking and dragging, which might be helpful to get more clarity on the connection to other nodes, although this is never required. Users can also displace the graph by clicking and dragging on an empty space, as well as zooming in and out by using the controls provided in the top-right corner, although these actions are not required either. Finally, in the top centre, the category of the target node is displayed.

Figure 2: The user interface of the knowledge graph exploration task.

Interaction controls for the displacement and zoom of the graph are located in the top right corner (from the bottom up: zoom out, zoom in, restore view). On the top centre, the category of the current target is indicated. The panel on the top left provides information about the node that is currently selected, which appears with a black outline and black connections in the graph. This panel also has the button to submit the solution, corresponding to the node currently selected.

We decided to use four different categories of nodes to provide enough diversity without being too distracting or overloading. These four categories are: person, vehicle, text, and location. Each category is differentiated from the others by using a different iconic figure and colour (see Figure 2 and Figure 3).

As mentioned before, the nodes surrounding the target provide relevant information that is needed to the solving the case. Depending on their closeness and relevance, four levels are established and displayed in the node information:

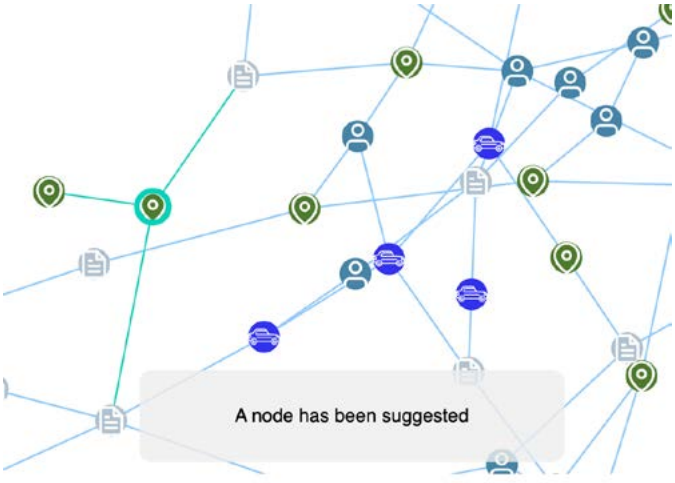
- *"This [category name] is suspicious"*: This appears for the target node and for all nodes of the same category that are within three degrees of separation from it.
- *"This [category name] is directly related to the target"*: This appears for nodes that are directly related to the target (first-degree connection), of a different category from it.
- *"This [category name] is indirectly related to the target"*: This appears for nodes that are indirectly related to the target (second-degree connection, which is, connected through exactly one node in between), of a different category from it.
- *"Unclear"*: This appears for all other nodes not covered in the previous three categories, i.e., all nodes that are too distant and unrelated from the target.

Using this information provided by the different nodes close to the target, the solution is implied. In each knowledge graph, there is only one possible solution, and the information, when enough nodes are explored, points unambiguously to it. Users must integrate this information in a logical manner. It is a matter of logically inferring the solution by integrating some simple relationship data.

The complexity of the task is modulated by the size of the knowledge graph, determined by the number of nodes and connections. The higher the number of nodes and connections, the higher the difficulty, as the visual complexity increases and there are more nodes to explore. We created three difficulty levels according to this: 50, 100, and 200 nodes and connections. Two graphs of each difficulty level are presented, in increasing difficulty, for a total of six cases for each participant.

As indicated, one of the key aspects of this system is the presentation of suggestions to the users. These suggestions are provided in the form of recommended nodes based on the actions of other users. When a node is suggested, it gets selected with a thicker light-blue outline. Its connections to other nodes also appear in the same colour (see Figure 3). When a node is suggested, a panel appears on the bottom of the screen, alerting users of this fact and thus ensuring that they notice the suggestion. This message stays on the screen for 3 seconds.

Figure 3: Example of a suggested node.



It appears with a thicker light blue outline, as well as its direct connections to other nodes. A temporary panel appears on the bottom, alerting the user that a node has been suggested.

Discussion and conclusion

Here, we have presented a novel assistive system capable of learning from interactions with users in order to provide relevant suggestions to other users, in the context of investigative work performed by law enforcement officials, with the aim of facilitating the learning of the use of a new system for the exploration of investigation information.

As explained, the assistive system developed, based on principles from recommender systems and cognitive science, is used in the exploration of a knowledge graph composed of different nodes and connections representing pieces of information collected during an investigation. This knowledge graph implemented here is analogous to one that could be used in a real investigation but customised to provide a goal-oriented task to users: exploring the graph to obtain information necessary to find a target node.

From a technical standpoint, in order to develop such a system, a multitude of components were implemented, as described, including a generator of knowledge graphs, the recommender system itself, a generator of synthetic interaction data used to bootstrap the recommender system, and a generator of recommendations for a given graph based on interaction data (either collected from actual users or generated synthetically).

For the experimental validation of this assistive system, two groups of participants are proposed: an experimental one, which receives suggestions as needed (based on different criteria), and a control one, which does not receive any assistance from the system. Thus, the expectation would be that participants who receive automated recommendations from the system perform better, both in objective metrics (such as performance), implicit features (such as mouse movements) and self-reports (in the questionnaire provided after the main tasks). In addition to an initial validation with civilian participants, a validation should be carried out in collaboration with LEAs and, especially, with the end users of the system.

As mentioned earlier, the system presented in this article works as a web application that runs on a web browser for it to be available online. Due to this, and as an initial implementation of the assistive system, the recommendations were triggered based on different interaction features like the time elapsed, the number of clicks, attempts to solve the task, etc., which were the most viable and appropriate sources, while still providing the necessary information for the knowledge transfer system that was used.

However, more sophisticated methods could be implemented to trigger these recommendations based on the internal states of the users, as inferred in real-time based on various signals. For example, suggestions could be provided based on the estimated cognitive load of the user using pupil dilation signals captured by an eye-tracker, or stress levels could be estimated from physiological signals such as the variation in heart rate using the appropriate sensor.

In conclusion, here, we have proposed a novel assistive system for transferring domain knowledge to novice officers, exploiting modern technologies to facilitate the training of officers in the use of new digital tools to be used in the field in the course of their work. With this work, the authors would like to highlight how state-of-the-art technologies can be applied by forward-thinking LEAs, with the aim of improving the training and education of current and future law enforcement officials in and for the Digital Age.

Acknowledgements

This research was conducted under the framework of the ANITA project, supported by the European Commission (H2020-787061). It was also supported by the European Commission project EIC 101058240 PHRASE. The authors would like to thank Riccardo Zucca for his contributions to this work, among other collaborators from the ANITA project.

References

- Adomavicius, G., Mobasher, B., Ricci, F. & Tuzhilin, A. (2011) What a Recommender System Knows About Contextual Factors. *AI Magazine* 32(3), 67–80.
- Adomavicius, G. & Tuzhilin, A. (2005) Towards the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. *IEEE Transactions on Knowledge & Data Engineering*. 17(6), 734–749.
- Asabere, N.Y. (2012) A survey of personalized television and video recommender systems and techniques. *Information and Communication Technology Research*. 2 (7), 602–608.
- Brusilovsky, P. (2007) Adaptive navigation support. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 4321 LNCS, 263–290. doi:10.1007/978-3-540-72079-9_8.
- Buder, J. & Schwind, C. (2012) Learning with personalized recommender systems: A psychological view. *Computers in Human Behavior*. 28 (1), 207–216. doi:10.1016/j.chb.2011.09.002.
- Burke, R. (2002) Hybrid recommender systems: Survey and experiments. *User modeling and user-adapted interaction*. 12 (4), 331–370.
- Ge, M. & Persia, F. (2017) A survey of multimedia recommender systems: Challenges and opportunities. *International Journal of Semantic Computing*. 11 (03), 411–428.
- Goldberg, D., Nichols, D., Oki, B.M. & Terry, D. (1992) Using collaborative filtering to weave an information tapestry. *Communications of the ACM*. 35 (12), 61–71.
- Jin, Y., Cardoso, B. & Verbert, K. (2017) How do different levels of user control affect cognitive load and acceptance of recommendations? *CEUR Workshop Proceedings*. 1884, 35–42.
- Park, D.H., Kim, H.K., Choi, I.Y. & Kim, J.K. (2012) A literature review and classification of recommender systems research. *Expert Systems with Applications*. 39 (11), 10059–10072. doi:10.1016/j.eswa.2012.02.038.
- Ricci, F., Rokach, L., Shapira, B., Kantor, P.B. & Ricci, F. (2011) *Recommender Systems Handbook*. doi:10.1007/978-0-387-85820-3.
- Richthammer, C. & Pernul, G. (2018) Situation awareness for recommender systems. *Electronic Commerce Research*. (0123456789). doi:10.1007/s10660-018-9321-z.
- Song, Y., Dixon, S. & Pearce, M. (2012) A survey of music recommendation systems and future perspectives. In: *9th International Symposium on Computer Music Modeling and Retrieval*. 2012 p.
- Verbert, K., Manouselis, N., Ochoa, X., Wolpers, M., Drachsler, H., Bosnic, I. & Duval, E. (2012) Context-aware recommender systems for learning: a survey and future challenges. *IEEE Transactions on Learning Technologies*. 5 (4), 318–335.
- Verschure, P.F.M.J. (2012) Distributed Adaptive Control: A theory of the Mind, Brain, Body Nexus. *Biologically Inspired Cognitive Architectures*. 1, 55–72. doi:10.1016/j.bica.2012.04.005.
- Villegas, N.M., Sánchez, C., Díaz-Cely, J. & Tamura, G. (2018) Characterizing context-aware recommender systems: A systematic literature review. *Knowledge-Based Systems*. 140, 173–200. doi:10.1016/j.knosys.2017.11.003.

Children on the Internet – Law Enforcement Challenges

Nicoleta Apolozan
Andreea-Ioana Jantea
General Inspectorate of Romanian Police –
Crime Research and Prevention Institute, Bucharest[1]

Abstract
The current technological development and the increased access of people of different ages to devices connected to the Internet pose new challenges to the law enforcement for preventing, as well as for investigating such crimes. Children, who have access to multiple devices connected to the internet, in association with other factors linked to their age, are a very vulnerable segment of population. As members of the implementation team of the Cyberex RO Project – Improving, cooperating and preventing in the fight against cybercrime, we conducted a research aiming to identify the main risks and vulnerabilities faced by young students aged 10 to 18 in Romania in the online environment. The results were used to train police officers from crime prevention units in Romania, in order to increase their understanding of cybercrime and current trends. This paper discusses the results of the qualitative analysis of interviews with law enforcement officers from ten counties in Romania regarding the main challenges that the police have faced in handling cyber cases involving children, in order to substantiate, on a scientific basis, the activities of preventing cybercrime against children.

Keywords: Challenges, Children victimisation, Cybercrime, Police; Prevention

Introduction

With the technological development and the increased access of people of different ages to more and more devices connected to the Internet, crime has either shifted from the real-life environment to the online world, either new vulnerabilities and types of attacks have emerged that can only take place online.

Without proper knowledge and appropriate skills, the risk of becoming a victim of cybercrime is high. Children are surrounded and have instant access to a myriad of information and if they are not taught how to handle it, they can easily endanger themselves or others (Phippen, 2017).

Therefore, the law enforcement has to tackle cyber offences in which children are involved more often than

1 Co-authors emails: nicoleta.apolozan@politiaromania.ro; andreea.jantea@politiaromana.ro

before (Europol, 2021) and must be kept up to date with the latest technologies and special juvenile hearing techniques to investigate these types of cases.

The same situation is faced by the police officers from the crime prevention units, who must be aware of the current trends in cybercrime, especially when it comes to such specific crimes as child pornography on the Internet or cyber-attacks with minor victims.

Several studies regarding the presence of children on the Internet have addressed this issue from the children's perspective (Barbovschi et al., 2021; Smahel et al., 2020; Velicu et al., 2019). There are also studies that focused on the legal issues and on the policy regarding online child safety (Molter et al., 2021; Pisaric, 2012; Savirimuthu, 2012). However there is a third category of studies concerning the emotional impact on the police officers investigating children exploitation on the internet (Burns et al., 2008; Powell et al., 2015; Powell et al., 2014).

The research questions that this research project aims to answer are the following:

- How do the police officers who investigate cyber-crimes portray the children who are victims of these crimes?
- What are the risks and vulnerabilities of children that they identified when they solved cyber-crimes cases involving minor victims?

The results of the qualitative analysis of interviews with law enforcement officers who handle cases of cyber-attacks involving children or cases of child pornography on the Internet have been discussed. These interviews focused on identifying the factors that favour children victimization on the Internet, on the difficulties in handling such cases and the ways in which victimization can be reduced.

Besides their scientific value, the results of the larger study of which these interviews were a part, were used for training police officers in Romania which deal with crime prevention, to make them more aware of the conducts that children have on the Internet, the risky situations they are confronted with and what determines them to commit or become victims of such crimes, according to their age. This knowledge is meant to substantiate, on a scientific basis, the activities of preventing cybercrime against children and to develop an adequate message for the target group, which consists of children aged between ten and eighteen years.

Methods

The interviews were conducted as part of a larger study, ***Risks and vulnerabilities of young students in the online environment*** (General Inspectorate of Romanian Police, 2021), initiating the prevention component of Ro Cyberex Project – Improving, cooperating and preventing in the fight against cybercrime.[2]

The interviews took place between 16 March and 30 April 2020 and were conducted by sociologists from the territorial units of crime analysis and prevention, on the basis of the interview guide that we made available to them. Twelve police officers fighting cyber-crime involving minor victims from ten counties in Romania

2 *Ro Cyberex Project* – Improving, cooperating and preventing in the fight against cybercrime, funded by the European Union from the Internal Security Fund – Component for Police Cooperation addresses the need to improve investigative and preventive capacity in the field of cybercrime, as well as to facilitate cooperation and the exchange of information and best practices in this area of crime.The two main components of the project initiated at the end of 2019, with a duration of three years, were supported by the training of Law enforcement personnel, both on combating and preventing cybercrimes with children victims.The prevention component started with a study (General Inspectorate of Romanian Police, 2021) aimed, first of all, at identifying the main risks and vulnerabilities faced by young students aged 10 to 18 in Romania in the online environment (mainly child pornography and cyber-attacks), in order to substantiate, on a scientific basis, the activities of preventing online crime against children. Within this project, we were members of the implementation team, as research experts, carrying out both the research methodology and the analysis, interpretation of data and drafting of the research report. To achieve the research objectives, we used a mixed approach, quantitative and qualitative methods altogether. The study itself was designed around 3 different stages: 1. A survey on a sample of 1445 young students, nationally representative for the population of students aged 10-18 years;The objectives of the survey included the description of children's usage habits and their behaviour on the Internet, the assessment of their level of knowledge and the safety measures that they use on the Internet, and identifying risk factors and vulnerabilities to cyber-attacks and child pornography; We also identified the need to inform this segment of population about online safety measures; 2. Interviews with teachers of children aged 10 to 18 (leading teachers and computer science teachers) from ten counties in Romania and Bucharest; 3. Interviews with police officers from units fighting against organized crime who have investigated cases of cyber-attacks involving minor victims and cases of child pornography from ten counties in Romania and Bucharest. Through the interviews, both with teachers and police officers, we tried to identify the main challenges that people dealing with children have faced in handling cyber cases, as well as to find ways in which the investigation and knowledge about risky conduct of children on the internet can be improved.

(Alba, Bacău, Caraș-Severin, Gorj, Galați, Giurgiu, Iași, Prahova, Suceava, Timiș) and Bucharest, the capital city, were interviewed.

The guide was divided into two sections – cyber-attacks involving minor victims and child pornography – each structured on the following dimensions: trends, modus operandi and reasoning behind the crime, methods used by criminals to approach the victims, the relationship between the victim and the author, the profile of the victims, the profile of the authors, the factors that influence victimization and its consequences, the main challenges faced in handling such cases, measures to increase the reporting rate and measures to reduce victimization of children.

For the analysis, we created a category system based on the interview guide and coded the material obtained from the interviews using the MaxQDa software and then we interpreted the results.

The results

The officers involved in investigating cybercrimes show that children have a rather small share in the total number of people involved in such crimes and they are more often victims than perpetrators. From the wide range of crimes that take place on the Internet, children are involved mainly in acts of child pornography and, less often, in cyber-attacks.

In addition to the upward trend of cybercrime that has occurred in recent years, the police officers interviewed also noticed an increase in groups of people who discuss and exchange information or software solutions to make cyber-attacks more efficient, but also in groups of individuals who have similar concerns and exchange materials that contain child pornography.

Child pornography on the internet

As shown by the police who investigated such cases, child pornography on the Internet is extremely diverse, ranging from the exchange of materials with explicit sexual content between two minors to adults exploiting minors for their own pleasure.

In the case of love relationships between two minors, they exchange different materials with explicit sexual content that they make by themselves, and when the two separate, blackmailing, threatening or mockery of the other in the group of friends or online occurs. In this situation, sexual images are required as a proof of love between the two of them and as a normal step in the development of these relationships,

"we are generally talking about teenagers who, within their emotional relationships, consider that, at a certain point in their relationship, exchanging such material is something very natural, everything happens by mutual consent... I think they have no real idea of the danger they are exposing themselves to. They don't realize that the actual relationship will end in a month, a year, after which those materials depicting them in such postures remain, they have no control over the respective materials" (Police officer fighting cybercrime).

Another reason why people get involved in child pornography cases, especially concerning minor perpetrators, is revenge or humiliation of certain people they already know in real life, even various "jokes" towards people in their entourage. They distribute images or videos of a sexual nature or that contain nudity without realizing that the materials they produce or share can have serious consequences for the victim in the long term, but also for the perpetrators, who do not realize that what they are doing is illegal.

Speaking of minor perpetrators, police officers noticed more and more kids that find by accident or to whom friends from various groups send pictures or videos illustrating other kids in pornographic stances. Without knowing that this is a crime, they save that material in their phone or send it to other friends.

In the same register there are also children who take nude photos or videos of themselves, and they do not pass them on, but they store the material on their phone. When the phone is given to friends or colleagues for another purpose, they find those images and they pass the recordings or the photos on to online groups or other people, without the knowledge of the victim. They do this as a prank and don't realize that it is a crime and the consequences of their actions.

Then, the police officers speak about the "classical" type of child pornography, when adults approach children in order to obtain images with an explicit sexual character, which consists either only in watching such images, or even in actually producing sexual acts with minors. The reason why they do this is either for their

own pleasure or to obtain amounts of money from those who "consume" such images with sexual content involving children. Others combine the two reasons and others just exchange such images between them, out of the desire to get as many such images as possible.

Usually, they use fake profiles on social media platforms and spend quite a lot of time choosing the perfect victim, using various information that they can access in advance. After compiling the list of information, criminals can build their speech and approach to the victim so that they can get what they want. Victims are usually approached progressively: initially, the perpetrator tries to create a connection with the victim and gain her or his trust, and later, the perpetrator starts asking the victim for images that do not necessarily have sexual content. Over time, the images requested become more and more explicit, "a progressive transition is made from a little girl dressed in a dress, who plays in the park, and after 2-3 conversations in which 'have you ever seen what it looks like...? Have you ever seen .....?', they move to an increasingly vulgar, pornographic mode of expression". (Police officer fighting cybercrime). Adult perpetrators who want to obtain child pornography for their own pleasure usually send victims images of other children in similar poses to convince them that everything is normal and that many other children of the same age do these things, "***everyone now has a set of photos, of videos, which they use as bait***" (Police officer fighting cybercrime).

In addition to gaining trust of the victim, she or he is getting blackmailed: after a period of time in which they had more and more vulgar discussions and obtained more and more compromising images, the perpetrator threatens the child that he will send the previously obtained materials to his group of friends, school colleagues or even parents, and the child – already having feelings of fear, shame or both and seeing himself in a hopeless situation – does what the offender asks, who is no longer his "friend" at this stage, but someone he hates and is terrified of.

There are also victims to whom promises of a material nature (money, goods, work contracts abroad, etc.) or affective (long-term relationship, founding a family, marriage, etc.) are made to determine them to produce and share CSAM. These promises are related to the process of studying the victim, through which the perpetrator can figure out what the victim's needs are.

Another situation is when children are abused by their own parents, on order to sell the images produces during the sexual abuse (videos or photos) to the interested people. In this case, the victims are very young children, from a few months of age, and the parents are usually starting to establish links with consumers of CSAM from the beginning of their pregnancy.

Although children of any age could become victims of child pornography on the Internet, from a few months up to the age of 18, interviewed police officers identified several common factors that can favour victimization in the cases of the children above ten years old. One of the risk factors is poor communication with their parents or the adults who take care of them. Such a relationship is either obvious, or the communication between the child and his or her parents is focused only on everyday issues, without in-depth conversations and without sharing their feelings in a real way. In this context, the adults don't supervise their children's use of the Internet and they have no idea what their children are doing when they are online, they do not know anything about the people their children meet online, even less about the content of their conversations or their posts.

Another common characteristic of the victims is that they use the internet since their early childhood, but do not have too much technical knowledge and do not have a clear picture of how information flows on the Internet. In addition, the police officers found that the victims had a low self-esteem as well as a need for affirmation and approval from others more pronounced than those specific to their age. This need prompts them to create content with a sexual touch that they distribute online, out of the desire to receive appreciation from those who follow them. Besides the very large number of friends on social platforms, this content is precisely what attracts the attention of criminals. It is a sign for perpetrators that they have chances to easily befriend the child and later gain his or her trust in order to obtain pornographic materials from him/her.

In cases of child pornography, the victimization is usually repeated over a long period of time. This happens because, once on the Internet, the CSAM can be distributed and stored millions times, in all corners of the world. The child may be re-victimized by the same perpetrator several times in order to get more from the victim or may be re-victimized by other persons who

had nothing to do with the original event, but who obtained the images from elsewhere.

The consequences of victimization are diverse: psychological trauma, decreased school performance, depression, insomnia, self-isolation tendencies, low self-esteem and distrust in other people, moving to another school or even school dropout, suicide. Besides the immediate physical and psychological consequences, a strong impact on the emotional development of the child occurs.

Law enforcement challenges in investigating online child pornography

The first difficulty comes from the very nature of the crime: the fact that it takes place online, where the perpetrators can successfully hide very well behind anonymised connections. The solutions for anonymization are very easy to find online and very cheap, often free of charge. Also, in this environment, sex offenders can be anywhere in the world, including in countries with which police cooperation is difficult.

Delayed reporting of cases and the high rate of non-reporting such crimes are also obstacles in the investigation. A large proportion of minors who fall victim to cybercrime believe that blocking certain sites or users is sufficient. These actions give them a false sense of security, but the personal data, information, photos remain in the possession of the authors or others who have come into their possession and can be used further.

Given that the reporting of events to the police is done quite late, when the images have been shared many times to a lot of people or have been posted on various sites, minimizing the consequences for the victim and managing the situation is difficult. The investigators warn that, if the victim would report the situation earlier, then the impact on his or her life could be reduced.

Considering the sexual nature of the crime, the victims are often tempted to hide some details to the police or even to delete the images that are the subject of the investigation. Especially if the parents do not know how to react when the child confesses the things he or she is going through, the child is much more reluctant to give all the details related to what happened. When there is no trust and good communication between parents and children, children try to hide certain details that could be useful to the investigation. They delete crucial information or delay reporting what happened.

There are also situations in which children talk to their parents about the experiences they have gone through, and parents sometimes make hasty decisions such as blocking certain people, websites, or deleting important evidence, before calling the police: "The first reaction is to delete all the pictures, to delete the child's profile from the Internet, to break any contact with the paedophile, with the aggressor", thus making the investigation more difficult.

The police officers also encountered parents who tried to catch the perpetrators themselves, organizing meetings with them on the child's profile, but not having the necessary experience, the perpetrators realized the trap and deleted many pieces of evidence.

Another challenge faced by the police officers that handle cases involving multiple juvenile perpetrators is their tendency to collude in order not to provide too many details. Believing that they only made a joke, they don't want to blame their friends that could be held criminally responsible for an act whose consequences they don't realize or understand. During the auditions, the police officers are perceived as strangers and enemies that want to harm their friends, even though nothing that bad happened in their perception.

Cyber attacks

When talking about cyber-attacks, and more specifically the ones in which children are involved either as perpetrators or victims, we must keep in mind that the numbers of such crimes that the police record do not reflect the reality due to the practice of low reporting or the small number of people that do realise that they have become a victim. Often, in these types of crimes, data is stolen without the person noticing it, and used later to commit other crimes or sold to organised crime groups.

Children are easy targets for cyber attackers because they have access to multiple devices, they do not use complex passwords, are easy to manipulate and because they do not understand the importance of their own data. Police officers have encountered cases in which the perpetrators have contacted the victims on

social media websites using fake or stolen accounts and have determined them to reveal their password or the reset code, taking over their account, in order to commit other types of crimes or to sell it on the dark web.

In recent years, law enforcement personnel have seen an increase and a development of online groups in which perpetrators are exchanging information or software to improve their attacks. Therefore, the attackers do not need special skills to orchestrate these attacks and can buy or borrow programmes from more experienced users and that is why they have seen very young children, without technical abilities or which have not studied programming, organise and commit cyber-attacks that seem to require a certain level of knowledge.

Concerning children as perpetrators of cyber-attacks, police officers are often confronted with cases in which the children use their parents' cards without permission and when the parents notice that their money disappear, they come to the police and file a complaint without knowing that the "thief" is their own child.

Another frequent type of case in which children are involved as authors that has been investigated by police officers is the one in which children access without right the social media accounts of their colleagues or friends, often by simply guessing their passwords which do not meet the minimum complexity requirements.

In most of the cases, data stolen by children during cyber-attacks is used only to brag about their skills in front of their peer group, and not with the purpose of doing something else with it.

Police officers have reported also cases in which children have committed a type of cyber-attack known as "defacement", which consists of unauthorised access to a webpage and changing certain visual elements. Behind the reasoning of this type of attack is again the need for approval, admiration and appreciation from others.

Law enforcement agents believe children commit such crimes in order to stand out, sometimes to obtain money or in order to take revenge on friends, boyfriends or girlfriends and teachers.

Most of the perpetrators are males over 15 years old, live mostly in urban areas and come from financially stable families. They act on their own and access forums or websites or get in contact with others only to improve their skills and obtain software programs that could facilitate their attacks.

"*The skills or the technological knowledge are obtained through accessing online resources or websites on which others teach them what to do*" (Police officer fighting cybercrime).

Ways to reduce online victimization

In order to reduce online children victimization, the police officers believe that there must be a solid partnership between the school, parents, police, non-governmental organizations and IT&C actors, so that the messages reach all the vectors involved in managing these situations.

Children need to be very clearly informed about the risks they can be exposed to on the Internet, so that they realize that what they do on the Internet or through the devices they use can also have consequences in real life. They need to acknowledge that the information and images that reach the Internet can no longer be completely deleted and can be distributed extremely quickly.

Moreover, those who have become a victim of cybercrimes must know that there are solutions for the problems they face and that there are people who can offer them help to get out of the situations they categorize as "no escape".

The police investigators say that informing children is essential, so that they realize that they are victim and that what happens to them is not unimportant. They need to know that they can ask for help from the authorities and the perpetrators can be punished for their actions.

Both parents and teachers should be informed about the applications for monitoring children's online activity, the importance of effective communication, the signs to look for in order to realize that the child has a problem, the steps to follow and the things they must avoid doing, but also information about the institu-

tions empowered to act and the procedure to follow when their children face this kind of crime.

At the same time, it is important that parents are taught to react when children confess certain things to them, to think ahead, to act very carefully and to realize that they need to call the police in such cases, in order to minimize the effects on the child and to avoid re-victimization, they ***"must learn to exploit the moment when the child is willing to talk"***. (Police officer fighting cybercrime).

Parents and teachers should also understand that such situations can have long-term consequences, that it is not enough to solve such events step by step as they appear and that it is necessary to contact specialists as soon as possible from the moment of learning about the occurrence of the negative event, so that the effects of victimization are minimized and the appropriate measures against the perpetrators are taken.

Discussion and Conclusions

First of all the survey aimed to investigate children habits of using the Internet and identifying the unpleasant situations which children have been confronted with on the Internet. The interviews with teachers were focused on the need for education regarding the safe use of the Internet by children. The interviews with the police officers investigating cybercrime brought up another aspect: the factors that favour the online victimization of children and the ways in which it could be reduced.

Cybercrime investigators most often encounter children rather as victims than as perpetrators in cases of child pornography or cyber-attacks. Both situations are closely related to social networks platforms, their accounts being targeted by attacks for the second category of crimes or used as communication channels in the first phase, and later as a means of distributing compromising content, in the case of child pornography.

Velicu et al. (2019) concluded that the main activity of children between ages 9 and 16 on the internet is related to social media networks, which explains why most of the crimes concerning minors are happening through these channels. In the interviews conducted with the police officers from Romania, it became apparent that the main means in which children are becoming involved in these types of crimes is related to their use of social media platforms, being consistent with the results of the above mentioned study.

Police officers state that the factors that favour the online victimization of children revolve around their young age and the naivety associated with it, in association with a low knowledge of the Internet use and the risks involved. Under the rule of curiosity and social pressures, the risk of victimization of young people increases. Moreover, easy access to digital services is an additional factor.

Not all factors concern children, but elements such as poor supervision of their online activity, poor communication, as well as the lack of knowledge regarding the risks of using the Internet also affect parents or those who take care of children.

Police officers identified the lack of adult supervision, of appropriate skills or of the awareness needed to adequately educate the children as risk factors regarding children's online safety. This finding is in accordance with Helsper's et al. study (2013), in which children in Romania were classified as "semi-supported risky gamers", because they are more likely to experience online bullying and to meet strangers offline and their parents are one of the most likely to have a passive attitude towards their children behaviour on the internet, caused by their own deficit of knowledge regarding online safety.

Furthermore, if some form of supervision exists, it is mainly focused on restrictions and not on actively teaching their children how to react in certain situations or on what measures they should adopt in order to avoid victimization. This confirms the results of Smahel et al. study (2020), which have emphasized the importance of adult supervision when talking about children's online safety, because they, on their own, cannot understand the impact that their online activity has. The parents should impose restrictive measures and should not rely solely on those, but they should also focus on communication and teach their children about the appropriate behaviour when accessing online apps or software.

Another study (Moore et al., 2012) has concluded that there are statistically significant associations between parent marital status and the risk of becoming a perpetrator or victim of electronic bullying, suggesting that

children which live with both their parents and children with married parents are less likely to be involved in such crimes.

These conclusions might relate to the lack of or deficiencies in parental supervision, given that it was identified by law enforcement officers as a risk factor for all types of internet-based crimes in which children are involved because in non-intact families, children might not have such good communication with their parents or one or both of the parents might neglect mediating their children internet use.

The long-term effects are the most severe and the risk increases given the fact that online child victimization can extend over a long period, with varied perpetrators, even long after the first event.

The difficulties in investigating cybercrimes with child victims refer both to the criminals' ability to remain anonymous and to the morale of the victim. It influences the smooth conduct of the investigation, since, due to fear or shame, the victim does not provide all the necessary information. Also, the desire of the victims or their relatives to solve problems with their own means, ignoring the proportions of the problem or the late reporting of the crime are elements that complicate the investigation.

For reducing the victimization of children, police officers emphasize the need for strong a partnership between all stakeholders involved in educating and preventing cybercrimes, so that a unified message could reach both children and their tutors.

The most important thing that all children need to be aware of is that the actions they take on the Internet or through their devices have real-life consequences. They also need to be aware of the risks they might face on the internet and the consequences of their actions online. Police officers have also suggested that children should be taught what precautions they can take to avoid victimization, the steps they need to take when they become victims, what are the actions on the Internet that are punished by law and the fact that they can ask for help from the authorities when they are faced with such situations.

References

- Barbovschi, M., Ní Bhroin, N., Chronaki, D., Ciboci, L., Farrugia, L., Lauri, M.A., Ševčíková, A.,Staksrud, E., Tsaliki, L. & Velicu, A. (2021) Young people's experiences with sexual messages online. Prevalence, types of sexting and emotional responses across European countries. EU Kids Online and the Department of Media and Communication, University of Oslo.
  Available at: http://urn.nb.no/URN:NBN:no91296
- Burns, C. M., Morley, J., Bradshaw, R. & Domene, J. (2008) The Emotional Impact on and Coping Strategies Employed by Police Teams Investigating Internet Child Exploitation. In Traumatology. pp. 20-31. DOI: 10.1177/1534765608319082.
- Europol (2021) Internet Organised Crime Threat Assessment (IOCTA) 2021. Luxembourg, Publications Office of the European Union.
  Available at: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021
- General Inspectorate of Romanian Police (2021) Risks and vulnerabilities of young students in the online environment. Bucharest, Crime Research and Prevention Institute.
  Available at: https://www.politiaromana.ro/files/pages_files/raport_cercetare_Proiect_Cyberex.pdf
- Helsper, E. J., Kalmus, V., Hasebrink, U., Sagvari, B. & de Haan, J. (2013) Country classification: opportunities, risks, harm and parental mediation. EU Kids Online, The London School of Economics and Political Science, London.
  Available at: http://eprints.lse.ac.uk/52023/1/Helsper_Country_classification_opportunities_2013.pdf
- Molter, S., Martinez, G., Garmendia, M., Croll, J. & Järventaus, A. (2021) Children's rights in the digital space. Observatory for sociopolitical developments in Europe.
  Available at: https://www.researchgate.net/publication/352821929_Children's_rights_in_the_digital_space
- Moore, P. M., Huebner, E. S., & Hills, K. J. (2012) Electronic Bullying and Victimization and Life Satisfaction in Middle School Students. Social Indicators Research, 107(3), 429–447.
  Available at: http://www.jstor.org/stable/41476587
- Phippen, A. (2017) What Do We Mean by "Child Online Safety"?. In: Children's Online Behaviour and Safety. London, Palgrave Macmillan. pp. 1-13. https://doi.org/10.1057/978-1-137-57095-6_1

- Pisaric, M. (2012) EU legal framework of fight against child pornography on the Internet.
  Available at: https://www.researchgate.net/publication/269660273_EU_legal_framework_of_fight_against_child_pornography_on_the_Internet
- Powell, M. B., Cassematis, P., Benson, M. S., Smallbone, S. & Wortley, R. (2014) Police officers' perceptions of the challenges involved in Internet Child Exploitation investigation. In Policing: An International Journal. Vol. 37 No. 3. pp. 543-557. https://doi.org/10.1108/PIJPSM-08-2013-0080
- Powell, M., Cassematis, P., Benson, M., Smallbone, S. &Wortley, R. (2014) Police officers' strategies for coping with the stress of investigating Internet child exploitation. In Traumatology: An International Journal. Vol. 20(1). pp. 32–42. https://doi.org/10.1037/h0099378
- Powell, M., Cassematis, P., Benson, M., Smallbone, S. & Wortley, R. (2015) Police Officers' Perceptions of their Reactions to Viewing Internet Child Exploitation Material. In Journal of Police and Criminal Psychology. Vol. 30. pp. 103–111. https://doi.org/10.1007/s11896-014-9148-z
- Savirimuthu, J. (2012) The Child, Media Literacy and Online Safety Policy Implications.
  Available at: https://www.researchgate.net/publication/304655900_The_Child_Media_Literacy_and_Online_Safety_Policy_Implications
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S. & Hasebrink, U. (2020) EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. https://doi.org/10.21953/lse.47fdeqj01ofo
- Velicu, A., Balea, B. & Barbovschi, M. (2019) Internet access, uses, risks and opportunities for children in Romania. EU Kids Online 2018 results. EU Kids Online and DigiLiv-REI.
  Available at: https://www.academia.edu/38372598/Acces_utiliza_ri_riscuri_s_i_oportunita_t_i_ale_Internetului_pentru_copiii_din_Roma_nia_Rezultatele_EU_Kids_Online_2018

Countering Crimes of the Digital

Investigating High-Risk Firms: A Machine Learning-based Approach to Cross-Border Ownership Data

Antonio Bosisio
Maria Jofre
Transcrime – Università Cattolica Sacro Cuore

Abstract
Corporate ownership secrecy has become a central issue in the global debate as the use of legitimate companies in illicit schemes has increased dramatically in recent times. While several measures have been implemented worldwide to increase the transparency of firms and their owners, empirical evidence and knowledge on the subject remain limited to few small-scale case studies. In addition, there is a lack of tools specifically designed for risk assessment and risk monitoring of firms to be used by public authorities. The present paper, based on the results of the EU-funded project DATACROS, addresses these gaps by (i) proposing and validating novel risk indicators of corporate ownership opacity in a large sample of companies, and (ii) implementing them in a user-friendly platform to be used by public institutions, a tool capable of identifying companies at risk of involvement in corruption and money laundering. Machine learning results confirm the relevance of corporate ownership opacity in the facilitation of financial crime. Firms with (i) more complex structures, (ii) links to secrecy jurisdictions, and (iii) links to opaque corporate vehicles, are, in fact, more prone to engage in illicit activities. This urgently calls for the innovation of risk assessment activities based on the intelligent use of corporate ownership information. As such, the present contribution could be used to support LEAs and other authorities in combating financial crime in the sometimes overwhelming and ever-evolving digital age.

Keywords: financial crime; ownership structure; risk indicators; machine learning; investigative tool

Introduction

Background

Legitimate companies play a crucial role in facilitating corruption schemes and money laundering of illicit proceeds (EFECC, 2020; Europol, 2018; Savona & Riccardi, 2018). Companies are exploited to create a 'screen' that makes it particularly difficult to trace the real identity of the individuals who ultimately control them – the so-called beneficial owners (hereinafter BOs). Recent investigations carried out by European law enforcement agencies (LEAs) and financial intelligence units (FIUs), and recent research highlights important trends in this domain.

First, there is an increased misuse of complex and opaque corporate ownership in illicit schemes that aim to conceal BO information, thus impeding the identification of the individuals who ultimately control a company. According to the World Bank, 70% of corruption

cases between 1980 and 2010 involved anonymous shell companies (van der Does de Willebois et al., 2011). Panama Papers (ICIJ, 2016) and Paradise Papers (ICIJ, 2017), among others journalistic investigations, uncovered dense and opaque networks of companies and trusts established to conceal the identity of their beneficial owners, and the criminal origin of their proceeds.

Second, financial crime schemes increasingly exploit cross-border structures: criminals use bank accounts, intermediaries, and firms located in different jurisdictions, including non-cooperative tax havens: in Europe, 1% of limited companies have ownership links with entities coming from blacklisted countries, but in some EU Member States this percentage goes up to 12% (Bosisio et al., 2021).

Third, there is a high volume of cross-links between corruption, organised crime, tax fraud, and money laundering. The outburst of the COVID-19 pandemic, and the introduction of recovery plans by EU Member States, have provided criminal networks with further opportunities to drain public resources through simultaneous use of different financial crime schemes (UNODC, 2020; FATF, 2020).

All these trends exploit weaknesses in the preparedness and capabilities of European law enforcement and judicial authorities to combat financial crimes. Moreover:

- There is a lack of risk assessment tools specifically designed for public authorities: current tools and solutions have been designed primarily for banks, financial institutions, and large corporations (e.g., for anti-money laundering and compliance purposes). There is a dearth of tools specifically designed to support criminal investigations dealing with the monitoring of companies potentially involved in corruption and financial crime. A survey conducted by Transcrime in 2019, involving 37 public authorities from 19 EU countries, including LEAs, FIUs, Anti-Corruption Agencies (ACAs), Competition Authorities (CAs), and Tax Authorities (TAs), revealed that 60% of public authorities do not use software for financial investigations, but 78% would like to have tools for tracing and assessing the risk of firms;
- There is a lack of (i) knowledge and skills for gathering information on companies and related entities/individuals, and (ii) ML-based indicators, models, and tools to identify high-risk companies, also when ownership structures deploy cross-border;
- There is a lack of communication and coordination among stakeholders in the exchange of best practices, investigation, and intelligence practices, and in the implementation of cooperation mechanisms, especially at the transnational level.

In Europe, efforts are being made to facilitate the identification of company owners with the establishment of BO registers, introduced by the fourth (and later fifth) Anti-Money Laundering Directive. However, to have a complete picture of potential risks, it is often not enough to know who controls a company, it is also crucial to understand how control occurs: which shareholding structure is used, what corporate vehicles and jurisdictions are involved, and with what degree of complexity.

Current research

In order to address these gaps, and to increase the knowledge on the issue, the EU-funded projects DATACROS I and II have produced the first analysis of the opacity in the ownership structure of 56 million companies across 29 European countries, and developed the first software for public authorities capable to identify companies at risk of involvement in corruption and money laundering.

The present study, conducted for the purposes of the project, further proposes a two-fold strategy:

1) To define, calculate, and validate relevant ownership risk indicators on corporate secrecy that relate to the three identified facets of opacity, including (i) complex ownership structures, (ii) links to secrecy jurisdictions, and (iii) links to opaque corporate vehicles;

2) To develop a prototype tool for risk assessment purposes based on the proposed secrecy risk indicators.

Methodology

Several risk factors related to features of ownership structures have been identified from the review of the literature, information that could be exploited to better understand and detect financial crimes. Risk factors include: (i) anomalous complexity of ownership structures, (ii) ownership links to high-risk countries, and (iii) ownership links to opaque corporate vehicles. In order to advance extant knowledge on ownership opacity,

we defined and assessed ownership risk indicators associated with these three factors.

Data

The datasets used in the present study were retrieved from different sources, including business ownership data, compliance data, and country black and grey lists.

Business ownership data

Information on 56 million companies across 29 European countries[1] was retrieved from Bureau van Dijk's Orbis Europe.[2] In order to guarantee both cross-country and cross-sector comparability, only limited companies with information on the ownership structure were included in the analysis. Consequently, the exploited dataset provided a snapshot of ownership information during the month of June 2019, containing information on 13.4 million companies, and about 20 million BOs.

Sanctions and enforcements

Information on companies and their owners that were either included in a sanction list, or associated with enforcement cases from 9 countries[3] were obtained from LexisNexis WorldCompliance.[4] This included information on companies and business owners reported in: (i) one or more of the global screening and sanction lists issued by the EU, US Office of Foreign Assets Control (OFAC), United Nations (UN), Bank of England, US Federal Bureau of Investigation (FBI), and US Bureau of Industry and Security (BIS), or (ii) associated with enforcement provisions (e.g. arrests, final judgments), and court filings around the world, data collated from various sources including national law enforcement reports, press releases, and other statements from public authorities.[5]

Country blacklists

To operationalise the concept of high-risk jurisdictions, we considered the following black and grey lists:[6]

- *Tax domain*: EU list of non-cooperative jurisdictions for tax purposes, which groups together countries that encourage abusive tax practices, and ultimately erode corporate tax revenues of EU Members States (European Commission, 2019);
- *AML/CTF domain*: FATF lists of non-cooperative jurisdictions (or jurisdictions under increased monitoring) in the global fight against money laundering and terrorist financing (FATF 2019). In particular, two lists were included: (i) Call for action (or so-called 'black list') that identifies countries that are considered by the FATF as non-cooperative in the global fight against money laundering and terrorist financing, who are flagged as 'Non-Cooperative Countries or Territories' (NCCTs), and (ii) Other monitored jurisdictions (or so-called 'grey list') comprising jurisdictions that have strategic AML/CFT deficiencies for which they have developed an action plan together with the FATF (FATF, 2019; 2017).

Risk indicators

For all the companies in the sample, the full ownership structure was reconstructed (Figure 1). For each firm, entities owning more than 10% of the share capital at each ownership level were identified. This process continued until we reached an individual ultimate beneficiary at the top of the chain (i.e. a BO). If it was not possible to identify an individual at the top of a chain, then the top shareholder was referred to as Other Ultimate Beneficiary (OUB). Entities separating a company from its ultimate beneficiaries, either BOs or OUBs, were labelled as intermediate shareholders (INTs).

Each of the proposed risk indicators were measured and operationalised as described below.

Beneficial ownership complexity (BOC)

The first analysed risk factor related to the anomalous complexity of corporate ownership structures. The complexity of an ownership structure was operationalised using the so-called *BO distance*, that is, the number of steps that separate a company from its BO(s). When the *BO distance* is equal to 1, then the company is directly controlled by its BO(s). The greater the BO distance, the higher the level of complexity of the company's ownership structure, hence the more difficult it is to trace its BOs, which in turn represents a greater risk that the company can be used to hide criminal profits and/or individuals (Knobel, 2021).

1 Countries included: EU27 + the United Kingdom + Switzerland.

2 https://www.bvdinfo.com/en-gb/ (last visited: August, 2022)

3 Belgium, Cyprus, France, Italy, Luxembourg, Malta, the Netherlands, Spain, and the United Kingdom.

4 For more information, see https://risk.lexisnexis.com/global/en/products/worldcompliance-data (last visited: August, 2022).

5 For the purposes of our analysis, all categories of crimes and predicate offences covered by LexisNexis were included.

6 For a full list of black and grey listed countries, see ***Annex 1: Black and grey lists considered in the study.***

Figure 1 – Illustration of the different actors of the ownership structure of a company (CO), which includes Beneficial Owners (BOs), Other Ultimate Beneficiaries (OUBs), and intermediate shareholders (INTs).

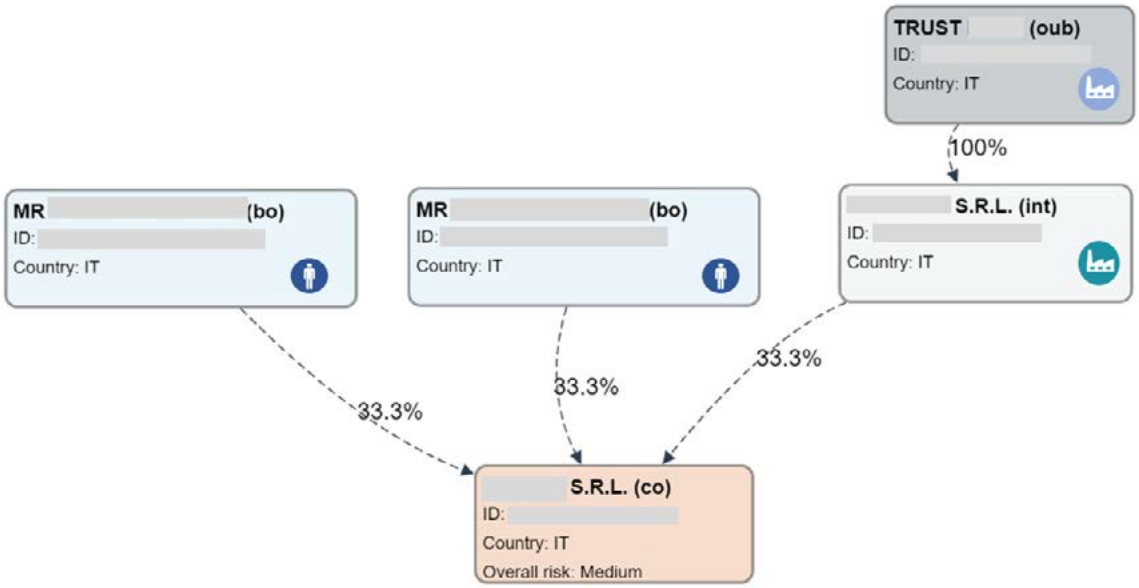
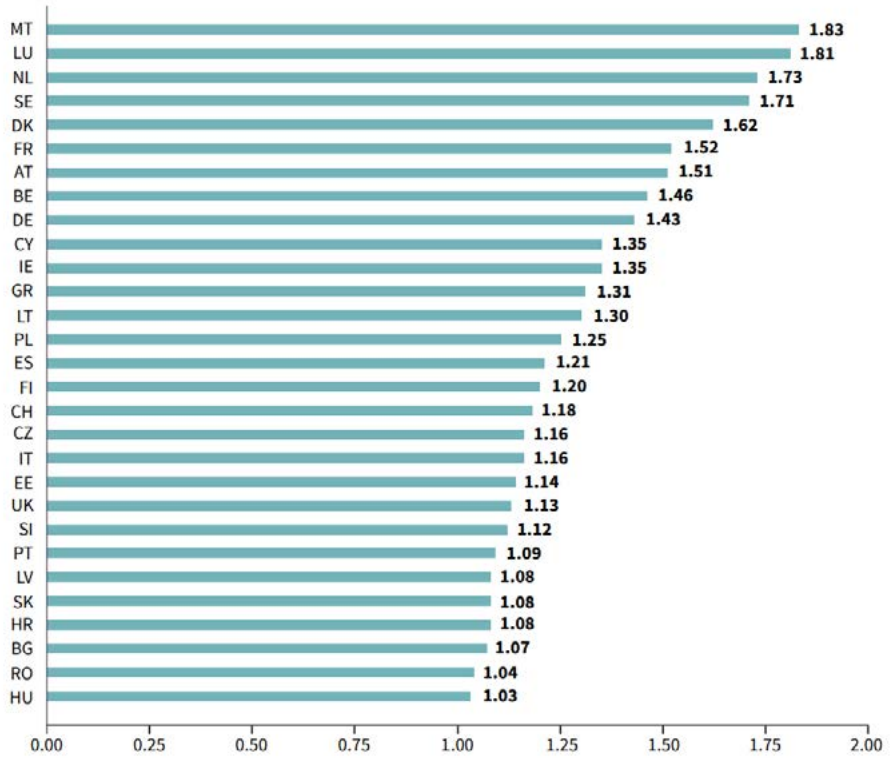


Figure 2 – Average BO distance across European countries (EU27 + UK + CH, 2019)



The average *BO distance* was calculated for all the companies in the sample, and the average observed values were computed at both the territory and sector level. While the average EU value of the BOC indicator was 1.21, significant differences can be observed across countries (Figure 2). Malta was the country that displayed the highest average BO distance among European countries (1.83), followed by Luxembourg (1.81), the Netherlands (1.73), and Sweden (1.71). Conversely, the lowest values were observed in Hungary (1.03), Romania (1.04), and Bulgaria (1.07). Moreover, the analysis conducted at a sector level (NACE rev.2 division) showed that some of the business sectors with the highest density of anomalous complex companies included Water transport (NACE division 50), and Gambling and betting activities (NACE division 92), which aligns with previous research (Savona and Riccardi 2018; 2017), and police investigations (DIA 2019; 2017; 2016).

Beneficial ownership secrecy (BOS)

When a company has ownership links to countries with high levels of secrecy, it is more difficult to trace BOs, hence to carry out financial investigations. Therefore, the greater the number of links to high-risk jurisdictions, the greater the risk that these companies may be misused for criminal purposes (Tax Justice Network, 2015; Tavares, 2013). Consequently, ownership data were matched with black and grey lists of risky jurisdictions issued by EU, and FATF. Then, the number of entities (i.e., BOs, OUBs, INTs) that were linked to risky countries for all the ownership structures under study were estimated.

Results showed that the average percentage of companies with ownership connections to black/grey listed jurisdictions across the EU is 0.91%. Furthermore, Luxembourg (8.7%), and Cyprus (8.5%) were by far the countries with the highest values (Figure 3), while the lowest estimates were observed in Portugal (0.1%), Estonia (0.2%), and Slovenia (0.2%). Interestingly, it can be seen that in some countries, such as Belgium, Switzerland, and the United Kingdom, a relevant portion of the links to blacklisted countries were to BOs (i.e., individuals), whilst in others, such as Cyprus, Luxembourg, and the Netherlands, the largest major proportion of these links were not related to individuals, but rather to other firms that were intermediate companies (i.e. firms somewhere in the ownership chain between the company at issue and its BOs), or other ultimate beneficiaries (i.e. firms and corporate vehicles that are at the top of an ownership chain, and do not allow for the identification of the BOs).

Beneficial ownership unavailability (BOU)

In some cases, the identification of the BO(s) of a company is not possible. This may be due to a highly fragmented share capital structure where no one individual owns more than 10% of the shares, or because certain specific corporate vehicles are used deliberately to conceal the identity of individuals at the top of the ownership chain. While the first case of fragmented structures is perfectly legal, and in some contexts even common, the latter option represents a risk factor since the more difficult it is to correctly identify the BOs, the higher the risk that the company can be used to conceal illicit activities. As such, we defined and calculated the BOU indicator for each of the companies as the number of ultimate owners, if any, that are an opaque corporate entity, including trusts, fiduciaries, foundations, and investment funds, which, by statute, do not allow for the identification of the BO(s).

Across the EU, on average, 1.45% of companies were controlled by a trust, a fiduciary, or a fund. As illustrated in Figure 4, the analysis outlined high values in the Netherlands, where 25.6% of the limited companies in our sample were in fact controlled by an opaque corporate vehicle. This is most likely connected to the extended domestic use of Dutch foundations (so-called *stichting*), which are legal arrangements exploited for a range of legitimate purposes: in the Netherlands are commonly used to control for-profit limited or unlimited firms. However, given their specific nature, it is not very meaningful to talk about 'owners' of a *stichting*, and for this purpose they may be misused to hide the identity of the ultimate beneficiaries (OECD, 2019).

Processing of risk indicators

A final processing of the proposed risk indicators involved the transformation from continuous values to risk scores. To this end, we separated the sample into groups of peer companies (so-called *peer groups*), that is, groups of companies active in the same business sector and with a comparable dimension, and further classified companies into five non-overlapping classes using a K-means hierarchical clustering algorithm. This resulted in each company in the sample being assigned a BOC, BOS, and BOU risk score ranging from 1 to 5: the greater this value, the higher the level of risk.

Correlation among risk indicators

As depicted in Table 1, all three ownership indicators showed a positive correlation with each other at the country, regional (nuts2), and sectoral (NACE rev.2 division) levels. The strongest correlation coefficients were observed at country level (a.), while smaller but still significant correlations were observed at regional level (b.). On the contrary, little to no dynamics were observed at sector level. These results suggest that each of the risk indicators captures different facets of corporate ownership features, and that the concentration of anomalous companies seems to be driven by country level-dynamics, such as national legislations and regulations, rather than by industry-driven factors.

Table 1 – Pearson correlation among ownership indicators at a. country level, b. sub-country level (NUTS2), and c. sector level (NACE rev.2 division)

	BOC	BOS	BOU
BOC	1		
BOS	a. 0.52*** b. 0.46*** c. 0.22**	1	
BOU	a. 0.78*** b. 0.58*** c. 0.07	a. 0.36* b. 0.23*** c. 0.10	1

Figure 3 – Percentage of companies with ownership links to black/grey listed jurisdictions (EU27 + UK + CH, 2019)

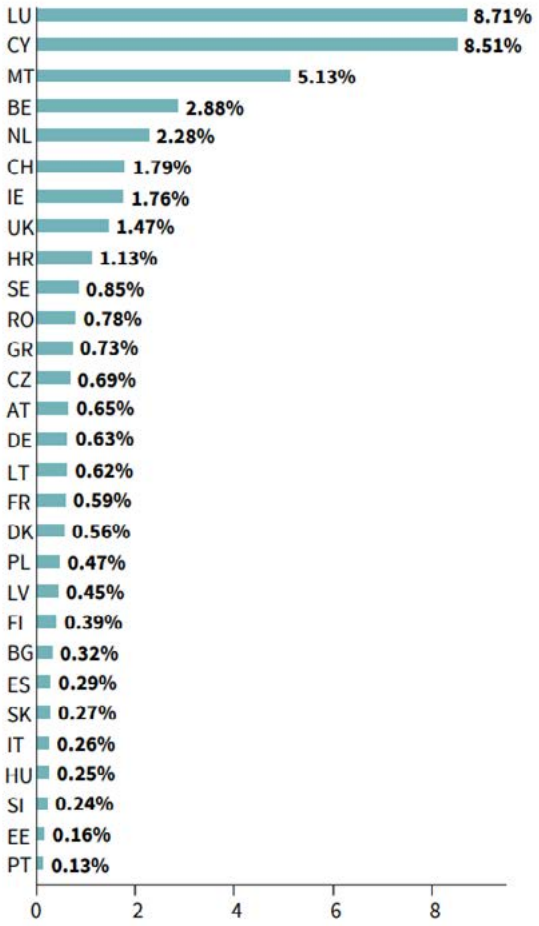
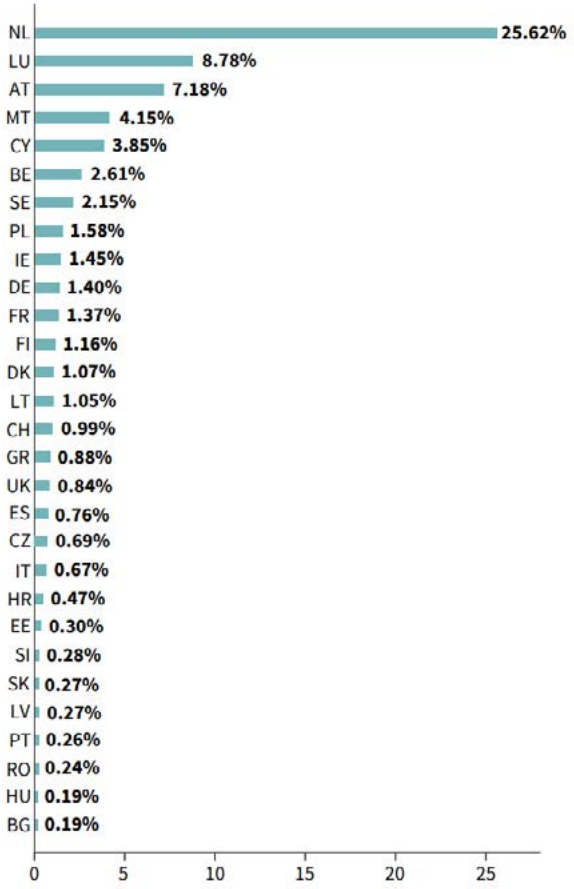


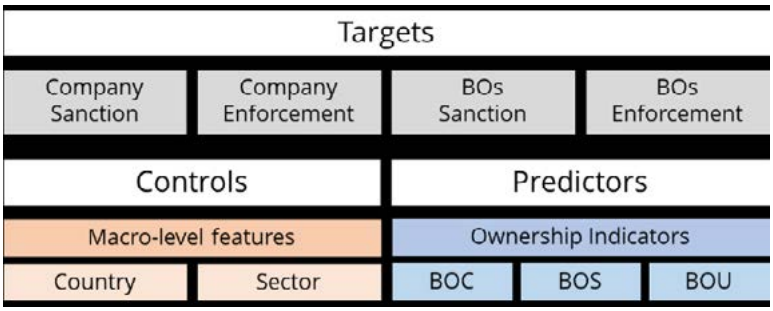
Figure 4 – Percentage of companies with ownership links to opaque corporate vehicles (EU27 + UK + CH, 2019)



Validation of indicators

The proposed risk indicators were then validated by training and testing various machine learning models, thus establishing their usefulness to identify companies that are potentially involved in illicit activities. For the purposes of validation, a sample of around 3 million limited companies registered in the nine European countries from where enforcement and sanction data was used.[7] In particular, we considered (i) as target variables, sanctions and enforcement flags from LexisNexis WorldCompliance, (ii) as predictors, the proposed ownership risk indicators (i.e., BOC, BOS, BOU), and (iii) as controls, a set of country and sector-level binary variables (Figure 5).

Figure 5 – Variables used for modelling: 4 target variable (sanctions on companies, enforcements on companies, sanctions on BOs, enforcements on BOs), three predictors (BOC, BOS, BOU), and two controls (country, economic sector).



Several machine learning models have been implemented, both for the detection of sanctions and enforcement cases, and for the assessment of the predictive performance of the ownership risk indicators. Machine learning models included logistic regression, decision trees, bagged trees, and random forests. All methods have been fitted using a training set (80% of the sample), and further validated on a test set (20%), which ultimately ensured a non-biased estimation of the predictive ability of both the models, and the risk indicators. To manage the imbalance of the target variables, we employed a simple but effective sampling strategy on the training set based on the under-sampling of the majority class (i.e. non-sanctioned/non-enforced observations) that we randomly matched to the number of observations in the minority class (i.e. sanctioned/enforced observations). A robustness analysis based on logistic regression was also performed to assess the stability of the results when cases from a certain country or business sector are excluded.

Satisfactory performance was achieved by all the considered machine learning methods, particularly regarding sanction offences.[8] In the case of logistic regression (Table 2), the algorithm correctly predicted 83.3% of sanctions on companies, and 88% of sanctions on owners. The prediction of companies and owners not subject to sanctions or prior enforcement was also good. The lowest performance occurred when predicting owners in the UK, who have either been subject to or not subject to enforcement, which is suggestive of a more complex country-specific phenomenon.

7 We separated UK from the sample since the number of observations (both number of companies and sanctions/enforcements) compared to the rest of the countries was extremely large, hence eroding the performance of models. This asymmetry can be explained by the higher coverage of LexisNexis in the UK.

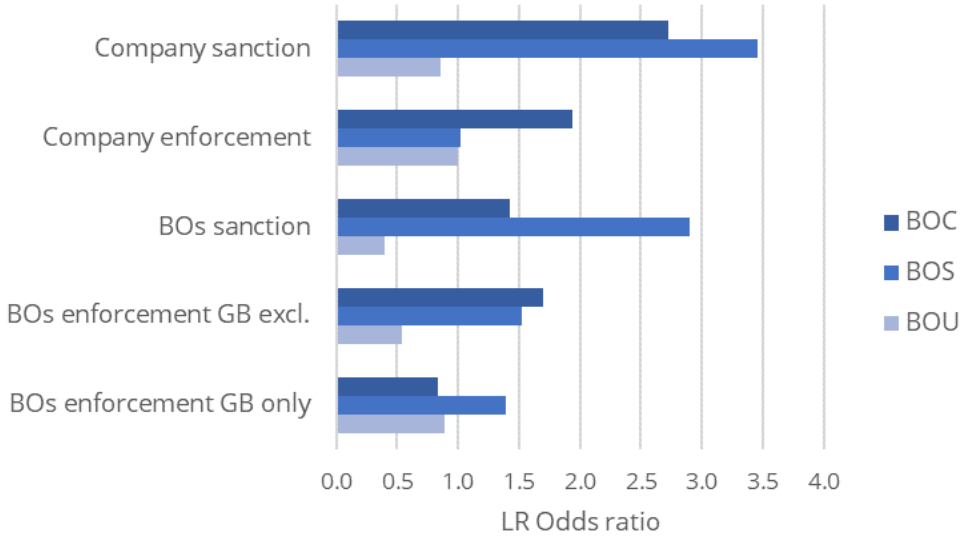
8 More details of machine learning results in Annex 2: Prediction accuracy of different models for the different target variables.

Table 2 – Overall predictive power (true positive and true negative rates) of risk indicators

Logistic regression (test set)	True positive rate	True negative rate
Company sanction	0.833	0.872
Company enforcement	0.679	0.729
BO sanction	0.879	0.851
BO enforcement excl. UK	0.615	0.564
BO enforcement UK	0.548	0.522

Regarding the predictive ability of the indicators, it is observed that BOS was notably important for detecting most offences, particularly with respect to sanction cases (Figure 6). Regarding BOC, there is also evidence of its ability to predict sanctions and enforcement on companies. The BOU indicator appeared to be less relevant in terms of predictive power, but still useful when used collectively.

Figure 6 – Logistic regression odd-ratios of risk indicators by target variable



While the results were stable across the whole sample, some country and sector-specific patterns were observed. For instance, in Italy, Cyprus, and Spain, ownership complexity (BOC) seemed to present a strong connection with illicit behaviour of companies. Ownership links to high-risk jurisdictions (BOS), and ownership links to opaque corporate vehicles (BOU) were more relevant in Malta and the Netherlands. At the sector level, we observed that anomalous ownership complexity (BOC), and ownership links to high-risk jurisdictions (BOS) were major determinants of enforcement and sanction offences in the Financial and insurance sector, while ownership links to opaque corporate vehicles (BOU) was an important factor in the Wholesale and retail trade, as well as Transporting and storage sector.[9]

To conclude, the proposed risk indicators have demonstrated a strong predictive power, confirming that firms with: (i) anomalous complexity of ownership, (ii) ownership links to high-risk jurisdictions, and (iii) ownership links to opaque corporate vehicles, are more prone to engage in illicit activities. Interesting country and sector-specific patterns were observed, evidencing a dynamic and transnational phenomenon, which needs to be tackled by means of innovative technologies, such as the DATACROS tool.

9 For more details see (Author. 2020).

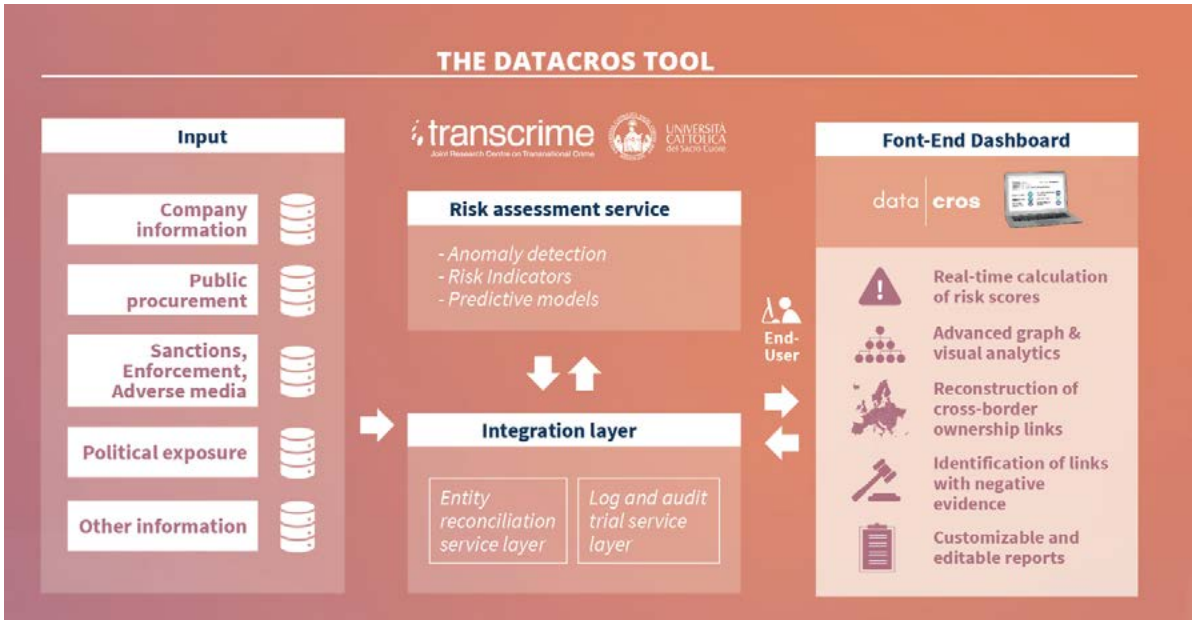
The DATACROS Tool

DATACROS is a research project co-funded by European Union Internal Security Fund – Police, and coordinated by the research centre Transcrime – Università Cattolica del Sacro Cuore, aimed at developing a tool to detect anomalies in firms' ownership structure that can flag high risks of money laundering, collusion, and corruption in the European single market. The first phase of the project (DATACROS I) was conducted between 2019 and 2021 with the participation of the French anti-corruption Authority (Agence Française Anticorruption), the Spanish Police (Cuerpo Nacional de la Policia), and investigative journalists from the IRPI consortium. A second phase of the project (DATACROS II) has started in February 2022 that will last for two years. It will aim at enhancing the Datacros prototype tool, and to test it in operational scenarios with a wide range of end-users, including LEAs, AROs, ACAs, CAs, and investigative journalists. The project consortium, led by Transcrime, is composed by 18 institutions located in 7 different EU countries (Italy, Romania, Spain, France, Belgium, Lithuania, and Czech Republic), including also international organisations and global networks, such as Europol and the Network of Corruption Prevention Authorities (NCPA). For more information, visit: https://www.transcrime.it/datacros/.

DATACROS is only one of several projects of the TOM – The Ownership Monitor research group, a joint initiative recently launched by Transcrime together with its spin-off Crime&tech, to study the opacity of corporate structures in Europe (and beyond).

Project DATACROS I has developed a prototype tool for risk assessment of legitimate companies, able to detect anomalies in firms' ownership structure that can flag high risks of collusion, corruption, and money laundering. This prototype tool is a real-time analytical platform that can be used to investigate anomalies in EU firms' ownership structures, and to conduct risk assessments. The tool complements traditional approaches (e.g. sanctions list checks) with innovative machine learning algorithms, such as the ones presented in the previous sections of this study. In particular, the tool allows to:

- Trace and reconstruct cross-border links among companies, individuals, and related entities (i.e., BOs, shareholders, directors);
- Calculate risk indicators at firm-level in real time, in order to orient, target, and prioritise investigations;
- Detect cartels and clusters of firms that may signal collusive behaviour;
- Identify links with firms and individuals targeted by sanctions and enforcement;
- Visualise graph, maps, and dynamic analytics components to simplify screening activities.



During the second phase of the project (DATACROS II, 2022-2024), the tool will be empowered, fully deployed, and validated by a wider set of public authorities (i.e., LEAs, AROs, ACAs, CAs, and investigative journalists) in different operational scenarios.

In particular, the tool will integrate:

- A wider set of risk indicators, suggested by the Project Consortium, such as financial anomalies, anomalous geographic concentrations, anomalies in turnover of owners and directors, and links to Free Trade Zones;
- New data sources (e.g., company financials, procurement data, sanctions and enforcement data, PEPs) with global coverage (200 countries, 300+ million firms), allowing to trace complex networks, also beyond EU borders;
- New risk assessment functionalities, and machine learning-based entity resolution algorithms;
- Enhanced IT security and personal data protection architecture, to ensure its compliance with governing laws at EU and national level (e.g. Directive 680/2016 and GDPR).

Conclusions

Due to the increased use of legitimate companies in illicit schemes, corporate ownership secrecy has become a central issue in the global political and economic debate. While several measures have been implemented worldwide to increase the transparency of firms and their owners, empirical evidence and knowledge on the subject remains limited to few case studies: there is a complete absence of large-scale analyses. Moreover, there is a lack of tools that are specifically designed for risk assessment and risk monitoring of firms to be used by public authorities (e.g., LEAs, FIUs, CAs, ACAs, TAs).

Schemes are getting more complex (e.g., cross-border, use of opaque vehicles, complex ownership schemes), but information is getting richer. Therefore, advance methodologies are required to prepare LEAs and other authorities as to adequately combat financial crime in the digital age. It is fundamental to develop knowledge and skills to support: (i) gathering of information on companies and related entities/individuals, (ii) developing of ML-based indicators and models to identify high-risk companies, and (iii) implementation of customised tools for investigation and risk assessment of companies and owners. In fact, current tools and solutions available on the market are designed primarily for financial institutions (e.g. for anti-money laundering and compliance purposes), revealing a lack of tools specifically designed for public authorities.

In response to this, we propose and validate an innovative analytical approach for measuring the opacity of corporate ownership through a set of secrecy risk indicators. The proposed risk indicators have demonstrated a strong predictive power, confirming the relevance of corporate ownership opacity as a key element to fight financial crime. The analysis conducted indicates that even strong and stable economies within the EU are vulnerable in this regard. Firms with (i) anomalous complexity of ownership, (ii) ownership links to high-risk jurisdictions, and (ii) ownership links to opaque corporate vehicles are, in fact, more prone to engage in illicit activities.

The present study also presents the DATACROS tool, a prototype software that allows to calculate in real time the ownership risk indicators discussed in this paper, integrating them in an analytical platform designed to support financial crime investigations by public authorities. In the first phase of the project

(2019-2021), the tool has been tested by different end users, including the French Anticorruption Agency, the Spanish Police, and the investigative journalists from IRPI, who have reported a high level of satisfaction with the tested tool. A second phase of the project (DATACROS II) has started in February 2022, and will last for two years. It will aim to enhance the DATACROS prototype tool, and to test it in operational scenarios with a wide range of end-users: LEAs, AROs, ACAs, CAs, and investigative journalists. The project consortium, led by Transcrime, is composed by 18 institutions located in 7 different EU countries (Italy, Romania, Spain, France, Belgium, Lithuania, Czech Republic), including also international organisations and global networks, such as Europol, and the Network of Corruption Prevention Authorities (NCPA).

The findings of the present research lead us to suggest various recommendations. First, it is required to improve the assessment and mapping of high-risk areas and sectors of activity, and how this impacts the misused of legitimate structures by organised crime, and other criminal actors. Improving the monitoring exercise could only enhance understanding of how risks evolve and change, overall and across territories and industries.

Second, there is a growing need for data analytics solutions and risk indicators to increase the effectiveness of monitoring and supervision of ownership opacity.

The last recommendation relates to the improvement of information exchange and cooperation among public authorities. As the latest SOCTA report highlighted, current criminal schemes entail crosslinks among corruption, money laundering, organised crime, and tax fraud (Europol 2021). This calls for the EU to support activities that promote communication, coordination, and cooperation among the wide variety of stakeholders active in the fight of corruption, money laundering, and other financial crimes, including LEAs, ACAs, CAs, FIUs, TAs, investigative journalists, and civil society NGOs.

Acknowledgements

The authors would like to acknowledge that the present study results from the research activity of DATACROS, project funded by the European Union Internal Security Fund – Police (ISFP-2017-AG-CORRUPT-823792).

Annexes

Annex 1: Black and grey lists considered in the study

Updated as of October/November 2019

List	Countries included
EU black list of non-cooperative jurisdictions for tax purposes (08/11/2019)	American Samoa, Fiji, Guam, Oman, Trinidad and Tobago, United States Virgin Islands, Vanuatu, Samoa
EU grey list of non-cooperative jurisdictions for tax purposes (08/11/2019)	Anguilla, Antigua and Barbuda, Armenia, Australia, Bahamas, Barbados, Bermuda, Bosnia and Herzegovina, Botswana, Belize, British Virgin Islands, Cape Verde, Cayman Islands, Cook Islands, Curacao, Jordan, Maldives, Marshall Islands, Mongolia, Montenegro, Morocco, Namibia, Nauru, Niue, Palau, Saint Kitts and Nevis, Saint Lucia, Seychelles, Swaziland, Thailand, Turkey, Vietnam
FATF AML black list (October 2019 statement) – Call for action	Iran, Democratic People's Republic of Korea
FATF AML grey list (October 2019 statement) – Other monitored jurisdictions	Bahamas, Bouvet Island, Cambodia, Ghana, Iceland, Mongolia, Palau, Papua New Guinea, Tajikistan, Tunisia, Yemen, Zimbabwe

Annex 2: Prediction accuracy of different models for the different target variables

Accuracy metrics include true positive rate (TPR), true negative rate (TNR), overall accuracy, and area under the curve (AUC)

	TPR	TNR	Accuracy	AUC
	Logistic Regression (LR)			
Company sanction	0.833	0.872	0.853	0.931
Company enforcement	0.679	0.729	0.704	0.785
BOs sanction	0.879	0.851	0.865	0.896
BOs enforcement UK excl.	0.615	0.564	0.589	0.634
BOs enforcement UK only	0.548	0.522	0.535	0.550
	Decision Tree (DT)			
Company sanction	0.876	0.846	0.861	0.919
Company enforcement	0.769	0.634	0.701	0.731
BOs sanction	0.869	0.856	0.863	0.879
BOs enforcement UK excl.	0.520	0.675	0.598	0.639
BOs enforcement UK only	0.874	0.164	0.524	0.533
	Bagged Trees (BT)			
Company sanction	0.910	0.778	0.844	0.918
Company enforcement	0.763	0.634	0.698	0.759
BOs sanction	0.856	0.841	0.849	0.890
BOs enforcement UK excl.	0.515	0.670	0.592	0.640
BOs enforcement UK only	0.874	0.164	0.524	0.533
	Random Forest (RF)			
Company sanction	0.752	0.868	0.810	0.922
Company enforcement	0.729	0.662	0.696	0.766
BOs sanction	0.851	0.859	0.855	0.885
BOs enforcement UK excl.	0.578	0.610	0.594	0.649
BOs enforcement UK only	0.550	0.523	0.537	0.554

References

- Bosisio, A., Nicolazzo, G. & Riccardi, M. (2021) *The changes in ownership of Italian companies during the Covid-19 emergency*. Milano: Transcrime – Università Cattolica del Sacro Cuore (Transcrime Research in Brief, 5).
  Available at: https://www.transcrime.it/en/publications/the-changes-in-ownership-of-italian-companies-during-the-covid-19-emergency/ (Accessed: 22 June 2021)
- DIA (2016) *Relazione semestrale sull'attività svolta e sui risultati conseguiti dalla Direzione investigativa antimafia – secondo semestre 2016*. Ministero dell'Interno.
- DIA (2017) *Relazione semestrale sull'attività svolta e sui risultati conseguiti dalla Direzione investigativa antimafia – secondo semestre 2017*. Ministero dell'Interno.
- DIA (2019) *Relazione semestrale sull'attività svolta e sui risultati conseguiti dalla Direzione investigativa antimafia – secondo semestre 2019*. Ministero dell'Interno.
- EFECC (2020) *Enterprising criminals – Europe's fight against the global networks of financial and economic crime*.
  Available at: https://www.europol.europa.eu/publications-documents/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime
- European Commission (2019) Evolution of the EU list of tax havens.
  Available at: https://ec.europa.eu/taxation_customs/sites/taxation/files/eu_list_update_08_11_2019_en.pdf.
- Europol (2018) EU-wide VAT fraud organised crime group busted, Europol.
  Available at: https://www.europol.europa.eu/newsroom/news/eu-wide-vat-fraud-organised-crime-group-busted (Accessed: 5 January 2021)

- Europol (2021) EU Serious and Organised Crime Threat Assessment 2021. The Hague: EUROPOL.
  Available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment
- FATF (2017) FATF Report to the G20 on Beneficial Ownership. Paris: Financial Action Task Force.
  Available at: http://www.fatf-gafi.org/publications/mutualevaluations/documents/report-g20-beneficial-ownership-2016.html (Accessed: 25 January 2017)
- FATF (2019) Improving Global AML/CFT Compliance: On-going Process – 18 October 2019.
  Available at: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/fatf-compliance-october-2019.html (Accessed: 5 January 2021)
- FATF (2020) COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses.
  Available at: https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf
- ICIJ (2016) About the Panama Papers Investigation, ICIJ.
  Available at: https://www.icij.org/panama-papers-about-the-investigation/ (Accessed: 5 January 2021)
- ICIJ (2017) Paradise Papers Exposes Donald Trump-Russia links and Piggy Banks of the Wealthiest 1 Percent, ICIJ.
  Available at: https://www.icij.org/investigations/paradise-papers/paradise-papers-exposes-donald-trump-russia-links-and-piggy-banks-of-the-wealthiest-1-percent/ (Accessed: 5 January 2021)
- Jofre, M., Bosisio, A., Guastamacchia, S., & Riccardi, M. (2021) 'Money laundering and the detection of bad entities: a machine learning approach for the risk assessment of anomalous ownership structures', *2020 Empirical AML Research Conference proceedings – The Central Bank of the Bahamas* [Preprint].
- Knobel, A. (2021) 'Complex Ownership Structures. Addressing the Risks for Beneficial Ownership Transparency', *Tax Justice Newrok Working paper* [Preprint].
- OECD (2019) Global Forum on Transparency and Exchange of Information for Tax Purposes: The Netherlands 2019 (Second Round).
  Available at: https://www.oecd.org/tax/transparency/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-the-netherlands-2019-second-round-fdce8e7f-en.htm
- Savona, E.U. & Riccardi, M. (eds) (2017) Assessing the risk of money laundering in Europe – Final report of project IARM. Milano: Transcrime – Università Cattolica Sacro Cuore.
  Available at: www.transcrime.it/iarm
- Savona, E.U. & Riccardi, M. (2018) Mapping the risk of organised crime infiltration in European businesses – Final report of project MORE. Università Cattolica del Sacro Cuore. Milano.
- Tavares, R. (2013) *Relationship between Money Laundering, Tax Evasion and Tax Havens*. Thematic Paper on Money Laundering. Bruxelles: European Parliament – Special Committee on Organised Crime, Corruption and Money Laundering.
  Available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/crim/dv/tavares_ml_/tavares_ml_en.pdf (Accessed: 16 March 2016)
- Tax Justice Network (2015) Financial Secrecy Index 2015 – Final results. Tax Justice Network.
  Available at: http://www.financialsecrecyindex.com/PDF/FSI-Rankings-2015.pdf
- UNODC (2020) Covid-19 Vaccines & Corruption Risks: Preventing Corruption In The Manufacture, Allocation And Distribution Of Vaccines. COVID-19 Policy Paper.
- Van der Does de Willebois, E. *et al.* (2011) The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It. The World Bank.
  Available at: http://elibrary.worldbank.org/doi/book/10.1596/978-0-8213-8894-5 (Accessed: 29 October 2014).

Open Source Intelligence and Cultural Property Crimes

Francisco José Rufián Fernández
Agustín José Constante Orrios
Madrid Municipal Police

Abstract
There is a vast dark market focused on the antiquities trade, the main character of which, when compared to other illicit businesses, is its capacity to intermix with the legal market. This makes it more difficult to investigate. We must also add to this the fact that digital tools have changed our way of life and the manner in which business is conducted, and people undertaking criminal activities have not been left out of this. In this regard, law enforcement agencies need to develop scientific knowledge and IT capacities, in cooperation with academics and society, in order to face the continuous challenges in this field. Open Source Intelligence (OSINTI techniques are some of the most valuable tools in this regard, such as carrying out provenance investigations, which are crucial to identifying and proving the illicit origin of any object. This presentation aims to provide a succinct overview of the issue to foster the development of new academic research and investigations within the field.

Keywords: OSINT, cultural property, heritage, illicit trafficking, law enforcement, training.

Introduction

The illicit trafficking of cultural goods is currently one of the most prominent markets in the world, and thus the considerable volume of police operations fighting the trade has not declined. We are going to give a very brief introduction to the main characteristics which make this market "special", in comparison with other illegal markets, and point out some of the causes behind why this trade has endured for centuries, and, finally, expose how OSINT techniques can help law enforcement agencies to fight against it.

Main characteristics of the illicit trade of cultural objects

Cultural property is a crucial part of the identity of any state and a sector with significant economic value. So, protecting it from criminals seeking economic benefits, or any attack in which the objective would be to damage the very identity of a people (e.g., armed conflicts or terrorist attacks), is an essential duty of law enforcement agencies.

International legislation, and subsequently, national legislation, started trying to establish control of the cultural goods market in 1970. The 1970 Convention

on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property, together with the 1995 UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects are the primary international regulations regarding this issue[1]. As a result of this legislation, specialised units of law enforcement agents were established, and nowadays, there is an international network between different countries working against the illicit trafficking of cultural goods, hand in hand with Europol, Interpol, the World Customs Organisation (WCO) and the United Nations Office on Drugs and Crime (UNODC).

Besides that, an enormous quantity of objects is seized every year, and the number of people arrested or investigated is not decreasing, as we can see in international police operations like Pandora[2]. In 2017, according to the statistics reporting the operation[3], 41,000 cultural objects were seized and 53 people were arrested through 200 investigations spanning 81 countries, which ran from October to December. We can see similar data every year, and how the importance of the online market is growing. In fact, for Operation Pandora 2021, the online market was an important objective, and a cyber patrol week was organised to focus efforts on the internet trade.

Currently, we see an elevated level of international concern regarding the illicit trade of cultural objects, and at the same time, we can see how that trade not only persists, but even thrives, and continues with its negative impact on society. Furthermore, other forms of crime, such as tax evasion and money laundering, are usually linked with it.

The prime reason for this is likely to be the conjunction of characteristics that make this illegal trade different from other illegal trades. The transnational nature of the illicit traffic in antiquities is what makes it possible, as with other illegal markets, but perhaps the most characteristic element of this particular market is the way it makes use of the great variety of heterogeneous national state laws, making it relatively easy to introduce illegal objects into the legal market (Alder & Polk, 2007), thus succeeding in uniting the two markets, the legal and the illegal, creating what some authors have called a "grey market" (McKenzie et al., 2020).

What we find is a market for which an intricate network of collaboration is used, employing highly variable methods and structures (Campbell, 2013; McKenzie, 2014). The trade is established as a network which functions in a similar way to other illegal trades. It is very closed, and the participants continuously vary their roles and components, as other modern criminal groups do. They are comprised of "fluid network structures rather than more formal hierarchies", an organisational structure that is particularly well suited to trafficking (Campbell, 2013).

All this together entails a complex transfer of objects, resulting in the mixing of cultural goods with very diverse origins, making them extremely difficult to trace. On top of this difficulty, we need to also bear in mind other related laws, aside from those regarding the import and export of cultural heritage goods[4].

Consequently, investigators and researchers must face too many limitations in their work. We do not have, for example, reliable data regarding the scope of the market and a very poor understanding of how the trade is actually organised and operates. On the other hand, we do know that the dark figure of crime is very high in this sector.

One example of our lack of knowledge regarding this data is the frequently repeated claim, not only by media outlets, but even by academics, which states that: "*the trade of cultural objects is valued at billions of dollars annually and ranks with drugs and arms as one of the three most serious illicit trades*". This claim has been refuted many times, but never seems to go away (Brodie, et al., 2022).

1 We should also bear in mind the 1954 Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict and the Council of Europe's 2017 Nicosia Convention on Offences relating to Cultural Property, as well as the European regulation regarding the export of cultural goods (Council Regulation (EC) No. 116/2009) and regarding the introduction and import of cultural goods into the Union (Regulation of the European Parliament and of the Council (EU) No. 2019/880).

2 Operation Pandora is the name of a joint pan-European operation of law enforcement authorities, along with Europol, Interpol, UNESCO and the WCO against the theft and illicit trafficking of cultural goods. The operation is repeated every year.

3 https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2018/Over-41-000-artefacts-seized-in-global-operation-targeting-trafficking-of-cultural-goods

4 There is a significant volume of potentially related crimes: receiving, looting, concealment, counterfeiting, fraud, money laundering or organised crime (European Commission, 2019). Today, any action against money laundering (Teichmann, 2019), terrorism financing or tax fraud must be implemented alongside measures to prevent the trafficking of cultural goods (UNESCO, 2018).

Another similar claim is that Da'esh has been financing its activities through antiquities trafficking, which is alleged to have been making the group tens, or even hundreds of millions of dollars, figures which, again, have been impossible to verify (Brodie, et al., 2022).

The damage caused by this activity is substantial. Aside from the loss of scientific knowledge[5], the illicit trafficking of antiquities can be viewed as:

— A political and cultural challenge to the sovereignty of the source countries (Mackenzie & Yates, 2016; McKenzie et al., 2020).

— A direct threat to religious identities, e.g., through iconoclastic destruction (Isakhan & González, 2018).

— A missed opportunity for society after an armed conflict or catastrophe (Viejo-Rose, 2013).

Taken together, these factors result in a great impact on economic and social systems (TRACID, 2019). It should also be borne in mind that cultural objects are a unique testimony to the evolution and identity of peoples and that the importance of protecting them takes on greater significant because they are irreplaceable. They are a vital educational resource that reveal the rich and complex story of humanity, comprised of many peoples, ideas, and faiths (Rufián, 2021).

OSINT as a source of intelligence.

Open-Source Intelligence is defined as intelligence produced using data accessed from public sources, which is subsequently processed by the intelligence cycle in order to gain insights (Böhm & Lolagar, 2021). We understand open sources to be those documentary resources that are within the public domain, in any medium, format and means of access (Felip i Sardà, 2004; Martín de Santos & Martín Vega, 2010).

On the other hand, the intelligence cycle consists of well-defined phases, through which a final product is obtained, a cycle that is designed to provide answers. To better explain this, we are going to follow one of the universal models of intelligence cycles, specifically the one used by the Spanish National Intelligence Centre (CNI, 2022), which consists of five phases:

- Direction phase: This is the phase in which the organisation determines the intelligence needs that are required.
- Planning phase: In this phase, the resources and methods for obtaining information are planned and organised.
- Collection phase: All relevant information is gathered and organised. OSINT is one of the disciplines in this phase.
- Processing phase: When all the information collected is processed, the final intelligence product is created through assessment, examination, integration, interpretation and drafting.
- Dissemination phase: This is the final phase of the cycle, when the intelligence is distributed to its intended recipients.

Although we have seen OSINT as a part of the intelligence cycle, since its inception in the 1940s up to the present, it has been configured as an autonomous discipline. This is due to the need to adopt a new approach to intelligence, derived from the universalisation of information and communication technologies.

The current context of hyperconnectivity favours the existence of a large amount of data flows available on the internet. The human need for communication is now widely covered and amplified through the use of internet platforms. We are now facing the paradox that individuals and organisations dump their information on the internet, and it is its processing that is now more complex than its storage. This, coupled with the fact that specific tools are being developed to automate processes and compile data, allows analysts to create intelligence products at little cost to agencies. The real cost is the need to train analysts to adapt to this new environment.

On the other hand, this data flow context means that internet users themselves are grouping into what we could call digital neighbourhoods and that social customs are evolving. This gives rise to new globalised models of communication and business, but also crime. In order to gather information through OSINT techniques, understanding globalisation and its effect on the determination of certain social networks or communication channels is essential.

The information gathering opportunities provided by both Big Data and OSINT have been learnt by a large

5 The indiscriminate excavation of archaeological sites, without regard for archaeological recording methodology, causes irreparable loss of scientific knowledge regarding the society and culture which created the objects (Brodie et al., 2000; Rodríguez, 2012; Renfrew & Bahn, 1991; McKenzie et al., 2020).

number of private sector organisations. Large corporations have their own corporate intelligence services that rely on open sources for intelligence and counter-intelligence activities.

There is an opportunity within the public sector for law enforcement agencies to fulfil their mission effectively by tapping into the flood of information flowing beyond closed databases. In this respect, OSINT focussed on organised property crime has been identified as a priority training need in the 'European Union Strategic Training Needs Assessment 2022-2025' (CEPOL, 2021). For this purpose, it would be desirable to train members of Law Enforcement both in the use of open source tools and in information analysis skills.

What OSINT can provide in the illicit trade of cultural objects

The Internet has created essential changes in the market, allowing new buyers and sellers to participate, with low-cost objects, and reaching more people (McKenzie et al., 2020). Social networks are also playing a significant role in the illicit trade (Sargent et al., 2020). Researchers have documented a substantial boost in recent years, especially during the Coronavirus crisis, when border closures have turned the Internet into a safer way to sell and buy antiquities. On the other hand, the marketing of illegal antiquities on a social platform, like Facebook, for example, represents a curious middle ground for regulation[6] (Votey, 2022), which makes it difficult for Law Enforcement to work and easy for the traders.

In that context, we need all actors involved in mitigating the illicit trafficking of cultural property to be well-prepared. Any loss of time only serves to favour the smugglers, while undermining cultural heritage, science and hope (UNESCO, 2018). The amount of information available online can be overwhelming, and the lack of expert knowledge can cause potential damage and lead to false beliefs (Yeboah-Ofori & Brimicombe, 2017).

The case study presented as proof of concept aims to provide another perspective on cultural heritage research within the context of law enforcement. It was carried out using entirely open source techniques in order to demonstrate their usefulness and the investigative capacity they offer, from the basics to more complex organisational structures.

After the direction phase, in which the need for knowledge about the looting of historical heritage in Ukraine using metal detectors was identified, the planning phase was established. First of all, contact was made with the target group. The aim was to understand what mechanisms drive and enable the trafficking of historical objects by individuals, as well as the channels that are chosen for their publicity and marketing. It was possible to determine that looting using metal detectors is a socially accepted practice, used as an element of exaltation of cultural heritage.

Using Google's online translator, searches were performed on the two main social networks that were determined to be the core networks for this research: Facebook and VKontakte. It was decided to work on these social networks because, as proof of concept to be developed in a summarised way, both have similar characteristics and are widely used within the geographical area where the research was carried out.

Facebook is one of the most popular social networks worldwide, with more than 2.8 billion users and VKontakte is a similar social network with more than 600 million users, which is widely used within the Russian sphere of influence.

The collection phase began with the identification of various user groups on the internet, dedicated to the recreational use of metal detectors. These were located in the communities of the Facebook social network.

Analysing the content of the messages and photographs of these groups, several items were found to bear the hallmarks of having been looted.

There were posts concerning ancient coins, pendants, medieval helmets and weapons, in which users asked about their possible sale price. In some cases, they even gave an estimate of the historical period to which they belonged.

This made it easier to target the investigation to specific individuals, specifically, the profiles of the users who posted these messages, as well as the relevant profiles

6 In this regard, the ATHAR project, an initiative led by anthropologists and heritage experts digging into the digital underworld of transnational trafficking, terrorism financing and organised crime, has shown how difficult is to deal with this kind of platform in their 2019 report called "Facebook's black market in antiquities". The report is available here: http://atharproject.org/report2019/

that interacted with them. After extracting the unique IDs of each profile and storing them, information about the profile holders was obtained.

Unique ID numbers correspond to each existing profile on a social network and enable it to subsequently be traced, even if its user name is changed. This number can be extracted from the URL by a calculation using various tools. From the basic publicly available information obtained from each profile, attention was turned to the VKontankte network to expand upon it and in some cases they were geolocated through the profile pictures.

For storage, the open source resource "archive.today" was used. Through this non-commercial service, a copy of any web page can be saved.

Subsequently, an open source tool called Eriys/SellerFB was used. This tool is publicly available on the Github platform in the repository of the user Eriys and allows the activity of a Facebook account on Facebook Marketplace to be known (Eriys Github repository 2022). SellerFB extracts the seller's profile information, as well as the items the seller has sold. It also returns information on the unique identifier of the Facebook Marketplace seller, the locations associated with that seller, the groups in which offers have been posted and the seller's rating. In this way, it was possible to correlate objects that had been displayed in metal detector user groups with transactions made on Facebook Marketplace, and these in turn could be correlated with the unique identifiers of Facebook and Facebook Marketplace accounts.

If necessary, based on the information obtained so far, the focus of the research could have been shifted to other social networks in order to expand it. Emulated geo-positioning techniques could have been used in order to locate profiles of certain social networks in physical locations, for example.

Conclusion

In conclusion, starting from a need to obtain information, it has been possible to obtain a large amount of accurate information collected entirely through open sources.

Firstly, a large number of individuals gather through communities on social networks, share and trade looted cultural property. For each of these individuals of interest to the investigation, it has been possible to obtain sufficient data to locate them physically. It has also been possible to identify individuals who have used Facebook Marketplace to carry out transactions with allegedly looted cultural objects. Next, it has been possible to obtain graphic evidence of a catalogue of items that, if necessary, could be used as evidence of the traceability of the origin of certain pieces, within the context of an official investigation.

Finally, through the interactions and study of the follow-ups carried out on certain user communities or sales pages, a large amount of identifying data can be obtained from them, and the scope of the research can be broadened.

From the public data obtained from these shops, it is possible to extract a great amount of information, and thus establish links between individuals and points of sale.

References

- Alder, C. & Polk, K. (2007) *Crime in the World of Art*. In: Pontell, H. N. & Geis, G. (eds), International Handbook of White-Collar and Corporate Crime. Springer Science+Business, pp. 347-357.
- Böhm, I. & Lolagar, S. (2021) Open-source intelligence. *Int. Cybersecur. Law Rev.* 2**,** 317–337. https://doi.org/10.1365/s43439-021-00042-7
- Brodie, N., Kersel, M., Mackenzie, S., Sabrine, I., Smith, E. & Yates, D. (2022) Why There is Still an Illicit Trade in Cultural Objects and What We Can Do About It, *Journal of Field Archaeology*, 47:2, 117-130, DOI: 10.1080/00934690.2021.1996979
- Brodie, N., Doole, J., Watson, P. (2000) Stealing History: The Illicit Trade in Cultural Material. The McDonald Institute for Archaeological Research. Cambridge.
  Available at: https://traffickingculture.org/publications/brodie-n-doole-j-and-watson-p-2000-stealing-history-the-illicit-trade-in-cultural-material-cambridge-mcdonald-institute/ Accessed 7 August 2022.

- Campbell, P. (2013) The Illicit Antiquities Trade as a Transnational Criminal Network:
- Characterizing and Anticipating Trafficking of Cultural Heritage. In: International *Journal of Cultural Property*, Vol. 20 p.113–153. DOI:10.1017/S0940739113000015
- CEPOL (2021) European Union Strategic Training Needs Assessment 2022-2025.
  Available at: https://www.cepol.europa.eu/sites/default/files/EU-STNA-2022-CEPOL.pdf Accessed 5 August 2022.
- CNI (2022) Centro Nacional de Inteligencia
  Available via: https://www.cni.es/la-inteligencia Accessed 10 August 2020.
- European Commission (2019) Illicit trade in cultural goods in Europe: Characteristics, criminal justice responses and an analysis of the applicability of technologies in the combat against the trade. Final report.
  Available via: https://op.europa.eu/en/publication-detail/-/publication/d79a105a-a6aa-11e9-9d01-01aa75ed71a1 Accessed 11 August 2020.
- Eriys Github repository 2022.
  Available at: https://github.com/Eriys/SellerFB Accessed 12 August 2022.
- Felip i Sardà, JM. (2004) La gestión de fuentes abiertas por los servicios de Inteligencia y los equipos de investigación: el estado de la cuestión. Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol, 48, pp. 41-50.
- Isakhan, B. & González Zarandona, J.A. (2018) Layers of religious and political iconoclasm under the Islamic State: symbolic sectarianism and pre-monotheistic iconoclasm. *International Journal of Heritage Studies*, 24:1, 1-16, DOI: 10.1080/13527258.2017.1325769
- Mackenzie, S., Brodie, N., Yates, D. & Tsirogiannis, C. (2020) Trafficking Culture: New Directions in Researching the global Market in Illicit Antiquities. Ed. Routledge
- Mackenzie, S. & Yates, D. (2016) Trafficking cultural objects and human rights. In: Weber L, Fishwick E and Marmo M (eds) The Routledge International Handbook of Criminology and Human Rights. New York: Routledge, p. 220–230.
  Available at: https://traffickingculture.org/publications/criminology-human-rights-and-trafficking-cultural-objects/ Accessed 5 August 2022.
- Mackenzie, S. (2014) Illicit Antiquities. In: Encyclopedia. Trafficking Culture.
  Available via: https://traffickingculture.org/encyclopedia/terminology/illicit-antiquities/ Accessed 5 August 2022.
- Martín de Santos, I. & Martín Vega, A. (2010) Open Sources Information. A System Of Perfect Competition. Inteligencia y Seguridad: Revista de Análisis y Prospectiva 8. pp. 91-112.
- Renfrew, C., & Bahn, P. (1991) Archaeology. Theory, Methods and Practice. Thames and Hudson.
- Rodríguez Temiño, I. (2012) *Indiana Jones sin futuro. La lucha contra el expolio del patrimonio arqueológico.* JAS Arqueología Editorial. Madrid.
- Rufián Fernández, F.J. & Sabrine, I. (2021) *Illicit Trafficking of Antiquities and Its Consequences on the SDGs*. In: Leal Filho, W., Azul, A.M., Brandli, L., Lange Salvia, A., Özuyar, P.G. & Wall, T. (eds) Peace, Justice and Strong Institutions. Encyclopedia of the UN Sustainable Development Goals. Springer, Cham. https://doi.org/10.1007/978-3-319-71066-2_124-1
- Sargent, M., Marrone, J.V., Evans, A., Lilly, B., Nemeth, E., Dalzell, S. (2020) Tracking and Disrupting the Illicit Antiquities Trade with Open-Source Data.
  Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2706/RAND_RR2706.pdf Accessed 9 August 2020.
- Teichmann, F.M.J. (2019) European antiquities trade: a refuge for money laundering and terrorism financing*, Journal of Money Laundering Control*, Vol. 22 No. 3, p. 410-416. https://doi.org/10.1108/JMLC-09-2017-0051
- Transnational Alliance to Combat Illicit Trade (2019) Mapping the impact of illicit trade on the sustainable development goals.
  Available at: https://www.tracit.org/publications_illicit-trade-and-the-unsdgs.html Accessed 10 August 2020.
- UNESCO (2018) Fighting the Illicit Trafficking of Cultural Property, a toolkit for European judiciary and law enforcement.
  Available at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CLT/movable/pdf/Toolkit.pdf Accessed 07 August 2022.
- Viejo-Rose, D. (2013) Reconstructing Heritage in the Aftermath of Civil War: Re-Visioning the Nation and the Implications of International Involvement, *Journal of Intervention and Statebuilding*, 7:2, 125-148, DOI: 10.1080/17502977.2012.714241
- Votey, M. (2022) *Illicit Antiquities and the Internet: The Trafficking of Heritage on Digital Platforms*, 54 N.Y.U. J. Int'l L. & Pol. 659.
  Available at: https://www.nyujilp.org/wp-content/uploads/2022/06/nyi_54-2-355-393_Votey..pdf Accessed 10 August 2022
- Yeboah-Ofori, A. & Brimicombe, A. (2018) *Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media.*. In: *International Journal of Cyber-Security and Digital Forensics*, 7(1): 87-98.
  Available at: https://repository.uel.ac.uk/download/699984104943e2a4baa5a1c3eaedac9860b8776b136595108a7c31a8cb70518a/528605/Cyber%20Intelligence%20%26%20OSINT%20-%20Developing%20Mitigation%20Techniques%20Against%20Cybercrimes%20Threats%20on%20Social%20Media.pdf
  Accessed 10 August 2022

Art of Money Laundering with Non-Fungible Tokens: A myth or reality?

Dimitrios Kafteranis
Umut Turksen
Centre for Financial & Corporate Integrity, Coventry University

Abstract
As the rules for countering money laundering constantly change, criminals find new methods and platforms to launder their "dirty" money. Recently, such new platforms have included the art market and the use of crypto currencies. Subsequently, both of these sectors were added to the list of sectors susceptible to facilitate money laundering. Apart from the traditional art market, criminals may use digital art in order to facilitate their activities. The rise of the digital art market with the expansion of Non-Fungible Tokens (NFTs) is a new area of concern for law enforcement agencies. Anonymity and price volatility of NFTs create a unique and exploitable environment for criminals. The complex nature and uncertain legal status of NFTs further complicate the counter measures one can take. This paper explains what NFTs are, analyses their relation to money laundering risks and scrutinises their legal status in the EU. In doing so, it identifies gaps in the law and training needs of law enforcement agencies. Finally, the paper provides potential solutions and recommendations in relation to these gaps. The paper offers a novel study on NFTs and aims to pave the way for further comparative studies related to NFTs.

Keywords: Non-Fungible tokens (NFTs), art market, money laundering, training

Introduction[1]

Money laundering is a global phenomenon which is under constant scrutiny. At international, European and national levels, new rules are constantly adopted in order to tackle money laundering. These new rules are dependent on the evolving character of markets and financial systems as well as the methods criminals use to launder their illegal proceeds. From laundering the proceeds of drug trafficking, which was the starting point in the fight against money laundering, to money laundering of cryptocurrencies gained from ransomware attacks (Akdemir, Lawless & Turksen, 2021), legislators have been adopting new rules to keep at pace. These new rules aim to address new phenomena and respond to new pathways used by criminals. One such phenomenon unfolding in a new platform is the art market which has been lately added to the list of sectors susceptible to facilitate money laundering.

1 Research for this paper received funding from the European Union's Horizon 2020 Research & Innovation Programme under Grant Agreement No. 101022004.

There are particular characteristics of art market which make it attractive to money launderers. Firstly, for many decades, the art market was characterised by a lack of robust regulation, and efforts to impose anti-money laundering rules on art market dealers have not succeeded in bringing tangible results (Akdemir, Lawless & Turksen, 2021; Transparency International UK, 2015; Hufnagel & King, 2019). Furthermore, the art market's lack of transparency and its volatile prices made it a perfect sector for money laundering (Purkey, 2010). Prices are, normally, quite high in the art market and the price of an art work can be speculative. The price can go up or down depending not only on the evaluation of the art work by art experts but also the price that potential buyers are willing to pay. As a result, an art work can be expensive but, if criminals want to launder a high amount of money through art, the price paid could easily be manipulated and/or forged in order to reduce the price value thus no suspicions would be raised (Purkey, 2010).

Moreover, the art sector is characterised by secrecy and anonymity which presents disadvantages (Burroughs, 2019). Secrecy and anonymity are problematic in relation to countering money laundering and recovery of criminal assets (International Monetary Fund, 2019). Art works are often offered for sale anonymously and potential buyers are represented by auction houses or art dealers. Therefore, criminals can sell or buy art without having their identities revealed to anyone. This path of secrecy and anonymity to art trade has risen the number of criminals involved in the art market (International Monetary Fund, 2019).[2]

For several years, the art market was not regulated in relation to anti-money laundering rules in the EU. The EU, in response to international concerns (Burroughs, 2019), adopted the Fifth Anti-Money Laundering Directive on April 2018 which requires "(…) *persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amount to EUR 10000 or more*" (European Parliament and European Council Directive, 2018, Article 1(c)(i)) to conduct due diligence searches and, when appropriate, to file a suspicious activity report (SAR) to national Financial Investigation Units (FIUs).

Despite the introduction of anti-money laundering rules, a new area of concern was identified: the expansion of NFTs (International Monetary Fund, 2019; Europol, 2022). There are several attributes that make NFTs attractive for criminals to launder their illegal funds through this medium. Firstly, the peer-to-peer transactions of NFTs without the involvement of intermediaries may or may not be recorded on a public ledger. Secondly, the fact that NFTs can be transferred online without limitations of geographical location and the anonymity of the internet make NFTs susceptible to be abused by money launderers.

The focus of this article is on NFTs and their relation to money laundering risks they pose. In the first part, the concept of NFTs in the art market is analysed. Then, their relation to money laundering and whether existing anti-money laundering rules at the EU level can capture NFTs are critically examined. In the final part, recommendations will be made on how to better regulate NFTs in the anti-money laundering context.

Definition of NFTs

NFTs can be considered as a new form of digital art. Traditionally, we think of art – or high art – as a painting by Picasso, Dali or Modigliani. The times are changing – so does art. NFTs are a new trend and, may be, the future of art. They became particularly "famous" during spring 2021 when Beeple's collage, 'Everydays – The First 5000 Days' was sold by Christie's for USD 69 million (Reyburn, 2021).[3] During the COVID-19 pandemic, art found new ways to expand or, from a more critical perspective, the rise of NFTs has coincided with the traditional art market being subjected to stricter anti-money laundering rules in the EU (European Parliament and European Council, 2018). Putting the traditional art market on the radar of anti-money laundering rules, Financial Intelligence Units (FIUs) and law enforcement agencies may have driven criminals to search for alternative methods of laundering their proceeds of crime.

NFTs can be various types of digital or virtual assets (Dowling, 2021) and the most common types are objects in virtual worlds, artworks and digitalised characters from sports, music or other artistic activities. NFTs are blockchain-based tokens which securely map

2 On page 33 of this IMF report, it is highlighted that as noted by the FBI and Interpol, "in comparison with other trade sectors, the art market faces a higher risk of exposure to dubious financial practices" because "the volume of legally questionable transactions in noticeably higher than in other global markets".

3 This has been the highest amount of money paid for an NFT so far.

ownership rights to digital/virtual assets (Ante, 2021). As paintings that belong to someone are exhibited in museums and art galleries for the public, NFTs are analogous to that as they provide a means of representing possession or ownership of digital assets such as games, art and music. The ownership of NFTs is usually registered on an Ethereum network.[4] The Ethereum network is functioning 'as one large computer which executes programs in lockstep' and which is 'virtualised by a network of other machines' (Dannen, 2017).

There is a specific distinction between NFTs and other types of blockchain and crypto tokens such as Bitcoin. Cryptocurrencies are fungible; there is no distinctive element between two Bitcoins as they have the same characteristics and they convey the same rights to their owners, thus called fungible tokens. NFTs, on the other hand, as their name suggests, are a special form of blockchain-based tokens as they represent a unique value that cannot be fully replaced by a different or similar token (Ante, 2021). Each NFT is unique and different from other NFTs, thus non-fungible (non-replaceable) as in the case of a unique piece of art. NFTs are traded on specialised marketplaces such as Opensea for digital artwork (Jordanoska, 2021). By purchasing NFTs, the collector or the purchaser acquires a certificate of authenticity which cannot be modified, lost or destroyed (Carron, 2021).

Money Laundering and NFTs

The sale of an NFT for USD 69 million and the rise in prices of CryptoPunks demonstrate a volatile market where exorbitant amounts of money are involved (Christies, 2021). Concerns have been raised by regulators and market experts around the globe whether these amounts of money spent on NFTs are used in order to circumvent the increasingly robust anti-money laundering legislation both at international and the EU levels (US Department of Treasure, 2022; Bluemel, 2022). These concerns were confirmed by the 2022 Crypto Crime Report which demonstrated that NFTs may be associated to money laundering. In the third quarter of 2021, the 'value sent to NFT marketplaces by illicit addresses jumped significantly', worth around 1 million US dollars' worth of cryptocurrency. In the fourth quarter, the number went to around 1.4 million US dollars. In both quarters, the big majority of the activities derived from 'scam-associated addresses sending funds to NFT marketplaces to make purchases'. In addition, both quarters present important amounts of stolen funds to be used to purchase NFTs. A bigger concern is that, in the fourth quarter of 2021, around 284,000 US dollars' worth of cryptocurrency are used to buy NFTs from 'addresses with sanctions risk' (Chainalysis, 2022).

One major challenge in the context of anti-money laundering compliance and law enforcement contexts is whether NFTs are considered as a work of art or not. For the money laundering concerns, this dilemma is significant. Recently, Wikipedia editors have voted not to classify NFTs as art which sparked outrage in the crypto community (Artnet News, 2022). The example of Wikipedia is not the one that will inform legislation or the judiciary but it demonstrates the challenging nature or acceptance of NFTs as art objects (Carron, 2021).[5] From the reactions coming from the crypto world, the common argument is that we cannot challenge digital art and cancel digital artists. This ongoing debate around NFTs as works of art is important for its ramifications in the fight against money laundering. While NFTs are unique pieces of code (tokens) linked to an underlying asset, it is not an artwork itself (Gould, 2022). Even if NFTs are not art *per se*, it is at least a means of trading in art or a digital asset with a significant value (Gould, 2022). Therefore, if NTFs are considered as digital art and a valuable asset, repercussions occur in the fight against money laundering.

At the EU level, the Fifth EU Anti-Money Laundering Directive does not provide an explicit definition of "works of art" nor does it define or mention NFTs. Thus, it is not certain whether NFTs would be considered as works of art under the Directive and be subject to anti-money laundering and terrorist financing rules including as CDD and Know Your Customer (KYC) practices. Because of the common features between traditional art market and NFTs such as price volatility and anonymity of buyers,[6] it may be the case that certain regulators will voluntarily decide to consider NFTs as works of art and put these under anti-money laundering rules for traders of NFTs.

4 Ethereum. (2022). Available from https://ethereum.org/en/ [Accessed 29th June 2022].

5 NFTs are linked to a unique asset that may be a GIF, a song, a limited-edition print, or even an "analogue" painting – as work of arts.

6 Anonymity is a major issue in relation to NFTs. From the trading perspective, there is a risk that users will trade with themselves (wash trading) and, thus, will be able to launder their money themselves. Criminals, by abusing anonymity, can create their own NFT, register it on a marketplace and then purchase it themselves.

At present, establishing what NFTs are seems to be a major challenge; should they be considered as virtual currencies, securities, crypto assets, digital art or collectibles. The Fifth EU Anti-Money Laundering Directive does not provide clear details on the reporting requirements on NFTs despite its regulatory extension to virtual currency exchanges and custodian wallets. One possible explanation is that, back in 2018 when the Fifth EU Anti-Money Laundering Directive was created, NFTs were not widely known or used; thus, they stayed out of regulatory scope of the EU's Anti-Money Laundering legal regime.

Nevertheless, the European Commission proposed in September 2020 a regulation which may include rules that would apply to NFTs. The Markets in Crypto-assets Regulation (MiCAR) provides a definition for crypto-assets, the first EU legal instrument to do so. MiCAR thus defines crypto-assets as "digital representation of value and rights which may be transferred electronically, using distributed ledger technology or similar technology" (European Commission, 2019, Article 3(1)(2)). The purpose of the MiCAR is to put in place control and monitoring measures for crypto-assets which are not regulated under the existing EU financial legal framework (European Parliament and European Council, 2014). The proposal is expected to be adopted in the next couple of years and to be implemented by Member States no later than 2024.

The MiCAR proposal aims to provide rules on the public offering of crypto-assets, the admission of crypto-assets on a trading platform, the licencing of crypto-asset service providers and the implementation of market abuse rules for crypto-assets businesses (European Commission, 2019, p.2). There are three main categories of token in the proposed MiCAR. These are asset-referenced token, e-money token and other crypto-assets with different requirements for each in relation to licencing and issues. NFTs may fall under the last category, "other crypto-assets". In this last category, issuers of crypto-assets do not have any specific licensing obligations but are required to be a legal entity (even if they are established outside the EU) and to comply with certain business and governance conduct requirements (European Commission, 2019, Article 13).

While this category of "other crypto-assets" will be subject to specific rules on *inter alia* admission to trading on a trading platform, the authorisation of related service providers and market abuse rules, the proposal *exempts* issuers of crypto-assets which are unique and non-fungible from the requirement to publish a white paper for public offerings. Consequently, NFTs providers and traders will be exempted from the obligation to publish such a white paper but they will be subject to anti-money laundering and counter-terrorist financing rules. In the recitals of the MiCAR, special reference is made to "virtual assets" as defined by the Financial Action Task Force (FATF). According to this definition, virtual asset 'is a digital representation of value that can be traded, or transferred, and can be used for payment or investment purposes' (FATF, 2021a). In its latest draft guidance on March 2021, FATF replaced a previous reference to "assets that are fungible" with "assets that are convertible and interchangeable" (FATF, 2021b). This definition from FATF may involve NFTs but this is not clear, yet.

Training for law enforcement agencies

The area of NFTs, as demonstrated, is a fast-evolving field that combines technology and art and which lacks a specific regulatory framework. The record sales of NFTs as well as the expanding creation and sale of them create an emerging need for training for those entities responsible for governance, suspicious transaction reporting and law enforcement in this growing area. LEAs need to be up to date and trained to understand how NFTs work and the risks they pose. The need for training was highlighted in the – long awaited – report of the US Department of Treasure (USDT) entitled "Money Laundering and Terror Finance Through the Trade in Works of Art" in February 2022 (US Department of the Treasure, 2022). The report stresses the need to regulate and control NFTs as an expanding area of digital art. The USDT rings the bell; as the traditional art market has to respect anti-money laundering and terrorist financing rules, the digital art is still in a grey – not adequately – regulated zone (US Department of the Treasure, 2022).

Thus, given the risks, the USDT recommends updating guidance and training for law enforcement agencies,as well as customs and asset recovery agencies. Law enforcement agencies should develop their internal training on money laundering and high-value art (including NFTs) which can include experts in the field of money laundering via the art market in order to "identify the risks and opportunities" available to launderers. The report proposes the creation of a "written toolkit and

specific methodology with strategies for investigating money laundering" in the art sector. While the need for training is apparent, the question of 'what is the most efficient way to organise this training?' remains. The novelty of NFTs and their fast development create a new sector where specialisation and expertise are scarce. Our research revealed that the number of academic training programmes on NFTs is limited and that hardly any LEA has so far received designated training on NFTs.[7]

Firstly, on an academic level, the teaching of art law, NFTs and money laundering is quite limited. Higher education institutions do not offer courses on NFTs and this means that law enforcement agencies may not benefit from these courses if they decide to follow it on an individual basis (Queen Mary – University of London, 2022; Skipp, 2022).[8] Secondly, there are several private organisations such as Christie's and the Blockchain Council which offer courses on NFTs (Christie's Education, 2022). While their courses are designed to provide a good understanding of NFTs, they are not focused on the nexus of NFTs, money laundering and other crime risks and anti-money laundering policies. Finally, there are certain initiatives for training in the crypto world. For example, Crypteya,[9] one of the websites offering NFTs courses, describes itself as "the biggest, meanest and baddest crypto academy in the world", a description which does not really fit with the classic academic approach to professional training and development.

Given the scarcity of relevant courses, an optimal solution for the training of law enforcement agencies will be the cooperation with the private sector by establishing Public Private Partnerships (PPPs) with experts in the field (Courtois, Gradon & Schmeh, 2021). Specialisation on NFTs can be created by combining expertise from academia, industry, and independent actors. Combination of such expertise, albeit very rare, can also be found in multidisciplinary European research project such as TRACE.[10] Law enforcement agencies would benefit from bringing all these actors together who could produce insightful work that will assist law enforcement agencies in rapidly emerging fields. Once the Public Private Partnerships are established, training can be designed and delivered by these stakeholders and lead to continuous building of knowledge exchange for NFTs and other new assets with risks.

If Public Private Partnerships are not an option, the alternative will be the creation of specific NFTs training within the police academies. It is widely known that police academies have their own training programme to educate and prepare their personnel. This training should involve NFTs both from the legal and technological perspectives. The responsible staff should find and hire the most appropriate persons to design this course. Legal scholars, technology experts and other related professionals should come together and train the future generations of police officers. The expertise on digital assets in general should be created within the police academy where possible, which will then allow them to redesign the NFTs course in tandem with their legal and operational eco-systems. As the quality of the training is under pressure and law enforcement agencies may lack personnel, modern equipment and/or facilities, it is imperative to demand better financial resources in order to reorganise and modernise their training (Kleygrewe et al., 2022). NFTs, and the crypto world in general, should have a special place given the global expansion of technology.

The training should include, at first, the genesis of NFTs in the art world. The trading of NFTs did not happen until two years ago when they started expanding but creation of NFTs can be traced back to 2017. Accordingly, the definition and design of NFTs from a technological perspective should be understood critically. Law enforcement agencies should be competent to understand the technological structure of NFTs and their position in the art market. NFTs do not focus on one artistic characteristic such as online images but they extend to other artistic activities such as sports events or music concerts and lyrics. This combination of technology and art should be clearly understood by law enforcement agencies to aid their investigative and forensics work in particular. Furthermore, a business risk analysis of NFTs should be considered; NFTs represent a new "asset" and this excites investors (Kaczynski & Kominers, 2021). It is not common to have a new "asset"

7 At the time of writing this article, several LEAs around Europe (including those present (64 people) in our CEPOL Conference 2022 presentation and the LEA partners in the TRACE Project https://trace-illicit-money-flows.eu) indicated that they have not received any specific training on NFTs.

8 The first one is an LLM about art, business and law where, this year, certain classes are introduced for NFTs. The second is the recent announcement of Miami Law School introduction of its innovative NFTs course.

9 Crypteya Academy. Available from: https://crypteya.academy [Accessed 29th June 2022].

10 For more information about the TRACE project, see: https://trace-illicit-money-flows.eu

in the market and certainly not in such a unique combination of art and technology.

Moreover, the training should extend to the legal aspects of NFTs. The first issue is related to the definition of NFTs from a legal perspective. As analysed above, law enforcement agencies should become aware of the legal uncertainty covering NFTs in the art market and to understand whether anti-money laundering rules apply to them. Are they art work, commodities, collectibles or virtual assets? This is a crucial point which will determine which legal rules are applied in terms of business practices, taxation, anti-money laundering reporting obligations and law enforcement. More specifically, law enforcement agencies should prepare lists of the different operators which trade in NFTs. These operators should be monitored and law enforcement agencies should present guidelines to investors and businesses on how to handle diligently their financial relations with traders of NFTs. In addition, specific guidelines should be developed for art dealers. These guidelines should be prepared once the training of law enforcement agencies is complete.

For all the different steps of this training, law enforcement agencies should collaborate with experts who will be able to explain and analyse the new phenomenon of NFTs. Academia, technology experts, businesses, industry, the art dealers and many others should become allies of the law enforcement agencies for better and efficient training activities.

Recommendations

Anonymity and volatility coupled with a lack of regulatory rules are all traits of NFTs which make them attractive to money launderers (Congressional Research Service, 2019).[11] A first solution to the challenges posed by NFTs is legal and regulatory certainty. Regulators should step in and provide answers to issues such as the definition of an NFT and the anti-money laundering rules that should be applicable to those trading in NFTs. As the market of NFTs expands, a pressing need is to define NFTs. As analysed above, by providing a clear definition, NFTs can be put under an existing category (e.g. other virtual assets under MiCAR) and be regulated by these legal provisions. Alternatively, if NFTs are considered to be works of art, then anti-money laundering rules, under EU law and its Fifth Anti-Money Laundering Directive, would apply.

Legal uncertainty surrounding NFTs create challenges not only for law enforcement agencies (i.e. police, tax authorities, FIUs, etc.) and regulators but also affect the legitimate traders of NFTs who respect, despite the absence of specific regulation, anti-money laundering rules. By regulating NFTs, legal clarity and consistency would be provided to legitimate traders of NFTs and to NFTs holders which in turn could boost the functioning of this new asset and optimise its benefits for the society (Congressional Research Service, 2019). The interest in legal certainty should be a driving force for regulators to enact legislation and clear the grey legal area where NFTs are positioned at the moment.

A legislative framework governing NFTs can be achieved not only by focusing on EU's *acquis communautaire* but also via national laws of Member States which can instigate model rules for others to emulate. Given the cross-border trading of NFTs with ease, the EU's legislative branches should at least conduct comparative research and refine and harmonise the best legal solutions that can be adopted at the EU level. As the EU does not have exclusive competence over money laundering and new technologies, Member States have a significant responsibility to develop their laws on these issues. Apart from the Member States, inspiration can be found to other legal systems such as the UK, the US or Japan where NFTs are widely traded. It should be borne in mind that the US and the UK are two countries where their respective governments have announced plans to reform crypto asset regulations in order to attract investments (HM Treasury, 2022; The White House, 2022). In tandem with the laws of these strategic partners, the EU can design and propose legislation on crypto assets and, most specifically, NFTs.

Whilst a new EU legislation may take several years to draft and come in to force, regulators and law enforcement agencies can take a proactive role by issuing guidelines as a soft law instrument. In the banking and financial sector, soft law instruments, such as the 40+ Recommendations of FATF, OECD's Ten Global Principles[12] or the Basel II Committee rules, have had consid-

11 The same characteristics make crypto currencies attractive to criminals.

12 OECD. Ten Global Principles. Available from: https://www.oecd.org/tax/crime/fighting-tax-crime-the-ten-global-principles-first-edition-63530cd2-en.htm [Accessed 29th June 2022].

erable success (Turner, 2015). Consequently, guidelines should be issued for NFTs in which more information on how to handle suspicious NFTs transactions and on how to apply anti-money laundering rules and policies are articulated. Filing of suspicious transaction reports (STRs) will be a significant aid for law enforcement agencies and if the crypto market starts submitting STRs, it will be a clear sign of their willingness to safeguard the crypto market against criminal activities. These STRs can inform the law enforcement agencies about the risk factor/s surrounding a particular NFTs transaction, and can include the usual know your customer information as well as the IP address and the value of the transaction. Legitimate traders of NFTs will, probably, follow the recommendation of filing STRs in order to be compliant with the issued guidelines and to avoid potential sanctions for non-compliance.

Furthermore, specific guidance in these guidelines should be given to compliance departments on how to address issues with NFTs and money laundering. Compliance professionals (e.g. money laundering reporting officers and auditors) will most likely follow these – non-compulsory – guidelines in an effort to keep their businesses "clean". At the same time, FIUs and law enforcement agencies will benefit from this as more information on NFTs will be available to them in order to investigate suspicions of money laundering. Such guidelines should be carefully drafted in sincere consultation with key stakeholders including art dealers and auction houses, cybersecurity professionals, blockchain specialists and crypto currencies experts. Finally, a registry for stolen or fraudulently purchased NFTs similar to existing databases maintained by Interpol, FBI and the Art Loss Register should be instigated urgently (Interpol, n.d.; FBI, n.d.; The International Art and Antique Loss Register, n.d.). Such a register will aid law enforcement agencies to monitor the NFTs market and pursue not only money laundering but also various predicate crimes such fraud, forgery and theft.

Finally, apart from the legal and regulatory changes needed in this field, it is necessary for law enforcement agencies to enhance their training on NFTs. As discussed above, law enforcement agencies should consider their training needs and design courses on NFTs. We have proposed in this article several ways to achieve these training needs. Law enforcement agencies should be proactive and ready to tackle this phenomenon. In this regard, law enforcement agencies should carefully design specific training on NFTs by combining legal and technology expertise from the inside (police academies) and from the outside (universities and/or private companies). The accomplishment of a good training will allow law enforcement agencies to better investigate and prosecute illegalities on NFTs.

References

- Akdemir, N., Lawless, C. J. & Turksen, U. (2021) Cybercrime in Action. Nobel Academic Publishing.
- Ante, L. (2021) Non-fungible token (NFT) markets on the Ethereum blockchain: Temporal development, cointegration and interrelations. Blockchain Research Lab Working Paper Series, 22, 1.
- Artnet News. (2022) Wikipedia Editors Have Voted Not to Classify NFTs as Art, Sparking Outrage in the Crypto Community. Available from: https://news.artnet.com/market/wikipedia-editors-nft-art-classification-2060018?utm_content=from_www.artnet.com&utm_source=Sailthru&utm_medium=email&utm_campaign=EU%20Jan%2014%20AM&utm_term=EUR%20Daily%20Newsletter%20%5BMORNING%5D [Accessed 29th June 2022]
- Bluemel, J. (2022) NFTs – the new art of Money Laundering. IDnow. Available from: https://www.idnow.io/blog/nft-non-fungible-tokens-new-art-money-laundering/ [Accessed 29th June 2022]
- Burroughs, T. E. (2019) US and EU Efforts to Combat International Money Laundering in the Art Market are no Masterpiece. *Vanderbilt Journal of Transnational Law* 52(4), 1061-1062.
- Carron, L. (2021) ABCs of NFTs, Art and Law. *NYSBA Entertainment, Arts and Sports Law Journal*, 32(2), 13.
- Chainalysis (2022) The 2022 Crypto Crime Report.
- Christies (2021) 10 things to know about CryptoPunks, the original NFTs. Available from: https://www.christies.com/features/10-things-to-know-about-CryptoPunks-11569-1.aspx [Accessed 29th June 2022]
- Christie's Education (2022) Virtual Course Understanding Crypto Art and NFTs. Available from: https://education.christies.com/courses/continuing-education/short-courses/understanding-crypto-art-nfts [Accessed 29th June 2022]

- Congressional Research Service. (2019) Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals.
  Available from: https://sgp.fas.org/crs/misc/R45664.pdf [Accessed 29th June 2022]
- Courtois, N.T., Gradon, K. T. & Schmeh, K. (2021) Crypto Currency Regulation and Law Enforcement Perspectives. Section 11.1.
  Available from: https://arxiv.org/abs/2109.01047 [Accessed 29th June 2022]
- Dannen, C. (ed.) (2017) Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. Berkeley, Apress.
- Dowling, M. (2021) Fertile LAND: Pricing non-fungible tokens. Finance Research Letters, 44, January.
- European Commission (2019) Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final.
- European Parliament and European Council (2018) Directive 2018/843 of 30 May 2018 amending Directive 2015/849/EU on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.
- Europol (2022) Illicit Trafficking in Cultural Goods, Including Antiquities and Works of Art.
  Available from: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/illicit-trafficking-in-cultural-goods-including-antiquities-and-works-of-art [Accessed 29th June 2022].
- FBI (n.d.) National Stolen Art File.
  Available from: https://www.fbi.gov/investigate/violent-crime/art-theft/national-stolen-art-file [Accessed 29th June 2022]
- Financial Action Task Force (2021a) Virtual Asset.
  Available from: https://www.fatf-gafi.org/glossary/u-z/ [Accessed 29th June 2022]
- Financial Action Task Force (2021b) Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers.
  Available from: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html [Accessed 29th June 2022]
- Gould, E. (2022) Can an NFT be art? And why it matters…. Institute of Art & Law.
  Available from: https://ial.uk.com/can-an-nft-be-art-and-why-it-matters/ [Accessed 29th June 2022]
- HM Treasury (2022) Government sets out plan to make UK a global cryptoasset technology hub.
  Available from: https://www.gov.uk/government/news/government-sets-out-plan-to-make-uk-a-global-cryptoasset-technology-hub [Accessed 29th June 2022]
- Hufnagel, S. & King, C. (2019) Anti-money laundering regulation and the art market. *Legal Studies,* 40 (1), 131-150.
- International Monetary Fund. (2019). The Art of Money Laundering. *Finance & Development*, 56(3), 30-33.
- INTERPOL (n.d.) Stolen Works of Art Database.
  Available from: https://www.interpol.int/Crimes/Cultural-heritage-crime/Stolen-Works-of-Art-Database [Accessed 29th June 2022]
- The International Art and Antique Loss Register (n.d.) The Art Loss Register.
  Available from: https://www.artloss.com [Accessed 29th June 2022]
- Jordanoska, A. (2021) The exciting world of NFTs: a consideration of regulatory and financial crime risks. *Butterworths Journal of International Banking and Financial Law*, (10) 716.
- Kaczynski, S. & Kominers, S.D. (2021) How NFTs Create Value. Harvard Business Review.
  Available from: https://hbr.org/2021/11/how-nfts-create-value *[Accessed 29th June 2022]*
- Kleygrewe, L., Oudejans, R.D., Koedijk, M. & Hutter, R.I. (2022) Police Training in Practice: Organization and Delivery According to European Law Enforcement Agencies. Frontiers in Psychology.
  Available from: https://www.frontiersin.org/articles/10.3389/fpsyg.2021.798067/full [Accessed 29th June 2022].
- Purkey, H. (2010) The Art of Money Laundering. *Florida Journal of International Law, 22*, 111-118.
- Reyburn, S. (2021) JPG File Sells for $69 Million, as 'NFT Mania' Gather Pace. The New York Times.
  Available from: https://www.nytimes.com/2021/03/11/arts/design/nft-auction-christies-beeple.html [Accessed 29th June 2022]
- Queen Mary – University of London. (2022) Art, Business and Law LLM.
  Available from: https://www.qmul.ac.uk/postgraduate/taught/coursefinder/courses/art-business-and-law-llm/ [Accessed 29th June 2022]
- Skipp, C. (n.d.) Available from: https://www.law.miami.edu/news/2022/january/innovation-and-tech-miami-law-first-law-school-us-nfts-course [Accessed 29th June (2022) Innovation and Tech at Miami Law – First Law School in U.S. with NFTs Course. Miami School of Law. 2022].

- The White House (2022) President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets. Available from: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/ [Accessed 29th June 2022]
- Transparency International UK (2015) 'Don't look, won't find – Weaknesses in the Supervision of the UK's Anti-Money Laundering Rules'. Available from: https://www.transparency.org.uk/sites/default/files/pdf/publications/TI_UK_Dont_Look_Wont_Find.pdf [Accessed 29th June 2022]
- Turner, N.W. (2015) The Financial Action Task Force: International Regulatory Convergence Through Soft Law. New York Law School, 59(3), 547.
- US Department of the Treasure (2022) Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art. Available from: https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf [Accessed 29th June 2022]

Borders, Identity & Interoperability

Technology Foresight on Biometrics for the Future of Travel

Luigi Raffaele
Darek Saunders
Magda Wojcikowska
Dragos Voicu
Claudiu Chiriac
Javier Quesada

Research and Innovation Unit,
Frontex – European Border and Coast Guard Agency[1]

Abstract

In 2021, Frontex conducted a Technology Foresight on Biometrics for the Future of Travel, with the objective of studying the future of biometrics for its implementation in border check systems that may benefit the work of the European Border and Coast Guard community in the short-, medium- and long-term perspectives. Three experts' consultation events (two Technology Foresight Workshops and a Delphi survey) took place during the project. A broad group of relevant stakeholders was involved in these events to exploit collective intelligence and stimulate consensus-oriented discussions. A custom Technology Foresight methodology was developed, opening the door to the exploration of the vast field of biometric technologies, which were analysed from various perspectives in the context of border checks. Each of the phases of this complex research study produced its own set of insights. Due to the substantial amount of information provided and the adopted participatory foresight approach, this study will directly contribute to an enhanced understanding of the relevance and applicability of novel biometrics and technology foresight, as well as to identify areas of strategic interest and to make informed decisions about paths of future developments in biometrics. In this article we summarise the main results of the research study (see Frontex, 2022).

Keywords: Research and Innovation, Technology Foresight, Future Scenarios, Biometrics, Border Security, Border Control, Border Checks, Patentometrics, Bibliometrics, Technological Roadmaps, Capability Mapping

1 About Frontex: Frontex, the European Border and Coast Guard Agency, promotes, coordinates and develops European border management in line with the EU fundamental rights charter and the concept of Integrated Border Management. The Agency also plays a key role in analysing and defining the capability needs in border control and in supporting the Member States in the development of these capacities. Furthermore, it provides qualified expertise to support the EU policy development process in the area of border control. Frontex Research and Innovation is responsible for leading and conducting transformational, need-driven research with academia, EU institutions and Agencies, international organisations and industries to stimulate and support innovation. The ultimate goal is to consistently enhance the capabilities of the European Border and Coast Guard in line with the Capabilities Development Plan, which includes those of the Member States and of the Agency itself.

Introduction

Millions of travellers cross the EU's external borders every year and their numbers will likely increase even further. Thus, border checks will need to undergo significant transformations, both to safeguard the EU's external borders and to improve the border crossing experience for travellers, e.g. by enabling seamless or near-seamless travel. Innovative technological solutions will play an essential role in the transformation of border checks; biometrics is one of the fields expected to enhance the security of border checks while at the same time facilitating seamless travel. However, additional research is required to identify the most useful and relevant biometric technologies as well as to find a path of actions that leads to the attainment of these goals. Since Frontex proactively monitors and contributes to research and innovation initiatives relevant to European integrated border management, including those for the adoption of advanced border control technologies, this *Technology Foresight on Biometrics for the Future of Travel* was conducted to gain additional insights into the potential of biometric technologies that could serve as a foundation for future-oriented decision-making.

Biometric technologies were identified, and their possible future evolution paths studied, using *Technology Foresight,* a method that provides anticipatory intelligence which can successfully support evidence-based decision-making, strategy development and capacity building in both public and private organisations. In short, Technology Foresight is an approach that delivers strategic insights by analysing possible future technological development paths. However, there is no single recipe for conducting a foresight exercise: each study needs to be tailored to the specific context, requirements and fields of interest, as well as to the assets and data sources available. The benefits of foresight analyses are numerous and include identifying threats and opportunities, stress-testing long-term strategies, uncovering vulnerable assumptions regarding the future and detecting potentially disruptive technologies and events.

Therefore, a tailor-made foresight process was developed for the purposes of the *Technology Foresight on Biometrics for the Future of Travel* to provide Frontex with general insights into the development and implementation of foresight exercises.

Motivation and goals

The primary goal of this research was to provide technology-related insights on the future of biometrics for its implementation in border check systems that could be utilised by the European Border and Coast Guard (EBCG) community in the short- (2022-2027), medium- (2028-2033) and long-term (2034-2040) perspectives. Secondly, Frontex wished to raise awareness about the relevance and applicability of foresight for forward-looking decision-making within its organisation and to acquire the related know-how. Finally, the study provided a comprehensive foresight methodology, tailor-made to Frontex's needs and outlined the implementation of this methodology using quantitative, qualitative and participatory approaches to identify biometric technologies of high relevance to future applications in border checks.

A good definition of the scope of the research was essential. The study was limited to biometric technologies and biometrics-enabled technological systems that could find applications in border checks, biometric recognition and access control. Additional constraints were imposed by disregarding the applications of biometrics in border surveillance as well as emotion and behaviour detection.

The outcomes of the exercise will provide Frontex with the practical knowledge required for further Technology Foresight (TF) studies in other technological fields and research areas. They will also supply in-depth information to underpin future strategic decisions on the application of biometric technologies in the context of border checks, e.g. with regard to future priorities, research directions and investment decisions.

More specifically, the following objectives were defined for the study in the context of border checks:

On a global scale:

- Identification of the current implementation status and future development pathways of biometric technologies by 2040;
- Identification of biometric technology accelerators, including the main actors and key Research and Development (R&D) initiatives.

On a European Union (EU) scale:

- Identification of future opportunities in terms of biometric technologies that could support EU external border management, e.g. facilitating seamless travel;
- Identification of biometrics-enabled technological solutions to future operational problems within the EBCG community;
- Analysis of legal, ethical and technological limitations intended to minimise the risks associated with applications of biometric technologies;
- Assessment of the impact of biometric technology trends on border checks and identification of future research needs.

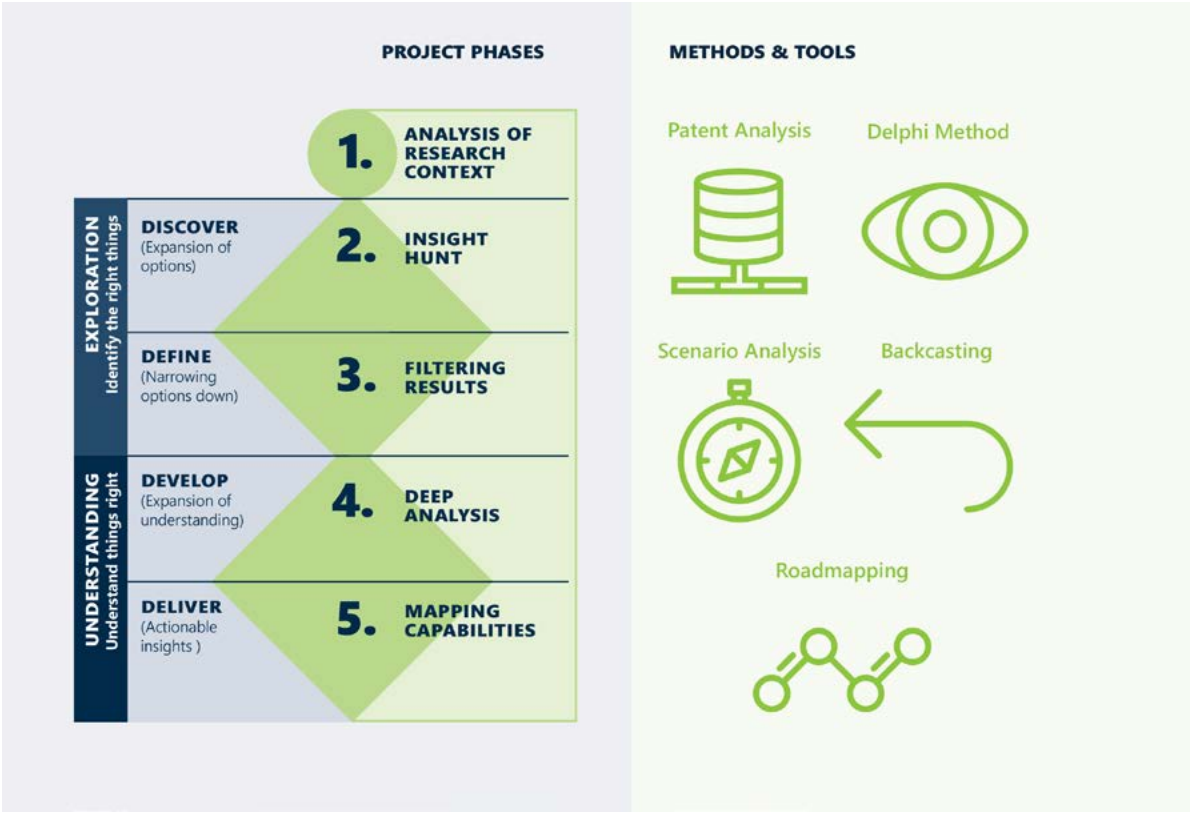
Within the EBCG community:

- Providing know-how on the implementation of TF projects;
- Raising awareness about the relevance and applicability of TF for forward-looking and evidence-based decision-making;
- Disseminating the results of this research study to encourage joint initiatives, the development of a shared vision and strengthened capability development.

Structure of the study

This research study was structured in five phases, as shown in Figure 1. The first phase defined the overall methodology and framed the context according to Frontex's needs. The subsequent phases were dedicated to putting this methodological framework into practice. They can be depicted as two diamonds: each begins by opening up the horizon and broadening the knowledge, eventually narrowing down the obtained insights and thus, identifying the targeted outcomes. Figure 1 also provides a selection of the methods used throughout the project.

Figure 1. Overview of the project set-up, as well as of the main methods used within the project



Phase 1 – Analysis of the Research Context

The identification of Frontex's needs regarding key functions and characteristics of biometric technologies and related systems was the first step of the Technology Foresight process (TFP). It aimed to specify the field and scope of the TFP and to set goals for the study, which in turn were used to tailor the TFP to Frontex-specific needs. The results of this step constituted the first filter for narrowing the area of further analysis to the technologies and technological systems of the greatest potential importance to Frontex.

As a result of the needs analysis, four "must-haves" were identified for reference in later phases of the project:

- low vulnerability to adversary attacks,
- seamlessness,
- applicability within pandemic-specific restrictions,
- compliance with fundamental EU values and regulations.

Phase 2 – Insight Hunt

Identification of main areas of research in biometrics and of key stakeholders

This study spans the operational fields of interest of the EBCG community in relation to border checks. To navigate the vast field of biometrics, 43 preliminary directions of analysis were defined. They included biometric technologies as well as biometrics-enabling technologies and applications.

Gaining further insights into stakeholders was another essential part of this phase, as the active involvement of stakeholders was a prerequisite for the study. This facilitated the dissemination and communication of project results within the EBCG community throughout the project, as well as ensuring that valuable insights from diverse fields of expertise were collected and could serve as the core input to the analyses. In total, over 200 stakeholders were initially identified, with more than 40 selected to participate in the study by way of three participatory activities: two *Technology Foresight Workshops* and a *Delphi Survey*.

Taxonomy of biometric technologies and biometrics-enabled technological systems

The field of biometrics is highly heterogeneous and complex. Thus, a systematic categorisation was needed to identify the technologies and systems with potential for finding applications in the operational fields associated with border checks. This step aimed to enhance the comprehension of how the area of research in biometrics is structured and how the technologies relate to one another. For this purpose, two taxonomies were developed to map *biometric technologies and biometrics-enabled technological systems*.

Two distinct design approaches, differing in thoroughness and complexity, were followed to construct the taxonomies. The taxonomy of biometric technologies, which used the preliminarily identified main areas of research for initial guidance, was developed through an iterative process based on an analysis of patents and scientific literature with the employment of Natural Language Processing (NLP) automatic tools. This approach led to the creation of the three-level taxonomy shown in Figure 2.

A set of technological systems of potential interest to Frontex served as the initial input for creating the taxonomy of biometrics-enabled technological systems. The set was later expanded and consolidated to construct the two-level taxonomy shown in Figure 3.

Together, the two taxonomies constituted an essential building block for the study:

- The taxonomy of biometric technologies was used to extract a set of *technological clusters* (TCs, shown in Table 1) required for the subsequent phases of the project.

- The taxonomy of biometrics-enabled technological systems played an essential role in guiding the development of technological roadmaps in Phase 4.

Figure 2. Taxonomy of biometric technologies

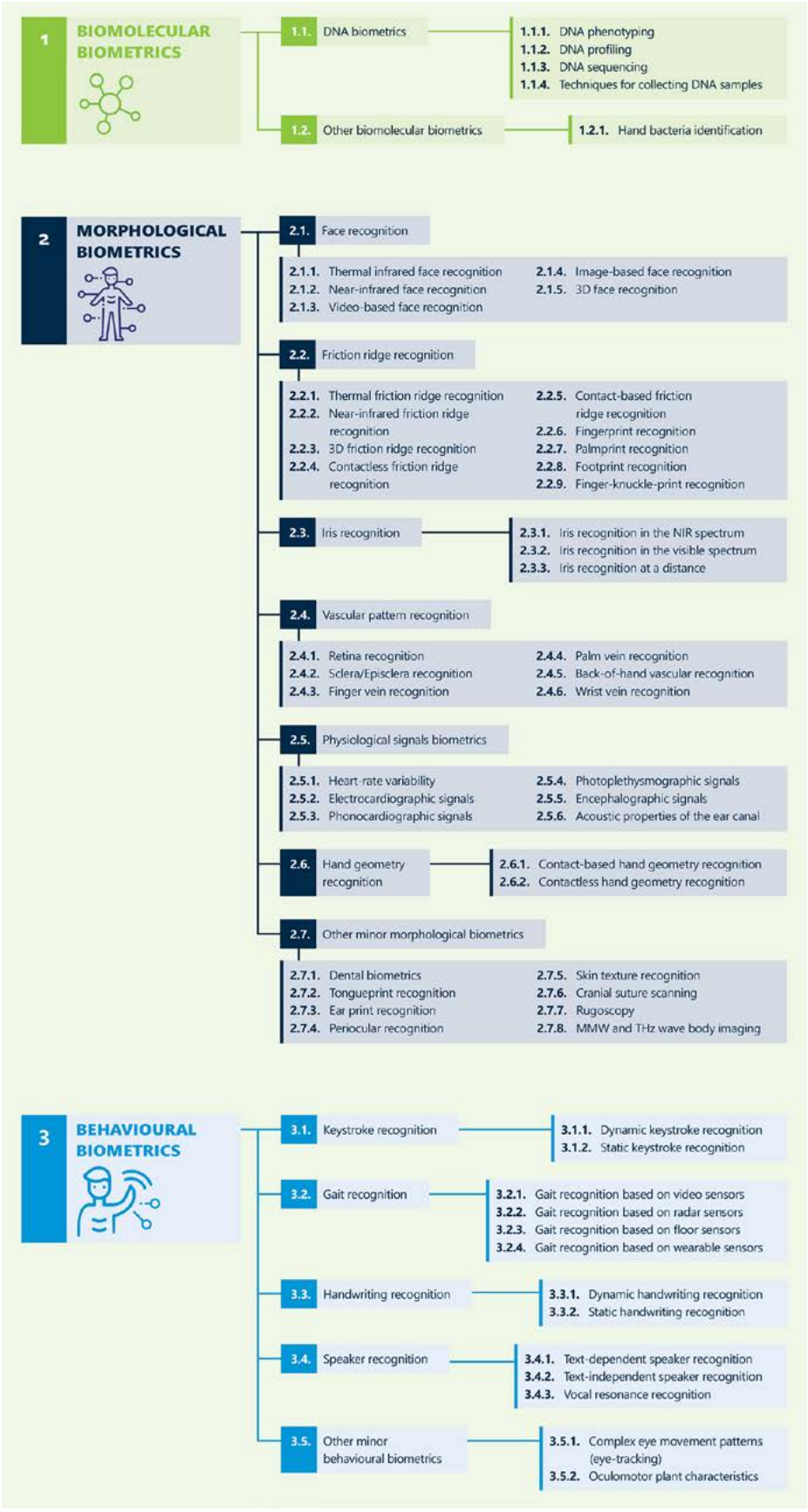
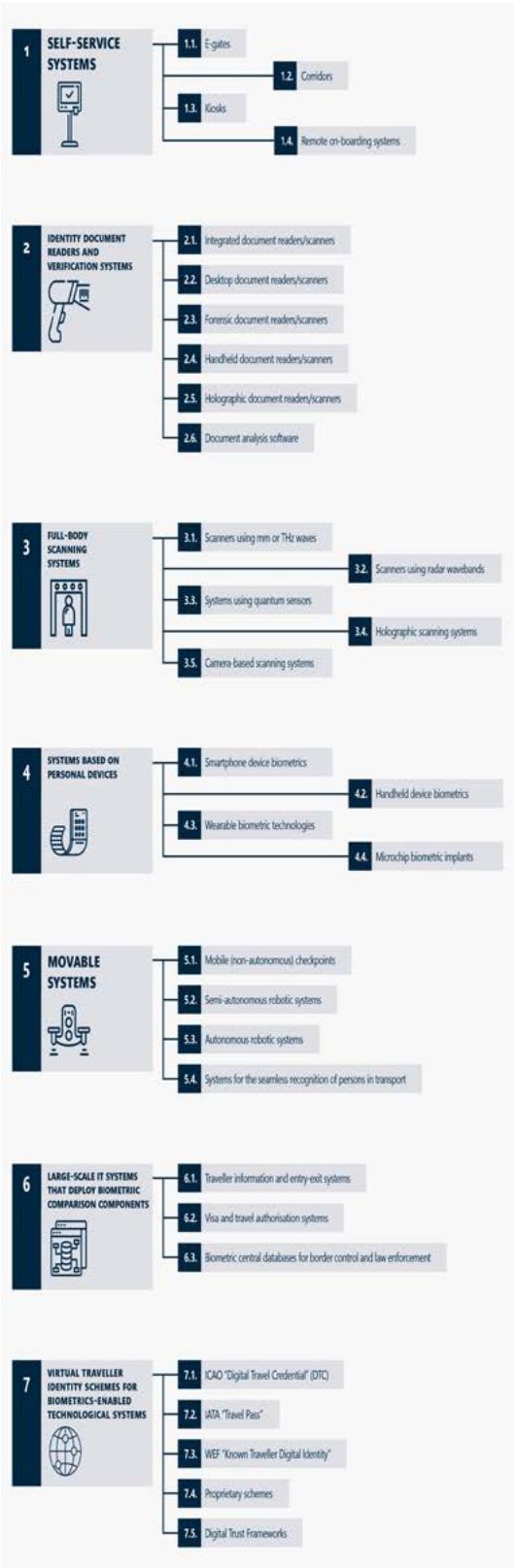


Figure 3. Taxonomy of biometrics-enabled technological systems



Patentometric and bibliometric analyses of biometric technologies

Patentometric and bibliometric analyses were conducted to identify and analyse patents and scientific literature related to the 20 TCs outlined above, and to obtain insights into global R&D activities in the identified biometric TCs.

EU-funded research and innovation projects on topics revolving around the TCs were also analysed to outline the priorities of the European research, technology development and innovation (RTDI) community within the biometrics domain. This analysis supplemented the picture of the technological landscape of biometrics by providing an overview of the EU's investments in R&D projects and by indicating where the highest levels of knowledge and expertise may be found within Europe.

Through the patentometric and bibliometric analyses, the clusters' technological lifecycles were analysed following Altshuller's Theory of Inventive Problem Solving (see Altshuller & Williams, 1984; Slocum, 1998; Mann, 1999), according to which a technology's evolution over time follows distinctive patterns that can be assessed by observing the trend in the number of inventions. Such an assessment helped identify the current stage of a technology's lifecycle and provided a basis for projections of its future evolution. As a result of the analysis, the TCs were categorised as follows:

- Childhood stage: 2 TCs (Periocular recognition and Gait recognition);
- Growth stage: 5 TCs (Infrared friction ridge recognition, 3D friction ridge recognition, Iris recognition in the visible spectrum, Iris recognition at a distance and Heart signal recognition);
- Maturity stage: 10 TCs (Infrared face recognition, 2D face recognition in the visible spectrum, 3D face recognition, Contactless friction ridge recognition, Contact-based friction ridge recognition, Iris recognition in the NIR spectrum, Eye vein recognition, Hand vein recognition, Handwriting recognition and Speaker recognition);
- Maturity stage (but of minor relevance):[2] 3 TCs (DNA biometrics, Hand geometry recognition and Keystroke recognition).

2 The temporal distributions of patenting and publishing activities regarding these clusters showed poor similarity with the theoretical pattern proposed by the Theory of Inventive Problem-Solving. These clusters are likely to be characterised by low efficiency in biometric recognition processes. The long-time and low volumes of inventive activities suggest that no growth is foreseen.

The patenting activity related to the TCs appears to be located primarily in the United States. Europe and China alternate as the second most common location. This indicates that R&D, commercial and manufacturing activities are performed on a large scale in these three regions. Germany and the United Kingdom represent the dominant European regions for patenting activity.

The bibliometric analysis further revealed that the Institute of Electrical and Electronics Engineers (IEEE) dominates the editorial activity that concerns the biometric field. It is the most prolific publisher for 19 out of the 20 TCs, making it a key source for monitoring developments in biometrics.

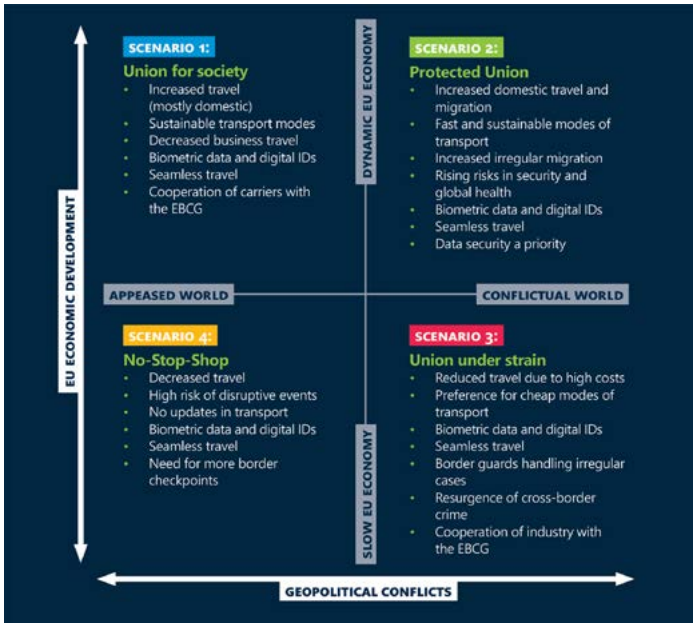
The analysis of EU-funded projects showed that five technological fields (*Face recognition, Friction ridge recognition, Vascular pattern recognition, Periocular recognition* and *Speaker recognition*) are of particular interest for co-funded industrial and academic research in the EU; F*ace recognition* and *Friction ridge recognition* seem to be dominating. Contrastingly, *Heart signal recognition* and *Handwriting recognition* are presumably of minor relevance to the EU.

The results also indicated that British, German, Spanish and French organisations are likely to possess the highest levels of knowledge and capability required to implement these technologies, as they participated in the largest number of EU-funded projects related to the considered TCs.

Scenarios for the future of travel, border checks and biometric technologies in 2040

Parallel to the patentometric and bibliometric analyses, we conducted scenario development. *Scenario Analysis* is one of the most widely used methods in strategic foresight. Its primary focus is on assessing how various futures might influence the subject of the analysis. The method involves stress-testing strategies, insights and solutions to verify the extent to which they can be considered "future-proof". The scenarios developed in the framework of this project were based on those presented in *The Future of Customs in the EU 2040: A foresight project for EU policy* (Ghiran et al., 2020).[3] During the first experts' consultation workshop, they were challenged and adapted to incorporate aspects relevant to the travel and border check context. An overview of the adapted scenarios in a 2x2 matrix is presented in Figure 4.

Figure 4. An overview of scenarios on the future of travel, border checks and biometric technologies used in this study – 2x2 scenario matrix



3 This study was published in 2020 by the European Commission's Joint Research Centre (JRC) and conducted in collaboration with the Directorate-General for Taxation and Customs Union (DG TAXUD). The scenarios were constructed using a 2x2 Matrix technique, wherein 2 important factors were selected and placed on 2 axes, thus forming 4 quadrants. The chosen factors were geopolitical conflicts (with a peaceful world at one end of the spectrum and a world in conflict on the other) and EU economic development (slow vs dynamic EU economy).

Table 1. Description of the examined biometric technological clusters

Technological clusters	Description
DNA biometrics 	Biometric technologies that rely on the recognition of human DNA. These technologies find easier applications in forensic science, however, applications in biometric recognition have also been proposed. Although these systems are still unsuitable for applications in border checks, advances are being made to expedite the analysis process. This technological cluster includes DNA phenotyping, DNA profiling and DNA sequencing.
Infrared face recognition 	Technologies for the recognition of human faces using infrared (IR) imaging, commonly subdivided into: near-infrared (NIR, 0.78-1.0 μm in wavelength) imaging; short-wavelength infrared (SWIR, 1-3 μm) imaging; mid-wavelength infrared (MWIR, 3-8 μm) imaging; long-wavelength infrared (LWIR, 8-15 μm) imaging. NIR and SWIR are sometimes called "reflected infrared", while passive MWIR and LWIR techniques are sometimes referred to as "thermal infrared". This cluster is formed by two biometric technologies: thermal infrared face recognition and near-infrared face recognition.
2D face recognition in the visible spectrum 	This technological cluster deals with the automated recognition of individuals through the matching of a face — from a digital image or a video frame acquired in the visible spectrum of light — against a database of face images or a specified biometric reference image. It encompasses video-based face recognition and image-based face recognition.
3D face recognition 	Solutions aimed at recognising an individual by the three-dimensional (3D) features of their facial components. Once the 3D geometry of the human face is acquired, it is used to extract distinctive features on its surfaces. 3D face recognition is claimed to have the potential to achieve better accuracy than its 2D counterpart.
Infrared friction ridge recognition 	The skin on the palms of hands, fingers, soles and toes is known as *friction ridge skin* in the biometric and forensic communities. This technological cluster includes biometric recognition modalities (such as *Fingerprint recognition*, *Palmprint recognition*, *Footprint recognition* and *Finger-knuckle-print recognition*) implemented through thermal imaging or near-infrared imaging of friction ridge skin.
3D friction ridge recognition 	Biometric modalities capable of acquiring the frictional ridges of one or multiple body parts (e.g. fingers, palms, feet or finger-knuckles) and producing three-dimensional representations in order to recognise an individual. For example, extracted features from 3D palmprint data usually include depth and curvature of the palm lines and wrinkles on the palm surface.
Contactless friction ridge recognition 	Biometric technologies in which the friction ridge mark signature of a finger, palm, foot or finger-knuckle is acquired without direct contact of the relevant body part with a sensing surface, mostly employing video or image acquisition.
Contact-based friction ridge recognition 	Biometric technologies in which the friction ridge mark signature of a finger, palm, foot or finger-knuckle is acquired through the contact of the relevant body part with an acquiring surface. For example, contact-based palmprint capture may be performed by asking users to put their hands on a planar surface where their fingers are typically restricted by pegs.
Iris recognition in the NIR spectrum 	The iris is a thin, circular structure in the eye that controls the diameter and size of the pupils. Its back surface is covered by a layer of pigmented epithelial tissue, which gives an eye its distinctive colour. *Iris recognition in the NIR spectrum* is the field of biometrics that deals with the recognition of individuals through images of the textural features of the iris captured using near-infrared illumination.
Iris recognition in the visible spectrum 	This cluster includes iris recognition technologies based on images of the iris captured in the visible spectrum of light. This presents many challenging aspects, especially in the case of individuals with dark irises (caused by higher melanin pigmentation and collagen fibrils) because the unique pattern of the iris is not clearly observable under visible light.

Technological clusters	Description
Iris recognition at a distance 	*Iris recognition at a distance* (metres away from the subject) might be implemented even for a person walking, thus enhancing travellers' experience at border checks by reducing the need for user cooperation and achieving low intrusiveness, high acceptance and transparency.
Eye vein recognition 	In general, vein (or vascular) pattern recognition uses a light source (usually near-infrared light) to acquire images of blood vessels. In the case of *Eye vein recognition*, scanners typically use low-energy lasers and users are typically asked to put their eyes in front of the scanner, as eyes must be very close to the sensors for the vein patterns to be acquired. This cluster encompasses retina recognition and sclera/episclera recognition technologies.
Hand vein recognition 	Recognition of individuals through images of the complex structure of larger blood vessels near the skin surface in human hands. These may be captured from hand surfaces as well as from fingers and wrist, using non-invasive and safe imaging techniques. This technological cluster includes finger, palm, back-of-hand and wrist vein recognition.
Heart signal recognition 	Heart signals belong to the wider group of physiological characteristics of an individual, i.e. signals that can be acquired and monitored to assess a person's clinical state. This technological cluster includes biometric recognition technologies based on the detection and acquisition of heart-rate variability (HRV), electrocardiographic (ECG) signals, phonocardiographic (PCG) signals and photoplethysmographic (PPG) signals.
Hand geometry recognition 	Hand geometry readers take measurements of an individual's hand — including height, width, deviation and angle — and compare those measurements to a reference sample. This cluster is formed by two biometric technologies: contact-based hand geometry recognition and contactless hand geometry recognition.
Periocular recognition 	The region around the eye, including the *sclera, eyelids, lashes, brows and skin*, is known as the *periocular region* and can be acquired non-intrusively and used as a biometric characteristic. *Periocular recognition* offers advantages over face recognition as it is least affected by expression variations, ageing effects and facial hair.
Keystroke recognition 	Keystroke dynamics is a behavioural biometric characteristic that describes the unique timing pattern used by a person to type on the keyboard of a digital device, derived mainly from the two events that make up a keystroke: Key-Down and Key-Up. *Keystroke recognition* utilises off-the-shelf computer keyboards or virtual keyboards. This technological cluster includes static keystroke recognition and dynamic keystroke recognition.
Gait recognition 	Gait is a behavioural biometric characteristic used to recognise individuals by their walking style and pace. Gait has several advantages compared to other biometric characteristics: in most modalities, *Gait recognition* is non-intrusive, does not require cooperation from the individual and can function at moderate distances from the subject. This technological cluster is formed by *Gait recognition* technologies based on video sensors, radar sensors, floor sensors and wearable sensors.
Handwriting recognition 	*Handwriting recognition* is the process of recognising the author of a text from their handwriting style; it can be applied to a generic text or to a specific predefined text (usually a signature) and implemented according to two main modalities: dynamic and static.
Speaker recognition 	Group of biometric technologies that use information extracted from a person's speech to perform biometric operations such as speaker identification and verification. It is based on the extraction of acoustic features of speech that differentiate individuals. This technological cluster includes text-dependent and text-independent recognition.

Clusters found especially vulnerable to future scenarios include *Handwriting recognition, Keystroke recognition, Eye vein recognition, Heart signal recognition, DNA biometrics* and *Hand geometry recognition,* primarily because of the challenges associated with the seamless acquisition of biometric data using these technologies. The analysis of technological clusters' compatibility with scenarios serves as a warning, especially in the case of clusters that received low compatibility ratings in some or all the analysed future realities. Futureproofing some of these clusters may be impossible due to fundamental incompatibilities with specific scenarios. This does not mean that they cannot be pursued, but such cases require a more detailed risk assessment and, preferably, also the introduction of a Strategic Early Warning System (SEWS) to indicate the emergence of unfavourable scenarios.

Phase 3 – Filtering the Results

Security aspects of biometric technologies

The security analysis helped filter the 20 biometric TCs, focusing on their comparative inherent vulnerability to adversary attacks. Only attacks at user-level (presentation attacks) and morphing attacks (in the case of face recognition) were considered. The lowest level of vulnerability was assigned to *DNA biometrics,* which is, at least at the current level of technological development, far from seamless and highly intrusive. On the other hand, it is highly secure. *DNA biometrics* is closely followed by *Infrared face recognition* and *Eye vein recognition,* which display relatively low vulnerability to adversary attacks. At the other end of the scale is *2D face recognition in the visible spectrum,* which is intrinsically highly vulnerable to presentation attacks (such as artefacts and make-up) and morphing attacks, but has a remarkably high level of social acceptance and – contrary to DNA biometrics – a simple acquisition process. The outcomes of the security analysis were used as an additional filter in the subsequent prioritisation of biometric technologies.

Prioritisation of biometric technologies – Findings of the Delphi Survey

Before proceeding with an in-depth analysis of future technological developments, the initial list of 20 technological clusters needed to be narrowed to a shortlist of the most promising ones. The tool selected for this filtering phase of the project was the so-called *4CF Matrix*. To prepare a 4CF Matrix, hypothetical future technological solutions for border checks that would use each of the 20 TCs needed to be quantitatively evaluated in terms of two criteria:

- *Relative Advantage (RA)*: is the advantage that the envisaged technological solution would have over the best available contemporary solutions. RA is rated on a scale of 0-10, where:
    - 0 means that the envisaged solution would not provide any significant advantage over currently available best-in-class solutions or would be impossible to achieve;
    - 10 indicates a game-changer, i.e., a solution that would drastically improve travellers' border check experience.
- *Earliest Time to Mainstream (ETM)*: is the shortest time (from the present moment) required for the solution to become available on the market and widely adopted in border checks at external EU borders. In other words, ETM represents the shortest time necessary for the development, commercialisation and adoption of such a solution, taking into account not only the possible technological barriers, but also other relevant factors, including social, political and economic ones. ETM is assessed on a scale of 0-20 years, with:
    - 0 signifying that the envisaged technological solution is already available on the market and is widely adopted;
    - 20 indicating periods of 20 years and longer, including technological solutions which can never be realised.

To assess the 20 TCs according to these criteria with the support of a group of experts, a *Delphi Survey* was set up using an online real-time platform. Pre-selected stakeholders were invited to assess the 20 TCs.

Based on the assessments from the *Delphi Survey,* the 4CF Matrix was constructed, allowing the identification of technological clusters belonging to the 4 quadrants of the matrix (see Figure 5): from areas containing solutions that show little promise in terms of relative advantage but could be implemented quickly *(Coral reef)* to those that are very distant in time but contain ground-breaking solutions *(Pirate treasure)*.

Figure 5. Names of the 4 quadrants of the 4CF Matrix

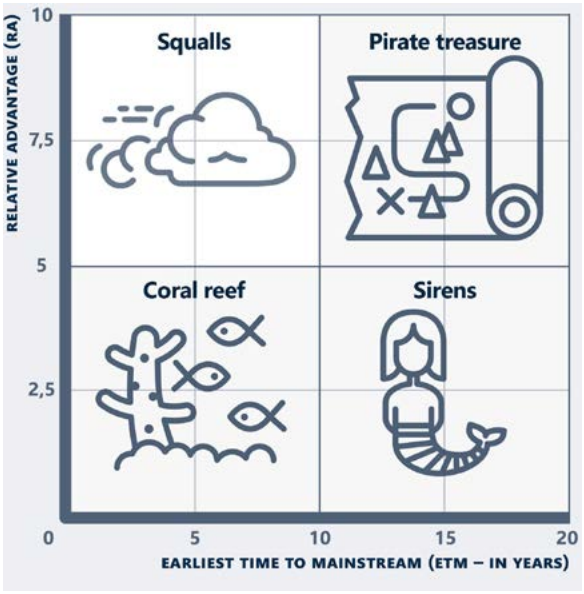
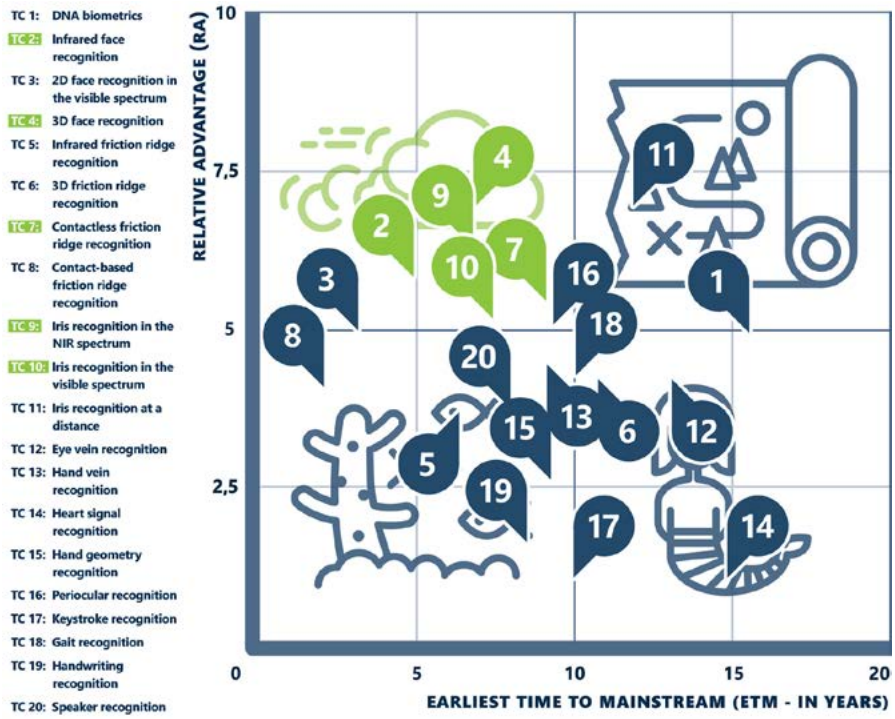


Figure 6. 4CF Matrix presenting the outcomes of the Delphi Survey. Assessment of the 20 biometric technological clusters in terms of their Relative Advantage and Earliest Time to Mainstream. The shortlisted KTCs are marked in green



The 33 participants in the *Delphi Survey* included representatives of selected stakeholders, Frontex representatives and the Research Team. Based on the results, a composite metric combining Relative Advantage and Earliest Time to Mainstream was calculated for each of the clusters to prioritise those closer to the top-left corner of the 4CF Matrix (those with a combination of high RA and low ETM).

After an additional cross-check that verified redundancy, ensured the inclusion of "must-haves" (identified in the needs assessment) and considered the inherent vulnerability to adversary attacks (rated in the security analysis), five key biometric technological clusters (KTCs) were selected for an in-depth analysis: 3D face recognition, Infrared face recognition, Iris recognition in the NIR spectrum, Iris recognition in the visible spec-

trum and Contactless friction ridge recognition. These 5 clusters are marked green in Figure 6, which presents their placement on the 4CF Matrix.

The five key technological clusters are all located in the "Squalls" quadrant of the 4CF Matrix, a clear indication that their importance should be emphasised in strategic plans. However, the placement of the other 15 technological clusters on the 4CF Matrix is equally important.

Phase 4 – Deep Analysis: Roadmaps for the key biometric technological clusters by 2040

Within the Deep Analysis phase of the project, technology roadmapping was the planning method of choice. In general, it is applied to envision the short-, medium- and long-term paths in the development and evolution of technologies and products. The roadmapping approach aligns with technology-push and market-pull perspectives, thus supporting innovation and strategic planning at the level of an organisation, a sector or even a nation. Its role in the Technology Foresight on Biometrics for the Future of Travel was threefold: (a) to identify the development paths of the key biometric technological clusters in the 2021-2040 timeframe, (b) to determine key turning points in technological developments (factors delaying or accelerating the envisioned developments) and (c) to confront technology roadmaps with alternative scenarios regarding border-check processes and the future of travel. Each of the roadmaps for the five KTCs which were created during a two-day participatory expert workshop consists of three layers: application areas, functions and products or systems (see an example in Figure 7).

The roadmapping analysis, conducted under business-as-usual conditions, included an assessment of the opportunities (drivers) and challenges (bottlenecks) that could potentially affect the technological projections. It should be noted that the roadmaps should not be treated as a forecast but rather as an invitation to analyse the development paths of the technological clusters further, monitoring associated opportunities and threats and questioning the assumptions underlying strategic plans. Among the crucial takeaways are the identified key opportunities and challenges to the development of the KTCs in the 2021-2040 timeframe (Table 2) and the qualitative assessment of the impact of the four scenarios on the clusters' development (Table 3).

Figure 7. Example of technology roadmap (for the *Contactless friction ridge recognition* technological cluster)

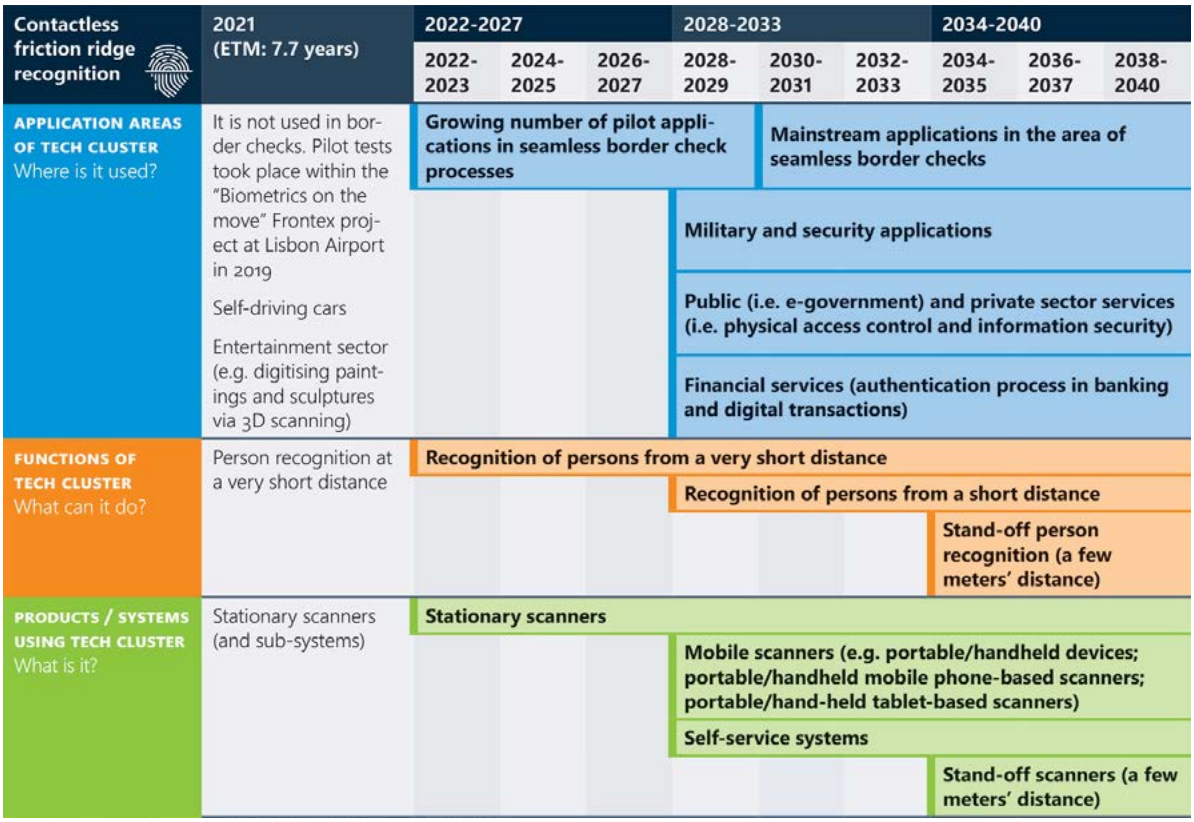
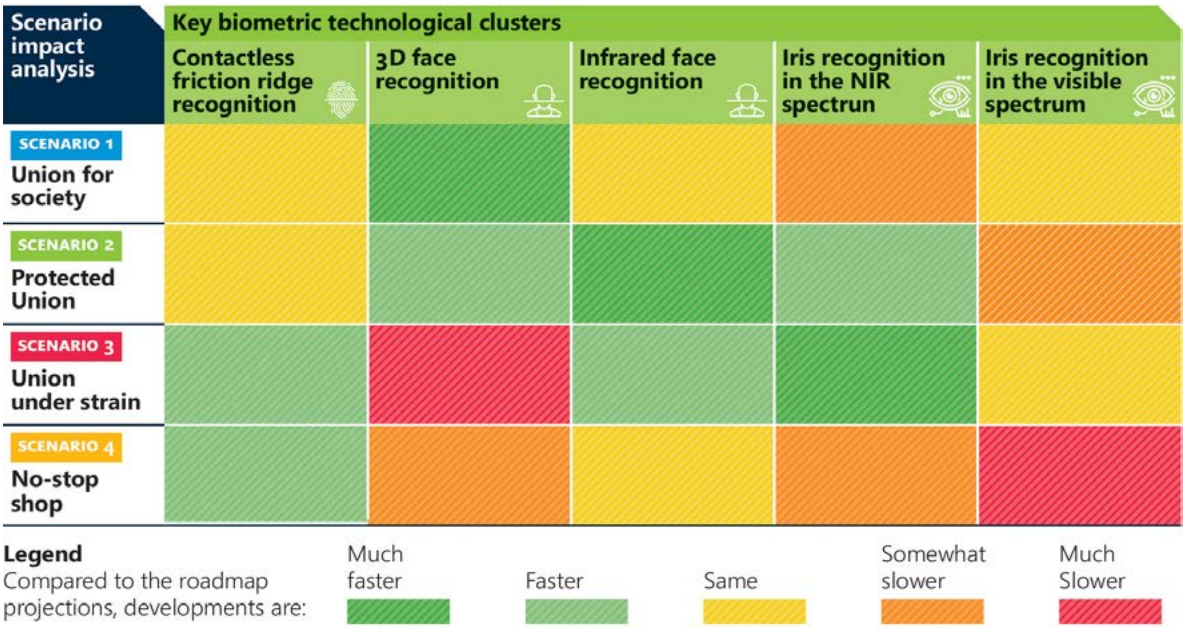


Table 2: Key factors (opportunities and challenges) in the timeframe up to 2040 – a cross-cluster comparison

Technology roadmap analysis		Key biometric technological clusters				
Key turning points	Layers of the roadmap	Contactless ridge recognition	3D face recognition	Infrared face recognition	Iris recognition in the NIR spectrun	Iris recognition in the visible spectrum
Opportunities	APPLICATION AREAS	Research aimed at the development and analysis of the quality of contactless fingerprint samples	Consumer market uptake (e.g. entertainment) would drive further development and reduce costs	Pilot programmes to compare wave-lengths and imple-ment sensor fusion	Low vulnerability to presentation attacks	Healthcare market uptake could increase under-standing that iris acquisition is eye-safe
	FUNCTIONS	Contactless biometrics is advantageous during pandemics	Adopting multi-modal biometric solutions which combine *3D face recognition* with other biometric modalities to achieve better accuracy	Use of thermal infrared cameras for temperature measurement, which can be an important feature in case of pandemics	NIR light sources (850, 905, 940 nm) are readily available	Research on the use of multi-spectral or hyperspectral iris imaging for the increased accuracy (spatial resolution)
	PRODUCTS AND SYSTEMS	Possibility of using existing sensors (e.g. cameras in smartphones)	Introduction of digital identity management schemes and novel algorithms for processing non-ideal images	Enabling acquisition (and processing) of IR images at different wave-length bands and effectively working at sensor fusion level via pilot projects	Integration of *Iris recognition in the NIR spectrum* into stand-off seamless systems for border checks would improve societal acceptance of this modality	Low technical bar-riers to implement digital identity wallets including Iris biometric reference data
Challenges	APPLICATION AREAS	Accuracy and security might be a challenge in mainstream use for border checks	Legal and ethical aspects (an agree-ment on what the biometric data might comprise)	Technology issues linked to IR illumination might require additional witness-based methods of recognition, which lowers seamlessness	Capturing biometric samples of such a small body part in motion and from a distance makes the technology difficult to develop and integrate into seamless systems	Functional limitations (stated below) might be a challenge for mainstream use in border checks
	FUNCTIONS	Extension of the distance and increase of the accuracy of the technology	Acquisition meth-ods for obtaining high-quality, reliable and interoperable data formats for 3D face images (especially for image acquisition at a distance)	Availability in the EU of foundries of affordable, accessible NIR-SWIR-LWIR image sensors	Eye safety issues when using IR illumination at wavelengths shorter than 1500 nm	Inclusivity (dark iris limitations) Suitable illuminators in visible light Iris image acquisition at a distance
	PRODUCTS AND SYSTEMS	Motion stability Interoperability Lack of harmonised regulations and standards for biometric data acquisition and exchange	The use of e-passports would require reading the passport and processing a large volume of data, which would rule out seamlessness	Development of EU regulations and standards for IR image acquisition	Introduction of enrolment via smartphone dependent on adoption of suitable solution by the mobile phone industry	Lack of harmon-ised guidelines and standards for the assessment of the operational performance of technological systems based on iris recognition

Table 3. The impact of external realities described in the four scenarios on the technological developments envisaged in the roadmaps — a cross-cluster comparison



During the road-mapping analysis, the stakeholders' experts underlined that biometrics is a highly regulated environment. Therefore, advances are introduced gradually and external conditions (e.g. unfavourable economic standing or geopolitical situation) do not have a crucial impact on technological evolution. Nevertheless, examining developments of the key clusters in light of possible scenarios of EU development through 2040 revealed that the solutions are not entirely resistant to changes in the external environment.

Phase 5 – Mapping the Capabilities for the key biometric technological clusters

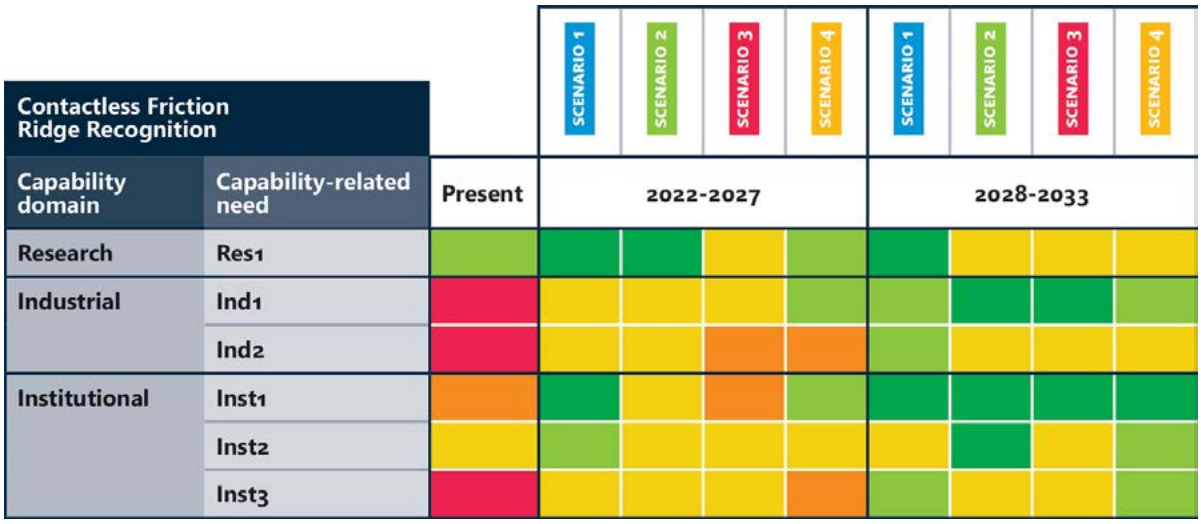
The road-mapping described above was accompanied and supplemented with a capability mapping exercise, the fifth and final phase of the research study. The exercise aimed to identify the existing capabilities for the five KTCs in the EU, as well as the expected development of capability readiness through 2040. The capability landscape shown by this exercise highlights opportunities and gaps associated with each of the technological clusters, providing a good foundation for strategic decision-making.

The outcomes of the capability mapping are presented in the form of heatmaps of capability readiness (defined as the degree to which cluster-specific capability-related needs are or will be met) for the five KTCs, distinguishing three timeframes (present, 2022-2027 and 2028-2033)[4] as well as the four customised scenarios (see an example in Figure 8). This analysis revealed that at present the majority of research, industrial and institutional overall capability readiness of any KTC is relatively low (with the exception of research capabilities for *Contactless friction ridge recognition*). Fortunately, most of those needs are expected to be met by 2027 or 2033 at the latest. *3D face recognition* and *Iris recognition in the NIR spectrum*, followed by *Iris recognition in the visible spectrum*, are expected to perform better than the other KTCs as they display good capability readiness from 2028 onwards.

One recommendation emerging from the study is that any assumptions on future capability readiness levels should be closely monitored, both to track which scenario best matches the emerging trends and to track whether the assumptions themselves are still realistic. Adapting capability-based planning to the actual unfolding trends minimises the risk of missing the defined capability target for each KTC.

4 It is assumed that once a biometric KTC has entered the mainstream, it will be available for implementation in border check systems and will not require any further capability development. Therefore, the long-term timeframe (2034-2040) was eliminated from the capability mapping exercise, as all five KTCs demonstrate an average ETM before 2033.

Figure 8. Example of heatmap of capability readiness (for the *Contactless friction ridge recognition* technological cluster)



Conclusions

This research study provided an overview of the foreseen evolution and future applications of biometric technologies in border check systems that may prove useful for the EBCG community in the short- (2022-2027), medium- (2028-2033) and long-term (2034-2040) perspectives. Each of the phases of this complex study comes with its own set of insights meant to support the EBCG community in deciding about the adoption of novel biometric technological solutions and exploiting new opportunities while avoiding or mitigating associated threats. When transferring these insights into actionable recommendations, the context, as well as the process during which they were identified, should be considered. The outcomes of the prioritisation and roadmapping of emerging biometric technologies with the strongest potential to influence the future strategic development of Integrated Border Management deserve particular attention. The following were identified as the five KTCs:

- Contactless friction ridge recognition,
- 3D face recognition,
- Infrared face recognition,
- Iris recognition in the NIR spectrum,
- Iris recognition in the visible spectrum.

Due to the substantial amount of information provided and the participatory foresight approach adopted, the research study will directly contribute to an enhanced understanding of the relevance and applicability of foresight for forward-looking decision-making within the EBCG community. We believe that a thorough analysis of the output will reveal that its benefits extend far beyond the immediate value of the information. To leverage this value, however, further effort is needed to merge the results with additional sources of knowledge-based evidence and fuse them into the relevant streams of innovation management and strategy development, thus arriving at a well-grounded vision of the future with clear implementation pathways. The expected result of such an approach is the increased application of innovative biometric technologies in border checks, which will benefit both travellers and the EBCG community in the coming years.

This project resulted in a number of outcomes and deliverables which are expected to provide essential insights for Frontex and the larger EBCG community regarding future research directions, strategic planning and decision-making:

- A **Technology Foresight Manual** was created to provide a thorough explanation of the TF process, customised to the needs of the project with successive future implementations in mind, as well as the adopted methods and tools.

- The **taxonomy of biometric technologies and biometrics-enabled technological systems** can be of great benefit to future research and innovation activities revolving around these subjects.

- The **analysis of patents, scientific literature and EU-funded projects** provides an overview of the global technological landscape and shows the evo-

lution of EU interest in biometrics over time. The results can help focus future research initiatives.

- The **customised set of scenarios** can be used to future-proof any potential new technology as well as systems or products intended for use in the areas of travel and border checks (not limited to biometric technologies).

- The **4CF Matrix** of biometric technological clusters can serve as the groundwork for future strategic planning, decision-making, research and investments, allowing for the systematic comparison of new biometric technologies (not limited to the five KTCs identified in the research study) as well as tracking the impact of technological advancements and other factors on the placement of those technologies on the Matrix.

- The **set of roadmaps** developed for the key biometric technological clusters can be used as a starting point for further analysis of these technological clusters' development paths, monitoring associated opportunities and threats and questioning the assumptions of underlying strategic plans.

- The **capability readiness heatmaps** show a comprehensive overview of the extent to which cluster-specific needs are met or will be fulfilled in the future. They can be used by the EBCG community to identify the actions needed for strategic capability development.

In conclusion, the information obtained during this Technology Foresight study provides multiple opportunities for the further use of the findings in other contexts. Beyond Frontex, it is hoped that the entire EBCG community can take stock of the results and employ them for strategic planning to take more immediate actions regarding the development and implementation of biometric technologies for border checks. Furthermore, we believe that the findings can be used by public organisations, research and technology organisations, academia and industrial entities in Europe to identify areas of strategic interest and to make informed decisions about paths of future developments in biometrics, acting towards strengthening European strategic autonomy in the field of biometrics.

Acknowledgements

This research study was conducted by Frontex under contract OP/515/2020/AH with Steinbeis 2i GmbH, supported by its subcontractors 4CF Sp. z o.o., Erre Quadro S.r.l. and the Instytut Optoelektroniki – Wojskowa Akademia Techniczna. The following Research Team members dedicated considerable time and effort to successfully completing this study: Sabine Hafner-Zimmermann, Melanie Gralow, Norbert Kołos, Anna Sacio-Szymańska, Maciej Jagaciak, Kacper Nosarzewski, Giovanni Pianigiani, Giovanni de Santis, Tommaso Pavanello, Dario Brugnoli, Donata Gabelloni, Riccardo Apreda, Marcin Kowalski, Norbert Pałka, Raffaele Bruno and Martin George.

Furthermore, the study took stock of the numerous and highly valuable contributions of all stakeholders' experts who actively participated in the two *Technology Foresight Workshops* and the *Delphi Survey*. Frontex expresses its special gratitude to all participants of the aforementioned activities, who generously shared their time and expertise.

References

- Altshuller, G. & Williams, A. (1984) *Creativity as an exact science.* New York, Gordon and Breach Science Publishers.
- Frontex (2022) *Technology foresight on biometrics for the future of travel : executive summary.* Publications Office of the European Union. https://data.europa.eu/doi/10.2819/387848.
- Frontex (2022) *Technology foresight on biometrics for the future of travel : research study.* Publications Office of the European Union. https://data.europa.eu/doi/10.2819/097463.
- Frontex (2022) *Technology foresight on biometrics for the future of travel – annex I : technology foresight manual.* Publications Office of the European Union. https://data.europa.eu/doi/10.2819/701134.
- Frontex (2022) *Technology foresight on biometrics for the future of travel – annex II : taxonomy of biometric technologies and biometrics-enabled technological systems.* Publications Office of the European Union. https://data.europa.eu/doi/10.2819.

- Frontex (2022) *Technology foresight on biometrics for the future of travel – annex III : patentometric and bibliometric analyses of biometric technologies.* Publications Office of the European Union. https://data.europa.eu/doi/10.2819/034552.
- Ghiran, A. et al. (2020) *The Future of Customs in the EU 2040: A foresight project for EU policy*. Luxembourg, Publications Office of the European Union.
  Available at: https://op.europa.eu/en/publication-detail/-/publication/15e0391b-3a9b-11eb-b27b-01aa75ed71a1/language-en/format-PDF/source-262061510 [accessed on 25/07/2022].
- Mann, D. (1999) *Using S-Curves and Trends of Evolution in R&D Strategy Planning*, in *The TRIZ Journal, July.*
  Available at: http://systematic-innovation.com/assets/199907-usings-curves-trendsofevolutioninr-dstrategyplanning.pdf
- Slocum, M. (1998) *Technology Maturity Using S-curve Descriptors*, in *The TRIZ Journal, July.*
  Available at: https://www.metodolog.ru/triz-journal/archives/1998/12/a/index.htm

Race, Ethnicity, Biotechnology and the Law:
Potentiality and challenges for law enforcement in the digital age

Eszter Kovács Szitkay
Eötvös Loránd Research Network, Centre for Social Sciences, Institute for Legal Studies & University of Public Service, Doctoral School of Law Enforcement, Budapest

Andras L. Pap
Eötvös Loránd Research Network, Centre for Social Sciences, Institute for Legal Studies, Eötvös University, Faculty of Business Economics, Budapest

Abstract
The authors, working on a project mapping how law conceptualizes and operationalizes race, ethnicity and nationality, provide an assessment of the triadic relationship between law, law enforcement practices and science. The article begins by providing an overview of the obstacles, challenges and controversies in the legal institutionalization and operationalization of ethnic/racial/national group affiliation. Subsequently, the article turns to the assessment of how "objective" criteria, data and constructions provided by science and biotechnology translate into the legal discourse and more specifically law enforcement practice in the digital age. The case study in the final section of the article provides an overview of how suspect description and the datafication is ethnicizied in Hungarian digital law enforcement registries.

Keywords: profiling, biotechnology, race, ethnicity, law

Introduction

The article revisits through the prism of the modern, digitalized technological environment, the long-standing question of how to relate to ethnicity in policing. The article begins by providing an overview of the obstacles, challenges and controversies in the legal institutionalization and operationalization of ethnic/racial/national group affiliation, and in particular in law enforcement. Subsequently, the paper turns to the assessment of how "objective" criteria, data and constructions provided by Artificial Intelligence (AI), and forensic biotechnology translate into conceptualizing ethnicity, and specifically in law enforcement practice and registries. To contextualize the discussion, the final section of the article provides an overview of how suspect description and the dataification is ethnicizied in Hungarian digital law enforcement registries.[1]

1 The research was conducted under the aegis of the 134962 and 138965 Hungarian National Research and Innovation Grants and the Artificial Intelligence National Laboratory Program.

The context: legal concepts and operationalization for race, ethnicity and nationality

Conceptualization and operationalization of race and ethnicity comes up in two dimensions: definitions and classifications pertaining to the groups, and how membership criteria are established in these communities.

The conceptualization of communities to be targeted by legal regimes takes place in a climate of ambiguity, sensitivity and suspicion. The terms are used in differing ways in academic literature, and in legal and administrative documents, also depending on the social and geographic context. For example, 'race' is used in reference to quite a different set of human characteristics in the US as in continental Europe. A controversial category, it is generally not considered to be a fruitful analytical concept in the social sciences, where it is widely understood to be a social construct rather than a biological trait without a theoretically or politically uniform definition (see Tajfel, 1981).

Race-based international and domestic legal instruments identify race with the apprehension of physical appearance, and put perception and external classifications in the center when prohibiting discrimination, or violence on racial grounds. In this, it is rarely distinguished from ethnicity. However, ethnic minorities are multifaceted groups. While many of their claims are grounded in the anti-discrimination rhetoric employed by racial minorities, some "ethnically defined" groups may also have cultural claims (and protections) that national minorities would make. The international legal terminology habitually differentiates between the two groups on the grounds that ethnic minorities are different from national minorities in the sense that they do not have nation states as national homelands (see e.g. Hannum, 2001). These groups make claims for collective rights, bypass the anti-discriminatory logic and seek recognition of cultural and political rights, particularly autonomy or the toleration of various cultural practices that differ from the majority's, which often require formal exceptions from generally applicable norms and regulations.

Conceptualizing and operationalizing membership is even less unambiguous (Pap 2021). Ethno-national group affiliation can be ascertained in several ways: (i) through self-identification; (ii) by other members or elected, appointed representatives of the community (leaving aside legitimacy-, or ontological questions regarding the authenticity or genuineness of these actors); (iii) through classification by the perception of outsiders; (iv) by using proxies such as names, residence, etc. and (v) by outsiders but using 'objective' criteria. In regard to operationalization strategies: for anti-discrimination measures, and hate crime protections subjective elements for identification with the protected group are secondary, and external perceptions should serve as the basis for classification. Policies implementing this anti-discrimination principle may rely on a number of markers: skin color, citizenship, place of birth, country of origin, language (mother tongue, language used), name, color, customs (like diet or clothing), religion, parents' origin, or even eating habits. Defining membership criteria comes up in a completely different way when group formation is based on claims for different kinds of preferences and privileges. In this case, subjective identification with the group is an essential requirement, but the legal frameworks may establish a set of objective criteria that needs to be met besides. In the context of drafting affirmative action and ethnicity-based social inclusion policies, external perception, self-declaration, and anonymized data collection may be varied and combined.

Law, law enforcement and ethnicity

As shown above, the field of law enforcement is not exempt from the dilemmas of conceptualizing and operationalizing race and ethnicity. For example, the legislator as well as officers and prosecutors need to navigate between self-identification and outsiders' perception when registering or classifying a racially motivated hate crime. Classification is also central in refugee procedures, where race, ethnicity, or membership in a "particular social group" (see e.g. Sternberg, 2011), which can be a basis for persecution is a crucial element, and where the asylum-seeker will make a claim pertaining to her affiliation, and recipient authorities will carry out a validation procedure: first establishing whether the group in question is actually in danger of persecution, and second, whether the claimant is a member of the group.

Operationalizing ethnicity also comes up in the "classic" police work of identifying missing victims or perpetrators (Pap 2008). Here creating, registering and processing ethno-racial data comes up if a suspect description by the victim or a witness includes ethno-racial descriptions. In this regard, there are four distinct scenarios how police action may rely upon ethnicity or race, and different constitutional measures apply for

each. The first, unproblematic scenario is when the victim or witness to a crime provides a detailed description of a specific suspect which includes ethno-racial characteristics. In these situations, courts have invariably found that it was legal to use such information—in search warrants, for example. A second, somewhat different scenario is in which the description provided by the victim or witness contains very little concrete detail about the suspect beyond her race or ethnicity. In such cases, on several occasions, the courts' stance was that race and ethnicity can be operative in negative descriptions only; for example, if the informant identified the perpetrator as black, then that information can serve as basis for the police not to stop whites and Asians, but it would border on discrimination for them to start stopping blacks without any further reason for doing so beside their skin color.

The third case is ethno-racial profiling, applied in traffic and border stop and search, anti-terrorist action, etc. This practice relies on the tenet that ethnicity in itself makes criminal involvement more likely, and this assumption is not based on any specific or general information about a given, concrete individual. Finally, the fourth case, which features prominently in the war against terror, involves preventive measures that rely on official, written directives about certain racial, ethnic, national or citizenship-based considerations. In these cases, the application of ethno-racial profiles is no longer left to the discretion of the police, border guards and airport security personnel. Instead, ethnic profiling becomes an officially formulated prescription.

Furthermore, are elaborated in more detail in the next section, ethno-racial conceptualization comes up in modern, digitalized, artificial intelligence (AI)-enhanced, algorithmic and molecularized policing in a diverse set of practices, from predictive law enforcement analytics, through forensic DNA to facial recognition software.

Law, law enforcement, science, datafication and ethnicity

Race, ethnicity and science

We need to begin with the observation that identity politics, political activity and "theorizing founded in the shared experiences of injustice of members of certain social groups" (Heyes, 2016) has been arguably the dominant trend in the second half of the twentieth century.[2] However, contemporary models for operationalizing ethnicity also rely on a variety of "objective" criteria. For example, ethnic preferences in citizenship often require the knowledge of the national language (see Pogonyi, 2022, 13), native American and other Indian tribes will determine membership by registered blood-quantum requirements. Furthermore, there are numerous accounts how "objective" conceptualization of ethnicity operationalizes "science" – irrespective that post-WWII social science discourse rejects biological approaches to race and ethnicity based on the stance that race is a social construct. However, as we will see, when there is a policy, commercial or political need and will, "scientific" language to describe and encapsulate ethnicity is revisited.

Technologies continuously expand the boundaries of ethno-racial conceptualization. For example, AI can accurately predict self-reported race, even from corrupted, cropped, and noised medical images, often when clinical experts cannot - and can also predict sex and distinguish between adult and pediatric patients from chest x-rays (Purkayastha *et al.*, 2022; Yi *et al.*, 2021; Eng *et al.*, 2021). The development of cheap and fast genetic analysis brought a sweeping change in how the understanding of the race and ethnicity is perceived, lived and operationalized.

It is peculiar that a significant contributor to these processes and mechanism is the highly lucrative commercial enterprise of providing genetic ancestry accounts. Various government/state services (from law enforcement to naturalization) and even the medical profession will to a varying degree rely on this form of direct to consumer commercial ancestry conceptualization of molecularized heritage – despite the fact that a large body of literature raises serious doubts on the scientific validity of these projects.

Forensic ethno-racial data generation

The new wave of innovations in forensics seeks to support criminal investigations by making inferences about the racial or ethnic appearance of unidentified suspects using genetic markers of phenotype or ancestry. The process had been termed as creating 'biological witnesses' within a new "forensic imaginary" (Williams, 2010). These new techniques analyze genetic traits for skin tone and the next, yet not fully developed stage of research targets face shape, and allow the 'prediction' of the race or ethnicity of a crime suspect (Skinner, 2018, 330-332).

2 See second wave feminism, the Black Civil Rights movement in the U.S., LGBT movements, indigenous movements, for example.

A recent project can, for example predict a person's ancestry and physical traits without the need for a match with an existing sample in a database. It was used to identify a sailor who died after his ship sank during World War II. In the United States, police departments have for years been using private DNA phenotyping services to generate facial images of suspects which then can be distributed as mugshots to the public to assist in investigations (Schwartz, 2022).

As Skinner explains, the application of genetic science to police forensics understood in terms of three overlapping waves (Williams & Wienroth, 2014):

> "*The first saw, from the 1980s onwards, the establishment of genetic testing as a credible identification tool and means of linking known suspects to crimes. The second involved, in the next two decades, the growth of national police DNA databases containing millions of records that are routinely, speculatively searched in an attempt to match as yet unknown people to offences. We are now entering a third wave where new techniques infer personal characteristics of as yet unknown suspects using crime scene samples. … The growing list of potentially detectable Externally Visible Characteristics (EVCs) includes age, eye colour, hair colour, and skin pigmentation"* (Skinner, 2013, p. 978).

The reliability of these technologies is questionable, for example, in 2012, the Minister of the Interior for the German federal state of Baden-Württemberg apologized to the Roma community for the bungled interpretation by police of DNA evidence in the investigation of a series of murders in Heilbronn in 2007 (Skinner, 2018, 332). Here DNA phenotyping predicted that a sample taken from a crime scene involving the murder of a police officer belonged to a woman of Eastern European ancestry. The same DNA was then linked to dozens of serious crimes across Western Europe, prompting a theory that the perpetrator was a serial offender from a traveling Roma community. It turned out that the recurring genetic material belonged to a female Polish factory worker who had accidentally contaminated the cotton swabs used to collect the samples (Schwartz, 2022).

Law enforcement agencies also build and apply Y-chromosome haplotype reference databases. Skinner explains that the database is racialised along a number of different dimensions, besides being

> *"(…) predominantly young and almost 80 per cent male. (…) now 27 per cent of the entire black population has a record on the database, including 42 per cent of black males and 77 per cent of young black men. (…) the NDNAD is racialised in its composition, the categorisation of all profiles by 'ethnic appearance', experiments with ethnic profiling of crime scene DNA, and the procedures of ethnic monitoring"* (Skinner, 2013, 982).

It needs to be added that "(…) *the harm of over-representation of ethnic minorities might be multiplied by the use of 'familial searching' – a technique that looks not only for exact matches between suspect DNA and database records but extends the search to near blood relatives*" (ibid).

Skinner argues that not only will such technologies implicate ethically dubious policing practices such as 'DNA dragnets' that involve mass testing of local suspect populations on the basis of the predicted ethnicity of an unknown suspect, but the DNA database also "can be misused for unethical scientific research purposes such as attempts to isolate genes that predispose particular ethnic populations to criminality" (ibid).

Besides questions pertaining to the overall efficiency and the potential abuses of the technology, Skinner also warns about the methodology for conceptualization for operationalization, arguing that

> *"(…) ethnic categories and systems of categorisation used in the NDNAD are deemed 'not fit for purpose' (as…) NDNAD race data is based on the judgement of the police officers who classify genetic samples usually at the time of arrest using the following 'ethnic appearance' codes (previously known as Identity Codes): … It is hard to reconcile data generated using these '6+1' categories with other datasets in the criminal justice system that use the 2001 Census '16+1' classification"* (ibid, 985).

Beyond the DNA

Controversies regarding modern technologies are not limited to genetics: in 2020, Google, IBM, Amazon and Microsoft announced that they were stepping back from facial-recognition software development amid concerns that it reinforces racial and gender bias. The widely applied technology uses a vast number of images to create 'faceprints' of people by mapping the geometry of certain facial features and classifies data into categories such as gender, age or race, and to compare it to other faceprints stored in databases. Ac-

cording to a 2019 report by the US National Institute of Standards and Technology, African-American and Asian faces were misidentified 10 to 100 times more often than Caucasian men, and the software also had difficulties identifying women (Dayton, 2020).

Predictive law enforcement habitually relies on big data and AI. An algorithmic bias was shown for example in investigating the risk scores used in the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) for recidivism. It was found that white defendants were more often mislabeled as 'low risk' compared to black defendants, and the risk score was more likely to falsely flag black defendants as 'high risk' (FRA, 2018, 7-8)[3].

Another scientific language through which ethnicity can be conceptualized and operationalized is voice recognition. While the traditional use of voice recognition in law enforcement was used in criminal proceedings matching a recording with an identified suspect, AI-enabled "language biometrics" has been used recently put in use in asylum procedures analyzing dialects in verifying applicants regarding their (geographic and ethnic) origin.[4] Language analysis is standard in the Netherlands and Norway for some nationalities and optional when there are indications that the applicant has provided false information. It is widely used in Belgium, Germany and Sweden (Kilpatrick & Jones, 2022, 15-17).

The case study of Hungary

This final section provides an overview of how suspect description and the datafication is ethnicizied in Hungarian digital law enforcement registries. We begin with the overview of the legal framework for processing of ethnic data, and continue by showing how ethnic data processing surfaces in law enforcement practice.

The legal framework for ethnic data processing

"Personal data indicating ethnic origin" is classified as special data by Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Infoact). The provision does not define ethnicity, but the law sets forth specific rules for processing these data types, including the requirement on "inevitable necessity and proportionality" to the implementation of an international agreement promulgated by law; being prescribed by law in connection to the enforcement of the fundamental rights ensured by the constitution, the Fundamental Law; for reasons of national security; national defense; for the "prevention, detection and prosecution of criminal offences"; being necessary for, and proportionate to, the protection of the vital interests of the data subject or of another person, or the elimination or the prevention of a direct threat to the life, physical integrity or property of persons; or if the data subject explicitly disclosed the processing of the data is necessary and proportionate (Act CXII of 2011, Article 5).

Besides EU norms (such as the GDPR), the strict regime has been present since the 1990 political transition. Before, for example, between 1971 and 1989, the ethnicity of Roma offenders were still registered (Kerezsi & Gosztonyi, 2014, 239-240). In sum, the collection and processing of ethnic data is not prohibited, but it is protected by a strict legal framework.

The "path" of ethnic data through law enforcement practices

In line with the above, information (data) pertaining to ethnicity may appear under a number of scenarios in the Hungarian legal and law enforcement framework Such cases involve hate crimes (where ethno-racial victim selection is part of the concept), in guidelines for police cooperation with (ethno-national) minority communities and for policing in multicultural communities. Let us address these in detail.

Criminal justice

There are several instances where the recognition (and processing) of ethno-racial data becomes part of the criminal process. One such case is where the perpetrator or the victim voluntarily declares his/her ethnicity, which may,or may not be relevant in the investigation/criminal proceedings, but could and should be part of the official transcript and case file. In practice, however, as we found, this this information is not mostly not re-

3 Note that machine learning also includes 'proxy information' such as postcode, which can indicate ethnic origin in cases of segregated areas in cities, or more directly, a person's country of birth, and combining 'likes' on social media with other data can also be used to determine a person's sexual orientation, ethnic origin or religion.

4 Automated text and speech recognition has been used by Germany's Federal Office for Migration and Refugees (BAMF) since 2017 (*AlgorithmWatch*, 2020; Federal Office for Migration and Refugees, 2020)

corded and stored separately, if anything, it is presented as part of the facts in a "free text" manner.

The next scenario relates to hate crimes: here, the very concept of (a racially motivated) hate crime implies that the victim is chosen due to her/his perceived membership in the given ethno-racial community. Since the victim may not immediately identify himself/herself as a hate crime victim, the investigators need to carry out a screening process: based on a set of indicators laid down by law: in ORFK Order 30/2019 (18 July) of the Chief of the National Police on the implementation of police tasks related to the handling of hate crimes. The following prejudice indicators shall be recorded in the police report of the incident and shall be investigated in the criminal proceedings to assist in the detection of hate crimes:

> (a) the perception and opinion of the victim or other witness in regards of the perception of the victim;
>
> (b) the suspect's characteristics, appearance and behaviour in relation to the offence, in particular his or her the gestures used, the clothing worn and the verbal expressions used;
>
> (c) the perceived or real group difference between the suspect and the victim, which may include persons acting on behalf of or belonging to the victim;
>
> d) the victim's appearance and behavior, including typically his/her preferred/chosen location, the foreign language or accent, clothing that symbolizes race, religion or belief;
>
> e) the suspect's prejudicial attitudes, which may be indicated by the programs/events he/she attends, preferred bands, reading material, social media platforms;
>
> (f) participation in organized hate groups, which may be indicated by the use of the suspect's group symbolism The presence of a suspect group may be indicated by its appearance and gestures, or by the group itself (by participating in the commission of the crime);
>
> (g) the location of the offence, which may be indicative of the victim's community affiliation or linked to a previous hate crime;
>
> (h) the date of the act, which may be linked to the victim's community celebrations, events or historical events favored by the suspect;
>
> (i) the degree, manner and means of the violence, in particular its exaggerated or particularly humiliating, self-serving or symbolic means;
>
> (j) the publicity, which is primarily intended to convey the perpetrator's message;
>
> (k) the absence of any other motive, in particular the unpremeditated assault or humiliation of an unknown victim." (ORFK Order 30/2019, Art. 8.)

A number of questions arise: can the police officer ask the victim about their ethnicity in order to reveal a prejudicial motive? Or, can the police record their perception in official registries? (Gyűlölet-bűncselekmények elleni Munkacsoport, n.d.) Unfortunately, the permissive conditional mode of the Order does not provide explicit guidance and officers find this extremely difficult. Even if the legal framework clearly allows for it. Act XC of 2017 on Criminal Procedure (Section 97 (1)) also stipulates that

> *"The court, the prosecution and the investigating authority may, for the purpose of conducting criminal proceedings, obtain and process all personal data necessary for the performance of its functions as defined in this Act".*

Thus not only can and should the police register ethno-racial data/information coming from the victim, witness or suspect, but it is also a legal and professional obligation, if it is a necessity for the potential classification of a (hate) crime.

The third scenario for the appearance of ethno-racial data/information in the criminal procedure pertains to suspect description. The victim's or witness's description of the perpetrator is recorded using the method of "personality description." Personality description is a forensic tool used for the identification of a person, corpse or body, containing a set of information designed and codified to include: the general human biological characteristics (biological sex, age, height, weight, build, type and location of obesity, posture, colour composition); the physiological characteristics of each part of the body (size, shape, asymmetry, deformity of the face and parts of the body); functional

characteristics (gait, speech, behaviour, smell); and - other characteristics (tattoos, body jewelry, clothing, etc.) (Anti, 2017, 75-82).

The description may point to a specific ethnicity - or the witness may make a statement about the perpetrator and Section 3 (2) c) of Act LXXXVIII of 2013 on the wanted persons registration system and on the search and identification of persons and things sets forth that "The register of wanted persons shall contain … specific data concerning the racial origin, religious beliefs, sexual conduct and political opinions of the wanted person". Nevertheless, ethno-racial features are never used *expressis verbis* in the description of the wanted person in Hungary – rather synonyms or euphemisms, such as "dark skinned" or "creol" are used that are commonly understood.

In sum, we have found that although the ever so strict rules would allow room for the processing of special ethnic data, and in certain cases, to do so is even a legal obligation: such data is not actually collected in any form by the criminal justice system. If it appears during the procedure (e.g. in the witness statement), such data is not recorded systematically either as personal or as desegregated, statistical data (Kerezsi & Gosztonyi, 2014, p. 240). The various registration systems do not have the IT facilities (a rubric) for processing.

Chief of Police Orders on multicultural policing

The other stream of recognizing ethnicity in police work relates to policies pertaining to policing multicultural communities. In line with international recommendations, in 2011 the chief of the national police issued two orders on policing multicultural communities and cooperation with Roma self-governments (and an adjacent methodological guideline in 2012),[5] which are identified as institutional partners for the force. ORFK Order 27/2011 (XII. 30.) on police measures in a multicultural environment establishes a "minority liaison" and a working group (Pap, 2019, 23-25). When mentioning minority communities, the instruction only mentions Roma and refugees explicitly, but not other minorities or immigrant groups listed in the Nationality Act. Thus, once again, we see an example of an explicit legal basis for the appearance and processing of ethnic data.

Concluding remarks on the Hungarian case

The collection and processing of ethnic data in the field provides a unique opportunity to scrutinize general problems of conceptualizing and operationalizing ethnicity. It reveals the challenges vague legal classification causes for practice. What emerges from the so-called Murphy's Law of racism, which aptly captures the problem that is common to all these cases: conceptualizing and operationalizing ethnicity is never a problem for the perpetrator, only for human rights defenders, academics, and the police (Pap, 2012, 88). The phenomenon is prevalent, beyond the criminal justice system, for example it is also present in desegregation litigation (Pap, 2012, 100-104). In sum, despite all good intentions, a counter-productive practice evolved: the (not-) collection of ethnic data is based on an overzealous interpretation of the law, which has failed to achieve its protective function on one hand, and also makes law enforcement practice difficult.

Conclusions

This article was aimed at triangulating models and languages of conceptualization and operationalization for race, ethnicity and nationality by law, and with a special focus on law enforcement. We showed that when there is a policy, commercial or political need and will, new, digitalized "scientific" language to describe and encapsulate ethnicity is revisited.

Ethno-racial data processing is a difficult question for policing, but there are strong arguments for the use of ethnic identifiers in data collection in order to be able to detect and correct discriminatory treatment and outcomes (see e.g. Chopin *et al.*, 2014; Osoba & Welser, 2017; FRA, 2019). Also, since the world is not colour-blind, it is an unreasonable expectation for police to be such. Furthermore, such data processing is a necessity for classifying certain (say, hate) crimes, and can serve as a useful and, it is important to stress, legal tool to identify suspects. While in the EU Article 9 of the GDPR confirms that the processing of sensitive data (including race and ethnicity) is prohibited, it does provide for ten exceptions, which should suffice for narrowly tailored, legally defined police work that duly takes into

5 a multikulturális környezetben végrehajtott rendőri intézkedésekről szóló 27/2011. (XII. 30.) ORFK utasítás, a roma kisebbségi önkormányzatok közötti együttműködésről, kapcsolattartásról szóló 22/2011. (X. 21.) ORFK utasítás, (2012. január 19-én kelt.) 29000/126311/2012 ált. számú módszertani útmutató.

consideration guidelines and recommendations European and other watchdog organizations.[6]

References

- AlgorithmWatch (2020)
  Available at: https://automatingsociety.algorithmwatch.org/report2020/g ermany/ (Accessed: 12 June 2022)
- Anti, Cs. (2017) *A személyleírás*. Budapest: Semmelweis Kiadó.
- Chopin I., Farkas L. & Germaine C. (2014) *Ethnic origin and disability data collection in Europe – Comparing discrimination*. n.d.: Migration Policy Group for Open Society Foundations.
- Dayton, L. (2020) 'Reading between the lines - From facial recognition to drug discovery, these emerging technologies are the ones to watch', *Nature* 588, pp. s126-s128.
- Eng, DK. *et al.* (2021) 'Artificial intelligence algorithm improves radiologist performance in skeletal age assessment: a prospective multicenter randomized controlled trial', *Radiology*, 301(3), 692–99.
- Federal Office for Migration and Refugees (2020) *Digitalising the asylum procedure.*
  Available at: https://www.bamf.de/EN/Themen/Digitalisierung/Digitales Asylverfahren/digitalesasylverfahren-node.html (Accessed: 12 June 2022)
- FRA Focus (2018) '#BigData: Discrimination in data-supported decision making'.
  Available at: https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making. (Accessed: 12 June 2022)
- FRA (2019) *Facial recognition technology: fundamental rights considerations in the context of law enforcement*. Luxembourg: Publications Office.
- Goldstein, D.B. (2008) *Jacob's Legacy: A Genetic View of Jewish History*. New Haven & London: Yale University Press.
- Gyűlölet-bűncselekmények elleni Munkacsoport (n.d.) Útmutató a gyűlölet-bűncselekmények sértettjeinek, egyéb tanúinak kihallgatásához, továbbá a hatóság sértettel kapcsolatos észlelésének jegyzőkönyvezéséhez különös tekintettel az adatvédelmi kérdésekre.
  Available at: https://gyuloletellen.hu/sites/default/files/gyem_kihallgutmutato_3.pdf. (Accessed: 14 July 2022)
- Hannum, H. (2000) 'International Law', in Motyl, A. (ed.) *Encyclopedia of Nationalism*. United States of America: Academic Press. pp. 405–419.
- Heyes, C. (2016) 'Identity Politics', in Zalta, E. N. (ed.) *The Stanford Encyclopedia of Philosophy (Summer 2016 Edition)*.
  Available at: http://plato.stanford.edu/archives/sum2016/entries/identity-politics/ (Accessed: 12June 2022)
- Kerezsi, K. & Gosztonyi, M. (2014) 'Roma is? Szegény is? Bűnös is?', in Borbíró, A. *et al.* (eds.), *A büntető hatalomkorlátainak megtartása: A büntetés mint végső eszköz. Tanulmányok Gönczöl Katalin tiszteletére.* Budapest: Elte Eötvös Kiadó, pp. 235-273.
- Kilpatrick, J. & Jones, C. (2022) *A clear and present danger Missing safeguards on migration and asylum in the EU's AI Act*. Statewatch.
  Available at: https://www.statewatch.org/media/3285/sw-a-clear-and-present-danger-ai-act-migration-11-5-22.pdf (Accessed 14 July 2022)
- Osoba, O. & Welser, IV W. (2017) *An Intelligence in Our Image. The Risks of Bias and Errors in Artificial Intelligence.* Santa Monica: RAND Corporation.
- Pap, A.L. (2008) "Ethnicity and Race-Based Profiling in Counter-Terrorism, Law Enforcement and Border Control." European Parliament's Committee on Civil Liberties, Justice and Home Affairs (2008).
- Pap, A.L. (2012) A megfigyelés társadalmának proliferációjától az etnikai profilalkotáson át az állami felelősség kiszervezéséig. Budapest: L'Harmattan,
- Pap, A. L. (2019) *Rendészet és sokszínűség*. Budapest, Dialóg Campus.

6 For guidance see the law enforcement directive, Directive (EU) 2016/680 of the European Parliament, and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89-131). Also consider how in 2017 the European Parliament called to identify and take measures to minimize algorithmic discrimination and bias and to develop a strong and common ethical framework for the transparent processing of personal data and automated decision (European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, nondiscrimination, security and law-enforcement (2016/2225(INI)).

- Pap, A. L. (2021) Conceptualizing and Operationalizing Identity, Race, Ethnicity, and Nationality by Law: An Introduction. Nationalities Papers, 49(2), 213-220.
- Pogonyi, Sz. (2022, January 12) 'The right of blood: 'ethnically' selective citizenship policies in Europe', *National Identities*, doi: 10.1080/14608944.2021.2013185.
- Purkayastha, S., *et al.* (2022) 'AI recognition of patient race in medical imaging: a modelling study'. *The Lancet. Digital health*, 4(6), e406–e414. doi: 10.1016/S2589-7500(22)00063-2.
- Schwartz, O. **(**2022**) '**Australia Wields a New DNA Tool to Crack Missing-Person Mysteries', *The New York Times,* May 28th. Available at: https://www.nytimes.com/2022/05/28/world/australia/dna-phenotyping.html (Accessed: 14 July, 2022)
- Skinner, D.L. (2018) 'Forensic genetics and the prediction of race: What is the problem?' *BioSocieties* 15, pp. 329–349.
- Skinner, D. (2013) 'The NDNAD Has No Ability in Itself to be Discriminatory: Ethnicity and the Governance of the UK National DNA Database', *Sociology*, 47(5), 976-992. Available at: https://journals.sagepub.com/doi/full/10.1177/0038038513493539. (Accessed 12 June 2022)
- Tajfel, H. (1981) *Human Groups and Social Categories: Studies in Social Psychology*. CUP Archive.
- Williams, R. (2010) 'DNA Databases and the Forensic Imaginar', in Hindmarsh, R. and Prainsack, B. (eds.) *Genetic suspects: Global governance of forensic DNA profiling and databasing.* Cambridge: Cambridge University Press, pp. 131–152.
- Williams, R. & M. Wienroth (2014) *Ethical, social and policy aspects of forensic genetics: A systematic review.* Basingstoke: Palgrave.
- Yi, PH. *et al.* (2021) 'Radiology "forensics": determination of age and sex from chest radiographs using deep learning', *Emerg Radiol*, 28(5), 949–954.

Artificial Intelligence and Interoperability for Solving Challenges of OSINT and Cross-Border Investigations

Amr el Rahwan
International Hellenic University[1]

Abstract

The major investigation challenges are summarised as multiple-identity, fraudulent actions, lack of interoperability and absence of an effective technical solution for exchanging Cross-Border information, and complexity of OSINT investigations.
The EU published Regulations (EU) 2019/817 and 2019/818 for establishing a framework for EU interoperability between information systems in the field of borders and visa information systems, police and judicial cooperation, asylum, and migration. Existing systems such as EURODAC, SIS / SISII, and VIS must share data, and new systems such as ECRIS-TCN, EES, and ETIAS also need to follow these guidelines. Although the eu-LISA will implement the interoperability framework in 2023, new challenges will emerge, such as investigating multiple-identity and identity frauds due to the different formats and structures of data, low quality of biographic and biometric data, and low accuracy of matching algorithms.
Furthermore, the Open Source Intelligence (OSINT) investigation process is not automated, consumes a lot of time, and is overwhelming. When border security and law enforcement officers use methods of OSINT to investigate terrorism and serious crime, it is very difficult to match and link the identity-related data and facial images of the suspects stored in the EU systems, Cross-Border systems, and open sources.
The paper argues different Artificial Intelligence (AI) methods and algorithms and interoperability could be the optimum solution for the challenges mentioned above. The paper highlights a Person-Centric approach using Artificial Intelligence and interoperability to solve the challenges that emerge during investigations, such as multiple-identity, identity frauds, exchanging Cross-Border information, and the complexity of OSINT investigations.

Keywords: Multiple-Identity, OSINT, Interoperability, Cross-Border, Artificial Intelligence

1 Author's email: amr.rahwan@secureidentityalliance.org

Introduction

The paper highlights using artificial intelligence and interoperability for solving the challenges of OSINT and Cross-Border investigations. The four major challenges are multiple-identity, fraudulent identity, cross-border investigations, and OSINT complexity. The multiple-identity and fraudulent identity challenges exist on the national level of the European Member States, and more challenges will emerge between the national level and the central EU level after implementing the new interoperability architecture. The newly established central and national ETIAS "European Travel Information and Authorisation System" units will face the challenge of confirming or rejecting the relations and links between the different encounters of the multiple-identity and fraudulent identity. The main challenge for cross-border investigation is the difficulty of exchanging cross-border information and the non-existence of a proper interoperable information system or a technical solution for exchanging information related to the cross-border investigation. The complexity of OSINT is challenging because only officers with strong information technology skills and background can obtain optimum results from OSINT investigations. In contrast, detectives and investigators with basic IT skills can't obtain good results from OSINT investigations, either for investigations for solving national or cross-border crimes.

Furthermore, the paper highlights the relevant technologies that could be used for solving the mentioned challenges, especially using interoperability and pre-trained Artificial Intelligence algorithms. Moreover, understanding the existing technology limitations is essential for obtaining good results and recommending the best practice for achieving optimal results. Furthermore, introducing a new Person-Centric OSINT approach complies with the UMF "Universal Message Format" standard of European interoperability. The newly introduced Person-Centric OSINT approach will allow the detectives and investigators with basic IT skills to achieve good results in identifying suspects and victims of terrorism and serious crimes without being overwhelmed with learning advanced IT or OSINT.

Moreover, the paper presents three hypothetical cases, recommends the HORUS system for SSI "Single Search Interface" as a practical technical solution for cross-border interoperability and exchanging of cross-border information, and simulating an automated search scenario for identifying an unknown terrorist.

Finally, the paper describes the required training for law enforcement officers in each Member State, and it concludes the required training for compliance with EU interoperability standards, the required support for purchasing and implementing AI, interoperability, and Single Search Interface, the required capacity building for technical, functional, and operational officers, and essential AI training on Facial Recognition and Person-Centric OSINT for cross-border investigations.

Challenges

Multiple-Identity

The central EU information systems were implemented in silos, creating information gaps due to a lack of interoperability. Implementing the information systems in silos has created challenges for detecting incorrect, incomplete, or fraudulent identities.

Subsequently, on the 22nd of May 2019, the EU published two new regulations. Regulation (EU) 2019/817: establishing a framework for EU interoperability between information systems in the field of borders and visa information systems (Council Regulation (EC) 817/2019). Regulation (EU) 2019/818: establishing a framework for EU interoperability between information systems in the field of police and judicial cooperation, asylum, and migration (Council Regulation (EC) 818/2019). Article (38) of the regulations established the UMF "Universal Message Format" standard to achieve interoperability.

The need to improve EU interoperability is clear. Existing systems such as EURODAC, SIS / SISII, and VIS must share data, and new IT systems such as ECRIS-TCN (Council Regulation (EC) 816/2019), EES (Council Regulation (EC) 2226/2017), and ETIAS also need to follow these guidelines. That must be done without adding new databases or changing access rights to existing systems.

The components needed as part of the move towards EU interoperability include the following: the European Search Portal (ESP) for fast and seamless simultaneous searches in EU information systems, in addition to Europol and Interpol data; the Shared Biometric Matching Service (sBMS) (European Union Agency for the

Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, 2018) that searches and compares biometric data (fingerprints and facial images), linking this data to other systems; the Common Identity Repository (CIR) (European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, 2018) to increase the accuracy of identification through automated comparison and matching, and the Multiple Identity Detector (MID) (European Council: Council of the European Union, 2019) for automatic detection of multiple identities linked to the same set of biometric data.

However, many common challenges will emerge due to the different formats and structures of data, low quality of biographic and biometric data, low accuracy of matching algorithms, errors in data entry, and fraudulent actions. For example, when the border authorities receive the Advance Passenger Information (API) and the Passenger Name Record (PNR) of air and sea passengers, it is difficult to exchange and match the identity of one passenger with his/her records stored in the EES, ETIAS, SIS, and VIS due to lack of interoperability and different data structures and formats. Another example of these challenges is the car license plate number. The license plate number has different formats and structures that vary from one Member State to another, creating difficulties in searching and finding the correct license plates and linking them with individuals, such as owners or suspects.

TCNs, or Third Country Nationals, are mainly the persons of interest stored in the EU information systems for different purposes, except for SIS, which also stores information about European citizens. The SIS / SIS-II (Council Regulation (EC) 1862/2018) stores security alerts on persons wanted by the Member States, and the officers can search the central information systems with biometric data such as fingerprints or biographic data such as first name, family name, gender, date of birth, place of birth, and nationality to find targeted persons or search object alerts such as A Vehicle; a Firearm; a Blank Document; an Issued Document; a Banknote; an Industrial Equipment; an Aircraft; a Boat; a Boat Engine; a Container; a License Plate; a Security; a Vehicle Registration Document. The EURODAC (Council Regulation (EC) 2013/603) system stores biometric information such as facial images, fingerprints, and identity-related biographic information of asylum seekers and illegal border crossers. The officers can search the central system by any element of the stored information. The VIS or Visa Information System stores the information such as facial images, fingerprints, name, gender, date of birth, place of birth, nationality, and address of the TCNs travelling with a short-stay visa, and the authorities have up to fifteen working days for vetting the travelers and checking for security clearance.

Important to mention that the central EU systems have gaps in covering all the persons of interest living or travelling to the Member States of the European Union. The gap could be summarised in three types of persons of interest: the short stay visa-exempted third country travellers, permanent foreign residents, and EU citizens. The eu-LISA will implement the ETIAS system and units for solving the gap for the visa-exempted TCNs. However, none of the existing or newly established central European information systems will solve the gap for permanent TCN residents and EU citizens. Each Member state is responsible for solving that gap by creating national systems and achieving interoperability between the national and central information systems as per the EU regulations for interoperability. Clause 22 of regulations (EU) 2019/817 and 2019/818 states that [Member States dispose of efficient ways to identify their citizens or registered permanent residents in their territory], so each Member State is responsible for solving the gap and issue related to its citizens and permanent residents to avoid security vulnerabilities and to reveal their identities if they became suspects or victims of terrorism or serious crime.

The security authorities have enough time to apply security check and clearance on the travellers on a standard short-stay visa with their information stored at the VIS. At the same time, only 48 hours are available to perform security clearance of the visa-exempted third country visitors as mentioned in the regulation (EU) 2018/1240 on establishing a European Travel Information and Authorisation System ETIAS (Council Regulation (EC) 1240/2018). The ETIAS will solve the existing security gap of the visa-exempted TCNs. However, the central and national ETIAS unit officers should be well-trained to solve the multiple-identity issues. The visa-exempted visitor will apply for a travel authorisation before arrival to the EU Member State. The visitor will submit identity-related information such as a facial image and biographical data, which will be stored and processed by the ETIAS. The identity-related information will be searched against all the central EU information systems to check the former existence of the

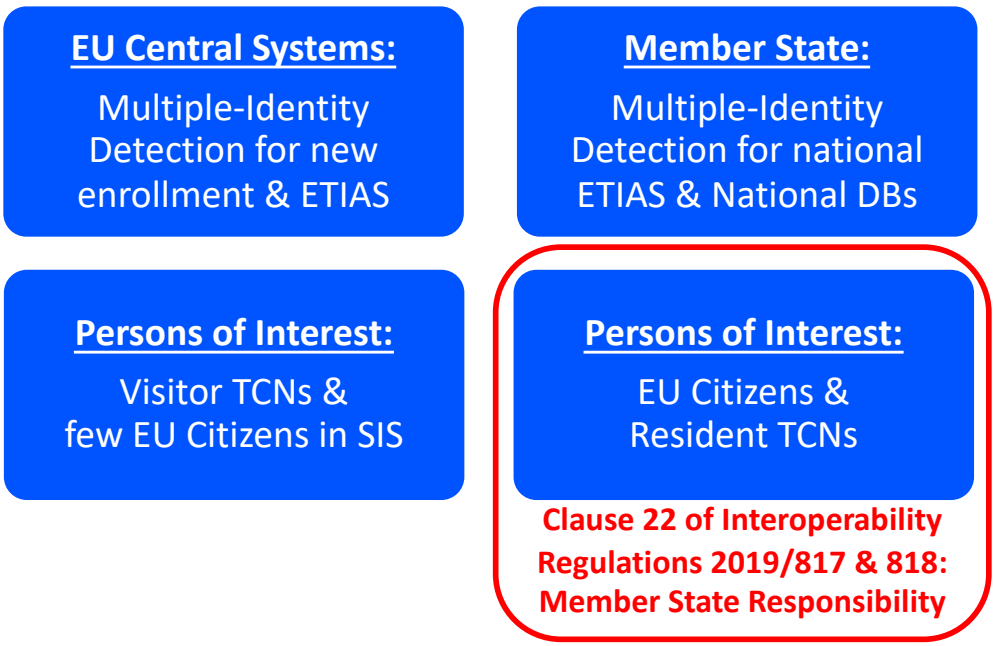
visa-exempted applicant in other EU systems than the ETIAS, and the central MID, Multiple-Identity Detector, will automatically flag the identities with similarities based on biometric matches or biographic matches. The ETIAS unit officers have to manually investigate all the elements of the multiple-identities and confirm or reject the link between identities.

Similarly, the multiple-identity issue may occur when using methods of OSINT to gather more information on suspects, victims, or travellers. The multiple-identity issue gets more complex if the identity-related results of OSINT search is in a language other than the language of the information stored in the EU or Member States information systems. For example, the name, gender, date of birth, place of birth, and nationality are stored using a Latin-based script in the EU information systems. It is very challenging for the officers, detectives, and investigators to decide on the similarities or differences of a multiple-identity with biographic information received from OSINT results and written in Arabic, Cyrillic, Chinese, Greek, Japanese, or Korean scripts. Especially if the officers didn't read or understand the foreign script. The first case of the cases section will clarify an example of multiple-identity.

Identity Fraud

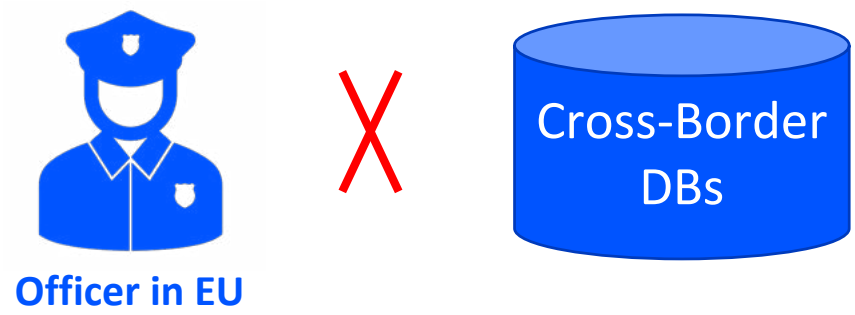
The fraudulent actions and wrong matches are other issues created due to the lack of interoperability and low accuracy of some biometric modalities. For example, the fingerprints of a third-country national could be enrolled in the VIS system with specific identity information, while the fingerprints of the same third-country national might be enrolled in the EURODAC system using different identity information. A second example is that the different facial images of a third-country national could be enrolled in the VIS and EURODAC systems. When submitting a facial query to both systems, the results could be two lists of candidates, instead of one "hit/no hit" from each system, due to the low quality of facial images and the low accuracy of facial recognition algorithms.

Finally, when the border security officers and the law enforcement officers use methods of Open Source Intelligence (OSINT) to investigate terrorism and serious crime, it is very difficult to match the identity-related data and facial images of the suspects stored in the EU systems with the data from open sources. Moreover, most law enforcement and border security officers' basic information technology skills are insufficient for detecting fraudulent identities when using OSINT for investigations. The officers should receive advanced biometric training, especially facial recognition training, and Person-Centric OSINT training to be qualified to detect, investigate, and match identity frauds from open source. The second case of the cases section will clarify an example of identity fraud.



Cross-Border Investigation

Cross-Border information exchange is required when revealing the identity of an involved suspect or victim depending on identity information or criminal information that resides in a foreign country outside the borders of European countries. Furthermore, exchanging of cross-border information is required by immigration authorities for the identification and security clearance of TCN asylum seekers and travellers. Cross-Border investigations are challenging because there is no proper way or technical solution for exchanging cross-border information, and the officers in the EU countries don't have access to the cross-border databases and information systems. The third case of the cases section will simulate the challenge and the solution for a valid hypothetical scenario for cross-border investigation.

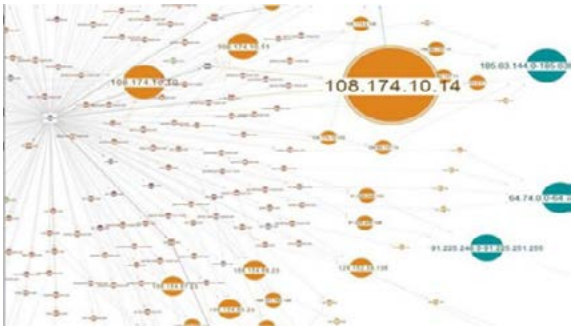


OSINT Complexity

Using tools and methods of OSINT is challenging because it contains various information technology elements such as domains, websites, protocols, headers, codes, scripts, IP addresses, certificates, hashes, usernames …etc. It requires strong IT skills to obtain optimum results in revealing the identities of suspects or victims related to terrorism or serious crime. Moreover, it is difficult to match the suspects' identity-related data and facial images stored across the different databases with the data from open sources. For example, a suspect has a record stored in a national or European database such as SIS or EURODAC. The stored record might be biographic data or a facial image. When the suspect has a different identity on the internet and social media, it is difficult to link the identity stored in the national and EU databases with the fraudulent identity claimed on the internet and social media.

Furthermore, the officers don't get the optimum results from the OSINT tools because they need to understand the tools' mechanism, accuracy, and demographics. Also, they may not differentiate between image recognition and facial recognition in many cases. For example, it is important to understand which type of human images could return good results when searching with tools such as Google, Bing, and Yandex. Those OSINT tools are Artificial Intelligence algorithms for image recognition, not facial recognition. Another example is the facial Recognition AI algorithms used for OSINT have limitations due to their recognition mechanism, the accuracy of algorithms, geographic coverage, and ethnicity bias. Understanding the limitations will lead to optimum results when using such OSINT tools dedicated to facial recognition.

Finally, the different encounters of the same identity are not linked across the different data sources, creating multiple-identity and fraudulent identity challenges due to lack of interoperability and the variations of names and languages.



Artificial Intelligence

The proposal of the European Artificial Intelligence Act defines Artificial Intelligence systems as " 'artificial intelligence system' (AI system) means software that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with." (Council Regulation proposal (EC) 2021/0106).

Artificial Intelligence technology and interoperability are keys to solving the multiple-identity and fraudulent identity issues. To clarify, the main trigger for the multiple-identity and fraudulent identity issues is that the information is stored in the systems and the databases in silos, and there is no link between the identity-related information stored in the national, European, international, and open sources. There is no SSI "Single Search Interface" till present, and the investigators and officers use separate interfaces for submitting the same queries to national systems, OSINT, and international systems and databases such as Interpol's SLTD "Stolen and Lost Travel Documents", EUROPOL, EURODAC, SIS/SISII, and VIS. When an officer submits a search with one or more identity elements to the different interfaces of data sources, the officer's decision on linking the different encounters of the same identity and discovering frauds depends on factors such as biographic information, name variation, and facial images.

Named Entity Relationship, or NER, is an artificial intelligence method used for automatic extracting, classifying, and categorising the content of a text. NER should be the early step for detectives and investigators when investigating a text written in a language they don't understand. NER will help the investigators understand and target the information useful for investigations, such as names, jobs, and addresses while decreasing the focus on the less useful or less relevant information. The cases section contains three examples for clarifying the practical usage of NER.

Although the stored fingerprints in the EU information systems have good quality, there are challenges to detecting similar or different identities. Natural Language Processing (NLP) AI algorithms can be used for biographic matching across multiple information systems. These algorithms can be trained to link between the different name variations of similar identities. They can detect identity fraud when the same person's fingerprints are enrolled in two systems or more under different identities. The paper demonstrates using an artificial intelligence algorithm for fuzzy name matching, a specific type of Natural Language Processing.

NLP and Named Entity Recognition (NER) AI methods can be combined with domain-specific knowledge to solve the issues related to unstructured data, different data formats, and data mapping. A good example is to search for a license plate number, as each Member State has a different structure and format than the others, and some Member States may have more than one format for license plate numbers. For this example, the AI algorithms will be trained to recognise the license plate number and country of origin. Using representative training data to support a Google-like search and get the best results is essential. However, the paper only presents the pre-trained Artificial Intelligence algorithms.

Using AI for fuzzy name matching for linking the different encounters of similar identities is essential for deciding on similarities and differences between identities triggered by biometric hits such as a fingerprint match or a facial recognition match. Within the paper, AI algorithms are recommended for extracting identity-related information, searching, and matching, while no algorithms will be introduced for anomaly detection or predictive analysis.

Moreover, AI algorithms for image recognition and facial recognition are important for verifying previously known identities and searching for unknown identities. For example, an investigator could search two sources using biographic elements of the identity that resulted in retrieving a facial image from each source. The investigator can use an AI algorithm for facial recognition to verify the facial images. Another example is that the authorities may not have any information about a suspect except a photograph. The authorities can submit the photo to AI algorithms for image recognition and facial recognition to gather more information about the unknown suspect.

The presented concept is to train officers on obtaining the best results from pre-trained commercially available AI algorithms, with any possibility of re-training the AI algorithms.

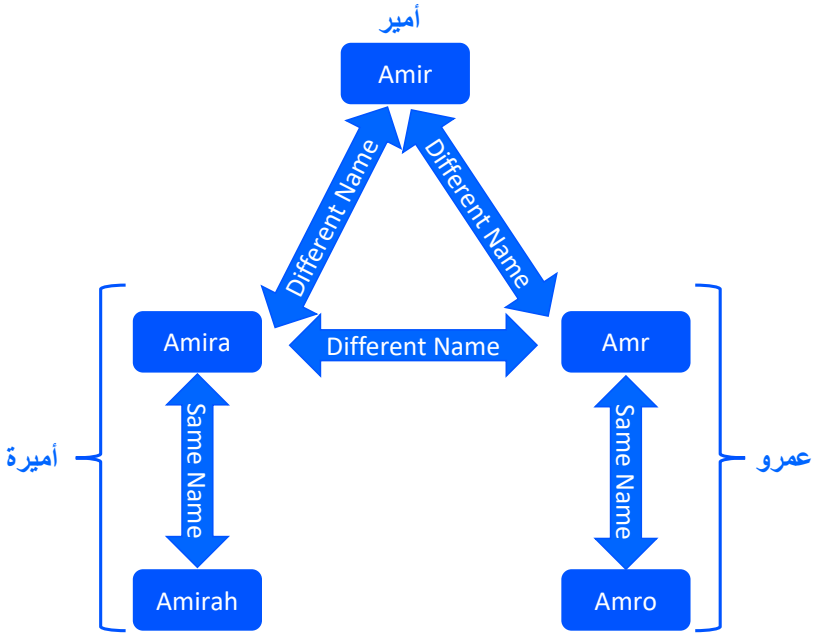
AI for Fuzzy Name Matching

Name matching is essential for linking or unlinking identities. Yet, understanding names is challenging

because the same name is written and pronounced differently across different languages, and the name may have variations due to regional and cultural effects. Furthermore, there are no clear rules for defining nicknames, and a nickname may sound very far from the original name, such as Sasha, a nickname for Alexander. Understanding name variations across different languages and using AI algorithms for fuzzy biographic matching will improve investigation results and solve the problems of multiple-identity and frauds.

In the Arabic language, for example, it is easy for Arabic speakers to identify persons of interest with Arabic names. Still, it is challenging for non-Arabic speakers because the Arabic names have a lot of variations when translated to other languages. Another challenge is that many Arabic letters don't have any phonetical equivalent in Latin-based languages (Sawalha et al, 2014). The below diagram depicts the complexity of name variations of Arabic names.

Figure 1. Complexity of name variations of Arabic names



The above diagram shows an example for three different names, ***Amr"*** عمرو**"**, ***Amir"*** أمير **"**, and ***Amira"*** أميرة**"**, and a good AI algorithm should be able to discover all the variations of one name such as ***Amr*** and ***Amro*** are the same name. ***Amira*** and ***Amirah*** are the same names. The three names are written and pronounced in one way only in Arabic, and Arabic speakers easily distinguish them. However, considering the spoken languages of the European officers, It is difficult for non-Arabic speakers to discover the variations and differentiate between the three names because the names contain letters that don't have phonetical equivalents in Latin-based languages. Each name could be written and pronounced in several ways when translated to other languages. For example, the first sound and letter of the name ***Amr"*** عمرو**"** doesn't exist in English, French, Spanish, Russian, German, Dutch, Italian, or Greek languages, and the letter ***"A"*** is an inaccurate compensation for the letter ***"ع"***, and it is not literal and not correct phonetically. The below table depicts the special phonetics of Arabic letters.

Figure 2. Source: QURANIC WORDS STEMMING (Yusof et al, 2010).

Unicode	*Arabic letter*	*Name*	*SATTS*
0621	ء	hamza	E
0622	آ	alef with madda above	(missing)
0623	أ	alef with hamza above	(missing)
0624	ؤ	waw with hamza above	(missing)
0625	إ	alef with hamza below	(missing)
0626	ئ	yeh with hamza above	(missing)
0627	ا	alef	A
0628	ب	beh	B
0629	ة	teh marbuta	?
062A	ت	teh	T
062B	ث	theh	C
062C	ج	jeem	J
062D	ح	hah	H
062E	خ	khah	O
062F	د	dal	D
0630	ذ	thal	Z
0631	ر	reh	R
0632	ز	zain	;
0633	س	seen	S
0634	ش	sheen	:
0635	ص	sad	X
0636	ض	dad	V
0637	ط	tah	U
0638	ظ	zah	Y
0639	ع	ain	"
063A	غ	ghain	G
0640	ـ	tatwheel	(missing)
0641	ف	feh	F
0642	ق	qaf	Q
0643	ك	kaf	K
0644	ل	lam	L
0645	م	meem	M
0646	ن	noon	N
0647	ه	heh	?
0648	و	waw	W
0649	ى	alef maksura	(missing)
064A	ي	yeh	I

Advanced Artificial Intelligence could help non-Arabic speakers identify and verify name variations for deciding on multiple-identities and frauds. The below table depicts the matching results obtained from a commercial fuzzy name matching AI algorithm for detecting the variations of the Arabic names.

Table 1. Fuzzy name matching AI algorithm

Name 1	Name2	Same Name	Gender	AI Score
Amr	عمرو	Yes	Same	99.0%
Amr	أمير	No	Same	72.7%
Amr	أميرة	No	Different	28.4%
Amr	Amira	No	Different	37.4%
Amr	Amir	No	Same	85.5%
Amir	عمرو	No	Same	72.7%
Amir	أمير	Yes	Same	99.0%
Amir	أميرة	No	Different	80.9%
Amir	Amira	No	Different	51.2%
Amira	عمرو	No	Different	60.9%
Amira	أمير	No	Different	80.3%
Amira	أميرة	Yes	Same	98.2%

Wrong Match

Wrong Match

The above results obtained by the AI algorithms for the three names help determine the similarities and differences between the variations of Arabic names. However, ***Artificial Intelligence is not an absolute source of truth***, and the existing AI algorithms for fuzzy name matching have issues matching Arabic names with their Latin variations. They are not fully matured and not well-trained, and they might wrongly create a high confidence score when matching two different Arabic names. For example, the names ***Amr*** in Latin letters and ***Amir"*** أمير ***"*** in Arabic letters in the second row are two different male names, but the similarity score is higher than 70% which is not correct. The same applies to the names ***Amir*** and ***Amr"*** عمرو***"*** in the sixth row. In the fifth row, the names ***Amr*** and ***Amir*** are wrongly matched with 85.5% because the number of letters is small, and the phonetical difference is minor when pronounced with a Latin-Based language; nevertheless, the two names are very different phonetically when written and pronounced in Arabic. Finally, the names ***Amir"*** أمير ***"*** and ***Amira"*** أميرة***"*** in the eighth and eleventh rows are matched with a score over 80%, although the genders are different because Amir is a male and Amira is a female. The AI algorithm should consider the genders while matching names, especially since the genders already exist in its knowledge base.

AI for Image Recognition vs Facial Recognition

Both Image Recognition and Facial Recognition technologies are based on analysing images. Still, the major difference is that image recognition analyses the whole image for detecting any type of object, such as bags, cars, glasses, clothes, humans, etc. In contrast, facial recognition technology focuses on detecting and analysing human faces. Facial recognition is the most understandable concept in biometric matching because people use it naturally to identify each other daily and without the need for computers. Moreover, facial recognition technology doesn't require special sensors. A facial image could be captured from simple types of sensors such as a webcam rather than fingerprint and iris recognition technologies that require specific and dedicated sensors such as fingerprint and iris scanners. Furthermore, it is easy to obtain facial images from various national, regional, and international data sources available for law enforcement agencies. The availability of facial images from the internet and open source increased after the massive use of social media without good protection of the privacy of personal information.

Understanding the mechanisms, accuracy, and demographics of image and facial recognition is important for recognising their differences. It is also important to

provide high-quality training for law enforcement officers to qualify them for using those AI algorithms to reveal the identities of suspects and victims. The below table shows a comparison between image recognition and facial recognition.

Table 2. Comparison between Image Recognition and Facial Recognition

Comparison	Image Recognition	Facial Recognition
Mechanism	Analyze full image	Analyze Faces
Limitations	Image-Related	Facial-Related
Accuracy	Low	High
Image Popularity	Important	Not Important
Background & Colors	Important	Not Important
Ethnicity Bias	No	Yes

The image recognition algorithms analyse the full image to classify the type of the image or object and search for similar images, while the first step of a facial recognition algorithm is to detect the existence of a human face inside the image and search for similar faces. The limitations of image recognition tools are related to the whole image of the submitted photo or the photo in the reference database. Nevertheless, the limitations of the facial recognition tools are related to the detected faces only. The accuracy of the image recognition algorithms is lower than the facial recognition algorithms when searching for human faces. The popularity of the equivalent images on the web is important when using image recognition to search for similar images. In contrast, the popularity of the equivalent images is not important when using a facial recognition tool because it searches for similar facial images, even if they are in different photos. Similarly, the backgrounds and colours are important to find equivalent images when using image recognition, while backgrounds and colours don't affect the facial recognition results. Finally, the AI algorithms for image recognition are not affected by ethnicity bias. In contrast, the AI algorithms for facial recognition are prone to ethnicity bias, especially if they were trained with a non-representative dataset.

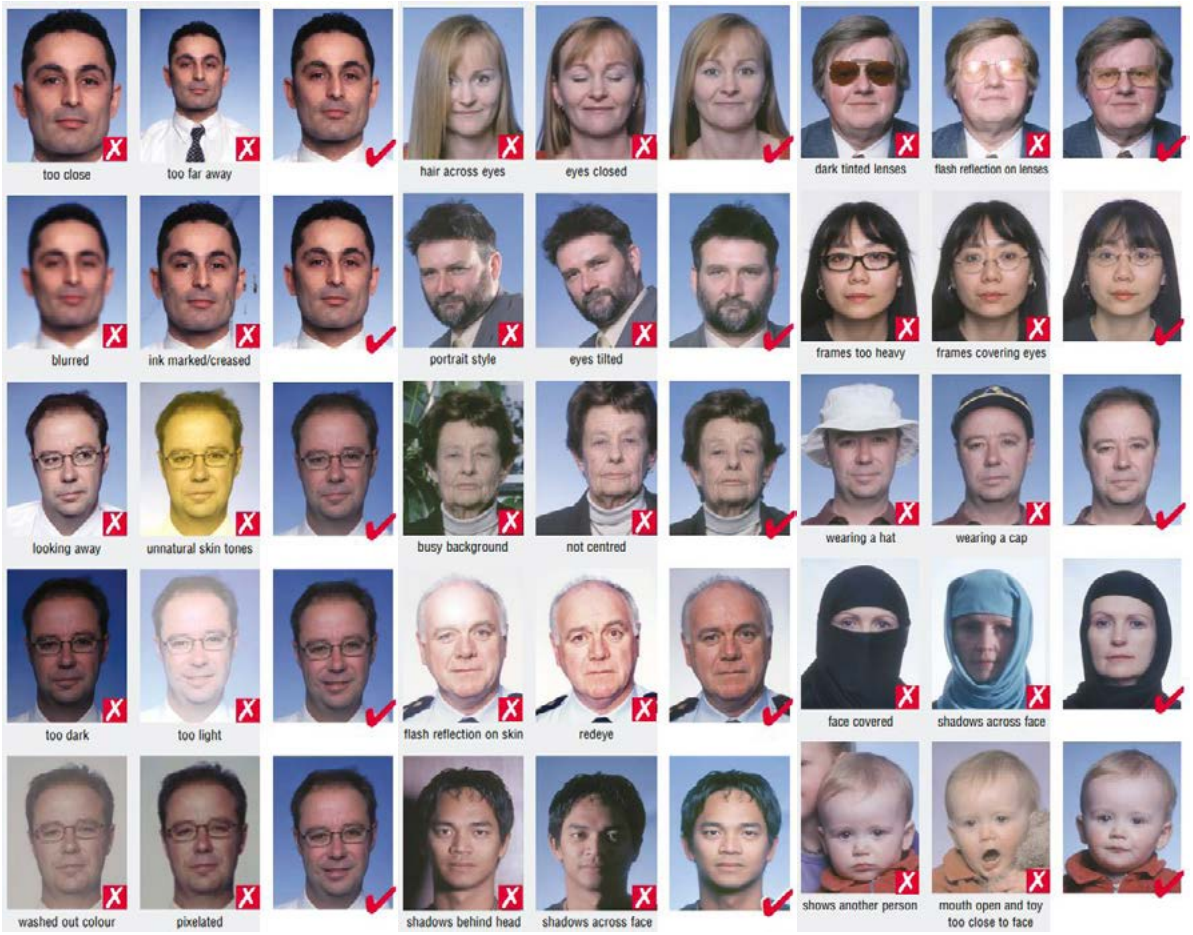
Image Recognition

Artificial Intelligence algorithms for image recognition are used to search for generic and different types of objects. Many image recognition AI algorithms and tools are available publicly and for free, such as Google, Bing, and Yandex. Users can submit an image to search for exactly similar images on the public internet. The detectives and investigators can use such AI algorithms to search and find persons of interest. However, the detectives and investigators should understand the mechanisms, limitations, and factors mentioned in the above table. They should receive high-quality training programs to achieve good results for deciding on multiple and fraudulent identities.

Facial Recognition

Over the last five years, AI has caused a leap in facial recognition technology and is the technology's reason for increasingly accurate results. Nevertheless, new challenges have occurred due to using non-representative data to train the AI algorithms, leading to wrong matches or mismatches. AI algorithms for facial recognition should be trained with representative data that is agnostic of nationality, skin tone, and ethnicity to achieve the target of linking similar identities across the different lists of candidates. The followed approach within the paper is to consider the pre-trained AI algorithms so that the results could be biased. Finally, the AI technology for facial recognition still has technology limitations related to the quality of the submitted images, the stored reference images, and the matching mechanisms. The users should understand the ICAO guidelines for high-quality passport photos (Poon, 2008) and the limitations and effects on matching results related to the distance between eyes, resolution, pose angles, facial expressions, natural skin tone, light exposure, brightness, contrast, and backgrounds. The below images clarify the ICAO guidelines.

Figure 3. ICAO guidelines for high-quality passport photos



The users of the facial recognition AI algorithms should be aware of the facial recognition techniques and the technology limitations and should be trained to achieve the best results from the pre-trained AI algorithms. Furthermore, the users should understand the accuracy levels of the algorithms, the bias of training data, AI mechanisms and demographics, and decide on the correct algorithms that fit the submitted images. The below table shows a comparison between the results of evaluating four commercial AI algorithms for Facial OSINT.

Table 3. Comparing Four Commercial AI Algorithms for Facial OSINT

Facial OSINT	American	Chinese	Polish	Eastern Country
Geographic Area	Americas	China	Europe	Eastern Europe
Identify Sunglasses	Yes	No	No	No
Identify Children	Yes	No	No	No
Ethnicity Bias	White, African, Hispanic	Asian	European	European
Websites Coverage	Criminal Records	Asia	Wide	No
Social Media	Facebook, Instagram, YouTube	No	No	VK, Tik Tok, Clubhouse

Facial recognition was limited to a closed set of internal databases for a few law enforcement agencies, but advanced AI tools were recently developed for Facial OSINT. Facial OSINT means submitting a facial image to search the public internet and revealing the identity of the target person through the data available from open sources such as web pages, blogs, and social media profiles. The table above compares four AI algorithms for facial OSINT from the USA, China, Poland, and an Eastern country. To obtain high-quality results, the detectives and investigators should understand each algorithm's demographics and geographic area. For example, each algorithm has better coverage of the area where it was developed, so the Chinese algorithm will not return any results if the investigator used the Chinese algorithm for querying a facial image of a person living in the US and vice versa for the American algorithm. Also, the investigator needs to understand which algorithm returns the best results if the person in the facial image is wearing dark sunglasses. Only the American algorithm returns good results for people wearing sunglasses, while the other three will either return irrelevant results or no results. For the sensitive cases of child abuse and trafficking in children, it is highly important to find an algorithm that can identify children across the web with high accuracy, and only the American algorithm can do that. Ethnicity bias is an important factor for getting good results for combatting terrorism and serious crime, and, unfortunately, all four algorithms have ethnicity bias. For example, the Chinese algorithm will provide inaccurate results if the ethnicity of the submitted facial image is White, African, or Hispanic. The Polish algorithm has the widest website coverage. In contrast, the American covers websites with criminal records only, the Chinese match results from websites hosted in Asia, and the Eastern algorithm doesn't cover any website except specific social media. Finally, and regarding social media coverage, the American covers Facebook, Instagram, YouTube, and Couchsurfing, the Chinese and Polish don't cover any social media, and the Eastern covers VK, Tik Tok, and Clubhouse.

European UMF Standard (P-O-L-I-C-E)

Clause 51 of regulations (EU) 2019/817 and 2019/818 for interoperability clearly states that: [The implementation of the UMF standard may be considered in VIS, SIS and in any other existing or new cross-border information exchange models and information systems in the area of Justice and Home Affairs developed by Member States.]. The UMF standard is well structured and was developed for exchanging information between law enforcement agencies. Complying with that standard format will help solve the challenges of multiple-identities, fraudulent identities, and cross-border investigations. The below image depicts the P-O-L-I-C-E "Person-Organisation-Location-Item-Connection-Event" format of the UMF structure.

UMF and POLE Pyramid

UMF (Council Regulation proposal (EC) 2018) is key to achieving EU Interoperability and solving the multiple-identity and fraud issues, especially for information concerning crimes and persons of interest; twelve countries have already introduced UMF for use by law enforcement authorities in Europe and beyond. At the same time, Police forces have long used Persons, Objects, Locations, and Events (POLE) to classify crimes. Similarly, UMF uses Person, Item (Object), Location, Event (Offence), and a fifth attribute: Biometric Data.

For example, consider a murder incident where an unknown person was the victim of a shooting. Witnesses later described the suspect as a middle-aged white male with blue eyes and red hair, wearing glasses, a red shirt, and blue trousers. Using POLE, the description is *Person*: victim; murderer (40-50, male, caucasian, blue eyes, red hair, glasses). *Object* (Item): gun; red shirt; blue trousers. *Location*: stadium. *Event* (Offence): murder.

With an eye to the future, UMF can represent the data obtained from surveillance systems. So in the above example, face recognition systems will find facial metadata such as age, gender, glasses, and other physical characteristics. Likewise, video analytics can add more metadata, and it can automatically identify items such as a shirt, trousers, and colours. The POLE data model makes it possible to search and correlate this metadata.

The below figures depict the structure of the UMF standard and the equivalent POLE Pyramid that represents a Person-Centric approach to achieving interoperability.

Figure 4. UMF Structure

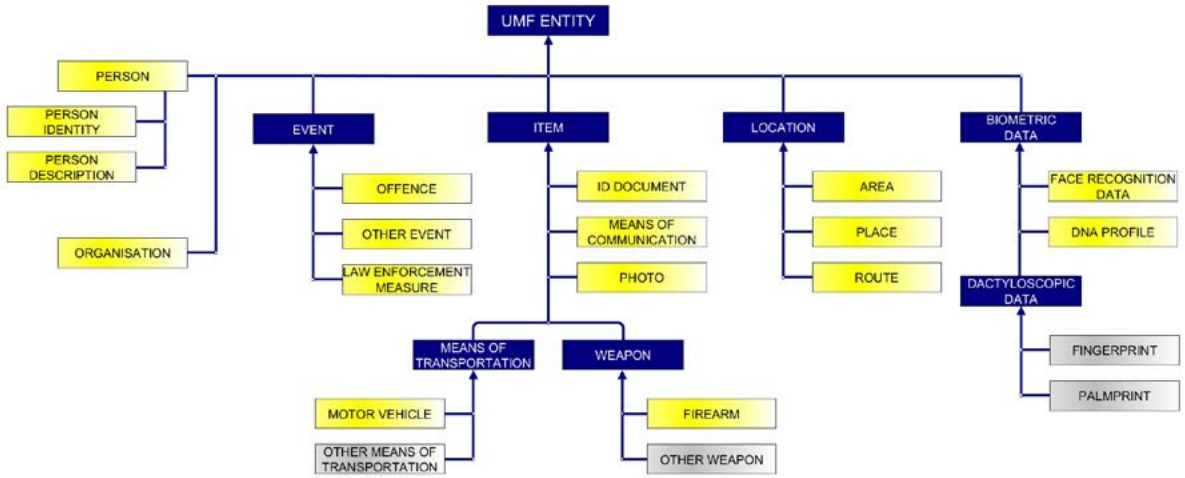
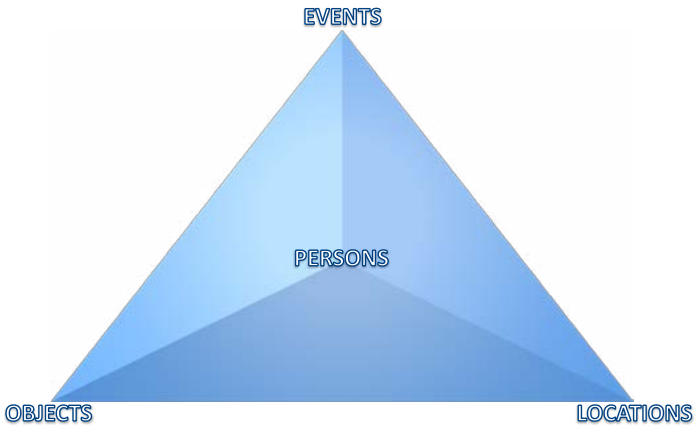
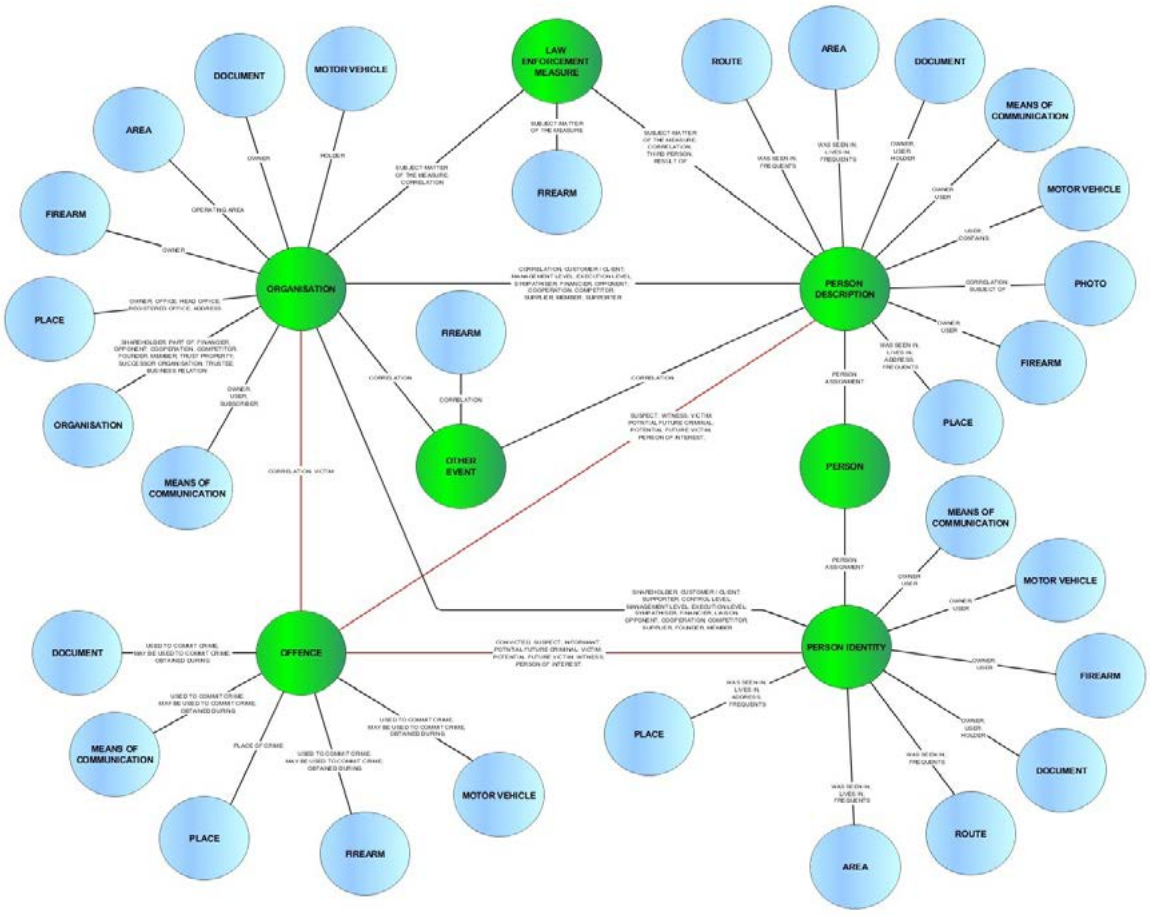


Figure 5. POLE Pyramid



The UMF standard is a Person-Centric representation for criminal investigations. Person-Centric means that all the elements, classes, subclasses, properties, objects, and instances are centred on a person, and revealing a person's identity, such as a suspect, target, or victim, is the optimum target of investigators. The Person-Centric structure is well-understood by law enforcement and border security officers. It can be used for searching or querying databases or exchanging criminal-related information among competent authorities. That structure helps the operational and field officers focus on the functional aspects they understand by heart while avoiding being involved and overwhelmed with learning about the complexity of the technical aspects. For example, biometric-based structures, such as the NIST format for fingerprints, facial images, and iris, focus on data representation and modelling technicalities. They don't highlight the full characteristics of a person. Furthermore, fingerprint and facial NIST formats are only interoperable on the biometric level but not on the higher identity levels. The below image depicts the Person-Centric approach of the UMF standard, where all the items and elements,

Figure 6. UMF Items



such as "Person Description", "Person Identity", Offence, Event, Organisation, Document, Motor Vehicle, Means of Communication, Firearm, Route, Area, and Place, are connected to a "Person".

HORUS Method - UMF Bidirectional Data Mapping

Data mapping and interoperability between the newly established and legacy systems will be required to correctly identify the different encounters of the same passenger across the different watchlists and information systems. The UMF standard can be used for bidirectional API and PNR data mapping with the EES, ETIAS, SIS, and VIS. The UMF "Person Identity" contains the "Person Core Name" to map the passenger's given name, family name, and other names. The value (Yes or No) of the "Primary ID" determines whether the

identity data belongs to the main passenger or the emergency contact. The address structure of the UMF contains "Location" and "Place" to map the passenger's contact address, billing address, mailing address, home address, and intended address. The UMF will map the email address and telephone details to the "Means of Communication" (MoC) item and specify the MoC type and identifier. The "ID Document" item of the UMF will map the travel document information. The UMF "Means of Transportation" (MoT) contains the License Plate Number, VIN, Make, Model, Vehicle Type, and Color to map the vehicle information. Finally, the UMF will map the fingerprints to the "Dactyloscopic Data" and the facial image to the "Face Recognition Data" of the "Biometric Data" item.

The table below depicts using the UMF to map the biographic and biometric data of the passengers with the central EU information systems.

Table 4. UMF Mapping of Air and Sea Passenger Information

Data Group	Data Element	UMF Mapping
Passenger Name Details	Passenger Name	Person Identity → Person Core Name
	Family Name	Person Identity → Person Core Name
	Given Name/Initial	Person Identity → Person Core Name
	Title	
	Other Names	Person Identity → Other Name
Address Details	Emergency Contact	Person Identity → Person Core Name Primary ID = No
	Contact Address	Location → Place → Address
	Billing Address	Location → Place → Address
	Mailing Address	Location → Place → Address
	Home Address	Location → Place → Address
	Intended Address	Location → Place → Address
	Email Address	Item → MoC → MoC Type Item → MoC → MoC Identifier
Contact Telephone Number	Telephone Details	Item → MoC → MoC Type Item → MoC → MoC Identifier
Travel Document Data	Name on Passport	Item → ID Document → MRZ Content
	Date of Birth	Item → ID Document → MRZ Content
	Sex	Item → ID Document → MRZ Content
	Nationality	Item → ID Document → MRZ Content
	Passport Number	Item → ID Document → Document Number
Vehicles Registration	License Plate Number	MoT → Motor Vehicle → VIN
	Car Brand	MoT → Motor Vehicle → Make
	Car Model	MoT → Motor Vehicle → Model
	Body Style	MoT → Motor Vehicle → Vehicle Type
	Color	MoT → Motor Vehicle → Colour
Biometric Data	Fingerprint	Biometric → Dactyloscopic → Fingerprint

Person-Centric OSINT

AI and UMF for enhanced interoperability will be the bridge between Cybersecurity and Biometric Technology. To clarify, linking similar identities from OSINT and the EU information systems can be achieved using a hybrid solution of Knowledge-Based Domain-Specific AI for UMF, NLP and NER for advanced matching identities and AI for facial recognition. All can be done within the legal framework and by considering the regulations for protecting personal data like the GDPR.

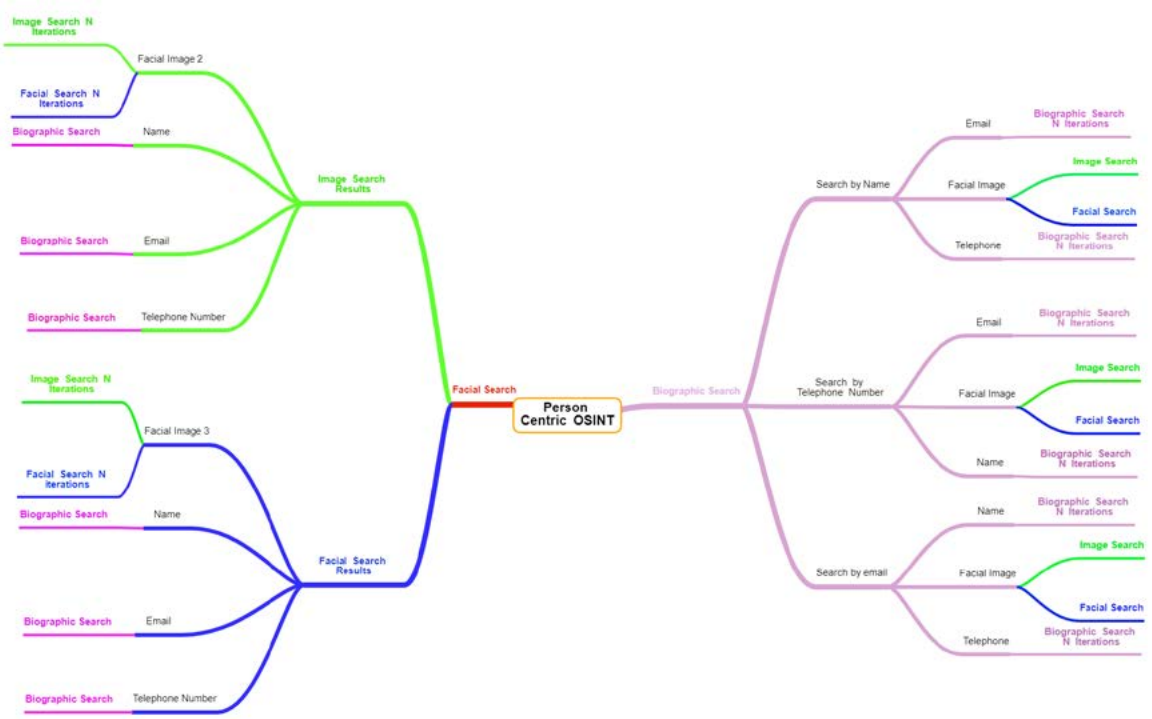
Person-Centric Approach

Person-Centric OSINT constructs the lost bridge between OSINT and biometrics, especially facial recognition. The Person-Centric OSINT approach uses open-source data to investigate cases and assemble their identity footprints to reveal their identities on the internet. The searches will be limited to a biometric search

using a facial image and a biographic search using first name & family name, email address, or telephone number. The cases can be categorised into three groups; the first group of cases is fully identified where the facial image and the identity-related biographic data are known to the investigator, the second group of cases is partially identified where the identity-related biographic data is known. Finally, the facial image is unknown to the investigator, and only the facial image is known for the last group of cases.

Searches will always have a single starting point in the Person-Centric approach, either to start with a facial search or a biographic search. The elements of the results will be submitted for successive iterations of searches until the identity is revealed or more information is gained. For example, the OSINT search could start by submitting a facial image for search using AI tools for image recognition or facial recognition. The result could be a name submitted for the second iteration of the biographic search to reveal an email. The email can be submitted for the third iteration of a biographic search to reveal a telephone number and so on. Another example, the Person-Centric iterations could start with a biographic search using the first name and family name. The result could be a facial image that could be used for the second iteration of a facial search or an email that could be used for the second iteration of a biographic search. The third iteration could fluctuate between a facial or biographic search, based on the obtained results, and so on. The below image depicts the mind map for the recommended iterated Person-Centric OSINT searches.

Figure 7. Mind map for the iterated Person-Centric OSINT searches



Rule-Based Decision Making

The final decision on confirming or rejecting the link between two identities is a human-based decision for that paper. The results are evaluated through a Multi-Attribute Rule-Based decision-making approach (Bohanec, M. and Rajkovic, V., 1999). The investigator can use that approach to identify and decide the similarities and differences between identities. The scale and weight of the rules are subject to change based on continuous studying and evaluating results. The below table depicts a weighted evaluation using a Rule-Based decision-making method for comparing the results of two identities.

Table 5. Multi-Attribute Rule-Based decision-making

Facial Match	Email	Telephone Number	Name	Decision
Different Persons	Different Emails	Different Numbers	Different Name	Different Persons
Different Persons	Different Emails	Different Numbers	Nickname or Variant	Different Persons
Different Persons	Different Emails	Different Numbers	Exact Name	Different Persons
Different Persons	Different Emails	Same Number	Different Name	Investigate more
Different Persons	Different Emails	Same Number	Nickname or Variant	Investigate more
Different Persons	Different Emails	Same Number	Exact Name	Investigate more
Different Persons	Same Email	Different Numbers	Different Name	Investigate more
Different Persons	Same Email	Different Numbers	Nickname or Variant	Investigate more
Different Persons	Same Email	Different Numbers	Exact Name	Investigate more
Different Persons	Same Email	Same Number	Different Name	Same Person
Different Persons	Same Email	Same Number	Nickname or Variant	Same Person
Different Persons	Same Email	Same Number	Exact Name	Same Person
Same Person	Different Emails	Different Numbers	Different Name	Investigate more
Same Person	Different Emails	Different Numbers	Nickname or Variant	Same Person
Same Person	Different Emails	Different Numbers	Exact Name	Same Person
Same Person	Different Emails	Same Number	Different Name	Same Person
Same Person	Different Emails	Same Number	Nickname or Variant	Same Person
Same Person	Different Emails	Same Number	Exact Name	Same Person
Same Person	Same Email	Different Numbers	Different Name	Same Person
Same Person	Same Email	Different Numbers	Nickname or Variant	Same Person
Same Person	Same Email	Different Numbers	Exact Name	Same Person
Same Person	Same Email	Same Number	Different Name	Same Person
Same Person	Same Email	Same Number	Nickname or Variant	Same Person
Same Person	Same Email	Same Number	Exact Name	Same Person

- Red is a low possibility.
- Black is a medium possibility.
- Green is a high possibility.

Conclusion

The major investigation challenges are summarised as multiple-identity, fraudulent actions, lack of interoperability and absence of an effective technical solution for exchanging Cross-Border information, and complexity of OSINT investigations.

The recent global threats such as the increase of illegal immigration, the high risks of terrorism and serious crime, the COVID-19 pandemic, and the war between Russia and Ukraine created the essential need for exchanging Cross-Border information for preventing, detecting, and investigating terrorism and serious crime across Europe and the neighbouring countries.

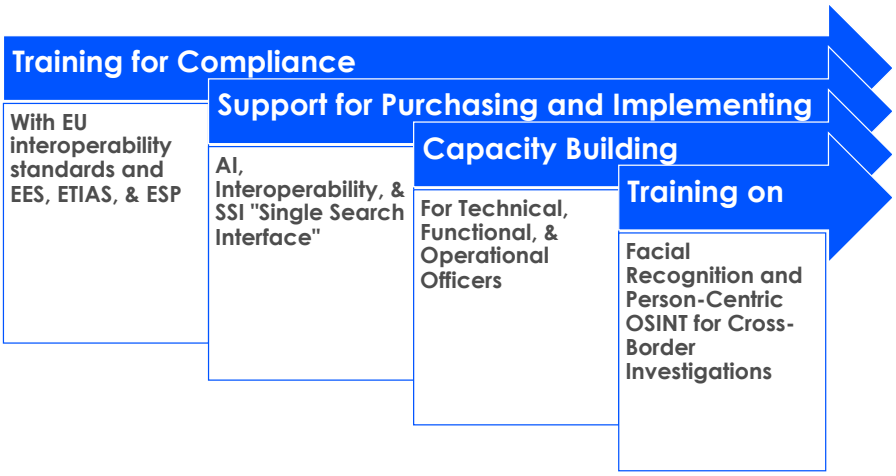
Providing high-quality training for law enforcement officers is an essential step for solving the investigation challenges. Importantly, *the training programs should contain Artificial Intelligence mechanisms, limitations, and demographics, and it is recommended to cover the proposed Person-Centric OSINT approach.*

Moreover, the training programs for each EU and non-EU Member State are recommended to include the following: Training for compliance with the EU interoperability regulations and standards and the new EU systems such as the EES, ETIAS, and ESP, Providing support for purchasing and implementing Artificial Intelligence, interoperability, and SSI "Single Search Interface", Capacity building for the border security and law enforcement agencies' technical, functional, and operational officers, and Training on facial recognition,

facial OSINT, and Person-Centric OSINT for cross-border investigations.

Finally, the training tools should include mock trials and criminal case simulation, and the training syllabuses should cover using modern technologies and digital skills for solving the challenges of multiple-identity, fraud, and cross-border investigation. The below image depicts the recommendations.

Figure 8. Recommendations for Member States



References

- Bohanec, M. & Rajkovic, V. (1999) Multi-attribute decision modeling: Industrial applications of DEX. Informatica (Ljubljana), 23(4), pp.487-491.
  Available at: https://kt.ijs.si/MarkoBohanec/pub/Inform99.pdf [Accessed 13 July 2022]
- Council Regulation (EC) No 2019/817 of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa.
  Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0817 [Accessed 7 July 2022]
- Council Regulation (EC) No 2019/818 of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration.
  Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0818 [Accessed 7 July 2022]
- Council Regulation (EC) No 2019/816 of 20 May 2019 on establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons.
  Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0816 [Accessed 7 July 2022]
- Council Regulation (EC) No 2017/2226 of 30 November 2017 on establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States.
  Available at: https://eur-lex.europa.eu/legal-/EN/TXT/?uri=CELEX%3A32017R2226 [Accessed 8 July 2022]
- Council Regulation (EC) No 2018/1862 of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters.
  Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018R1862 [Accessed 8 July 2022]
- Council Regulation (EC) No 603/2013 of 26 June 2013 on the establishment of ·Eurodac· for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013.
  Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32013R0603 [Accessed 8 July 2022]
- Council Regulation (EC) 2018/1240 of 12 September 2018 on establishing a European Travel Information and Authorisation System (ETIAS).
  Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1240 [Accessed 8 July 2022]
- Council Regulation amended proposal (EC) No 2018/480 of 13 June 2018 on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) and amending regulations.
  Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0480&from=EN [Accessed 10 July 2022]

- Council Regulation proposal (EC) No 2021/0106 on 21 April 2021 for laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts of 21 April 2022.
  Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206[Accessed 11 July 2022]
- European Commission, Directorate-General for Migration and Home Affairs (2018) *Feasibility study of a Common Identity Repository (CIR): management summary.* Publications Office.
  Available at: https://data.europa.eu/doi/10.2837/330396
- European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (2018) *Shared Biometric Matching Service (sBMS): feasibility study - final report*. Publications Office.
  Available at: https://data.europa.eu/doi/10.2857/84504
- European Council: Council of the European Union (2019) *Interoperability between EU information systems: Council adopts regulations.*
  Available at: https://www.consilium.europa.eu/en/press/press-releases/2019/05/14/interoperability-between-eu-information-systems-council-adopts-regulations/ [Accessed 10 July 2022]
- Europol (2014) Universal Message Format: faster, cheaper, better. Publications Office.
- Poon, J. (2008) Annex A Photograph Guidelines.
  Available at: https://www.icao.int/Security/mrtd/Downloads/technical%20reports/annex_A-photograph_guidelines.pdf [Accessed 8 July 2022]
- Sawalha, M., Brierley, C. & Atwell, E. (2014) Automatically generated, phonemic Arabic-IPA pronunciation tiers for the Boundary Annotated Qur'an Dataset for Machine Learning (version 2.0). *In Proceedings of LRE-Rel 2: 2nd Workshop on Language Resource and Evaluation for Religious Texts, post-conference workshop (LREC 2014)*, Reykjavik, Iceland, 31 May (pp. 42-47). https://doi.org/10.13140/2.1.2887.2640
- Yusof, R.R., Zainuddin, R., Baba, M.S. & Yusoff, Z.M. (2010). Qur'anic words stemming. *Arabian Journal for Science and Engineering*, *35*(2), pp.37-49.
  Available at: https://www.researchgate.net/publication/298945997_QUR%27ANIC_WORDS_STEMMING [Accessed 12 July 2022]

About Developing a Cross-Check System for Judicial Case Searching and Correlation

Gerardo Giardiello
Fabrizio Turchi
Institute of Legal Informatics and Judicial Systems,
National Research Council of Italy (CNR-IGSG)[1]

Abstract
In a recent EU publication, a report commissioned by the European Union related to the Cross-border Digital Criminal Justice environment, a set of specific business needs have been identified. Some of the most relevant ones have been: i) the interoperability across different systems needs to be ensured, ii) the stakeholders need to easily manage the data and ensure its quality, allowing them to properly make use of it (e.g. use the data as evidence in a given case) and iii) the stakeholders investigating a given case should be able to identify links between cross-border cases. Therefore, solutions are needed to allow the stakeholder to search and find relevant information they need for the case they are handling. The article presents a set of solutions to address the highlighted needs, including a 'Judicial Cases Cross-Check System'. Such a system should provide a tool being able to search for case-related information and identify links among cases that are being investigated in other EU Member States or by Justice and Home Affairs (JHA) agencies and EU bodies. To facilitate the development of the above solution, a standard representation of the metadata and data of the evidence should be adopted. In particular the Unified Cyber Ontology (UCO) and Cyber-investigation Analysis Standard Expression (CASE), dedicated to the digital forensic domain, seem the most promising one to this aim. Moreover it provides a structured specification for representing information that are analysed and exchanged during investigations involving digital evidence.

Keywords: Judicial Case Correlation, Evidence Standard, Case Ontology, Judicial Investigation

Introduction

A recent report prepared for the European Commission on Cross-border Digital Criminal Justice (Debski et al. 2020), has highlighted how the modernisation of judicial cooperation is paramount for an efficient fight against crime in view of the rapid progress of the technologies and their potential malicious or threatening use. EU Member States and Justice and Home Affairs (JHA) agencies stressed the need to be able to search for case-related information and identify correlations with cases under investigation in other EU Member

1 Authors' emails: gerardo.giardiello@igsg.cnr.it, fabrizio.tuchi@igsg.cnr.it.

States/JHA agencies and EU bodies. To accomplish that goal and devise a technical solution, it is important to address all the issues raised by the involved stakeholders, of which the most important are:

- Is it acceptable, for all Member States, to maintain a central criminal cases database considering the potential data protection issues?
- Would a central database require a legal basis?
- Keeping information/evidence at national level and providing query system from abroad might be an alternative solution but would it generate a duplication of the same data being stored in multiple systems?

In this article none of the above issues will be addressed, instead the focus will be put on the standard representation of the metadata and data of a piece of evidence, based on an ontology that has been developing as an open and cost-free resource for the digital forensic community in a broad sense, including all the stakeholders involved in cross-border judicial cooperation.

Nevertheless, the adoption of the standard (see Section "The UCO/CASE standard") would facilitate both central and distributed technical solutions. In the case of a central solution, the first option, it is easy to imagine how powerful a system can be, considering that each digital trace would be represented in the same formally structured manner. In the second option, the distributed solution, the investigative information could be easily retrieved relying on the metadata representation of the pieces of evidence, also taking into account that UCO/CASE provides specific explicit ontology properties to support appropriate handling of shared information, based on the Information Exchange Policy[2] or the Traffic Light Protocol,[3] and also on enhancing data protection and intelligent analysis of digital evidence (Casey, E., Barnum, S., Griffith, R., Snyder, J., van Beek, H. & Nelson, A. (2017).

The UCO/CASE standard

UCO[4] stands for Unified Cyber Ontology, a foundation for standardized information representation across the cyber security domain; CASE[5] that stands for Cyber-Investigation Analysis Standard. UCO/CASE provides a standard language, actually a set of ontologies, for representing information collected, extracted, analysed and exchanged during investigations involving digital evidence. UCO/CASE is a community-developed ontology designed to provide a standard for interoperability and analysis of investigative information in a broad range of cyber-investigation domains, including digital forensic science, incident response, counter-terrorism, criminal justice, forensic intelligence. The UCO/CASE community is a consortium of academic, government and law enforcement, plus commercial and non-profit organisations. To perform digital investigations effectively, there is a pressing need to harmonise how information significant to cyber-investigations is represented and exchanged. UCO/CASE enables the merge of information from different data sources and forensic tool outputs to allow more comprehensive and cohesive analysis (Casey et al., 2018). The main UCO/CASE goals are:

- to foster Interoperability between digital investigation systems and tools;
- to automate normalisation and combination of differing data sources to facilitate analysis and exploration of investigative questions (who, when, where, what, etc.), maintaining provenance at all phases of digital investigation lifecycle;
- to ensure all analysis results are traceable to their sources (Chain of Evidence).

The first two points foster the development of a Judicial Cases Cross-Check system for case searching and correlation, based on the interoperability and normalisation of the data and metadata. The last point is more connected to the admissibility of a piece of evidence because it reveals which file a relevant digital trace comes from.

2 Information Exchange Policy (IEP), https://www.first.org/iep

3 Traffic Light Protocol Definitions and Usage, https://www.cisa.gov/tlp

4 Unified Cyber Ontology (UCO) A foundation for standardized information representation across the cyber security domain/ecosystem, see unifiedcyberontology.org.

5 An international standard supporting automated combination, validation, and analysis of cyber-investigation information, see caseontology.org.

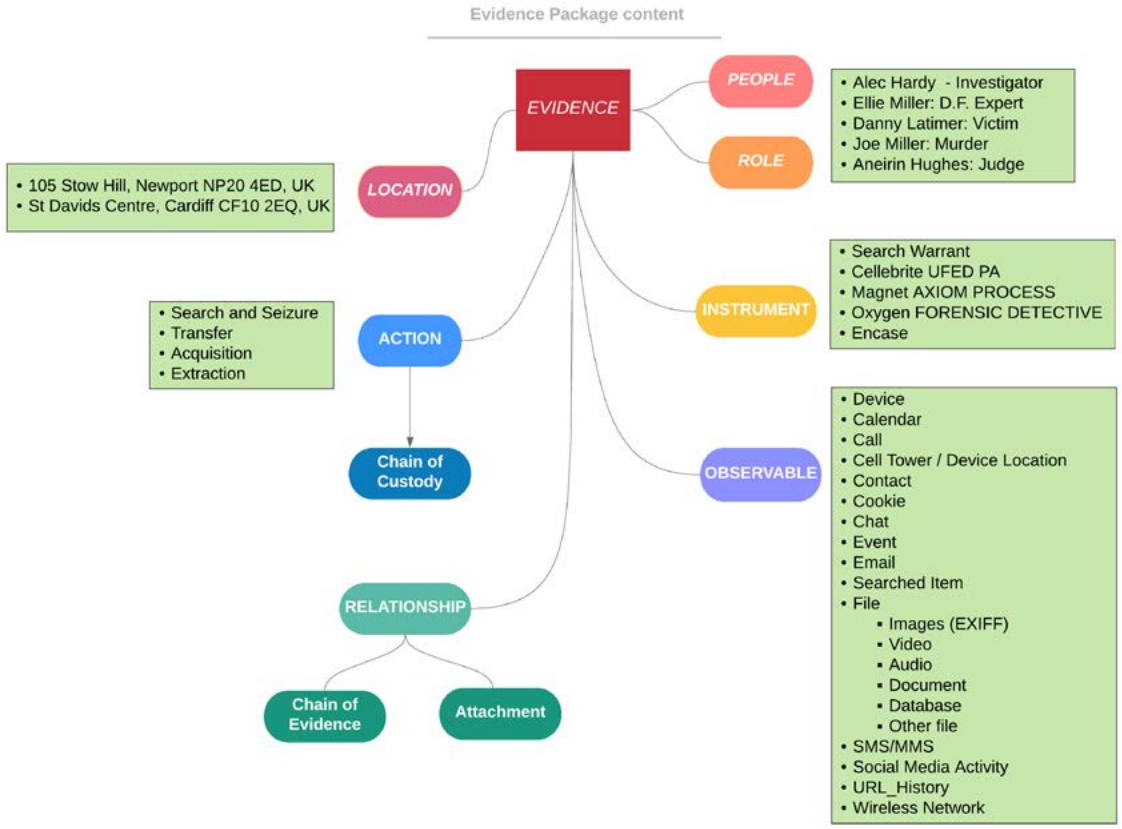
These features allow significant advantages because they comprise a wider view of the need for representing relevant cyber information and the adoption of more neutral solutions without promoting proprietary models. On the other hand, the approval of change proposals or the implementation of new cyber items to be included in the ontologies is quite slow because a broad consensus is needed/required from all the members of the community.

UCO/CASE ontology classes

The ontologies consist of the following main classes (see Figure 1):

- People involved in the evidence life-cycle, from search and seizure to the report before the Court, technical and legal (subjects, victims, authorities, examiners etc.).
- Surrounding information about Legal authorization (i.e., search warrant).
- Information about the Process/Lifecycle (i.e. seizing, acquisition, analysis etc.).
- Information about the Chain of custody by identifying Who did What, When and Where from the moment the Evidence has been gathered.
- Actions performed by people (seizing, acquisition, analysis etc.).
- Source of evidence, that is physical objects involved in the investigative case (e.g., hard disk, smartphone) but even digital source of evidence (i.e., memory dump).
- Description of the Objects inside the digital evidence and their Relationships (e.g., *Contained_Within, Extracted_From* etc.).

Figure 1: UCO/CASE ontology, main Classes (Source: by authors)



UCO/CASE to meet investigation needs

The need for a standard to represent and exchange electronic evidence has been augmented by the rising relevance of the digital evidence in a wide range of circumstances within investigative cases and the requirement upon a standard language to represent a broad range of forensics information and processing results has become an increasing need within the forensics community (Casey, 2011). The standard language is also able to meet another pressing need: processing big volumes of investigative information from different various data sources and finding correlation within them in an accurate and efficient manner. Research activities conducted in this field have been used to develop and propose many languages, but, at the moment, UCO/CASE represents the most suitable standards to representing data and metadata related to evidence for a variety of goals including the availability of a more powerful processing relying on artificial intelligence techniques. This is due to the following reasons:

- it has been developed in the cyber security environment but it also includes lots of essential elements to representing digital forensics information;
- it allows to describe technical, procedural and judicial information as well;
- it has been developed with the extensibility in mind so it is adaptable to the fast-pace development of technology, therefore permits the introduction of new elements to incorporate forensics information not envisaged yet.

It is also worth mentioning that UCO/CASE standard is able to represent the provenance of an evidence. For cyber-investigation purposes, to help establish the authenticity and reliability of information, it is important to capture where it originated or was found, as well as how it was handled after it was found. Provenance includes collection documentation, chain of custody details, audit logs from forensic acquisition tools, and integrity records, which all help to establish the trustworthiness of cyber-investigation information (Casey et al., 2017).

UCO/CASE and other standards

It is worth mentioning that existing standards for exchanging general criminal justice information, including the National Information Exchange Model (NIEM), have not kept pace with the evolution of electronic evidence. Moreover, there are there some similarities between the UCO/CASE standard and ISO/IEC 27037:2012 (Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence). ISO standards developed for Information Security (2700 series) and Forensic Science (ISO/TC 272 Forensic sciences) provide high level requirements and recommendations for specific practices/processes. Nevertheless, they do not provide a standard for representing and exchanging data. On the contrary UCO/CASE can be used to implement and strengthen certain requirements illustrated in ISO standards to fulfil the objectives of efficiency and quality.

It should be also highlighted that the UCO/CASE standard language that has become popular among many important stakeholders such as Europol, U.S. Department of Defence Cyber Crime Centre - DC3, NFI, Cellebrite, Magnet Forensic and others.

Another UCO/CASE feature worthy of attention is that the standard language has been recently moved under the Linux Foundation: a quite remarkable news that encourages widespread use of this standard in a broad range of cyber-investigation domains to foster interoperability, establish authenticity, and advance analysis.

The UCO/CASE standard has been used in many European projects, among which it is worth mentioning:

- Intelligence Network & Secure Platform for Evidence Correlation and Transfer[6] (INSPECTr, GA 833276). It aims at developing a shared intelligent platform for gathering, analysing and presenting key data to help in the prediction, detection and management of crime in support of many LEA at local, national and international level. The data will originate from the outputs of free and commercial forensic tools integrated by online resource gathering. The data

6 INSPECTr Project, Intelligence Network & Secure Platform for Evidence Correlation and Transfer. The principal objective of INSPECTr will be to develop a shared intelligent platform and a novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime in support of multiple agencies at local, national and international level, see https://inspectr-project.eu.

from the tools will be represented in UCO/CASE standard using a set of parsers still under development for Cellebrite UFED_PA, Magnet Forensic AXIOM, MASB XAMN and OXYGEN Forensic Detective.

- Electronic Xchange of e-Evidences with e-CODEX[7] (EXEC II, GA INEA/CEF/ICT/A2019/2065024). Within the project's activities it has been developed a proof of concept (Evidence Exchange Standard Application, EESP Application) being able to create/prepare the Evidence Package (E-Package), safely encrypted, for facilitating its exchange through e-EDES and over e-CODEX and being able to support a standard for the representation of metadata of the Evidence, by using the UCO/CASE language/ontology to propose sensible solutions for the exchange of large file of evidence, based on a decentralised architecture

- Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe[8] (EVIDENCE2e-Codex, GA 766468): the project provided a contribution to the exchange of digital evidence within the EIO/MLA legal instruments among Competent/Judicial Authorities in the EU Member States and beyond.

UCO/CASE main aims

One of the most common issues in dealing with the outcome of a forensic acquisition or analysis, concerns the possibility to verify findings extracted/generated by forensics tools. This need is becoming even clearer considering the ever-increasing speed of innovation involving digital devices and the consequences on forensics tools (i.e., operating system, data storage strategies, etc.). The lack of a standardised format for representing the output of forensics tools makes it difficult to compare results produced by different tools with similar features/functionalities. The use of a common standard language would offer many advantages:

- it would allow comparing results produced by different versions of the same forensics tool in order to evaluate the progress in terms of information extraction and interpretation;

- it would speed the automatic search activity avoiding analysing the same information already processed by the previous version of the tool;

- it would foster the data and information exchange between different organisations and different actors involved in the investigation.

At the moment no commercial forensic tool is able to directly generate their output in UCO/CASE standard. The UCO/CASE community is endeavouring to create a middle-layer software (parser) to convert the output from an open format (i.e., XML, CSV etc.) generated by the commercial tool into UCO/CASE standard. At the time of writing this article a parser for both Cellebrite UFED-PA and Magnet Forensic AXIOM is available in UCO/CASE repositories,[9] freely accessible to all Community members and broadly to all forensic community.

An investigation generally involves many different tools and data sources, therefore pulling together information from these various data sources and tools is time consuming, and error prone. Tools that support UCO/CASE can extract and ingest data, along with their context, in a normalized format that can be automatically combined into a unified collection to strengthen correlation and analysis.

Moreover, cyber-investigation information, to be effective, needs to be represented and shared in a form that is usable in any contexts (i.e., digital forensic science, incident response, and situational awareness etc.) and is flexible enough to accommodate evolving requirements.

The main aim of UCO/CASE is the interoperability - to enable the exchange of cyber-investigation information between tools, organizations, and countries. The power of such a standard is that it supports automated

7 The EXEC II project (Electronic Xchange of e-Evidences) is the follow-up project of the previous EXEC and EVIDENCE2-e-CODEX projects. See https://www.e-codex.eu/EXECII.

8 The EVIDENCE2e-CODEX project aimed at creating a legally valid instrument to exchange digital evidence related to MLA and EIO procedures over e-CODEX by providing the legal and technical communities with 'ready to use' information on EIO, digital evidence and e-CODEX and a 'true to life' example of how electronic evidence can be shared over e-CODEX in a secure and standardized way to support MLA and EIO cases, see https://evidence2e-codex.eu.

9 The XML SAX parser for UFED/Cellebrite extracts some digital traces (Cyber items) from XML reports generated by UFED Physical Analyser (version 7.x) and convert them into UCO/CASE as JSON-LD files, see https://github.com/casework/CASE-Implementation-UFED-XML and https://github.com/casework/CASE-Implementation-AXIOM.

normalization, combination correlation, and validation of information, which means less time extracting and combining data, and more time analysing information. The interoperability is ensured not only within a single investigative case that may include many digital devices, but also throughout different investigative cases to find correlation and overcome, for instance, issues like the linkage blindness that is the failure to recognise a pattern that links one crime to another, such as crimes committed by the same perpetrator in different jurisdictions.

UCO/CASE observables

To represent cyber-investigations information, it is necessary to capture details about specific traces and their context such as manufacturers and serial numbers of storage media, network connection details, and names of files stored on a removable USB device with associated date-time stamps and cryptographic hash values. To represent this variety of information, as well as other non-trace cyber-investigation information (identities, locations, tools, etc.), UCO/CASE defines "Objects" and potentially associated "Property Bundles" containing details about the object itself.

Objects encompass any concept pertaining to cyber-investigations including traces such as a mobile device, a file extracted from a device, an email address extracted from a file, a location extracted from EXIF metadata, or non-trace concepts such as a forensic action carried out by an examiner.

UCO/CASE is able to represent certain types of information that cross the cyber domain as core entities. They consist of a set of data and metadata for describing (see Figure 6) the following items:

- Objects and their associated properties, including data sources (mobile devices, storage media, memory) and well-known digital objects such as files and folders, messages, documents, files (images, video, audio etc.) and logs (browser history, events).
- A set of data and metadata for describing all actions (i.e., tasks).
- Actors (e.g.: subjects, victims, authorities, examiners etc.).
- Tools (i.e., digital tools for carrying out different forensics processes).
- Objects relationships (e.g., Contains, Extracted From etc.), in particular for expressing the Chain of Evidence, that is which file (archive, database, etc.) a specific digital trace (Observable in term of the ontologies) has been extracted from.
- Objects inside the digital evidence and their Relationships (e.g., Contained_Within, Extracted_From etc.).

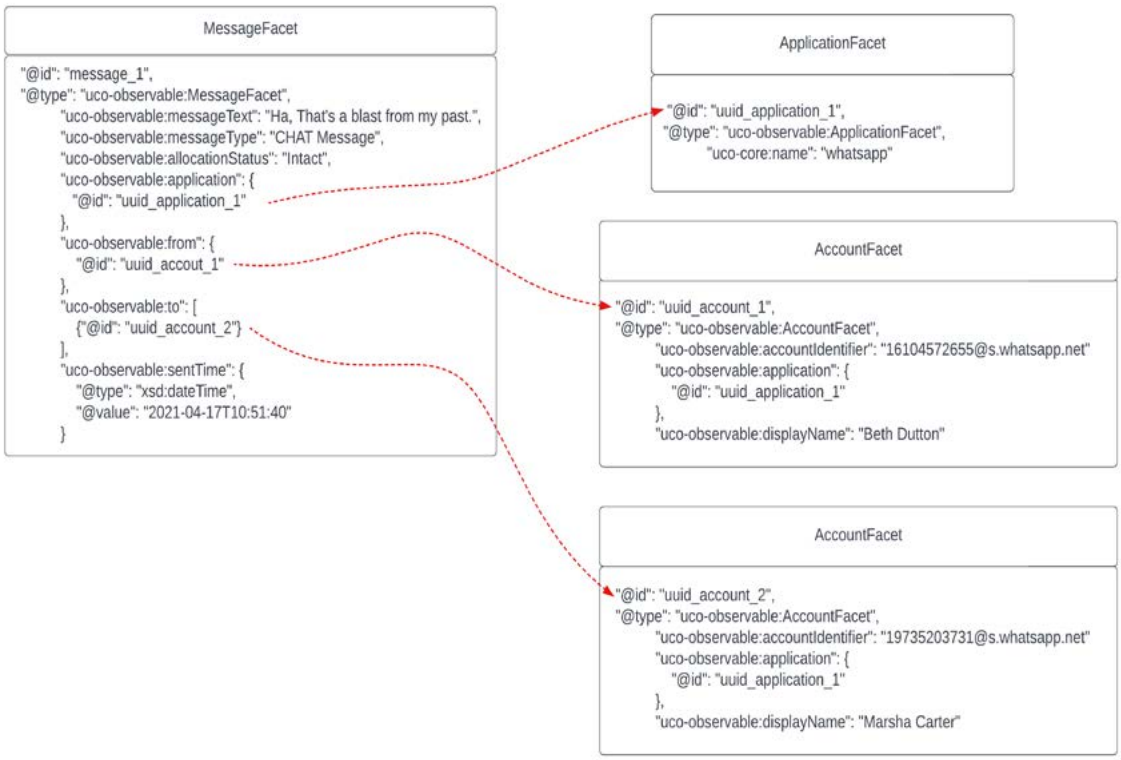
CASE supports any serialisation (default JSON-LD),[10] and can be utilised in any context, including criminal, corporate and intelligence. JSON-LD is 100% valid JSON with some specific JSON structures defined which allow full structural and semantic validation of each object, array and field in the JSON content to a relevant ontological specification for that element.

Each Object is assigned an identifier (@id) that can be used to refer to the Object that cannot be changed that points to another Object, representing a relationship to that other Object. In the proposed approach, such references are represented using an embedded property that specifies the @id of another Object.

Figures 2, 3 and 4 show a CHAT message, represented in CASE and serialised in /JSON-LD format, along with the references to an Application Account and Application Observable Objects that contain the Accounts involved in the communication (Message) and the Application in use.

10 JSON-LD is a lightweight Linked Data format. It is easy for humans to read and write. It is based on the already successful JSON format and provides a way to help JSON data interoperate at Web-scale. JSON-LD is an ideal data format for programming environments, REST Web services, and unstructured databases such as Apache CouchDB and MongoDB, see https://json-ld.org.

Figure 2: UCO/CASE representation of a Chat Message, along with Account and Application Observables (Source: by authors)



Correlations examples

An investigation generally involves many different tools and data sources, creating separate store-room of information. Manually pulling together information from these various data sources and tools is time consuming, and error prone. Tools that support CASE can extract and ingest data, along with their context, in a standard format that can be automatically combined into a unified collection to strengthen correlation and analysis. This offers new opportunities for searching, contextual analysis, pattern recognition, machine learning, and visualisation. Moreover, organisations involved in joint investigations can share information using CASE.

In addition to searching for specific keywords or characteristics within a single case or across multiple cases, having a structured representation of cyber-investigation information allows more sophisticated processing such as data mining, or NLP techniques.

A crucial aspect of information representation and exchange is being able to specify the allowed/authorised conditions for sharing and to enforce exchange policies. At this aim UCO/CASE provides for data markings that CASE can use to support proper handling of shared information: practically any marking mechanism can be employed, including Traffic Light Protocol (TLP) and Information Exchange Policy (IEP).

Overall system

The potentialities of the system, illustrated trough the below examples, and explained in a descriptive manner are underpinned by the following conditions:

- having at disposal a shared criminal cases database either based on a decentralised solution, or a central solution, including both metadata and data of the pieces of evidence. It is almost needless to say that the issues of location and jurisdiction need to be addressed, taking into account the increasingly frequency of cross-border crimes;

- a common format (UCO/CASE ontology) for data homogenisation and data discovery. Once the information is represented in a format not tied to a proprietary system where the possibilities to develop tailored tools are all open to each need that can arise.

Correlation example: ascertain if a file has been exchanged during communication between two suspects, relying on the hash file value

The investigative context is the following: two mobile devices, belonging to two suspects, have been seized and the investigative aim is to discover if a specific file, whose hash value HASH_1 is known, has been exchanged between the two devices (DEVICE_1 and DEVICE_2). The data extracted from the DEVICE_1 is not complete; the sought communication has been deleted by the SUSPECT_1 and the carved data, extracted by using a forensic tool, don't allow the potential evidence to be found because is incomplete.

To bear in mind that the example refers to the same investigative case, but the sought data could also be retrieved throughout different investigative cases, provided that the two requirements described above at the beginning of Section 3.1, are met.

Considering how the Artifact/Digital Traces are expressed in UCO/CASE the retrieval process is the following (see Figure 3):

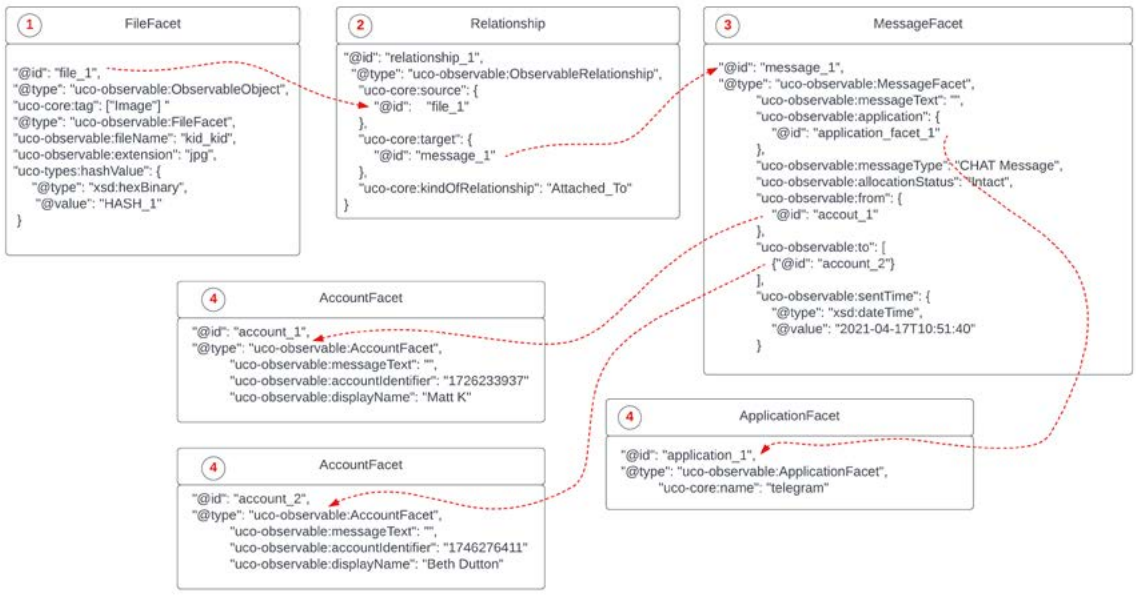
- The HASH_1 is scanned among all the File Observables of the shared database, serialised in JSON format. From this Observable the unique identifier (UUID_FILE) is taken, an identifier that is associated with each Observable.
- The Relationships Observables of kind "Attached_To" are raked to find the value UUID_X in the source property. Once that Observable has been identified its target property, the unique identifier (UUID_MESSAGE), is obtained. That Observable is a Chat/Message, that had the file as an attachment.
- By using the UUID_MESSAGE it is possible to detect the Message Observable and in turn the phone numbers involved in the communication, relying on the properties FROM and TO, always expressed as @id references.
- By retrieving the @id of the two identifiers involved in the Chat/Message Telegram it turns out that the two people who exchange the file with the hash HASH_1 are the ones identified by the following properties:

  PERSON_1: *accountIdentifier*=1726233937 and *displayName*=Matt K

  PERSON_2: *accountIdentifier*=1746276411 and *displayName*=Beth Dutton

that are the suspects under investigation.

Figure 3: Correlation example based on hash file, retrieval process based on UCO/CASE, overview (Source: by authors)



Correlation example: to find any kind of outgoing communication originating from a given phone number

The investigative context is the following: starting from a lot of seized devices, the correlation aims to find any kind of outgoing communication originating from the phone number PHONE_NUM_1. The phone number will be searched in Call, SMS, MMS and Chat Messages selecting only the ones where the PHONE_NUM_1 plays the role of Caller/Sender property.

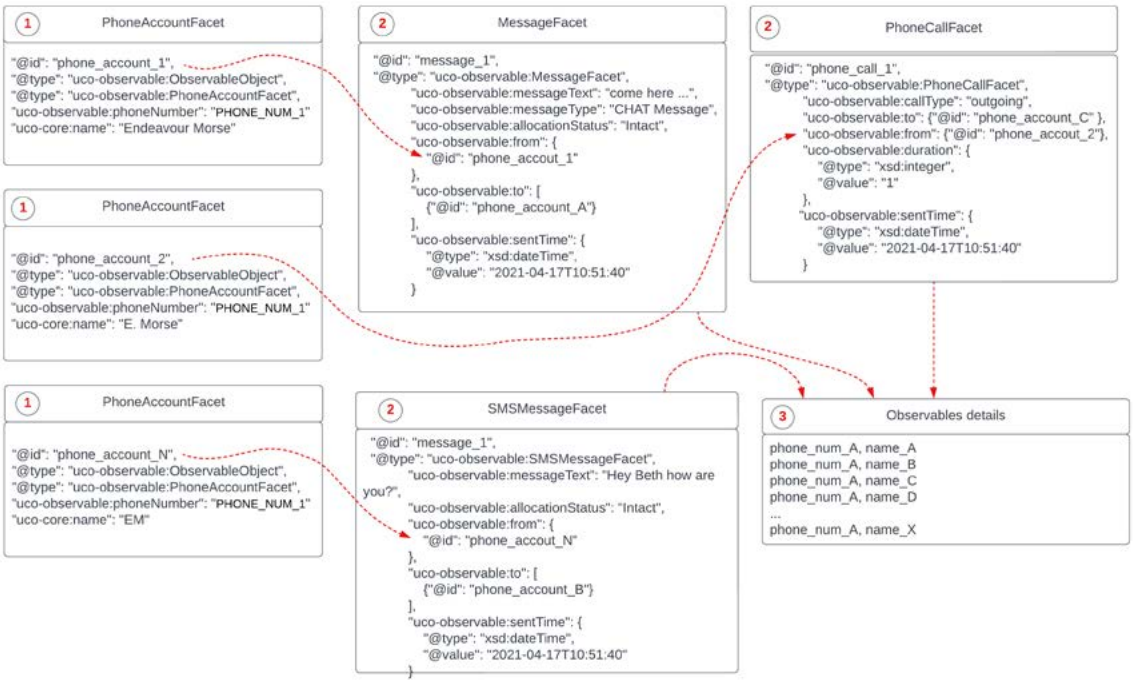
The retrieval process is the following (see Figure 4):

1. The phone number PHONE_NUM_1 is dug among all the Phone Account Observables of the shared criminal cases database. From the list of the retrieved Observables, all the unique identifiers (UUID_PHONE_NUM_1, UUID_PHONE_NUM2, …, UUID_PHONE_NUM_N) are taken.

2. All the UUID_PHONE_NUM_X identifiers selected in the previous step are searched in the FROM property of all Observables of kind PhoneCallFacet, SMSMessageFacet, MMSMessageFacet and MessageFacet (Chat).

3. The details of each retrieved Observable are presented below (Figure 4, frame labelled with number 3) along with the data related to the people involved in each communication item spotted.

Figure 4: Correlation example based on phone number, retrieval process based on UCO/CASE, overview (Source: by authors)



Conclusions

To perform digital investigations effectively, there is a pressing need to harmonise how information relevant to cyber-investigations is represented and exchanged. The CASE specification language and underlying UCO support information standardization and interoperability for tools and organizations dealing with cyber-investigations. In addition to sharing cyber-investigation information on a specific case, sharing traces or patterns of particular activities in a standardized format can help others find similar traces and patterns in new cases, both in national and international judicial cooperation.

The standard is one of the most effective formalisms to represent data and metadata of an evidence and it appears particularly versatile to both a central criminal cases database and distributed databases incorporated into national systems. Moreover, it encompasses relevant aspects: it allows to indicate the grade of information sharing, preserving their privacy, and also to strengthen the admissibility of a potential evidence based on the detailed description of its Chain of Document and Chain of Evidence.

This article has illustrated a draft retrieval system based on the open and free UCO/CASE language standard highlighting the significant advantage provided by the standard, especially considering alternative proprietary systems that are closed and hinder the interoperability among different systems and various organisations. A significant example of the use of the standard has been implementing within the INSPECTr project, by using ElasticSearch[11] as storage of the data represented in UCO/CASE and Kibana as a user interface to visualize the evidence data and navigate the Elastic Stack.

Having at its disposal a standard representation would streamline the investigations and improve the effectiveness of the search for correlation within different cases both in national and cross-border scenarios. Such a system would also be beneficial for joint investigation team (JIT) scene where it is of utter importance to efficiently carry out criminal investigations in one or more of the involved States, achieving one of the main impacts of the use of the standard: to dedicate less time extracting and combining data and more time analysing info to find links and patterns.

References

- Casey, E. (2011) "Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet". 3rd edition, Elsevier, Amsterdam.
- Casey, E., Barnum, S., Griffith, R., Snyder, J., van Beek, H. & Nelson, A. (2017) Advancing coordinated cyber- investigations and tool interoperability using a community developed specification language, *Digital Investigation,* vol. 22, pp.14–45.
- Casey, E., Barnum, S., Griffith, R., Snyder, J., van Beek, H. & Nelson, A. (2018) The Evolution of Expressing and Exchanging Cyber-Investigation Information in a Standardized Form. In: Biasiotti, M., Mifsud Bonnici, J., Cannataci, J., Turchi, F. (eds) Handling and Exchanging Electronic Evidence Across Europe. Law, Governance and Technology Series, vol 39. Springer, pp. 43-58.
- Casey, E., Biasiotti. M.A., Turchi, F. (2017) "Using Standardization and Ontology to Enhance Data Protection and Intelligent Analysis of Electronic Evidence", ICAIL 17, DESI VII Workshop on "Using Advanced Data Analysis in eDiscovery & Related Disciplines to Identify and Protect Sensitive Information in Large Collections", Strand Campus, King's College London, UK, pp. 10.
  Available at: http://users.umiacs.umd.edu/~oard/desi7/papers/EC.pdf
- Debski T., Heimans D., Verheggen H., Bille W. & Kamarás E. (2020) "Cross-border Digital Criminal Justice, Final Report", by Deloitte, Luxembourg: Publication Office of the European Union.
  Available at: https://www.legalbusinessworld.com/post/report-xbordercriminaljustice

11 Elasticsearch is a distributed, JSON-based search and analytics engine, https://www.elastic.co.

Towards AI-backed Digital Investigation

Mobile Forensics and Digital Solutions:
Current status, challenges and future directions

Nikolaos Papadoudis
Hellenic Police Forensic Science Division & Department of Computer Science and Engineering, European University Cyprus[1]

Alexandros Vasilaras
Ilias Panagiotopoulos
Hellenic Police Forensic Science Division.
Department of Informatics and Telematics, Harokopio University of Athens

Panagiotis Rizomiliotis
Department of Informatics and Telematics, Harokopio University of Athens

Abstract
Mobile devices have become an indispensable part of modern society and are used throughout the world on a daily basis. The proliferation of such devices has rendered them a crucial part of criminal investigations and has led to the rapid advancement of the scientific field of Mobile Forensics. The forensic examination of mobile devices provides essential information for authorities in the investigation of cases and their relative importance advances as more evidence and traces of criminal activity can be acquired through the analysis of the corresponding forensic artifacts. Data related to the device user, call logs, text messages, contacts, image and video files, notes, communication records, networking activity and application related data, among others, with correct technical interpretation and correlation through expert analysis, can significantly contribute to the successful completion of digital criminal investigations. The above underline the necessity for advanced forensic tools that will utilize the most prominent achievements in Data Science. In this paper, the current status of Mobile Forensics as a branch of Digital Forensics is examined by exploring the most important challenges that digital forensic examiners face and investigating whether Artificial Intelligence and Machine Learning solutions can revolutionize the daily practice with respect to digital forensics investigations. The utilization of these emerging technologies provides crucial tools and enhances the professional expertise of digital forensic scientists, paving the way to overcome the critical challenges of digital criminal investigations.

Keywords: Mobile Forensics, Artificial Intelligence, Big Data, Forensic Science, Digital Forensics.

1 Corresponding author, email Address: nikos.papadoudis@gmail.com

Introduction

Mobile Forensics is the field of Digital Forensics that deals with the acquisition, examination and analysis of mobile devices, in order to recover digital evidence in a forensically sound manner, respecting the chain of custody and ensuring that they will be admissible in a court of law. The term "mobile devices" is usually used to refer to mobile phones, but in reality, it can be extended to include any digital device which can store data in local memory and act as a means of communication. Therefore, Mobile Forensics is also related to the acquisition, examination and analysis of tablet computers, GPS devices and Personal Digital Assistants (PDAs).

Mobile devices contain plenty of data in a digital format, which includes, but is not limited to, call logs, messages, contacts, pictures, videos, web browsing information and location data. Mobile devices play a very critical role in criminal investigations, and therefore, there is an increasing demand for reliable software and hardware tools to assist digital forensics investigators in their efforts.

In recent years there has been an increasing interest in mobile devices, due to their expanding capabilities, the multiple benefits they provide in personal and professional communication, the ability to transmit and access information quickly, as well as recent developments, such as access to online banking. The advancements in mobile technology in combination with the acceptance and widespread adoption of mobile devices by the community have led to a significant rise in mobile forensics cases. The digital forensics market is expected to grow from $4.62B in 2017 to $9.68B by 2022, an annual compound growth rate of almost 16%. The anticipated market drivers are government regulations, increasing cyber incidents experienced by businesses, and the rapidly growing presence of Internet of Things (IoT) applications and devices.[2]

Artificial Intelligence (AI) already has several applications in mobile devices, such as smart voice assistants, smart cameras, facial recognition for security purposes, improved graphics in augmented reality applications, improved search functions and power efficiency. The utilization of AI algorithms has significant benefits in general towards automation in the analysis of digital evidence. According to Homem, I. (2018), a pilot study has demonstrated how automation can be advanced in digital forensics in identifying and acquiring forensic evidence, as well as in the phase of forensic analysis.

Another study related to the subject by Mohammed, Clarke and Li (2016) focused on an automation-based approach for Big Data analysis regarding specifically digital forensic investigation. Jarrett and Choo (2021) proposed the term Intelligent Automation in their research on the impact of automation and AI in digital forensics. They concluded that Intelligent Automation can provide cost-reduction, improved efficiency and speed of forensic investigation, more accurate data and information processing, and increased probability of solving a higher number of cases in limited amounts of time.

Following the above research efforts, the present study aims to explore the current applications of AI in Mobile Forensics and the corresponding solutions it provides to the challenges that investigators face, as well as indicating particularly useful AI research topics that would benefit the field in the long term.

Regarding the structure of the paper, section 2 provides an examination of the current status of mobile forensics as a subfield of digital forensics and the associations with cloud forensics, network forensics and the domain of IoT. Section 3 inspects the most important challenges that mobile forensics investigators face in the examination of cases, whereas section 4 presents AI tools and solutions available at the present time for mobile forensic investigations in conjunction with legal issues related to their practice in Digital Forensics, as well as an overview of the main evaluation metrics for AI classification models. Finally, conclusions and recommendations for future work are presented in Section 5.

Mobile Investigations and Digital Forensics

Links between mobile investigations and Digital Forensics field

Digital forensics has grown rapidly due in part to the increase in mobile devices (Harrill & Mislan, 2007). Forensic investigators face numerous challenges dealing with digital evidence obtained from mobile devices,

2 Market Insider, Digital Forensics Market – Global Forecast to 2022, (16 March 2018)
Available at "https://markets.businessinsider.com/news/stocks/digital-forensics-market-global-forecast-to-2022-1018885400"

which are correlated with several other branches of the field, such as Computer Forensics, IoT Forensics, Cloud Forensics and Big Data Forensics. The efforts to examine mobile devices originated from traditional digital forensic techniques, but, along the way, new, specialist tools, commercial and open-source, have been developed to provide solutions and automation in the extraction, examination and analysis of mobile device data.

In the modern world of competition new mobile device manufacturers are coming into the market every day with the same operating system but with their own variations, in their implementation, resulting in a myriad of file system and structural permutations (Roy, Khanna & Aneja, 2016). Meanwhile, mobile devices receive data from many sources, such as computers, cloud servers, social media platforms, network components, drones, smart vehicles, wireless cameras and smart home devices, as illustrated in Figure 1, while new technologies come into existence and are integrated into this diverse ecosystem with the progression of science and industry.

Figure 1. Mobile Phones and Data Sources

Cloud Computing

Mobile cloud computing uses cloud computing to deliver applications to mobile devices[3] and bring rich computational resources to mobile users, network operators, as well as cloud computing providers (Khan et al. 2014). The technology offers many advantages to mobile device users, such as flexibility in the transmission of information and the creation of applications, device and location independence, resource sharing among multiple users which results in increased productivity, as well as easier maintenance and advanced security. With regards to mobile forensic investigations, cloud computing provides large amounts of data that can be utilized by examiners to discover valuable artifacts for criminal cases.

In a study done by IDC, it is expected that by 2025 we will have more than 175 zettabytes of data (Reinsel, Gantz & Rydning, 2017). In addition to the ever-increasing need for data storage services, the availability of high-capacity networks, low-cost computers and storage devices, as well as the widespread adoption

3 https://www.ibm.com/cloud/learn/what-is-mobile-cloud-computing.

of hardware virtualization, service-oriented architecture and autonomic and utility computing has led to growth in cloud computing (Soric, 2021).

According to Forbes Contributor Louis Columbus (2014), a key point from an IBM study was that "Cloud computing has rapidly accelerated from 30% of Chief Information Officers (CIOs) mentioning it as a crucial technology for customer engagement in 2009 to 64% in 2014".

Other than the three standard models of cloud computing, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)[4], a relatively recent model in cloud computing is the Mobile backend as a Service model (MBaaS). This model provides web app and mobile app developers with a way to link their applications to cloud storage and cloud computing services[5]. Trends indicate that these services are gaining significant mainstream traction with enterprise consumers (Boyd, 2014). Taking into consideration the afore-mentioned models of Cloud Computing, we can understand that it is closely related to mobile technology and therefore the advancements in the field are of great interest to forensic investigators.

Internet of Things

The Internet of Things (IoT) describes the network of physical objects that are embedded with sensors, software and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet (Boyd, 2014). It is particularly important for mobile forensic examiners, as IoT devices generate high-quality artifacts that can be critical to the outcome of mobile forensic examinations and serve as important evidence in a court of law.

Internet of Things includes multiple different categories, such as Wireless Sensor Networks, use of mobile phones to interact with the real world (e.g. sensing), devices that connect via Bluetooth enabled mobile phones to the Internet, connected homes & connected Cars, RFID enabled tracking, low power embedded systems and Internet-connected wearables[6]. IoT utilizes many connectivity methods and technologies, the most important of which are presented in Figure 2 below:

Figure 2. IoT Connectivity Methods and Technologies

Wireless 101	RF 101	ZigBee PRO, ZigBee 3.0 and ZigBee IP	6LowPAN	RFID	Bluetooth LE or Bluetooth Smart Technology
Z-Wave	Home Automation (HA) Profile	Smart Energy (SE) Profile	Health Care	IEEE 802.15.4, IEEE 802.15.4e, 802.11ah	802.11ah,Wi-Fi HaLow
Relay Access Point (AP)	Grouping of stations	Target Wake Time (TWT)	Speed Frame Exchange	Sectorization	GSM, CDMA, GPRS, 3G, LTE, small cells, SATCOM
Sensors and sensor networks	Serial communication	Power consumption and optimization	MIPI, M-PHY, UniPro, SPMI, BIF, SuperSpeed USB Inter-Chip (SSIC), and SPI	Mobile PCIe (M-PCIe)	Wired connectivity
IPv4/IPv6 • Ethernet/ GigE	Real-time systems and embedded software	Big data	Analytics	Cloud computing and storage	Augmented Reality

4 The NIST Definition of Cloud Computing, SP800-145, September 2011.

5 https://en.wikipedia.org/wiki/Cloud_computing#Mobile_%22backend%22_as_a_service_(MBaaS)

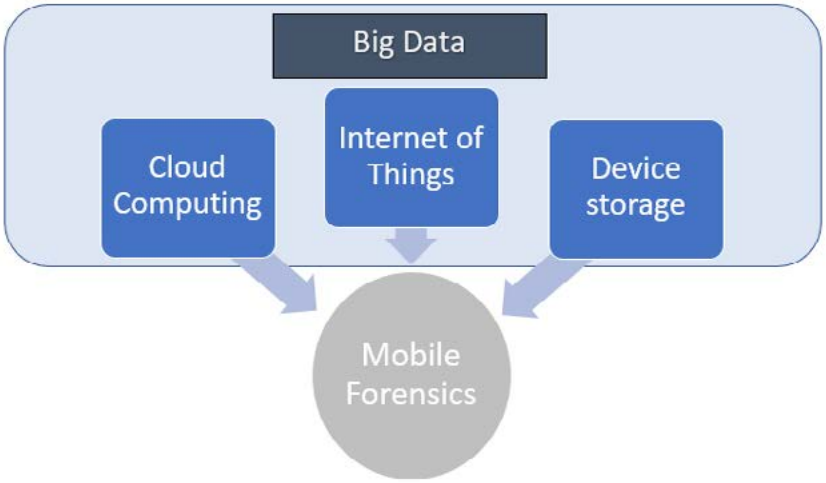
6 See IoT Forensics, eForensics Magazine 2019, 8 (6), p. 37.

Through the usage of these technologies, the IoT environment is deeply interconnected with smartphones and the respective applications, which are used for communication between devices and transmission of data. Besides, the IoT's major significant trend in recent years is the explosive growth of devices connected and controlled by the Internet (Nordrum, 2016). By the definition of the IoT ecosystem, as well as the respective connectivity methods and technologies involved, we can infer that the Internet of Things is deeply connected to recent technology advancements and that, alongside Cloud Computing and Storage, it is of particular importance for the field of Mobile Forensics.

Big Data

Due to the conjunction of Big Data with Information Technology, Cloud computing and the IoT ecosystem, it is a particularly important research subject in the domain of Digital Forensics. Big data sets come with algorithmic challenges that previously did not exist. Hence, there is seen by some to be a need to fundamentally change the processing ways (Sejdić, 2014). In addition, the ability of Internet of Things devices to gather sensory data and utilize them in everyday activities in modern society, along with the fact that data extracted from these devices reveal the device inter-connectivity, suggests that further exploring Artificial Intelligence and Big Data principles in the context of Internet of Things forensics could provide significant solutions to many challenges in the field of Mobile Forensics and Digital Forensics in general. A representation of the correlations indicated above is provided in Figure 3.

Figure 3. Big Data correlations with Mobile Forensic Investigations



Mobile devices play a key role as a terminal point of computer communication systems, collecting data from a variety of different sources and exist as most significant factors in criminal investigations. From the analysis of the current status of Mobile Forensics, we can conclude that it is affiliated with all aspects of Digital Forensics, most notably with Cloud Forensics, IoT and Big Data Forensics.

Issues in Mobile Forensics

Mobile forensics incorporates many different, but inherently interconnected, sub-branches of modern science. Forensic specialists need to navigate into this multidisciplinary field and make use of effective and efficient modern techniques to successfully combat ever more sophisticated crime. While the number and individual importance of challenges that mobile forensic experts face on a daily basis, may vary, there are some issues that every professional in the field has come across to a certain degree. The most important ones from a practitioner's perspective are analyzed below.

Volume of data

The volume of data and complexity of investigation are among the major issues in Mobile Forensics (Alzaabi, Jones & Martin, 2013). Gartner Glossary defines big data as high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation[7]. Big Data requires a new generation of technologies and architectures, designed to efficiently extract value from very large volumes of a wide variety of data, by enabling high-velocity capture, discovery and/or analysis (Gantz & Reinsel, 2011).

Therefore, one of the main characteristics of Big Data is Volume, which refers to the amount of data that is available for processing. If the size of data is sufficiently large, then it can be considered as Big Data. Even though in most cases the concept is approximate and relative to many factors, such as computing power and available technology, the effects on mobile investigations have become apparent in recent years.

In the context of mobile forensics, the meaning and value of the data volume to be examined and analyzed is inherently interconnected to the requirement for fast, efficient procedures and techniques, as well as accurate and concrete results. Hence the solutions to this problem need to account for the legal timeframes and the information flow in a criminal investigation.

Cloud services further exacerbate this challenge for forensic investigators, as there are multiple issues created by the widespread adoption of this technology, such as the rapidly increasing storage space available and the sheer amount of data transmissions for mobile device users. Other relevant factors contributing to the issue are preserving the chain of custody, resolving jurisdiction problems, overriding encryption technologies, the lack of log framework for many Cloud Service Providers, as well as the lack of cloud specific forensic tools.

Variety and variability of data

Big Data examination incorporates both structured and unstructured data processing, which are fundamental to the case analysis by the digital evidence examiner. When discussing structured data, it is usually referred to data that has a defined known structure. This could be numbers, dates, groups of words or strings accessed within the storage medium. It is data regularly tapped into during an investigation and generally stored in database files[8].

Unstructured data is information that either does not have a pre-defined data model or cannot be structured in an orderly fashion (such as in ordered rows and columns as found in databases). Unstructured data can include text in all forms, emails, video, audio files, web pages and social media.

One of the main contributors to the variety and variability of data in mobile forensic investigations is the IoT ecosystem. IoT devices can be an important source of artefacts for forensic investigations, but they pose several challenges for forensic examiners. The most important ones are data storage, data format, the diversity of IoT devices, as well as the support for these devices by current digital evidence software.

Collection, examination and analysis of data in an IoT environment becomes difficult as some of the device data is stored on the provider's cloud platforms, which may also be located in another country. Accessing the data for an investigation can be an issue if the cloud stored data is in another jurisdiction, privacy issues are not carefully considered, and maybe subject to security measures (Quick & Choo, 2018), which aggravates the complexity of an investigation, in combination with the ever-expanding storage space size.

Furthermore, within the IoT environment, evidence can be extracted from sensors and appliances, of which most of the data can be unstructured. To add to that, proprietary data formats, protocols, and physical interfaces all complicate the process of evidence extraction (Miorandi et al., 2012). The variety of data formats also makes it difficult to define a standardized approach to extracting and analyzing, as some devices may require specific approaches.

Then there is a challenge that evidence needs to be extracted from a wide range of IoT devices, such as smart refrigerators, smart watches and wireless cameras. In their study, Yaqoob et al. (2019) consider various broad groupings of IoT devices with a view to constructing an IoT digital forensics taxonomy. Their groupings are

7 https://www.gartner.com/en/information-technology/glossary/big-data

8 https://www.msab.com/blog/big-data-in-digital-forensics-the-challenges-impact-and-solutions/

smart home, smart vehicles, smartphones, drones, BitTorrent Sync peer-to-peer cloud storage service, and general IoT systems. They then go onto elucidate the taxonomy: 1) forensics phases, 2) enablers, 3) networks, 4) sources of evidence, 5) investigation modes, 6) forensics models, 7) forensics layers, 8) forensics tools, and 9) forensics data processing.

Extracting information from these devices becomes challenging as various manufacturers use different software platforms, operating systems, and hardware, leading to variation in file format of the devices. Thus, proper retrieval of artefacts from the storage devices still remains a challenge. Additionally, digital forensics tools and technologies are meant for conventional computing and are incapable of fitting forensic analysis within the IoT environment.

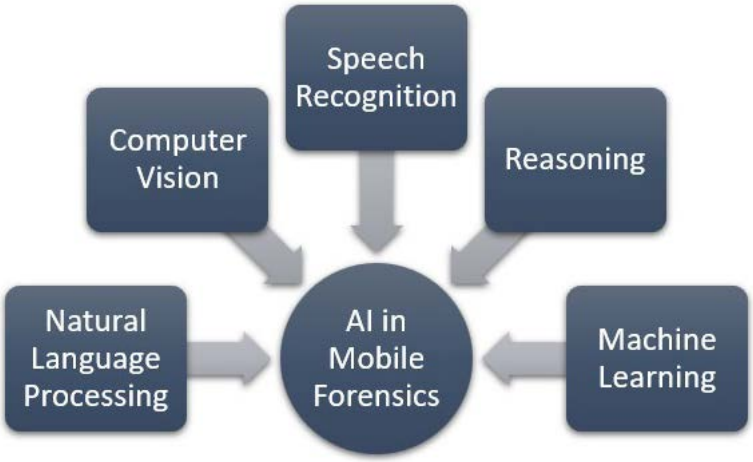
The challenges detailed in this section are derived from fields directly correlated with mobile forensics and significantly affect the work of forensic experts. While these issues became apparent with the conception of the corresponding branches of Digital Forensics, the evolution of mobile phones and the rapid advancements in related cutting-edge technology make the discussion over possible solutions more relevant than ever before. The following section features the tools that Artificial Intelligence provides us with to address these challenges and explore the current status of the AI related technologies in the field of mobile forensics.

Mobile Forensics and AI Solutions

Current tools

Artificial Intelligence has the potential for providing the necessary expertise and helps in the standardization, management and exchange of a large amount of data, information and knowledge in the forensic domain[9]. In the process of addressing the most important issues that we have examined, in the context of Big Data and the associated fields and domains of Forensic Science, AI could provide significant, efficient and effective solutions. Important Artificial Intelligence domains that are utilized in Mobile Forensic investigations are depicted in Figure 4 below.

Figure 4. Artificial Intelligence Domains in Mobile Forensics



Applications of AI in the Digital Forensics domain have already been present in research, such as the use of MADIK, a Multi-Agent System to assist the experts during computer forensic examinations. The study pointed out that the combination of the reduction in the volume of evidence to be examined by the expert and the reduction in execution times obtained with the distributed processing of the evidence already show the potential of the tool and the productivity gains it can offer to computer forensic experts and to investigators facing an ever-increasing volume of digital evidence (Hoelz et al., 2008). Another AI model that uses machine learning techniques has been proposed by Platzer, Stuetz and Lindhofer (2014) in their study that provides a potential solution to detecting nudity or pornography by using, among others, an SVM (Sup-

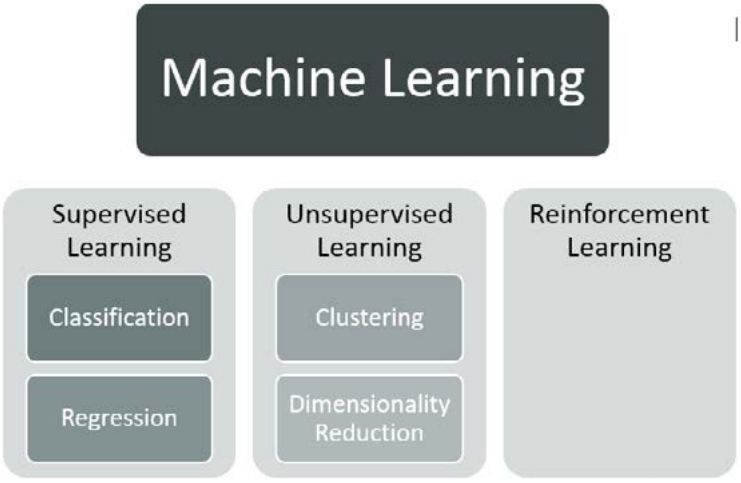
9 https://en.wikipedia.org/wiki/Digital_forensics.

port Vector Machine) algorithm for the classification of images.

In the subject of Knowledge representation and knowledge engineering, which are central to classical AI research (Poole, Mackworth & Goebel 1998; Russell & Norvik 2010), the implementation of systems that can reduce human knowledge into a set of standardized rules would be beneficial to digital forensics practitioners, as they could use the concepts and relations interpreted by software agents to discover more relevant artifacts in the investigation of cases. A recent approach to the subject is the COST Action DigForASP, a system that aims at creating a research infrastructure for the application of Artificial Intelligence (AI), in particular from the area of Knowledge Representation and Reasoning, together with other complementary areas, in the field of Digital Forensics (Constantini, Lisi & Olivieri, 2019).

By categorizing data with labels through supervised learning and identifying patterns in data sets via unsupervised learning, the process gives devices the ability to help us make decisions quicker and with greater accuracy. With reinforcement learning methods, a process which resembles how people and animals learn through trial and error, machines and devices can expand their capabilities independently without explicit programming[10]. A special part of machine learning algorithms, which is capable of assisting human expert performance and even surpassing it in certain cases, is Deep Learning. This class of AI systems generally refers to Artificial Neural Networks and it is prominently featured in modern research. The main approaches of Machine Learning, which correspond to learning paradigms, are outlined in Figure 5.

Figure 5. Machine Learning



Artificial Intelligence techniques that can be applied in digital forensics in general, as well as mobile forensics in particular, include Case Based Reasoners (CBRs), Pattern Recognition, Knowledge Discovery, System Adaptation, Refinement of Knowledge and Machine Learning (Symbolic Learners and Sub Symbolic Learners) (Mitchell 2010). There are several commercial tools and forensic software that have implemented features related to Artificial Intelligence and Machine Learning, which are provided by companies such as Magnet, Cellebrite, Belkasoft, Grayshift, Oxygen Forensics and MSAB. The respective software enables image and video categorization in an automated way, based on media classification algorithms, for predetermined categories.

The available categories generally correspond to important artifacts for examiners and include, but are not limited to, drugs, weapons, documents, nudity, faces and vehicles. These features that are provided with mobile forensics software allow for quick sorting and analysis of large volumes of data, resulting in a substantial improvement in examination speed and efficiency.

10 https://www.samsung.com/semiconductor/minisite/exynos/technology/ai/

Technology Integration – adoption and legal issues

The complete integration of AI related forensic technologies has not yet happened and will be delayed in practice as long as AI is facing the current barriers and challenges. Those challenges include the lack of proper regulatory framework, the general fear and absence of trust for the technology, promoted by inadequate knowledge and information for AI algorithms, as well as the shortage of computer systems capable of supporting AI applications and features. In addition, there is still a lot of complexity in AI and ML algorithms and insufficiency of relevant datasets, which are necessary for machine learning.

As AI research finds its way into digital forensics applications, there are many legal issues that surface and create the need for reliable solutions. First of all, the current legal framework does not have concrete rules regarding the legal value and presentation of artifacts detected and categorized by artificial intelligence systems. Currently, any conclusions reached by artificial intelligence software needs to be analyzed and verified by human investigators, but as artificially intelligent software continues to become more sophisticated and accurate, the traditional rules might prove to be insufficient in the future of Digital Forensics. On a similar note, the lack of algorithmic transparency is a significant issue that is at the forefront of legal discussions on AI (Mitchell, 2010).

Furthermore, the protection of data privacy is a major challenge for forensic software that offers features utilizing machine learning algorithms. In order to train models based on ML techniques, that achieve significant scores using the available evaluation metrics, it is necessary to process extensive datasets of relevant forensic artifacts, such as images. While these models are being developed, it is vital that the techniques used for data processing are compliant with existing legislation and preserve data confidentiality and privacy.

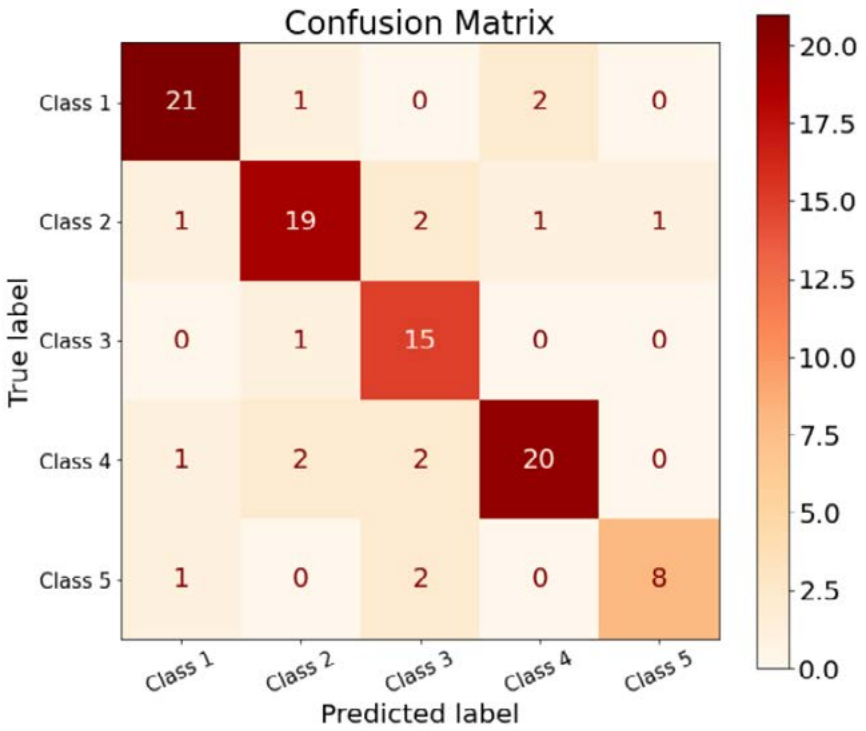
Evaluation metrics

Special reference should be reserved for the aforementioned evaluation metrics that correspond to the ML models, as the related assessment would significantly affect the interpretability and explainability of Artificial Intelligence with regards to digital forensic investigations, with direct correlations to forensic reporting and the presentation of the evidence in a court of law. The most prominent one is accuracy, which refers to the ratio of the number of correct predictions – classifications to the total number of inputs.

Even though a high accuracy score in media classification can provide essential benefits, the cost of misclassification, whether it is a false positive or a false negative, needs to be accounted for, in order to determine the performance and actual contribution of the model. Along with total Accuracy, True Positive Rate (Sensitivity) and True Negative rate (Specificity) can be used as metrics to determine the model's ability to predict the true positives and true negatives, respectively, for each available class. With high Sensitivity, a negative result means that an artifact probably does not belong to the specified category (rate of actual positives which are correctly identified), while with high Specificity a positive result means that an artifact probably belongs to the specified category (rate of actual negatives which are correctly identified).

Additionally, the confusion matrix is a two-dimensional matrix that visualizes the performance of a model and can be used for a complete demonstration of the output results and the explanation of the conclusions, by providing a picture of interrelation between different categories. A confusion matrix example for an image classification of five random image categories (Class 1 – Class 5) is displayed in Figure 6. Each row represents a number of the actual or True class and each column represents a number of the predicted class.

Figure 6. Confusion Matrix



The confusion matrix is a table that provides the combinations of actual and predicted values for a certain category and includes the True Positives, True Negatives, False Positives and False Negatives of a classification instance, which can be used to discover further information about the model's effectiveness. These values can be used to calculate Precision and Recall (same as sensitivity), as well as the F1 score, which are also useful evaluation metrics that can offer important insights into the performance of the algorithms. Precision is the number of positive predictions that actually belong to the positive class and Recall is the number of positive predictions out of all positive instances in the data. Higher precision values mean that the model returns more relevant than irrelevant results and higher recall values mean that the model returns most of the relevant results for a specified category. In addition, F1 score is calculated using the values of precision and recall, as the harmonic mean of these metrics, providing a balance between them. All the afore mentioned metrics can be used in determining the efficacy and usefulness of a model in classification problems, which are prevalent in Mobile Forensics cases. It should be noted that the impact of the evaluation metrics is case dependent, and the appropriate usage is vital for the implementation of a transparent and scientifically accurate forensic examination framework.

Conclusion

Artificial Intelligence has become a prominent feature in our lives, with intelligent machines affecting many scientific fields, business environments and everyday life. With the ongoing research showing potential in providing significant solutions in important challenges of our time, the arrival and establishment of AI and Machine Learning techniques in the field of Mobile Forensics seems inevitable and it could revolutionize the practice of digital forensics investigations.

In this paper we have shown that there are already readily available solutions in the market relevant to the advancements in AI technology and that many promising projects are also in progress. The breakthroughs in Artificial intelligence have prompted optimism and further interest from commercial and scientific entities and organizations, but legal issues should be taken into consideration and regulatory measures should be put in place in order to utilize the benefits of the research with respect to legal proceedings, while protecting the individual rights and privacy of the people. The rapid advancements in Mobile Networks, Cloud Computing, Internet of Things and Big Data technologies indicate that a new era in Digital and Mobile Forensics is entering, so the potential and the concerns regarding

Artificial Intelligence should be examined as soon as possible.

The review of the current status of Mobile Forensics, the major challenges and the solutions currently provided for digital forensics investigators indicates the following areas as recommendation for future research.

Research into the automated recognition of patterns and regularities in data and implementation of reliable solutions in forensic software would be very advantageous for analysts. Topics could include optical character recognition, image classification, text classification and data clustering.

In addition, advancements in link analysis could be valuable, since it can be used by machine learning forensics to discover the content and structure of a body of information by transferring the information into a set of interconnected entities or objects that are linked together (Qadir & Valor, 2020). Through this technique, digital forensic investigators can reveal associations between individuals, associations between individuals and organizations, as well as associations between a place and an individual (Mena, 2003). Furthermore, improvements into the accuracy of image and video classification would be very beneficial for the field of Mobile Forensics.

The domain of Digital Forensics could be substantially benefited by research and development regarding the capability of forensic software to read and understand human language. The acquisition of knowledge directly from human created artifacts could lead to faster classification and importance evaluation of data during the examination and analysis of digital evidence. For example, word clustering can be achieved from emails, call site transcripts, instant messages, website forms, chats, phone calls and texts (Mena, 2016).

Specialized software that is publicly accessible and reflects the culmination of a problem-solving initiative in a scientific domain could help reduce the severity of the issues negatively affecting the current state of Mobile Forensics. Open-source tools with AI capabilities can provide examiners with problem-specific solutions in a number of highly technical cases, where available software might prove to be insufficient. Raising awareness of the importance of the development and adoption of such tools should therefore be at the forefront of the mobile forensics' community.

The international standards for forensic sciences and related scientific methods are essential for the credibility and transparency of evidence and legal prosecution of cases. As Artificial Intelligence claims a bigger and more significant role in the forensic examination of mobile devices, the conception and application of new concrete standards and legal procedures, accepted by the scientific community and applied by Forensic Institutes and Law Enforcement Agencies should be considered as developments of utmost importance.

References

- Alzaabi,M. Jones, A. & Martin, T. A. (2013) An ontology-based forensic analysis of mobile devices. Annual ADFSL Conference on Digital Forensics, Security and Law. 5.
  Available at: https://commons.erau.edu/cgi/viewcontent.cgi?article=1245&context=adfsl
- Boyd, M. (2014). built.io Is Building an Enterprise MBaas Platform for IoT. Programmableweb.
  Available at: https://www.programmableweb.com/news/builtio-building-enterprise-mbaas-platform-iot/interview/2014/03/03
- Columbus, L. (2014) Roundup of cloud computing forecasts and market estimates, 2014. *Forbes*.
  Available at: https://www.forbes.com/sites/louiscolumbus/2014/03/14/roundup-of-cloud-computing-forecasts-and-market-estimates-2014/?sh=59f2de4057a2
- Constantini, S., Lisi, F. & Olivieri, R (2019) Knowledge Representation and Reasoning meets Digital Forensics: The COST Action DigForASP (short paper). RCRA/RiCeRcA@AI*IA. January.
  Available at: http://ceur-ws.org/Vol-2538/paper5.pdf
- Gantz, J. & Reinsel, E. (2011) Extracting Value from Chaos. IDC's Digital Universe Study.
  Available at: http://www.kushima.org/wp-content/uploads/2013/05/DigitalUniverse2011.pdf
- Harrill, D.C., & Mislan, R.P. (2007) A Small Scale Digital Device Forensics ontology. *Small Scale Digital Device Forensics Journal*, 1 (1), pp. 1-7.
  Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.444.4475&rep=rep1&type=pdf

- Hoelz, B., Ralha, C., Geeverghese, R. & Junior, H. (2008) A cooperative multi-agent approach to computer forensics. Proceedings – 2008 IEEE/WIC/ACM International Conference on Intelligent Agent Technology, 2, pp. 477-483.
- Homem, I. (2018) Advancing Automation in Digital Forensic Investigations. *Academic dissertation Stockholm University.* Available at: https://www.diva-portal.org/smash/get/diva2:1259778/FULLTEXT01.pdf
- Jarrett, A. & Choo, K.-K. (2021) The impact of automation and artificial intelligence on digital forensics. WIREs Forensic Science 3, e1418, pp. 1-17. Available at: https://wires.onlinelibrary.wiley.com/doi/epdf/10.1002/wfs2.1418
- Khan, A-U., Othman, M. Madani, S.& Khan, S. (2014) A Survey of Mobile Cloud Computing Application Models. *IEEE Communications Surveys and Tutorials 16 (1), 393-413*.
- Mena, J. (2003) Investigative data mining for security and criminal detection. Butterworth-Heinemann.
- Mena, J. (2016) Machine learning forensics for law enforcement, security, and intelligence. Auerbach Publications.
- Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012) Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10 (7), pp. 1497–1516.
- Mitchell, F. (2010) The use of Artificial Intelligence in digital forensics: An Introduction. *Digital Evidence and Electronic Signature Law Review*, 7, pp. 35-41. Available at: https://sas-space.sas.ac.uk/5533/1/1922-2707-1-SM.pdf
- Mohammed, H.J., Clarke, N., & Li, F. (2016) An Automated Approach for Digital Forensic Analysis of Heterogeneous Big Data. *J. Digit. Forensics Secur. Law*, 11, pp. 137-152.
- Nordrum, A. (2016) Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. *IEEE Spectrum*.
- Platzer, C., Stuetz, M. & Lindorfer, M. (2014) Skin sheriff: a machine learning solution for detecting explicit images, Proceedings of the 2nd International workshop on security and forensics in communication systems. pp. 45-56: ACM Available at: https://publik.tuwien.ac.at/files/publik_273619.pdf
- Poole, D., Mackworth, A., & Goebel, R. (1998) *Computational intelligence: A logical approach*. Oxford: Oxford University Press.
- Qadir, A. & Varol, A. (2020) The Role of Machine Learning in Digital Forensics. Paper presented at the 8th International Symposium on Digital Forensics and Security (ISDFS), June 1-2, Beirut, Lebanon. Available at: https://www.researchgate.net/publication/342193343_The_Role_of_Machine_Learning_in_Digital_Forensics
- Quick, R. & Choo, K.-K. (2018) Big Digital Forensic Data. In Volume 2: Quick Analysis for Evidence and Intelligence. Springer Briefs on Cyber Security Systems and Networks. Springer.
- Reinsel, D., Gantz, J. & Rydning, J. (2017). Data Age. IDC White Paper. Available at: https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017.pdf
- Roy, N., Khanna, A. & Aneja, L. (2016) Android phone forensic: Tools and techniques. International Conference on Computing, Communication and Automation (ICCCA2016), 605-610. Available at: https://www.researchgate.net/profile/Nihar-Roy-4/publication/312559420_Android_phone_forensic_Tools_and_techniques/links/5eecdad1458515814a6b45df/Android-phone-forensic-Tools-and-techniques.pdf
- Russell, S. J., & Norvig, P. (2010) Artificial intelligence: A modern approach. *Applied Mechanics & Materials*, 263(5), pp. 2829–2833.
- Sejdić, E. (2014) Correspondence: Adapt current tools for use with big data. *Nature* 507 (7492), p. 306. Available at: https://www.nature.com/articles/507306a.pdf
- Soric, D. (2021) Cloud computing 101. *Digital Reflections*. Available at: https://medium.com/digital-reflections/cloud-computing-101-2b66e54c66c4
- Yaqoob, I., Hashem, I., T. Ahmed, A. Ahsan Kazmi, S. & Hong, C. (2019) Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*, 92, pp. 265-275.

Forensic Linguistics:
The potential of language for law enforcement in the digital age

Rui Sousa-Silva
University of Porto – Faculty of Arts and Humanities[1]

Abstract
The recent technological developments have granted citizens worldwide access to the Internet, including in handheld devices, and offered them new communication possibilities. Nevertheless, they have also exposed them to more cybernetic attacks, as criminals gained new opportunities for cybercriminal practice. The (perceived) increase in the number of cyberattacks faces Law Enforcement with two major challenges: firstly, the higher the volume of cyberattacks, the harder it is to dedicate the necessary resources, including human, to fight them; secondly, the range of sophisticated stealth technologies used by cybercriminals to remain anonymous online hamper the work of the forces. This paper argues that, since (cyber)criminals use language to communicate, their anonymisation can be undermined by the language that they use because language use is idiosyncratic, so each speaker makes a particular use of their language (Coulthard, 2004). This is enabled by Forensic Linguistics, which can be broadly defined as the application of linguistic analyses in legal or Law Enforcement contexts. This article presents two illustrative cases of cybercrime to show the potential of the forensic linguistic analysis. The first is the case of an anonymous set of text messages spreading defamatory contents, whose linguistic analysis enabled the sociolinguistic profiling of the author, and hence narrow down the pool of suspects. The second presents a cross border cybercriminal practice: fraudulent and deceptive messages sent to citizens for purposes of extortion. The article concludes by discussing the potential of the linguistic analyses in the fight against (cyber)-crime, and making recommendations for Law Enforcement.

Keywords: cybercrime, threatening language, darkweb, anonymity, investigative linguistics

Introduction

Over the last decades, the world has witnessed unprecedented technological developments that have, among others, granted citizens worldwide immediate access to the Internet, including in handheld devices. As a result, new communication possibilities emerged, with obvious advantages for users, who have gained immediate access to information; additionally, anyone, virtually anywhere, has been granted the power to post, share or comment on anything at any time. As they grew more acquainted with technology, users have gained a more prominent participatory role in society. Nevertheless, the new possibilities offered by technology have also exposed citizens to more cybernetic attacks, i.e. cybercrime.

1 rssilva@letras.up.pt

Cybercrime is a borderless issue that can be classified in three broad definitions: (a) crimes specific to the internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts); (b) online fraud and forgery: large-scale fraud that can be committed online through instruments e.g. identity theft, phishing, spam and malicious code; and (c) illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia[2].

The overall preparedness of the users for the current technologically connected world was tested over the last two years, when, due to the COVID-19 pandemic, the world went massively on lockdown, and people everywhere had to quickly adapt to living a significant part of their lives online; office work was replaced to a large extent by telework, in-person education gave way to online learning and teaching, online meetings replaced face-to-face meetings, and shopping was superseded by online shopping. Leading online lives was a way of mitigating at least part of the negative impact of the pandemic. The sudden move from in-person to online daily activities came at a cost: the massive use of online platforms put a strain on technological systems and infrastructure, which were not ready for the boom of users; hardware often failed to meet the increasingly demanding needs of users; and software revealed vulnerabilities that were previously unimaginable. Simultaneously, social practices had to be adapted and adjusted to meet the requirements of the so-called 'new normal'. This was not problematic for digital natives and tech-savvy users, and digital immigrants, who were expected to struggle to adapt, appear to have coped surprisingly well with this technological leap. This readiness was only apparent, because, under the surface, they remained digital immigrants whose self-perceived competences left them vulnerable to criminals, who in turn found in this new scenario unprecedented opportunities for cybercriminal practice. Cybercrime thus became more evident, by attracting the public and the media attention.

As a result of the growing number of cyberattacks, and of their diverse nature, Law Enforcement is faced with two major challenges. Firstly, the higher the volume of cyberattacks, the harder it is for Law Enforcement to dedicate the necessary resources (including human) to fight them. Additionally, as the volume of cybercrimes increases, so does the diversity and variety of such crimes, which in turn demands a constant realignment of Law Enforcement. Secondly, the range of sophisticated stealth and obfuscation technologies used by cybercriminals to help them remain anonymous online have a serious negative impact on the work of Law Enforcement. In extreme cases, where highly sophisticated means are used to cover for any traces of their online crimes, the positive identification of those criminals may be very hard, even nearly impossible; in other cases, access to crucial data – including metadata – may be barred by data holders, such as big techs, or even by the Law, leaving the forces with very little tangible data to investigate (cyber)crimes. Hence, granting legal access to data is essential to investigate cases of cybercrime.

An often-underestimated type of such data is language. As previously argued (Sousa-Silva, 2017), despite their anonymisation efforts, in a significant proportion of crimes (cyber)criminals resort to communication, and consequently use language in their criminal practice to communicate with victims, fellow criminals, or others. By doing so, they ignore the potential of language data to identify them (just like, metaphorically speaking, a 'linguistic fingerprint'). Indeed, as has been theoretically and empirically demonstrated, use of language is idiosyncratic, so every speaker of a language has a particular way of speaking and writing that distinguishes them from other speakers of the same language(s) (Coulthard, 2004). This field, which is known as forensic authorship analysis, is one of the many different applications of forensic linguistics.

The potential of forensic linguistic analysis for law enforcement

Language, which can be briefly defined as the system that humans have developed and use to communicate, is at the basis of the field of scientific enquiry known as Linguistics: the science that studies language structures and its use (see e.g. Finegan, 2008).

Linguistics as a (forensic) science has been victim of two mistaken assumptions. The first is that, because language is a social science, linguistics is often accused of being 'subjective' and lacking the validity and reliability criteria required by science, which prevents con-

2 See for further reference the website of the EU Commission at https://ec.europa.eu/home-affairs/cybercrime_en.

clusions to be measured and quantified, and error rates to be known. The second is that, because language is wrongly seen to be subjective, speakers frequently take themselves to be able to analyse language scientifically simply because they are native speakers (this fallacy is sometimes phrased as 'I could call upon the expertise of a linguist, but why would I need one if I can also read and write'?). Both these assumptions are obviously wrong; linguistics is indeed a science, it is objective, and it is bound by principles of validity and reliability, in much the same way as any other science. Additionally, although it is still very hard – if possible – to establish a known error rate, linguistic patterns can be measured and quantified, if the volume of data so permits. Moreover, no matter how proficient a native speaker of a language may be, their competence cannot compare to that of linguists, who have a deep knowledge of language acquisition and language structures, as well as of how language is used, depending on purposes, participants, contexts, etc. It is this knowledge of linguistics that is at the basis of Forensic linguistics.

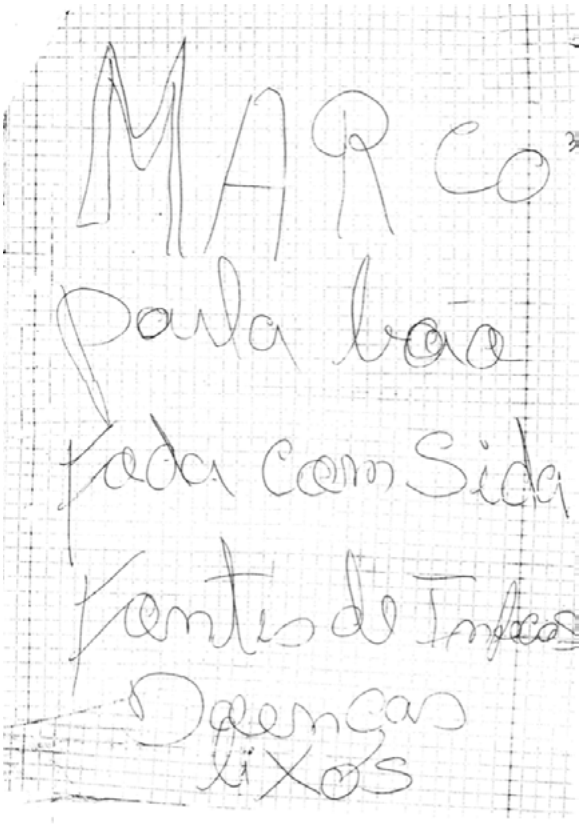
Linguistics can be approached from two main perspectives: a theoretical, which seeks to provide explanations for observable or possible linguistic phenomena; and an applied perspective, which focuses on language use in social interaction. Forensic linguistics is part of the latter, i.e., it is the branch of applied linguistics that consists of applying theories, knowledge and expertise of language sciences in forensic contexts (see e.g. Coulthard & Sousa-Silva, 2016) – whether to assist the courts of law, the investigative process or other issues that are of interest to the 'forum' in the traditional sense (i.e., the society in general (Turell, 2013)). Forensic Linguistic can thus be defined in a broad sense and in a narrow sense. In a broad sense, it subsumes three sub-areas: the study of the written language of the law, including interpretation of the language used in legal texts, such as laws and contracts, or the comprehensibility of legal language; the study of interaction in the legal process, which, in criminal cases, may include communications from phone calls to the police or to the emergency services, as well as police interrogation and interviewing, or interaction in a court of law; and the study of language as evidence (Coulthard, May, & Sousa-Silva, 2021), which includes, among others, authorship analysis (to establish which of a set of suspects is the most likely author of an incriminating anonymous text, or whether a suspect can be excluded as the author of that text), plagiarism detection and analysis (to help establish whether a text has been produced independently, and hence is original, or whether it was based on someone else's text), analysis of disputed meanings (in order to establish the more likely meaning of a disputed utterance), or sociolinguistic profiling (in order to establish the sociolinguistic features of the author of a suspect text). In a narrow sense, Forensic Linguistics is limited to the latter application, i.e., the study of language as evidence, including as an assistance to the investigation.

In the following two sections, two cases of cybercrime that illustrate the potential of the forensic linguistic analysis to uncover (cyber)criminal activities are presented and discussed, which are relevant for law enforcement. The first is the case of an anonymous set of text messages spreading defamatory contents, whose linguistic analysis enabled the investigation to establish the sociolinguistic profiling of the author, and consequently to narrow down the pool of suspects. The second case discusses a cross border cybercriminal practice: fraudulent and deceptive messages sent to citizens for purposes of extortion.

Establishing the sociolinguistic profiling of suspects

The first case in point is one of cyber-stalking. A set of anonymous text messages were sent from a pre-paid, unregistered mobile phone number spreading defamatory contents; they stated that a man (Marco) was HIV positive. An anonymous handwritten note (see Figure 1) was also circulated, reading that he and a woman he'd been seeing were 'spreading the disease.'

Figure 1: Handwritten anonymous message.



The complexity of the case was furthered by the fact that, if there were suspects, a set of texts known to have been written by each of them could be collected and compared to the suspect texts; safe assumptions could then be made as to whether the writing style of any of the suspects matched the writing style of the anonymous texts, as is common in authorship analysis tasks. However, since there were no suspects, no texts were available for comparison. Therefore, at best the investigation could try and establish the sociolinguistic profiling of the anonymous author(s) to narrow down the pool of suspects. Typically, sociolinguistic profiling (Coulthard & Sousa-Silva, 2016), which should not be confused with psychological profiling, is requested when the investigators do not have strong hypotheses about the identity of the author(s) of the suspect texts. The linguist is asked to find linguistic clues in the text that help establish social features of the author that reflect on the language used, such as age, gender, social and regional background, or level of education, among others. The purpose of sociolinguistic profiling is to identify the linguistic features of the group (in linguistics, the sociolect) to which the anonymous speaker may belong, rather than the linguistic features of the individual speaker (in linguistics, their idiolect). In other words, the aim of sociolinguistic profiling is not to find the exact (or even the most likely author) from all speakers of a language.

One of the challenges forensic linguists commonly face is related to the amount of data available for analysis. Ideally, linguists need considerable volumes of data to extract patterns from texts, and hence make safe assumptions about the writer. However, in forensic cases, the volume of text for analysis is usually small. In this particular case, the linguistic analysis focused on three sets of texts: the first set consists of text messages sent from an unregistered phone number (448 words in total); the second set consists of text messages sent from a second unregistered phone number (122 words in total); and the third set consists of the handwritten message shown in Figure 1 (16 words). The linguist was thus asked two questions by the investigation: (1) whether the three sets of texts were written by the same person; and (2) if they were written by the same person, whether there are some clues in the text that enable the identification of social characteristics (sociolinguistic profile) of the author.

The linguistic analysis of the three sets of texts revealed that they are highly likely to have been written by the same person because they share a large number of atypical linguistic patterns, including: use of slang and swear words, lack of prepositions, lack of punctuation (especially at the end of sentences), missing spaces between words, homophonic substitution (i.e., the correct spelling is replaced by how the words are pronounced), lack of accents in words, spelling errors[3] and lack of agreement in gender and number (in accordance with Portuguese grammar). Each of these patterns, individually, may not be relevant, since speakers from the same speech community, and who share identical social backgrounds, can share particular linguistic patterns, regardless of how idiosyncratic they may be. However, when used in combination with other idiosyncratic patterns, they can be highly identifying (or 'idiolectal', in linguistic terms), thus contributing to build the idiolectal style (Turell, 2010) of the writer. In this case, since the three sets of anonymous texts share identical linguistic features, it can be safely

3 The words 'error' and 'mistake' are used here with two distinct meanings: 'mistake' is used to refer to instances where an error is introduced by accident (as happens, for instance, with typos), regardless of the speaker's linguistic competence, whereas the word 'error' is used to refer to instances where those mistakes are made systematically, and hence do not result from accidental production.

assumed that they were written by the same person (even though the third set, the handwritten message, is very short, hence sharing fewer linguistic patterns). The following features, which are shared mostly by sets 1 and 2, are particularly idiolectal and hence relevant: (1) use of slang and swear words (e.g., 'merda'); (2) lack of agreement in number and gender (e.g. '*as merda* do' or '*dois bêbado*'); homophonic substitution (e.g., 'vo' for 'vou', 'inferniza' for 'infernizar', 'emcomoda' for 'incomodar'); and (3) misspelt words (e.g. 'emcomoda' for 'incomodar' or 'vo te' for 'vou-te').

In addition, these messages also include a unique phrase that is highly idiolectal: 'homem de sida' (literally translated into English as 'man of aids' to mean 'man with aids'). An example of a sentence where this phrase is used is 'Puta paga hotel para foder com homem de sida' (literally translated as 'Bitch pays hotel to fuck man of aids'). This phrase, which reads odd to any native speaker of Portuguese, is unique: when this analysis was first conducted, the exact phrase 'homem de sida' did not return any hits in Google[4]. What makes this phrase so unique is the use of the preposition, 'de' (English 'of'); although the words 'homem' (English 'man') and 'sida' (English 'aids') tend to keep company to each other very often (in linguistic terms, they are said to collocate very frequently), the grammatically correct preposition to be expected is 'com' (English 'with') and not 'de'. However, this phrase is used several times in different messages across the two sets, which demonstrates that its use is neither accidental, nor the result of an odd mistake; rather, its use is systematic, so the use of the correct alternative is not under the control of the writer.

Altogether, the analysis of these linguistic patterns provides us with several sociolinguistic clues to the origin and social characteristics of the writer, who is highly likely to be a woman in her mid-20s to mid-30s, with a low level of education, and from a low socioeconomic background. These patterns also indicate that the writer, most probably a black woman, originates from a Portuguese-speaking African country, highly likely, Angola. These patterns help narrow down the pool of suspects, by establishing that the writer probably belongs to a particular group of people, although they do not allow the analysis to precisely identify the individual writer of the questioned messages. This identification is only possible after the investigation has narrowed down the pool of suspects to just a few (typically two or three) writers, and a comparison is made between the questioned messages and sets of texts that are known to have been previously written by each of the suspects. When such an analysis is conducted, the unique phrase 'homem de sida' can potentially be highly idiolectal, and hence discriminatory, to identify the individual writer.

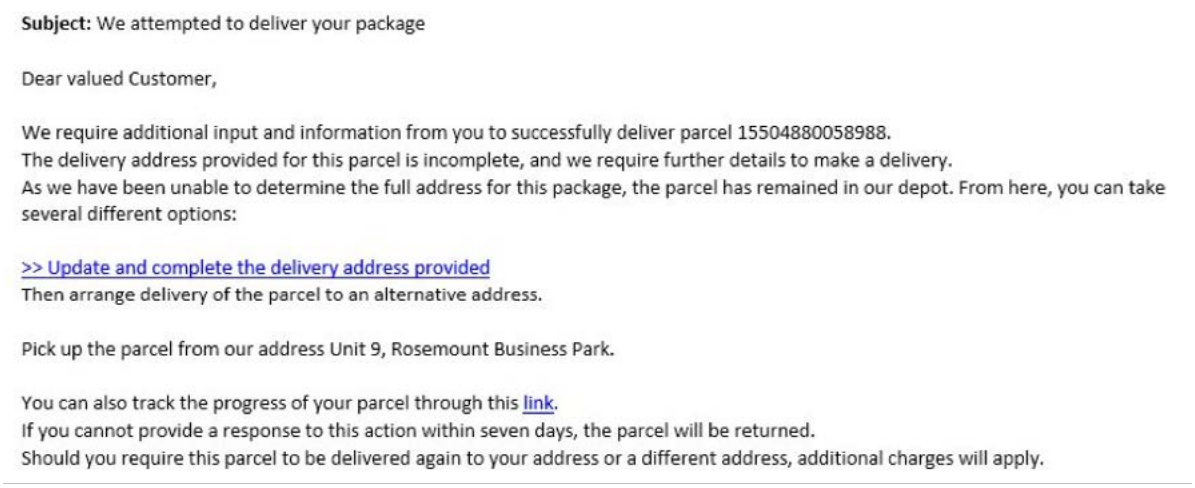
These findings, of course, need to be interpreted with caution because language is fluid, and although different social groups tend to share stable sociolinguistic patterns (see e.g. Labov, 1972), some features may span beyond those groups and be used by individual members of other groups. For this reason, sociolinguistic profiling is a very valuable tool for investigative purposes, but can hardly ever be used as evidence; for evidential purposes, forensic authorship analyses are more reliable.

Language use in cross-border cybercriminal practice

The previous section showed that sociolinguistic profiling consists of identifying a set of features that are typical of a certain sociolect, i.e., characteristics that are shared by a group of people from the same speech community. From a linguistics perspective, it is thus common for groups of criminals to share the same sociolect, that is, the same group of features. Therefore, an analysis identical to the one that is used for sociolinguistic profiling can also be relevant to identify cross border cybercriminal practices. Unlike traditional criminal practices, where criminals were, for the most part, geographically close, criminal groups are now expected to gather and operate cross-border. Therefore, it can be argued that technology has powered new, global forms of cybercriminal practices, which cross territories and jurisdictions. These practices may include, though not exclusively, threats, extorsion, fraud, or cybercrimes such as cyber-trespass, cyber-fraud, cyber-piracy, cyber-porn and cyber-paedophilia, cyber-violence or cyber-stalking (see e.g. Wall, 2001), as well as scams, spoofing and phishing. Figures 2 and 3, written in English and in Portuguese, respectively, illustrate such criminal practices.

4 At the time of writing, Google only returns two results, both of which point to a book chapter where this case is mentioned to discuss linguistic identities.

Figure 2: Phishing email (in English).



Subject: We attempted to deliver your package

Dear valued Customer,

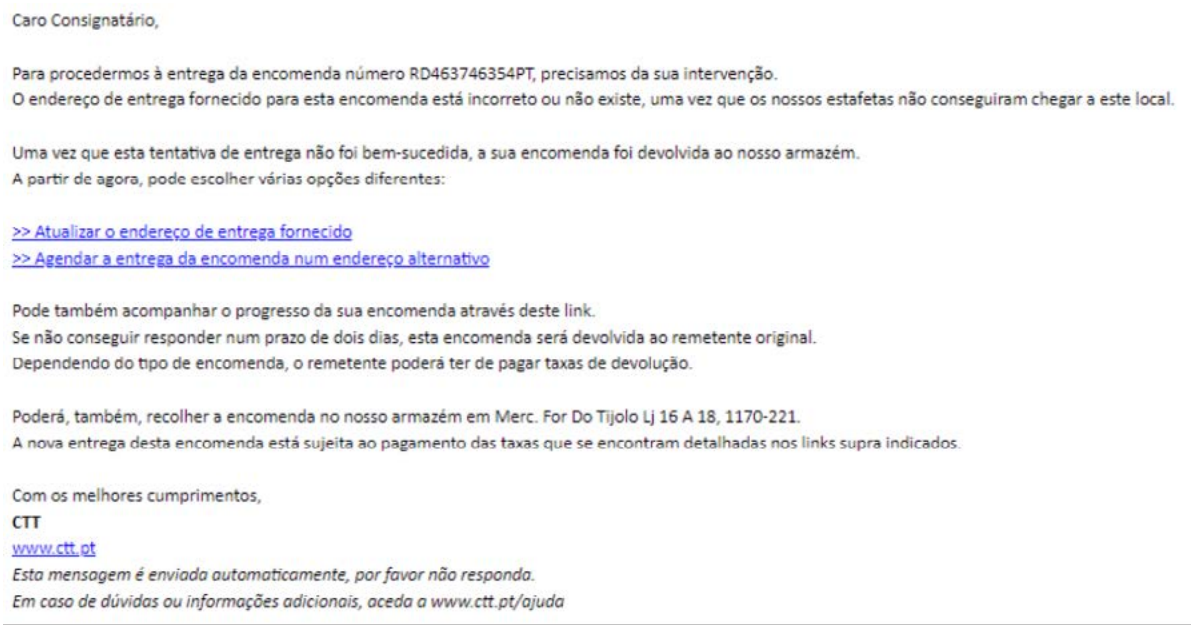
We require additional input and information from you to successfully deliver parcel 15504880058988.
The delivery address provided for this parcel is incomplete, and we require further details to make a delivery.
As we have been unable to determine the full address for this package, the parcel has remained in our depot. From here, you can take several different options:

>> Update and complete the delivery address provided
Then arrange delivery of the parcel to an alternative address.

Pick up the parcel from our address Unit 9, Rosemount Business Park.

You can also track the progress of your parcel through this link.
If you cannot provide a response to this action within seven days, the parcel will be returned.
Should you require this parcel to be delivered again to your address or a different address, additional charges will apply.

Figure 3: Phishing email (in Portuguese).



Caro Consignatário,

Para procedermos à entrega da encomenda número RD463746354PT, precisamos da sua intervenção.
O endereço de entrega fornecido para esta encomenda está incorreto ou não existe, uma vez que os nossos estafetas não conseguiram chegar a este local.

Uma vez que esta tentativa de entrega não foi bem-sucedida, a sua encomenda foi devolvida ao nosso armazém.
A partir de agora, pode escolher várias opções diferentes:

>> Atualizar o endereço de entrega fornecido
>> Agendar a entrega da encomenda num endereço alternativo

Pode também acompanhar o progresso da sua encomenda através deste link.
Se não conseguir responder num prazo de dois dias, esta encomenda será devolvida ao remetente original.
Dependendo do tipo de encomenda, o remetente poderá ter de pagar taxas de devolução.

Poderá, também, recolher a encomenda no nosso armazém em Merc. For Do Tijolo Lj 16 A 18, 1170-221.
A nova entrega desta encomenda está sujeita ao pagamento das taxas que se encontram detalhadas nos links supra indicados.

Com os melhores cumprimentos,
CTT
www.ctt.pt
Esta mensagem é enviada automaticamente, por favor não responda.
Em caso de dúvidas ou informações adicionais, aceda a www.ctt.pt/ajuda

The two emails, supposedly sent from legitimate post/parcel services, inform the recipient that a parcel could not be delivered to them because the address was incomplete (or incorrect, in the case of the email in Portuguese). The similarities between the two messages, despite their being written in two different languages, are striking, both in form and in contents. The Portuguese message even includes a reference to the official post website, which makes it more credible. However, both emails are phishing messages: "a fraudulent electronic communication that appears to be a genuine message from a legitimate entity or business for the purpose of inducing the recipient to disclose sensitive personal information" (Garner, 2009, p. 1263), such as login details, passwords or bank details. These deceitful communications usually attempt to route the user to false websites, where they are encouraged to provide confidential data.

Other deceitful communications include emails apparently sent from one's own email address stating that the sender is in full control of the computer, after malware has been installed upon visiting adult websites. Figures 4, in English, and 5, in Portuguese, illustrate these messages.

Figure 4: Extortion email (in English).

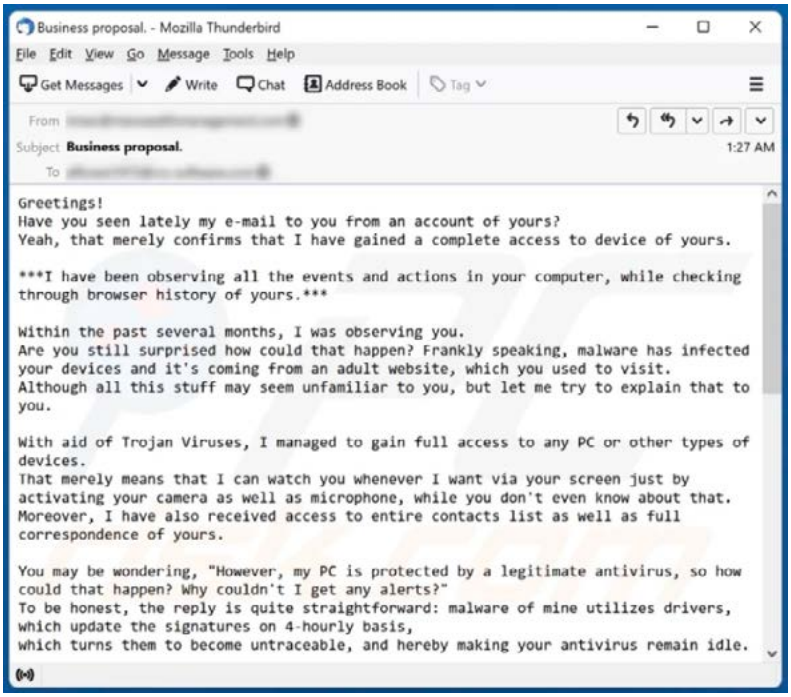
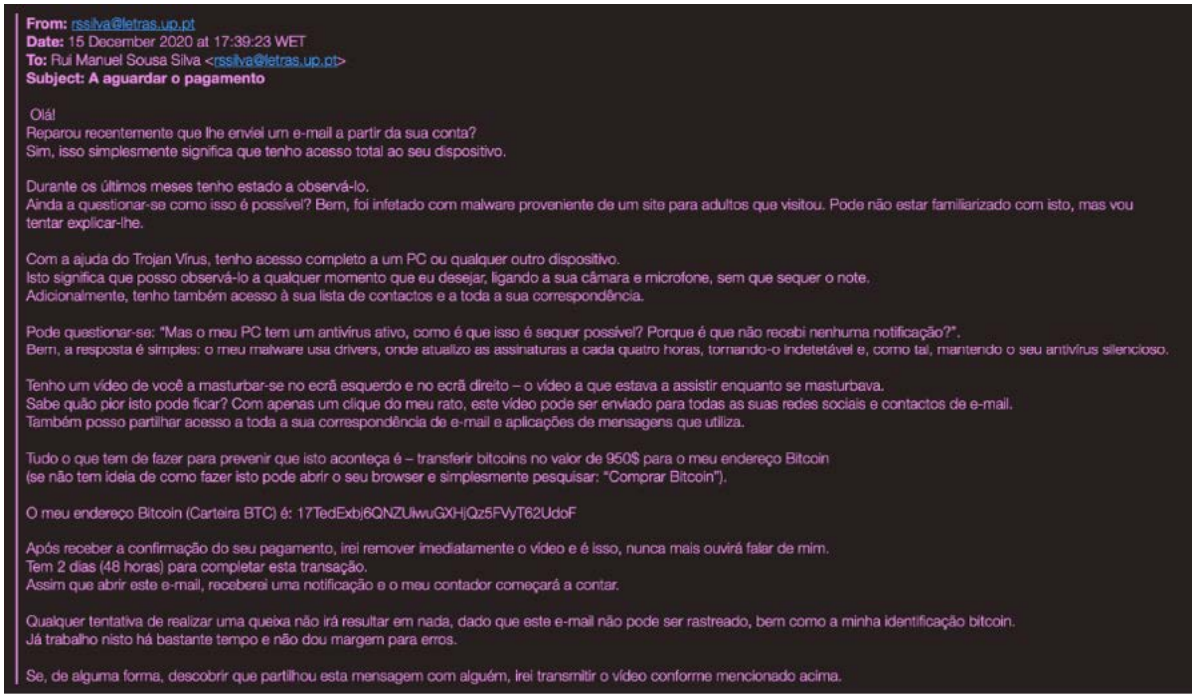


Figure 5: Extortion email (in Portuguese).



Communications of this type, which are attempts of extortion, are usually accompanied by a 'business proposal' or 'request for payment' and a ransom note stating that, if a sum is not paid (typically in crypto currency), then videos recorded by the sender showing immoral activities will be published or sent to the all the recipients in the victim's contact list. Although these messages are known to be fraudulent by a large part of the population, some users still worry that someone might have gained access to their computer,

so whether they have performed the action described or not is irrelevant to them; consequently, many victims still pay the sum demanded.

In both cases, the messages share some linguistic features that enable the identification of patterns of fraudulent and deceptive messages sent to recipients; in other words, a thorough forensic linguistic analysis allows the identification of features of language that enable the identification of the sociolect of the (cyber) criminals. Fraudulent and deceptive messages of this type traditionally contained a vast array of errors at all levels of language, including grammar, spelling, and punctuation. Over time, however, the quality of the deceitful text improved, and currently these communications very rarely include serious linguistic errors. Nevertheless, a careful reading and analysis of the texts reveals inconsistencies at the levels of cohesion (i.e., the relationship between items in a text) and coherence (i.e., the relationship between the items in the text and the extra-textual world), as well as minor grammatical mistakes. For example, the sentence 'I have gained a complete access to device of yours', although understandable to any speaker of English, is clearly not grammatically correct: 'a' in 'a complete access' is in excess, while 'to device of yours' is missing an article ('to a device of yours' would be more appropriate) or, even more appropriately, a possessive pronoun (e.g., 'to your device'), since the sender refers specifically to that same computer. Another grammatical mistake can be found in the sentence *'Although* all this stuff may seem unfamiliar to you, *but* let me try to explain that to you': in this sentence, the use of the two conjunctions ('although' and 'but', in italics) makes the sentence agrammatical. Examples like these abound in the texts.

It is also worth noting that the texts reveal peculiar patterns at the level of syntax (i.e., in sentence structure), which show that they were not originally written in that language. For instance, the structure of the sentences of the extortion text in Portuguese (Figure 5) is typical of English, so native speakers of the language (even non-linguists) will feel that the text is unidiomatic (or unnatural). Non-speakers of Portuguese can test this hypothesis by machine-translating the text into English: the more linguistically correct is the machine-translated text (called in translation studies the 'target text'), the closer the syntax of the source text (in this case, the Portuguese) is to English; conversely, the more the syntax of the target text differs from English syntax, the more likely it is that the source text has not been originally produced in English (see e.g. Sousa-Silva, 2013). The machine translated version, however, does not show major issues, which reveals that it is very close to English syntax.

These cases show that forensic authorship analyses, as well as an analysis identical to the one conducted in cases of sociolinguistic profiling, allows the identification of linguistic patterns that are typical of cross-border (cyber)criminal communications.

Linguistic analysis of disputed meanings

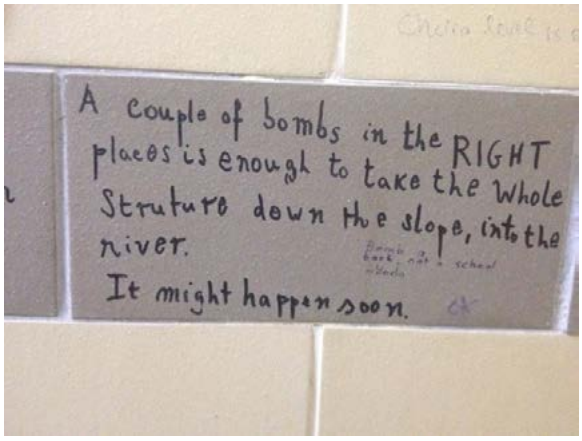
A relevant area of research in Forensic Linguistics is the analysis of disputed meanings, which consists of establishing the meaning of a textual element (such as a word, a phrase, or a sentence), confirming or rejecting the meaning associated with it, or analysing its linguistic uniqueness. Meanings are crucial because they underlie all instances of interaction among the speakers of a language and work to guarantee the communication among these speakers. In forensic contexts, the analysis of disputed meanings includes the study of suspect or illegal communications, cybercriminal messages, defamatory contents, text that infringes the 'property' of certain words (as in cases of plagiarism, copyright infringement or trademark disputes), as well as detection of hate speech and threatening messages (or, conversely, false threats).

Analysing disputed meanings can be problematic. When speakers of a language want to learn the meaning of a word, they usually refer to dictionaries, as these are supposed to compile the meanings of all the words in a language. Nevertheless, dictionaries do not suffice: firstly, new meanings emerge every day, either because new words are created, or because old words are re-signified (i.e., existing words can be given new meanings); secondly, dictionaries include the standard meaning(s) for words, but the precise meaning of an utterance can only be established in context. For instance, the sentence 'The bus was late.' can be used simply to inform the reader that the bus did not arrive on schedule, or – if the speaker is late – operate as a justification for their being late. Therefore, lexicographic definitions – the ones provided in dictionaries – can be useful to give speakers a general idea of the meaning of a word, but the precise meaning of an utterance always depends on its context, including setting, participants, purpose, etc.

Figure 6: Disputed meaning of a threatening utterance.

Figure 6 shows an illustrative example of disputed meanings. The message was written on the bathroom wall of FLUP ('Faculdade de Letras da Universidade do Porto', the Faculty of Arts and Humanities of the University of Porto). The utterance starts with the word 'Beware', thus cautioning the reader about something. The remaining of the message, however, is of a more informative nature, so most readers, when asked whether this utterance is a threat, will likely say it isn't. This message, however, is accompanied by another one, shown in Figure 7:

Figure 7: Disputed meaning of a threatening utterance.



The message illustrated in Figure 6 will gain a new meaning after reading the message in Figure 7: that of a threat. In combination, the two messages state the intention to conduct a certain (violent) act, convey the belief that this act will have negative consequences on the recipient, and have the intention to intimidate (Fraser, 1998). This threat is strengthened by the choice of words (e.g., 'bombs'), by the final sentence ('It might happen soon.'), and by contextual information: the Faculty is geographically located in the valley of the river Douro, hence the reference to 'down the slope'. This example shows that meanings are largely context-dependent, so an appropriate analysis of disputed meanings is essential, especially in investigative contexts.

Final remarks and recommendations for Law Enforcement

Language underlies all acts of human communication, including in criminal contexts, where it is crucial to interact with both victims and other criminals. Linguistic analysis is therefore a powerful tool in investigative contexts because criminals ignore that they can be identified by the language that they use – and even if they become aware of this fact, disguising one's language is usually not within the control of the speaker. Nonetheless, the power of linguistic analysis in forensic contexts has been underestimated, in no small part due to the mistaken assumption that, if we all learn the same language from the same books, then we all speak the language exactly the same; as has been empirically demonstrated, each speaker/writer of a language makes an idiosyncratic use of their language – their own 'idiolect,' in linguistic terms (Coulthard, 2004) – and that particular use is identifying. Therefore, this article strongly argues that linguistic analysis is crucial when investigating criminal activities, in general, and cybercriminal practices in particular, including: acts of cyber-violence; defamation; cyber-threats; dissemination of dangerous material; online harassment, cyber-bullying, cyber-stalking, or sexting; cyber-terrorism; hate speech; copyright infringement and piracy; and child pornography.

Despite its relevance for investigative purposes, research in forensic linguistics is frequently limited by access to data, and consequently insufficiently studied; in academic contexts, researchers can investigate and explore hypotheses using ordinary, naturally occurring data, so that the methods and techniques developed can later be used in forensic cases, if necessary. Ideally, however, such methods will be more reliable if developed and tested on real forensic data.

This article therefore concludes by making some recommendations for law enforcement: the first is that qualified forensic linguistics scholars are usually open to research collaboration with the forces, so police investigation, too, can take advantage of such research. This collaboration can start, for instance, by sharing fo-

rensic data for analysis. Notwithstanding the fact that there are often access restrictions, including legal, to real forensic data, gains for the forces are potentially significant if authorisation is cleared.

My second recommendation is related to training: law enforcement officers do not usually have in-depth training in forensic linguistic analysis, and neither are all of them expected to further their knowledge in the short run; instead, cooperation with forensic linguistics scholars to provide expertise in the field to assist with real cases can be coupled with the offer of training activities for the forces, so as to allow officers to gain at least some basic knowledge of the relevance of linguistic analysis in forensic contexts.

In the future, technology will be increasingly integrated with human communication, which means that the boundaries between crime and cybercrime will tend to fade; therefore, language (and its analysis) will play a core role in the fight against crime. This is the future of digital age, so may law enforcement be ready for it.

Acknowledgements

This work was partially supported by grant SFRH/BD/47890/2008 and post-doctoral research grant SFRH/BPD/100425/2014, FCT-Fundação para a Ciência e Tecnologia, Portugal, co-financed by POPH/FSE, and by national funds by FCT – Fundação para a Ciência e a Tecnologia, I.P., project UID/00022/2020. The present research was conducted in cooperation with the Cybercrime Office of the Prosecutor General's Office.

References

- Coulthard, M. (2004) Author identification, idiolect, and linguistic uniqueness. *Applied Linguistics*, *24*(4), 431–447.
- Coulthard, Malcolm, May, A., & Sousa-Silva, R. (Eds.) (2021). *The Routledge Handbook of Forensic Linguistics* (2.ª ed.). London and New York: Routledge.
- Coulthard, Malcolm, & Sousa-Silva, R. (2016) Forensic Linguistics. Em R. J. Dinis-Oliveira & T. Magalhães (Eds.), *What are Forensic Sciences? – Concepts, Scope and Future Perspectives*. Lisbon: Pactor.
- Finegan, E. (2008) *Language: Its Structure and Use* (6th, Inter ed.). Australia; United Kingdom: Wadsworth.
- Fraser, B. (1998) Threatening revisited. *Forensic Linguistics*, *5*(2), 159--173.
- Garner, B. A. (2009) *Black's Law Dictionary* (9th ed.). St. Paul, MN: West.
- Labov, W. (1972) *Sociolinguistic patterns*. Oxford: Basil Blackwell.
- Sousa-Silva, R. (2013) *Detecting plagiarism in the forensic linguistics turn* (PhD Thesis). Aston University.
- Sousa-Silva, R. (2017) *CybercrimeLab: A (computational) forensic linguistics approach against cybercrime*. Conference presentation at CEPOL 2017 Research and Science Conference INNOVATIONS IN LAW ENFORCEMENT Implications for practice, education and civil society, Budapest, Hungary.
- Turell, M. T. (2010) The use of textual, grammatical and sociolinguistic evidence in forensic text comparison. *The International Journal of Speech, Language and the Law*, *17*(2), 211–250.
- Turell, M. T. (2013) Presidential Address. In *Proceedings of the 3rd European Conference of The International Association of Forensic Linguists on the theme of «Bidging the Gaps between Language and the Law»*. Porto: Universidade do Porto - Faculdade de Letras.
- Wall, D. S. (2001) Cybercrimes and the Internet. In *Crime and the Internet* (pp. 1–17). London and New York: Routledge.

Identification of Invalid Information about the COVID-19 Coronavirus Pandemic on a Social Network Platform

Georgios Lygeros
Hellenic Police, Department of Patras

Abstract
The outbreak of COVID-19 caused a parallel contagion which affected the sphere of information called infodemic. Social media as a popular communication channel, enhanced the phenomenon of misinformation causing multidimensional effects both in societal and individual level. Twitter as a web forum, host various types of false content that either deliberately or unintentionally were posted from experts, politicians or civilians. This democratized environment may offer the opportunity of opinion exchange but can maximize the consequences of misinformation. Conspiracy theories, false therapies and dystopian future prediction monopolized Twitters daily activity highlighting the need of a supervisory mechanism which would eliminate such content. In this paper, Machine learning techniques are implemented in order to detect fake COVID-19 related content. For this purpose, algorithms of Natural Language Processing (NLP) are utilized.
The data used to train the algorithms are derived from a publicly accessible dataset that contains tweets related to the current pandemic and were published in Greek language. These tweets were classified and annotated in three categories, true, irrelevant, or false. Once a sufficient number of data has been annotated, the most common words are visualized through word clouds for each category. In addition, a set of linguistic and morphological features were extracted from them by applying methods of converting texts into vectors, as well as features related to the subjectivity of the tweets' texts.

Keywords: COVID-19, Social Media, Misinformation, Fake news, Machine Learning

Introduction

One of the most popular hashtags in 2020 on Twitter was #covid19. However, with the emergence of the COVID-19 pandemic, political and medical misinformation has grown rapidly, creating consequences that can actually exacerbate the spread of the epidemic itself. Conspiracy theories, pseudo-scientific treatments and lawsuits are just two indicative categories of misinformation and fake news that have found fertile ground due to the evolving situation. This pandemic of misinformation could not leave our country unaffected.

Given the dangers of spreading fake news, it is essential to address the phenomenon in a timely manner. However, with knowledge of how information is disseminated on a social network such as Twitter, patterns and potentially malicious activities aimed at misleading users can be detected. Computer science and Machine Learning are proving to be well suited for this purpose.

By utilising Machine Learning methods in the effort to detect fake news, the process can be automated, reducing the time required in the effort to control information to detect fake news but also helping to stop its spread.

The aim of this paper is to investigate the automated categorization of Tweets published on the Twitter platform, which are written in Greek and have as their thematic content the pandemic of COVID-19 and its evolution. The categorization is based on the computation of a set of morphological, semantic, PoS (Part of Speech) and statistical features, which are obtained by applying advanced NLP (NaturalLanguageProcessing) techniques to the text of the tweets. The categories into which it is desirable for tweets to be classified are derived based on the validity of their content i.e. whether they contain true, false or irrelevant information in relation to the pandemic. The automatic classification of tweets based on these characteristics is investigated through the application of Machine Learning algorithms.

The contribution of this work lies in the fact that for the first time, as far as we know, an attempt is made to detect false news and automatically categorize news originating from tweets written in Greek concerning the COVID-19 pandemic. Our language makes such an analysis a challenging task, which is why related work is quite difficult to come across. Also, in order to speed up the research, a web-based tool was built which enables the mass categorization of tweets. This tool makes the process of tagging tweets for a volunteer easier and more manageable and also brings about the acceleration of the pace of the process. In addition, the morphological and semantic features extracted are added features which are obtained by applying the TF-IDF method to the dataset. This addition adds new information that other implementations have not been taken into account.

Literature review

Many researches have been conducted focusing on the issue of the automatic categorization of fake content. A lot of them present the challenges that the specific scientific field is facing regarding the implementation of the NLP. These challenges are connected with the mining and processing of datasets and the performances of the models (ShuKai *et al.*, 2017) και (Oshikawa, Qian & Wang, 2018). Buntain and Golbeck (2017) used Twitter in order to detect fake news trying at the same time to identify the most important characteristics that compile the picture of fake news. There are many initiative that attempted to evaluate the trustworthiness of a particular tweet (Qazvinian *et al.*, 2011) or a user (Kang, O'Donovan & Höllerer, 2012), while others have focused more on temporal reputation propagation dynamics (Kwon *et al.*, 2013). Zervopoulos *et al.* (2020) approached the problem of automatic text categorization regarding valid and invalid news based on Twitter platform and concerning protests in the Hong Kong region. The authors of the specific work implemented various Machine Learning (ML) algorithms regardless the language of the Twitter post.

Another issue that NLP works have to overcome is the labelling processes that are followed. Labeling is a crucial step as the generated results are strongly connected with the quality of the labeling process. The available dataset usually is not categorized and the categorization is a part of the implementation.

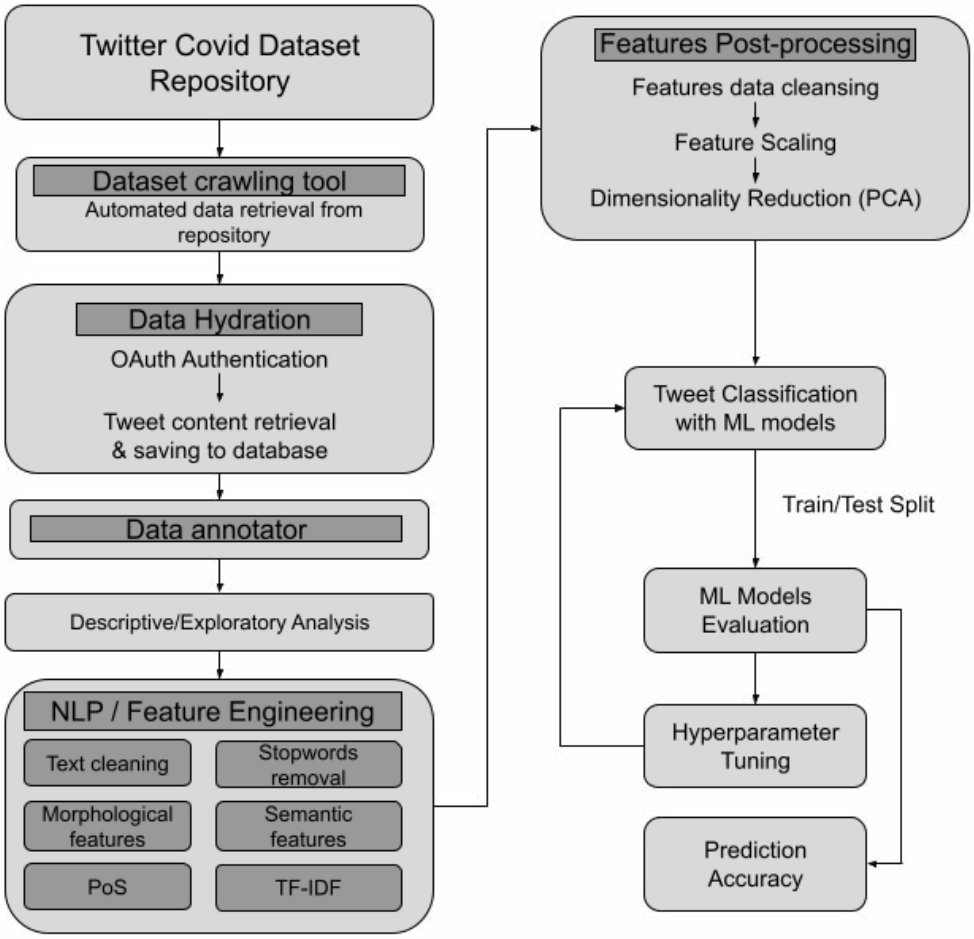
Recently a number of COVID-19 oriented datasets have been published whose data are not categorized based on the criterion of the detection of misinformation (Cui & Lee, 2020; Memon & Carley, 2020; Qazi *et al.*, 2020). Although there are datasets which characterize the data as disinformation data (Brennen *et al.*, 2020), datasets containing data with "true" news about COVID-19 are also rare. Memon and Carley (2020) focused on the characterization of disinformation communities on the subject of COVID-19 through data collected from Twitter.

Methodology

System Architecture and Implementation

The system implemented in this thesis can be analysed according to the diagram in Figure 1. Firstly, the identifiers of the tweets of interest are retrieved from the online repository hosting the dataset. For this purpose, a special crawler tool was created, which can search the data in the repository using criteria such as the date and language of the tweets. Then, based on the tweets' identifiers, a connection to Twitter's API for hydration of the tweets is made and the tweets are stored in the mongoDB database. The process of tagging the data into three categories follows. To facilitate this time-consuming process, a web application was implemented which downloads the content of the tweets stored in the database and through appropriate interface tools allows the quick selection of the most appropriate category to which each one belongs

Figure 1. System Implementation



After the tagging process is completed, a descriptive analysis of the data is performed for basic understanding and drawing conclusions about their structure and finding characteristic patterns. This is followed by a process of applying natural language processing methods, through which the available texts from each tweet are cleaned of unnecessary elements or elements that do not contribute meaningfully to the sentence and a set of features is extracted from the morphology, topic and words of each text. In addition, the TF-IDF method is applied through which the most significant words in the available dataset are identified.

This is followed by the process in which the extracted feature set, together with the categories of significant words obtained by applying TF-IDF are added to a single feature matrix. Post-processing techniques such as scaling and extraction of the most significant features by PCA method are applied to this matrix to reduce the dimensions of the matrix. After this step, the features matrix is divided into train-set and test-set which are then used to train and evaluate the machine learning algorithms being tested. Finally, for each algorithm, the basic parameters are optimized to obtain more accurate results.

Data collection

To solve the problem of identifying and categorizing tweets, a portion of the COVID-19 Twitter chatter dataset was used (Banda *et al.*, 2021). This dataset started to be generated from March 11, 2020, yielding over 4 million tweets per day. Daily hashtags, references to other users, emojis and their frequencies have been included. To make the dataset easier to use, the language in which the tweets are written is included in addition to the unique identifiers (IDs) of the tweets. The full dataset covers all languages; however, the most prevalent ones are English, Spanish and French. The dataset includes 903,223,501 tweets and retweets. In addition, a clean version without retweets is provided (226,582,903 unique tweets). For the convenience of NLP applications, the top 1000 most frequently en-

countered terms are additionally provided, as well as the top 1000 bigrams and trigrams, which are stored, separated by day, daily in an online repository on the github platform.

Description and download of data

The information related to the tweets within the datasets stored on github consists only of their unique attribute (tweet ID), the date and time of publication, the language they are written in and the country they originated from.

For the purpose of this Thesis, tweets published between November 1, 2020 and December 30, 2020 were used. To achieve the collection of these tweets, a tool was built using the Python language that allows automatic storage of tweets from github to the local computer storage in CSV format. This tool also gives the possibility to select the range of dates for which the collection of tweets is desired and the language in which they are written. In this particular case, the dates are the range mentioned earlier while the language is Greek whose abbreviation in which the tweets are stored on github is "el". Important to say is the fact that the tweets are collected from the clean versions of the dataset so there is no concern about duplicates of the tweets being collected. A total of 61,147 tweetIDs were collected.

Tweethydrator

Obviously, the information stored locally is not sufficient for the purposes of this Thesis as the full texts of the tweets need to be available in order to perform the appropriate analysis. To achieve this a tool was built to interface with the Twitter API. Through this tool, the data of the tweets included in the local data is identified, their content is downloaded locally to the server running the tool and then stored in a mongoDB database.

Data annotation

The algorithms used in this Thesis require the prior knowledge of the category a tweet belongs to depending on how valid their thematic content is in order to be trained correctly (to perform accurate training) and then generate models that will categorize new tweets accurately. In the context of this Work, the discretization of tweets into three categories was chosen. As there was no professional support in the tagging process, only three categories were chosen which characterize a tweet according to its content. These categories are:

1) Tweets which are objectively true. Such tweets are for example news posts related to the pandemic, news about Sars-Cov-2 virus, posts related to pandemic containment measures and so on.

2) Tweets that are considered false. False posts are defined as posts that are related to the virus but have controversial or satirical content. However, this classification is difficult as it requires knowledge of the facts that are being reported.

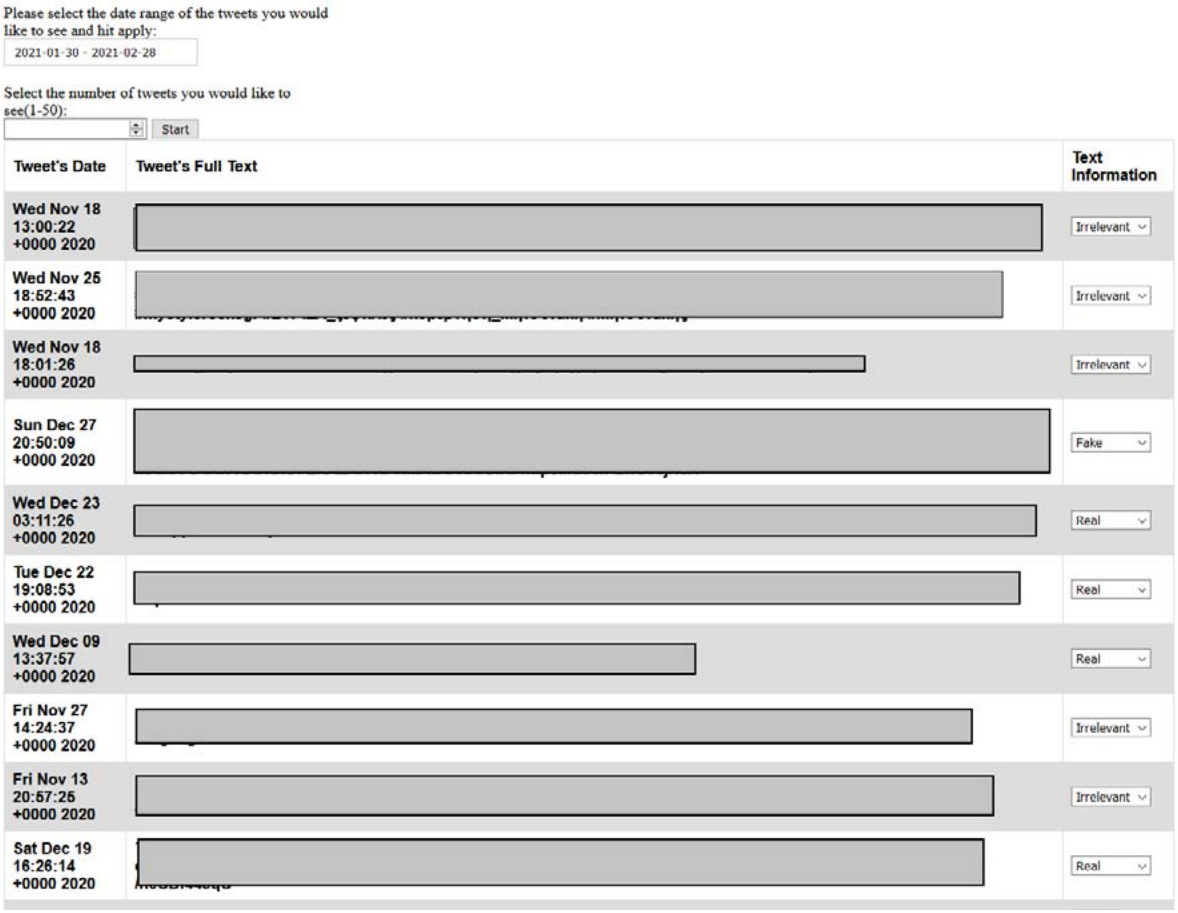
3) Finally, publications which are not related to the development of the events of the pandemic are classified as irrelevant. For example, the post "With #COVID19 only Playstation and Netflix" is easily classified as irrelevant.

It should be noted at this point that the selection of the curves based on which to discretize the categories of the dataset is a complex task that requires a good knowledge of the problem and therefore the correctness of the categories and the method of characterization of the tweets can be reviewed.

However, for tagging another problem exists. Selecting tweets one by one and adding tag is an extremely time-consuming process. For this reason, an online annotator tool (online Tweet Annotator) was built using the Python language with the help of its library, flask, or which is oriented towards web application development.

Through this application a user can select a date range for which he/she wishes to tag tweets and also the number of tweets he/she wishes to display on his/her screen. These tweets are randomly selected from the database as long as they are within the range selected by the user and have not been tagged previously. The tweets are then displayed on the website showing their full text. The tweets are then stored in the mongodb database, updated by adding their categorization to their information, following a user selection.

Figure 2. Online Tweet Annotator



For the purposes of this paper, a total of 3931 tweets were tagged. Of these tweets, 1906 belong to the real category, 1017 to the fake category and 1018 to the irrelevant category. The distribution of annotated tweets is shown in Figure 3.

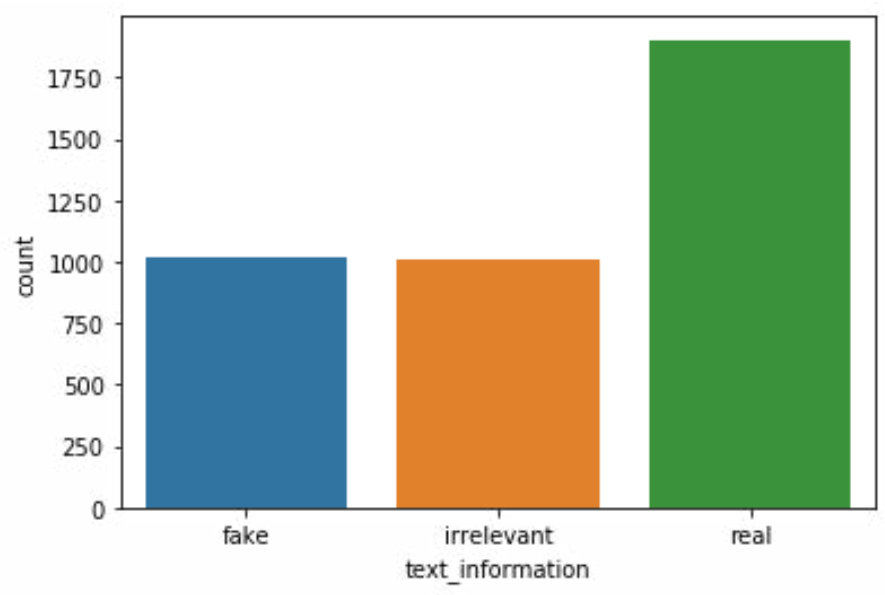
Descriptive analysis of the data

In order to understand the available data, check their validity and draw primary conclusions about the categories chosen to discriminate the dataset (fake, irrelevant, clear), a descriptive analysis of the available data is performed. In particular, it is checked whether there are incomplete fields or fields that have been lost due to an error. In addition, descriptive graphs are extracted which depict various statistics such as for each category the number of words contained in the tweets as well as the length in characters.

Extraction of features

To extract the features, first those tweets are retrieved from the mongoDB database that have been categorized and then converted into a Pandas Data Frame to make them easier to manage. The fields chosen to be retrieved from the tweets' information are their full text, their publication date and the category they belong to. Through an iteration structure that runs through the entire content of the Data Frame, various preprocessing techniques are performed, through appropriate functions, to extract the features effectively. The extraction of all features is done through special functions implemented for this purpose, in combination with functions from the spaCy and NLTK libraries in cases where this is necessary.

Figure 3. Distribution of annotated tweets



Text cleaning and extraction of morphological features

Two basic functions were implemented with which to perform text cleaning. Text cleaning is defined as the stripping of URLs, emojis, entities (mentions), and hashtags from their content. This was implemented with the help of a function that was implemented which cuts out the above according to specific regexes that cover the criteria by which they appear. What this function returns is the content of the texts of the tweets without the parts that have been cut off with the clean_text nomenclature, which is very useful for extracting various features as in some cases it is necessary for the texts to be in this format.

The next function implemented for clearing the texts converts the texts into lists of tokens. Before this is done some steps are taken to ensure that the tokens have the desired format. These are as follows:

- Deleting emojis from the text of the tweets
- Deleting all digits from the text and replacing them with the blank
- Deleting all the punctuation marks
- Deleting all stopwords (via spaCy and NLTK functions)
- Deleting tokens of less than 3 characters

The lists of words returned by this function contain the content of the text free of what was deleted during its execution with the words nomenclature.

The clean_text returned by the above function is used as input to the functions which extract most of the morphological features. To be precise the extraction of the features concerning, the length of the text, the count of the different punctuation marks ("?!", "?", "!", ".", ";" etc.) and their total number and finally tweet_entropy is done via functions implemented with "plain" Python in combination with the re library which provides an easy way to identify regex within the text. The tweet_entropy is extracted by a function implemented that does the mathematical calculation for the entropy of the text.

There are two more functions which take clean_text as input. The first one calculates the number of consonants and vowels present in a tweet and therefore the corresponding attributes are calculated through it. First, any suffix and tone of words are removed from clean_text and then each character is categorized according to whether it is a consonant or a vowel. As a result, their count is easily computable. The second function returns using "plain" Python the number of capitals, lowercase, digits, letters and the letter-to-digit ratio which also correspond to the corresponding attributes.

The attribute corresponding to the average word count per sentence comes from a function which, with the argument clean_text, initially converts the text content into tokens with the help of the NLTK library which supports this function in Greek as well. Then the punctuation marks are subtracted and from there the average is calculated with a simple calculation.

The last features that use clean_text to produce the text have to do with the number of consecutive consonants, the number of consecutive vowels and the number of occurrences of repeated identical characters. These three attributes are computed through a function that has similar logic to the function that computes the total number of consonants and vowels described above. The calculation of the first two features is calculated directly from lists of characters (consonants, vowels) generated at runtime, while the number of consecutive occurrences of a character (>3) is calculated from a list containing all characters of a text.

The function that returns the words is useful in extracting two features. The first attribute concerns the average length of words which is computed by a function that takes words as an argument. The first step that this function performs is to call the function that generates clean_text by giving the list of words as an argument. Then the calculation of the average is again done through a simple mathematical calculation. The second feature concerns the number of words present in a text which is quite easy to calculate through the length of the words list.

Finally, there are features which can be calculated from the original text of the tweets without any processing. For example, the attributes related to the number of urls, mentions and hashtags are generated through functions that check the content for words starting with "http{.....}", "@" and "#" respectively, which are numbered. The attribute having to do with the number of entities is calculated from the sum of the above. It is important to say that a check is performed to see whether a url is functional or not, so in the counting only the functional ones are taken into account. Stopwords are one of the attributes counted via a function that again has the original text of a tweet in its argument. This function returns the number of stopwords contained in a tweet with the help of the functions that extract them from the spaCy and NLTK libraries. Although these functions recognize most of the Greek stopwords, some were added that these functions do not recognize.

Exporting SemanticFeatures

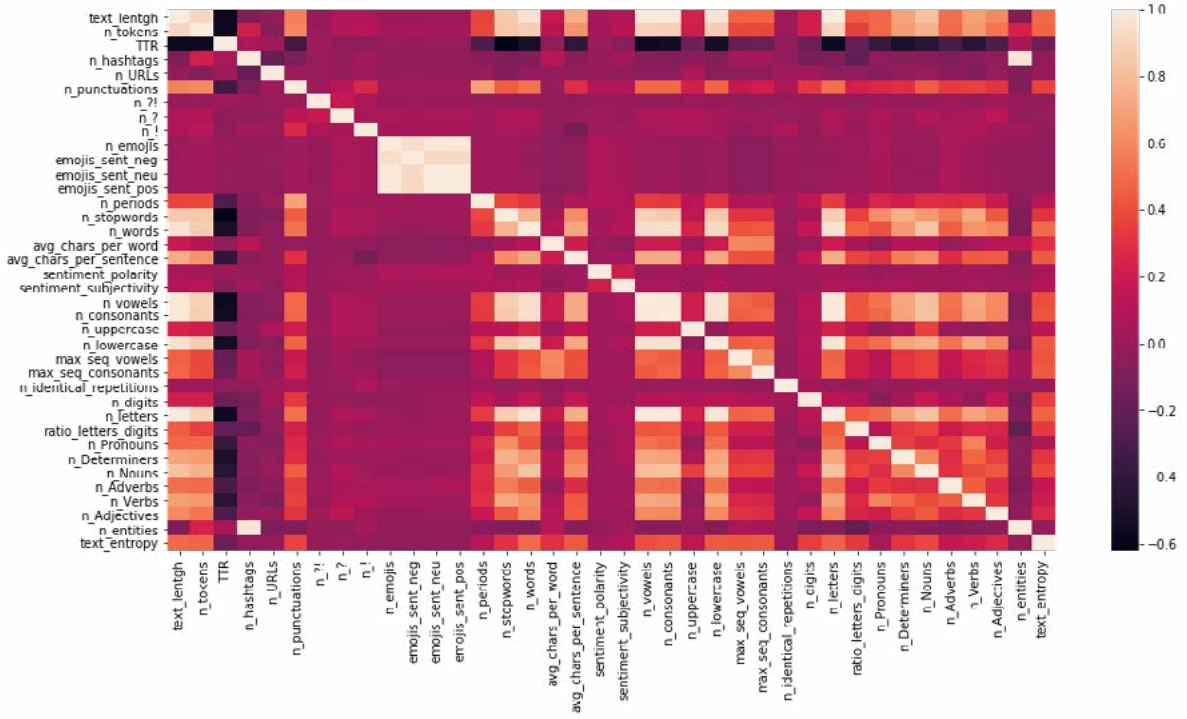
Exporting semanticfeatures is a difficult task to implement. However, as the field is constantly evolving, libraries have been developed which can extract such features in a partially automated way. For the purposes of this thesis, the spaCy library was used through which, with two simple commands, the objectivity of a text and its polarity can be extracted, and thus the corresponding features are computed directly. Also a successful metric, is the counting of positive, negative and neutral emoji contained in a text. The computation of these attributes is done in two steps. In the first stage all emoticons contained in a tweet are searched through a function and then in the second stage they are categorized into negative, positive and neutral emoticons and counted. The former are implemented through regexmatching, a very common way to find emoji as well as the categorization is done based on a list of emojis containing all possible emojis and their rating, which is provided by the emosent library.

Exporting PoS (Part of Speech) features

The calculation of PoSfeatures is done through the nlp_post_processing function implemented with the help of experts in the spaCy library, which has special tools for calculating such features. Initially, LexicalRichness is used through which a metric is computed that represents the "richness" of the text with respect to the variety of words used. Through this metric another function of LexicalRichness can be used which calculates the TTR of the text which corresponds to the corresponding feature. Then, three lists are generated containing tokens into which the text is divided, the PoS categorizations found and the lemmas (lemmas) generated respectively. These lists are generated via special spaCy text processing and parsing functions that support the Greek language and grammar. From the list of categorised PoS found, the features concerning the number of occurrences of pronouns, determiners, adjectives, nouns, adverbs and entities present in a tweet are directly computed. In nlp_post_processing there are also the functions that compute the objectivity and polarization of the text.

The set of extracted features and the degree of correlation between them is illustrated in Figure 4:

Figure 4. Correlation matrix of the key features extracted from the texts of the available tweets



Calculation of the TF-IDF feature

Next, the TF-IDF method is implemented using the TfidffVectorizer function of the scikit-learn library. To generate the text vectors needed to implement TF-IDF, a function is used to join the entries generated by nlp_post_processing. This is done so that the number of different words, and thus the number of feature dimensions, is significantly reduced as the TfidffVectorizer function generates features for each individual word it detects within the text. A set of features are thus extracted which correspond to the most significant words in the dataset. These features are combined with the previous morphological features, PoS and semanticfeatures, into a single featurematrix which has dimensions (3931 x 10923), i.e. a total of 10923 features are computed!

Algorithm training

Before training the algorithms, the collected features are transformed so that they all have the same range of values. The Standard Scaler class of scikit-learn is used for the normalization.

After the features are transformed, PCA is then applied to reduce the dimensionality of the features matrix, which is deemed necessary due to the number of features. PCA is parameterized to extract the minimum number of dimensions needed to maintain 95% of the variance. The results show that instead of 10923, only 2745 basic features are needed! It also turns out that, this data represents almost 25% of the size of the original feature smatrix. In a way, this is a kind of Feature Selection. Obviously, after dimensionality reduction, the feature matrix takes up much less space and this can significantly speed up a classification algorithm (such as classification based on the SVM algorithm).

Finally, the data is divided into train and test. The train data will be used to train the learning algorithm and the test data will be used to verify the results. For the separation, 80% of all available data is used as train data and 20% as test data.

The SVM algorithm is the first algorithm tested for its ability to classify tweets based on the classes defined. Initially the parameters of the algorithm are set which are as follows:

- Kernel: the “rbf” kernel is used.
- C: 1
- Gamma: Scale. this means that the gamma is derived from the ratio 1/ (<number of features> x <scale of trainmatrix>)

Hyperparameter Tuning is then applied using the GridSearch method (Bao and Liu, 2006). In this case, “line-

ar" is additionally tested as kernel, as well as different combinations of C and gamma values. Next algorithm tested is Random Forest. For Random Forest a similar procedure is followed. Initially training is done with the initial training parameters. Then using the function Randomized Search CV a set of combinations of the parameters is generated, from which the algorithm randomly selects which ones to train. Finally, training is performed using Multinomial Naïve Bayes. As this algorithm relies on the use of probabilities it cannot accept negative values. Therefore, in this case the data is normalized in the interval 0 to 1 using the Min Max Scaler class.

Results

This chapter presents the results of the descriptive analysis and the Machine Learning algorithms applied. First, within the descriptive analysis, some basic statistics characterizing the tweets are visualized.

Figure 5. Number of characters in a tweet depending on the category it belongs to.

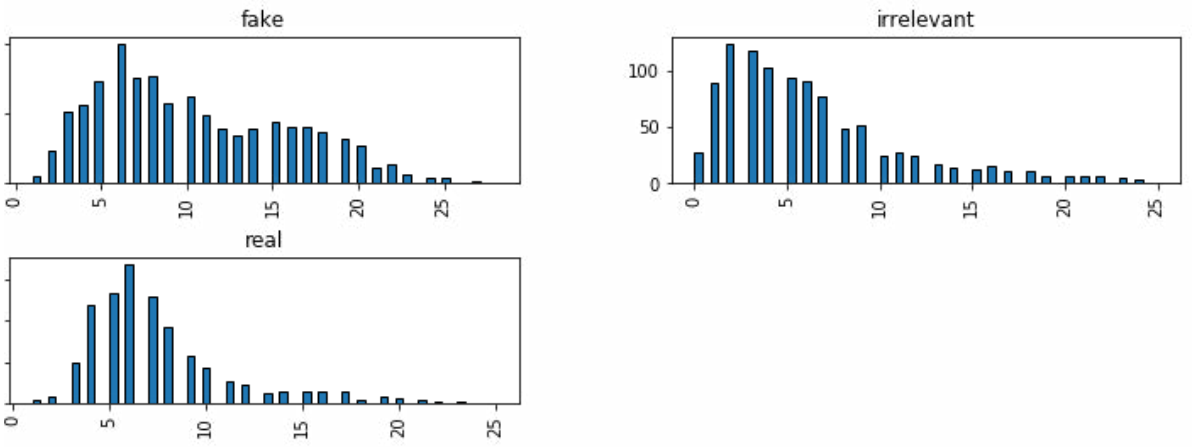
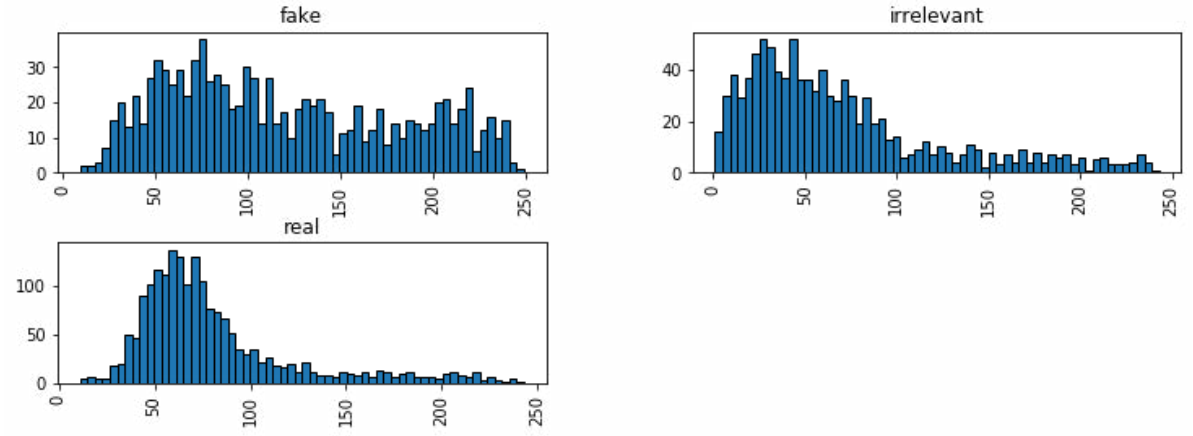


Figure 6. Number of words in a tweet depending on the category it belongs to.



As can be seen from Figures 5 and 6, there seems to be some correlation between the length of the tweet in words and the number of characters with the fake category, i.e. compared to the other two categories, many tweets have a larger number of words and characters.

In addition, visualization of the most important terms in wordclouds is done. More specifically, for each category the 50 most frequently encountered words are identified and visualized. In addition to the most frequent words per category, the most frequent words in the dataset are also presented, which are visualized in Figure 7.

Figure 7. Wordcloud for the whole dataset

In the following, the results of the algorithms tested for the categorization of tweets are presented and analyzed. As described in the previous chapter, the training of the set of algorithms is done using those features that correspond to 95% of the dataset. As the results of the algorithms show, although with a low percentage, it is possible to identify a tweet as real, fake or irrelevant based on the characteristics described in the previous chapter. Among the algorithms tested, the best performance is achieved by the Random Forest algorithm using the Randomized Search method as it better distinguishes tweets of each category compared to the other algorithms. Worst performance was achieved by the Multinomial Naïve Bayes algorithm.

Table 1. Summary results of the algorithms tested

Algorithm	Precision	Recall	F1-Score
SVM	0.68	0.53	0.51
SVM + Gridsearch	0.59	0.57	0.57
RandomForest	0.65	0.61	0.62
RandomForest + Randomizedsearch	0.66	0.61	0.62
MultinomialNaiveBayes	0.65	0.47	0.45

Conclusion

Currents' work aim was to approach computationally the posts in the social network of Twitter, assisting the task of identifying false or irrelevant posts related to the current pandemic COVID-19 and its spread in Greece. We focused on Twitter as its structure and main features allow the detection of trends which are related to the current events. The aim of the activities was to find morphological features of the tweets, as well as features related to the subjectivity of the texts, which allow automatic discriminating between false and true statements in order to categorize them according to their reliability.

For the purposes of our work, we used a ready-made dataset related to tweets that are related to the pandemic. For convenience, our study period is only the period between November 1, 2020 and December 31, 2020. Two tools were implemented, one to automatically retrieve from the dataset the identifiers of tweets that were published during the specific period and are written in Greek. In addition, another tool is implemented which for each of the collected identifiers retrieves their full content from the Twitter platform and stores it in a MongoDB database.

As Machine Learning classification algorithms rely on the use of training data for which the classification category is known in advance, a part of the work involved recording the category for the collected tweets. A total of 3931 tweets were manually classified into three categories, real, fake and irrelevant. To speed up this process, a new tool was created to allow for quick viewing of tweets and tagging.

From the data, by applying transformation methods these 38 features were extracted which are related to the linguistic morphology of the tweets, their subjectivity, sentiment analysis and the type of words used. Moreover, an innovation of this Work is the use of features obtained by applying the TF-IDF method to the texts of the collected publications. However, as the dimensions of the features were exploded, it was necessary to use dimensionality reduction using the PCA method.

The application of these features to Machine Learning algorithms for automatic classification showed unsatisfactory but encouraging results for solving the problem. The cause of the low accuracy of the algorithms is traced to two factors. On the one hand, the difficulty of discriminating even for skilled personnel between publications of different categories, as the distinction between correct and false news is based on factual knowledge. This cannot be achieved by exploiting only linguistic features. Also, the number of categories into which tweets are distinguished is certainly expected to affect accuracy, as specialized knowledge is also required for the number and characterization of the categories selected.

With these two findings as a starting point, the impetus for further research on the problem is given. To begin with, the extraction of knowledge about the subject matter and the use of this information in classification can be studied. Also important is the contribution to the validity of a publication of the credibility of the user who made the publication. Finally, the discretization of tweets into different categories as well as the characterization of larger volumes of data will certainly reveal new ways to achieve the final goal.

In conclusion, at a time when conspiracies and fear abound, the police science/ law enforcement have an opportunity to protect the public from misinformation, as well as to enforce the law to protect public health and public safety. This research is intended to help law enforcement authorities detect immediately false news and provide an understanding of what is driving the misinformation that might compromise public safety.

Gaining the first-mover advantage by distributing correct information about COVID-19 and going first, has been shown to reduce the influence of subsequent misinformation, as the first piece of information heard tends to be what sticks.

By detecting fake news in a timely manner, citizens will be able to be informed of the truth and not be misled by individuals or organizations whose purpose is to harm social cohesion, the state and the well-being of society in general.

References

- Banda, J. M. *et al.* (2021) 'A large-scale COVID-19 Twitter chatter dataset for open scientific research—an international collaboration', *Epidemiologia*. MDPI, 2(3), pp. 315–324.
- Bao, Y. & Liu, Z. (2006) 'A fast grid search method in support vector regression forecasting time series', in *International Conference on Intelligent Data Engineering and Automated Learning*, pp. 504–511.
- Brennen, J. S. *et al.* (2020) *Types, sources, and claims of COVID-19 misinformation*. University of Oxford.
- Buntain, C. & Golbeck, J. (2017) 'Automatically Identifying Fake News in Popular Twitter Threads', in *Proceedings - 2nd IEEE International Conference on Smart Cloud, SmartCloud 2017*, pp. 208–215. doi: 10.1109/SmartCloud.2017.40.

- Cui, L. & Lee, D. (2020) 'Coaid: Covid-19 healthcare misinformation dataset', *arXiv preprint arXiv:2006.00885*.
- Kang, B., O'Donovan, J. & Höllerer, T. (2012) 'Modeling topic specific credibility on twitter', in *Proceedings of the 2012 ACM international conference on Intelligent User Interfaces*, pp. 179–188.
- Kwon, S. *et al.* (2013) 'Prominent features of rumor propagation in online social media', in *2013 IEEE 13th international conference on data mining*, pp. 1103–1108.
- Memon, S. A. & Carley, K. M. (2020) 'Characterizing covid-19 misinformation communities using a novel twitter dataset', *arXiv preprint arXiv:2008.00791*.
- Oshikawa, R., Qian, J. & Wang, W. Y. (2018) 'A survey on natural language processing for fake news detection', *arXiv preprint arXiv:1811.00770*.
- Qazi, U., Imran, M. & Ofli, F. (2020) 'GeoCoV19: a dataset of hundreds of millions of multilingual COVID-19 tweets with location information', *SIGSPATIAL Special*. ACM New York, NY, USA, 12(1), pp. 6–15.
- Qazvinian, V. *et al.* (2011) 'Rumor has it: Identifying misinformation in microblogs', in *Proceedings of the 2011 conference on empirical methods in natural language processing*, pp. 1589–1599.
- ShuKai *et al.* (2017) 'Fake News Detection on Social Media', *ACM SIGKDD Explorations Newsletter*. ACM PUB27 New York, NY, USA, 19(1), pp. 22–36. doi: 10.1145/3137597.3137600.
- Zervopoulos, A. *et al.* (2020) 'Hong Kong protests: using natural language processing for fake news detection on twitter', in *IFIP International Conference on Artificial Intelligence Applications and Innovations*, pp. 408–419.

Cold Case – Solved & Unsolved: Use of digital tools and data science techniques to facilitate cold case investigation

Tatjana Kuznecova
Dimitar Rangelov
Saxion University of Applied Sciences, Enschede[1]

Jaap Knotter
Saxion University of Applied Sciences, Enschede & Dutch Police Academy

Abstract
On average 125 murders take place in the Netherlands on an annual basis. However, not all such incidents can be solved. Currently there are more than 1700 unsolved homicide cases on the shelf at the National Police that classify as a 'cold case'. Investigation into these types of capital offenses takes a lot of time, money, and capacity. Applications of the current working method and available techniques are very labor-intensive and time-consuming. In addition, the pressure on the executive Police officers is high - from the Police organization, the Public Prosecution Service, the media, the next of kin, as well as society in general.
From an investigative point of view, it is relevant to provide direction in the criminal investigation and formulate and evaluate various case scenarios, while reducing a risk of 'tunnel vision'. From a scientific point of view, more research into homicide cases in the Netherlands is of eminent importance. Remarkably little has been written in scientific literature about this type of crime.
The project 'Cold Case: Solved & Unsolved' focused on the use of open, publicly available information sources to collect the data and gain more insight into homicide cases in The Netherlands. Applicability of various modern techniques, such as web-scraping, API software and Artificial Intelligence (AI) was explored to facilitate and automate data collection and processing tasks. A first concept of a 'smart' database was proposed, combining a web-based database platform with AI modules to filter and (pre-)process the data. With further development and training of AI modules, such a database might eventually support data-driven generation and/or prioritization of investigative scenarios. The data collected in the process was used in three scientific studies aimed at uncovering the relationships and patterns in the homicide data for The Netherlands.

Keywords: homicide, natural language processing, artificial intelligence, data science, open source data

1 Corresponding author's email: t.kuznecova@saxion.nl

Introduction

On average 125 murders take place in the Netherlands on an annual basis since 2015 (CBS, 2021). Investigation into these types of capital offenses takes a lot of time, money, and capacity. In addition, the pressure on the executive Police officers is high. Both from the Police organization, the Public Prosecution Service, the media, the next of kin, but also from society in general. The investigations by the Police are often followed closely.

Unfortunately, not all murder and manslaughter incidents can be solved. Currently there are more than 1700 unsolved murder and manslaughter cases that are on the shelf at the National Police that classify as "cold case" (see: National Police/Cold case infographic at Politie (2020)).

Within these types of unresolved files, there is often a lack of technologies and tools to deal with the crimes more effectively and efficiently. Applications of the current working methods and available techniques are very labor-intensive and time-consuming. It is crucial that a perpetrator is quickly identified and that he or she can be convicted for the offense committed.

From a scientific point of view, more research into murder and homicide in the Netherlands is of eminent importance. Still rather little has been written in scientific literature about this type of crime, especially compared to the United States (Liem *et al.*, 2013). Within the Dutch Police Academy, the insights from international studies are largely used (such as Adcock & Chancellor (2016) and Adcock & Stein (2017)). However, the question is whether that knowledge can apply to the Dutch situation one-to-one.

There is also a lack of consolidated datasets/databases that use an effective data structure, which may enable detection and exploration of patterns and relationships in the historical homicide cases in The Netherlands. One of the most widely used sources for international comparisons on homicide is the data about the cause of death, such as WHO Mortality Database[2], which only contains information on the number and characteristics of victims. One attempt at developing a unified homicide database framework is The European Homicide Monitor (EHM) that offers a dataset including 85 variables describing homicides in 2003-2006 in Sweden, Netherlands and Finland (Ganpat *et al.*, 2011; Liem *et al.*, 2013). However, a shortage of well-structured or labelled data still poses a serious limitation to the use of data-driven computational approaches, like machine learning, that often require structured datasets as an input.

Data-driven techniques are sometimes used in Police work, at least at a level of research and innovation development. An example of this are tools for predictive policing. For instance, CAS tool was developed for burglary prediction in The Netherlands (Mali, Bronkhorst-Giesen and den Hengst, 2017). However, a previously highlighted limited amount of structured data, as well as inconsistency in data collection and processing methods, create a significant bottleneck in implementing such methods and systems in practice. Given that data-driven techniques may eventually support scenario development and prioritization in crime investigation, it is beneficial to develop a database, where the variables and values are consistent and standardized, when possible. However, collection, pre-processing and analysis of large amounts of information on homicide cases can be very time-consuming and laborious. Therefore it is also paramount to explore what modern techniques and to what extent can be used to automate these processes and reduce data collection or digitization efforts.

Research group Technologies for Crime Investigation (formerly known as Advanced Forensic Technology) is a joint research group between Saxion University of Applied Sciences and Dutch Police Academy. The research group focuses on several pillar topics – CrimeBots (Robotics applications), Nano4Crime (Nanotechnology and sensing) and - a new research line - Data Science & Crime. The first project in the research line of Data Science & Crime is the project 'Cold Case: Solved and Unsolved'. One of the goals of this project was to investigate to what extent modern digital technologies and data science techniques can be used to collect, process, store and analyze data on homicide cases. The project also used a framework by de Kock (2014) as an inspiration to design the data structure for a dataset development. In this framework, twelve so-called Elementary Scenario Components (further referred to as ESC12) can be used to describe any storyline, including a crime scenario. De Kock proposed that ESC12 can be used to build a (smart) database combined with modern data science techniques that could facilitate

2 WHO Mortality Database: https://platform.who.int/mortality

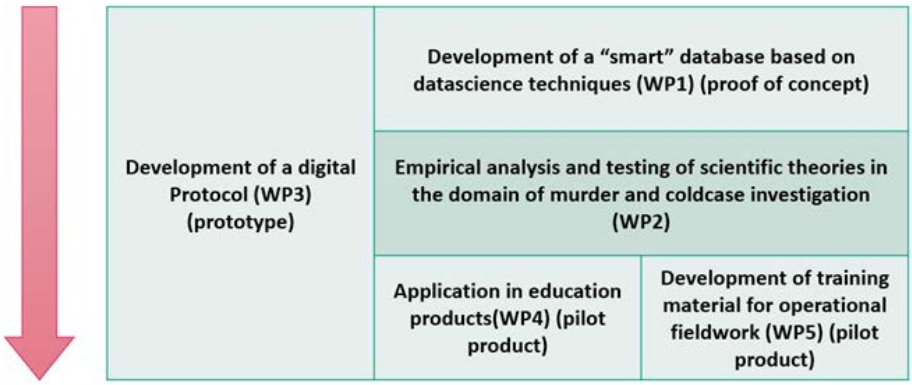
the analysis of the crime cases, make predictions, fill in the knowledge gaps by analyzing historical cases and comparing them with the current investigations (de Kock, 2014).

Furthermore, we focused almost exclusively on the use of open source data. While it could be highly beneficial to use confidential Police data or a combination of confidential and public data, access to such data was not possible in the frames of this project. It should be noted, however, that techniques discussed in this paper can apply to open source and confidential data alike.

Research scope

The project 'Cold Case: Solved & Unsolved' investigated to what extent modern digital tools, computational approaches and data science techniques can facilitate data collection and processing on homicide cases and help organize and direct the investigations. Another objective of the project was to integrate the developed knowledge and tools in the educational process and training materials for the forensic and police science students. The project consisted of five work packages, where each work package had its own objectives (Figure 1). This paper mostly covers the work done with in Work Packages 1 and 2 that focused on data collection, pre-processing, storage, and analysis of patterns and relationships.

Figure 1. 'Cold Case: Solved & Unsolved' project structure (source: authors)



Work Package 1 'Data collection and development of a 'smart' homicide database' mostly dealt with technology development to facilitate collection, pre-processing, and storage of the homicide data. It also covered the actual collection of the data from open sources using a combination of manual and (semi-)automated methods. As an important objective, various possibilities for automation of data (pre-)processing have been explored using Artificial Intelligence (AI) techniques, such as: a) automatically distinguish articles about homicides from other topics (pre-filtering); b) generate a short summary of an article; c) extract interesting information/components from an articles, such as ESC12. In the future, collected data and identified techniques are envisaged for the integration in a 'smart' database platform that can eventually facilitate crime analysis and investigation with data-driven methods.

The goal of Work Package 2 'Empirical analysis of the homicide data in The Netherlands' was to conduct scientific studies using the data collected in Work Package 1. It included application of various statistical methods and data modelling techniques to test theories and hypotheses. The results of this work package can reinforce theoretical understanding of the relationships and patterns occurring in the homicide cases specifically in The Netherlands, which can further be compared to the similar studies in other countries.

Main results and outputs

This section provides an overview on the main outcomes for the sub-objectives described in Chapter 2, concerning data collection, AI research and analysis of relationships and patterns in the homicide data.

Data collection

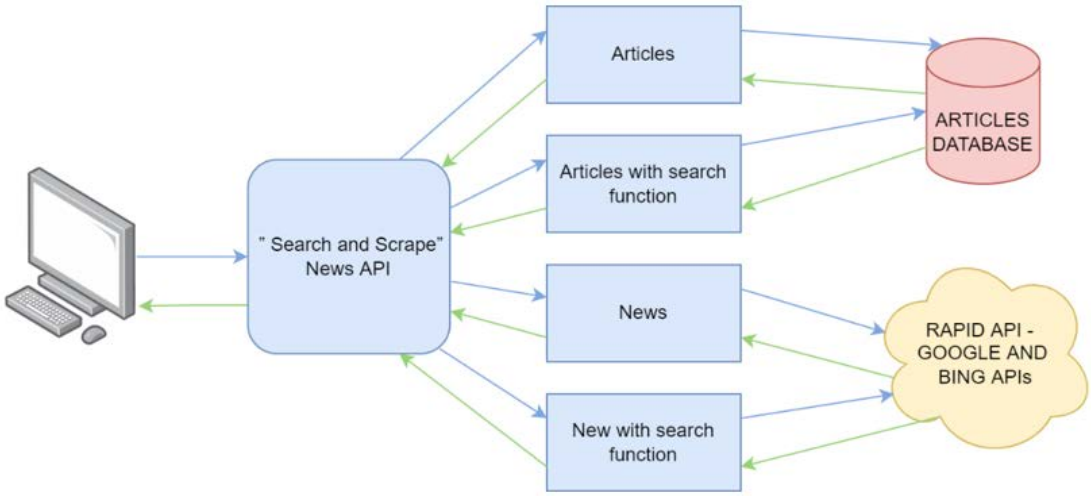
In this project, several types of data were collected using a variety of techniques. One stream of data consisted of a collection of articles on homicide-related topics. Another dataset was created manually by structuring information on homicide cases into a database template for further applications in data analysis and modelling studies. Lastly, a software tool (API) was developed to facilitate and automate collection of homicide-related articles from open sources.

The collection of articles about homicide cases was performed with the help of Python programming language. It was split in two flows. The first flow was a *'site scraper bot'*, which scraped the news, archives, and articles about homicide cases in a variety of websites. The second flow was based on *'Optical Character Recognition'* (OCR), which was used to process old newspaper archives from the Delpher portal[3]. The articles from these two approaches were filtered through the algorithm that decided whether articles concern homicide cases or other topics. With the combination of these two approaches, around 11 000 articles mentioning homicide cases were collected.

With the help of the students of Cold Case Minor course (year 2020) at Saxion University of Applied Sciences, another dataset was collected and processed in detail with manual techniques using information on around 300 homicide cases in The Netherlands for the period of 2006-2015. Each student was assigned a list of cases that he/she had to collect the data on. A template was developed and provided to the students that contained the desired data structure. In this project, a framework by de Kock (2014) on ESC12 was used as a basis for the dataset structure. For each case, students had to use at least five information sources (when possible). Further, students had to extract the necessary information and fill in the provided template. The resulting dataset was used in the studies on data analysis and modelling to uncover the patterns in the data.

It is paramount to have as much data on homicides as possible to make use of data-driven approaches. This data can be used: a) for empirical analysis and development of data models and analysis of relationships and patterns; b) and training and tuning of AI algorithms. Furthermore, the relevant data can come in different formats and from different sources. To facilitate the data collection process, an API (Figure 2) was developed that can be used as a standalone tool, or eventually in conjunction with other software (e.g., connected with a database platform). Several sources were pre-defined for the tool (such as BING News, Google News). The tool's architecture allows for an easy connection to a wider range of sources in the future.

Figure 2. 'Search and Scrape API schematic (source: authors)



3 Delpher newspaper archive: https://www.delpher.nl

Research and Development in AI

AI development was conducted in three directions:

1. distinguish homicide article from other topics
2. generate a summary of an article
3. automate extraction of interesting components, such as ESC12.

The work method is mainly focused on Natural Language Processing (NLP) family of algorithms. NLP is usually used to process, analyze, and extract information from natural human language data (such as texts). Given the complexity of human language, different neural network-based methods have been developed to date, among them Word2Vec, Sense2Vec and other. The main model used within the project is the Bidirectional Encoder Representations from Transformers (BERT) (Devlin *et al.*, 2019). Processing pipelines based on known methods were developed to tackle the described tasks.

The most challenging part of AI research was extracting the interesting components from text automatically (for instance, name of a victim or perpetrator, date or location of a crime, etc.). The AI model worked well in some cases, however, at the same time, it performed badly on some other difficult examples. Initially the pipeline was tested on Dutch articles translated to English via Google Translate. Therefore, retraining and testing algorithms with data in the Dutch language is required in order to further work with Dutch texts. Most of the mistakes in text processing come from the Coreference Resolution component. Coreference Resolution is a critical component of natural language understanding and higher-level NLP applications including information extraction, text summarization, and machine translation. It is the process of determining whether two expressions in natural language refer to the same entity in the world (Soon, Lim & Ng, 2001). The complexity of the human language processing and text interpretation still limits the effectiveness of the current AI algorithms. Data collection and labelling for AI training is an extremely time-consuming and laborious task, and the current project could not ensure the necessary resources for that. Therefore, the Coreference Resolution problem will require further work in the context of this research.

Summary generation algorithm worked quite successfully, as well as a filtering algorithm to classify homicide-related articles. For this task various methods were tested, with the most successful (BERT algorithm) reaching accuracy of more than 96% (Table 1).

Table 1. Test results of the algorithms to distinguish homicide articles from other topics (source: authors)

Methods	Accuracy
Bernoulli NB	87.42%
Naive Bayes	87.63%
MNB	87.97%
NuSVC	88.58%
Voted	93.06%
Linear SVC	94.85%
Logistic Regression	95.36%
SVC	95.82%
BERT	96.11%

Development of a (smart) database concept

The ultimate goal of this research is to eventually develop a homicide database equipped with 'smart' features driven by AI algorithms to support investigative process with data-driven insights. The first steps were taken towards that goal. A prototype of a web-based database platform was developed that can store the data (text articles) collected on homicide cases (Figure 3).

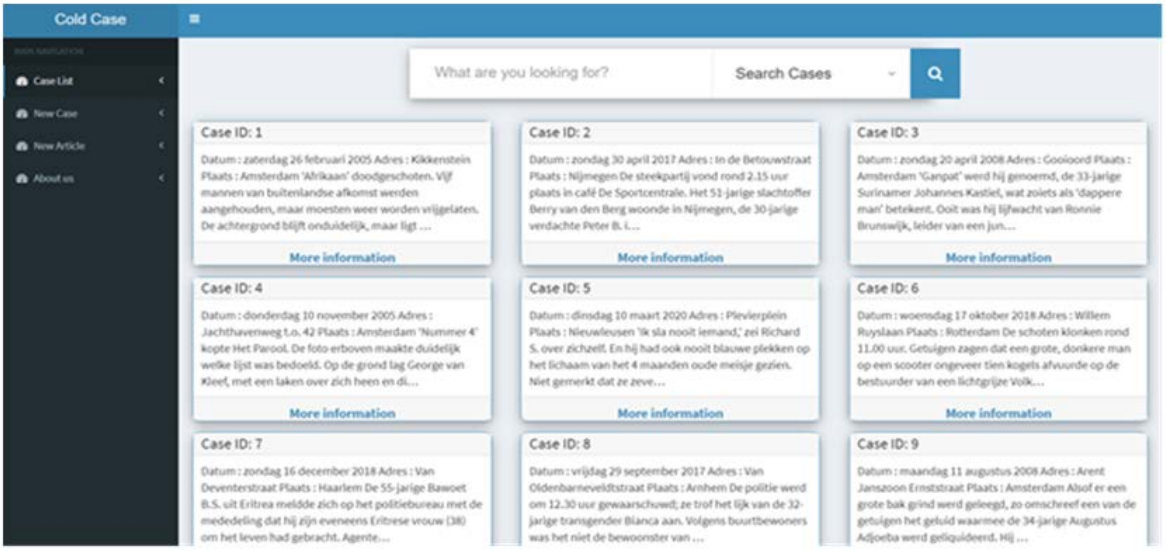
The database organizes articles on a case-by-case basis (so one homicide case can have multiple articles linked to it). Furthermore, a case description includes a ESC12 components structure based on the framework by de Kock (2014). The connection with AI engine was also set up and tested. We foresee that in the future it will be possible to integrate all the tools described in this paper to achieve a fully functional 'smart' database platform. The 'Search and Scrape API' will automatically take new information from the news portals or other sources (such as Police information systems, if data use permits allow) about homicide cases, which will be analyzed and filtered by an AI algorithm. The function of Artificial Intelligence to generate short summaries or overviews of articles or case descriptions can be implemented directly in the platform. On the other hand, the AI models for extraction of interesting components from the text can be re-trained with new data and developed further with other methodologies and approaches. While the AI module is not yet ready to re-

place the capabilities of humans for text interpretation, it may become a useful tool in the future as a kind of an assisting/recommendation feature for the users.

The current research was not able to tackle the actual generation or prioritization of crime scenarios. This part can be tested in the future, when sufficient amount of information on homicide cases is collected, thus enabling effective pattern mining by means of data-driven techniques.

The design of the platform and the user experience can be made to match the needs of Police officers involved in detecting homicide cases. This means embedding the platform with their workflow and fully or partially covering their needs.

Figure 3. Database platform (source: authors)



Empirical analysis of homicide data

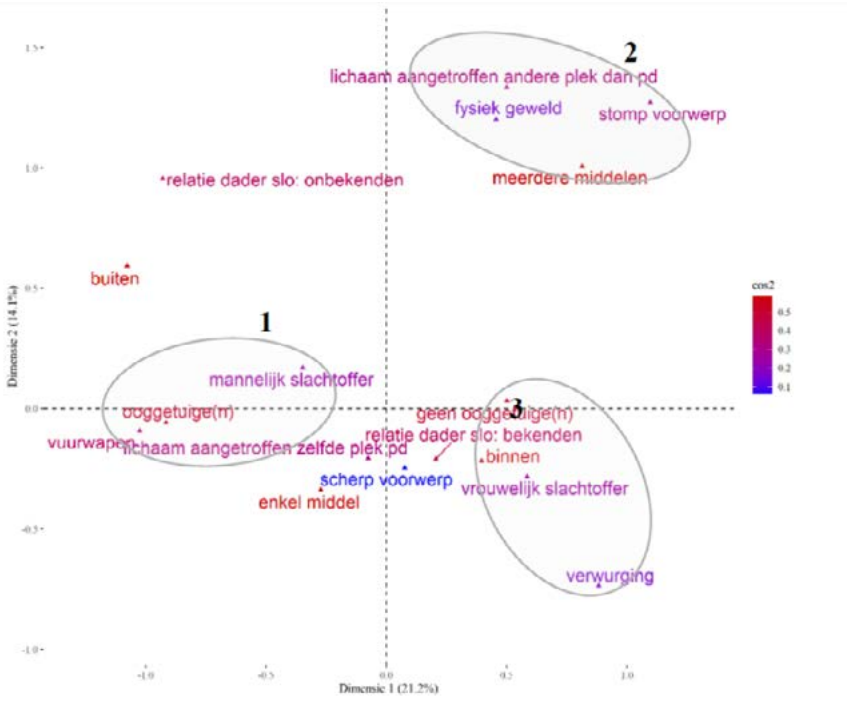
Data collected during the project was used to explore meaningful relationships and patterns in the homicide cases in The Netherlands. This can be considered the first step in determining the potential of (open source) data on homicide cases to be used in predictive or pre-

scriptive data-driven systems. Several scientific studies were conducted and final theses were developed by students in collaboration with University of Leiden, Dutch Police Academy and Amsterdam University of Applied Sciences (HvA).

The first research was conducted by Hanneke van de Mortel, University of Leiden (van de Mortel, 2020) as her MSc thesis. The research focused on predicting the relationship between the perpetrator and the victim on the basis of victim characteristics and the modus operandi. Such research is the first step to identify relevant relationships in the homicide cases that can help determine a direction of the investigation. This study was conducted using a dataset of ~300 homicide cases in The Netherlands for the period of 2006-2015 (manual data collection). The research method included bi-variate correlation analysis and predictive modelling with Logistic Regression method.

The second research was conducted by the student of Dutch Police Academy, Rob Schipperheyn, as his MSc graduation research (Schipperheyn, 2021). This scientific work focused on identifying the clusters of co-occurring variables in the homicide dataset and translating them into practical scenario-based investigation recommendations. The global objective of this research was to facilitate the development and use of more scientifically substantiated scenarios in police investigation using data science insights. The research methodology included: univariate analyses, bi-variate analysis, and multi-variate analysis in a form of Multiple Correspondence Analysis (MCA) method (Figure 4). Like the previous study, this research was based on the data on ~300 homicide cases for the period of 2006-2015.

Figure 4. Output of an MCA model (Schipperheyn, 2021)



The third study was conducted by the student of Amsterdam University of Applied Sciences, Izzy van der Veur, as his BSc graduation thesis (van der Veur, 2021). The research focused on the question: 'To what extent can the nature of a homicide be determined on the basis of social economical, geographical and demographic characteristics of the location of a homicide?'. In contrast to the first two studies of this work package, this research used the data scraped from a website Moordatlas[4], for the period of 2016-2020. This time period was chosen due to a higher degree of completeness of the available data, which makes the results more valid and reliable. The data scraped from Moordatlas was further processed to develop a data-

4 Moordatlas website: www.moordatlas.nl

set. Bi-variate correlation analysis was used to explore meaningful relationships, while geographic mapping was used to look at the spatial distribution of homicide cases in The Netherlands.

Conclusions

This paper described the outputs of the project 'Cold Case: Solved & Unsolved' completed in the research group of 'Technologies for Criminal Investigations' at Saxion University of Applied Sciences and Dutch Police Academy. The project explored and tested development and applications of various digital tools and data science techniques to facilitate and automate collection, pre-processing and analysis of open source data on homicide cases.

It was possible to achieve a certain degree of automation of some of the data collection and processing steps. For example, AI algorithm for classifying articles about homicides performed well (highest accuracy >96%). However, the complexity of the human language processing and text interpretation still limits the effectiveness of the current AI algorithms for more difficult tasks. Hence, development of a 'smart' database equipped with a fully functional and effective AI engine was not attainable in this project. Thus, further research is needed to achieve a more effective extraction and structuring of interesting information from the text. Current efforts were also limited by the lack of suitable data for training of the AI models. Furthermore, AI training and testing were restricted by the available computational capacity and some technical disruptions during the development stage.

The prototype of the web-based database platform currently allows for manual entry of the data, therefore it can be used without AI as well. Overall conclusion is that AI does not yet match the human capacity to interpret text, however with proper training AI has the potential to be used as an assisting or recommending tool in addition to experts' judgement.

Concerning the applicability of open-source data for homicide research (and eventually investigation), we can conclude that use of open-source data is associated with certain limitations and risks. Over- or under-representation of certain (groups of) cases is possible, especially due to differences in media attention to certain types of homicide cases: for instance, unusual, scandalous, or somewhat mysterious cases often receive more media coverage. Given that data collection is an extremely time-consuming and laborious process, in this project it was possible to only collect the data on a limited number of cases (around 300 cases). Furthermore, in those cases, not all the variables could be filled in, thus many variables became unusable in the analysis due to a large amount of missing values.

For further research, a number of reliable public sources may be pre-defined using a set of specific criteria. Research presented here aimed to explore usability of a wider range of sources, which might have led to inclusion of incorrect information in a dataset.

Relatively small set of cases included in a detailed structured dataset (~300 cases) and a large amount of missing values for many of the variables limited the exploration of relationships and patterns. However, some significant relationships could still be identified in the three scientific studies conducted. This suggests that potential to use predictive and prescriptive data modelling techniques in homicide research should be investigated further.

Discussion and recommendations

While working with the open source data for the homicide cases in The Netherlands, we found that the amount of detail in the open source data is limited. Moreover, the data may be biased or not trustworthy. This creates a serious limitation for data analysis using open source data. Further research could be devoted to working with Police data or a combination of Police files and open source data. This is, however, associated with significant difficulties of getting access to the confidential data.

AI can be a powerful tool in recognizing complex patterns. However, more research is necessary in order to automate the processing of (big) textual data. With the state-of-the-art of the technology and considering a sensitive nature of the forensic or criminological applications, it is not possible to completely replace a human expert with an AI algorithm. Further work is required concerning both data collection and AI development to enable the use of data-driven insights and/or predictive algorithms in the homicide investigation. We suggest that AI can be potentially used in combination with human judgement, as a recommendation tool. With sufficient data, AI-powered tools can even-

tually support scenario generation and prioritization, identify groups of similar cases in the historical database and compare historical records to an ongoing case.

It should be noted, however, that more research on ethical issues should be conducted, in order to avoid biases and ensure the correct use of the information generated by computer algorithms. As suggested by van Brakel (2016), big data and predictive tools can have benefits for policing, but such techniques may also bring disempowerment of individuals, groups, and society depending on implementation and intentions behind their use. Moreover, an open question still remains - how do we make sure that data-driven techniques actually help prevent a tunnel vision, instead of reinforcing it? With this concern in mind, carefully designed operational workflows and application strategies should be embedded in the Police practice to accommodate the correct use of data-driven techniques.

Data-driven research often requires good quality structured datasets. Our first step in that direction was development of a structured dataset with about 300 cases on homicides in The Netherlands in the period of 2006-2015, using information from published news and other open sources. With more than 200 variables in the dataset structure, this is an extremely time- and resource-consuming endeavor. Techniques for more efficient methods of information extraction and structuring from big (textual) data should be further explored. Another possibility may lie with collaborations with volunteers, universities or other organizations that might contribute to the task of data collection.

Closer collaboration with the Police (or other potential user groups) is crucial for the development of a relevant data-driven tool. We suggest that the future projects should fit in the development agenda of the National Police, and the tools should be developed with the input from the Police experts.

Acknowledgment

We cordially thank *Tech For Future* - programme for co-funding the project 'Cold Case: Solved & Unsolved' and making this research possible. We also thank our project partners - Pandora Intelligence, Icologiq, SDProject, Saxion University of Applied Sciences, Dutch Police Academy, Factor Veiligheid - for contributions in research and development. We thank University of Leiden and Amsterdam University of Applied Sciences for contributions to this research. Our sincere gratitude goes to researchers Dung Le and Dimitar Rangelov – for their work on AI and web-scraping methods; Hanneke van de Mortel, Izzy van der Veur and Rob Schipperheyn – for their applications of the collected data in empirical data analyses; 'Smart Solutions Semester' student Luuk Cloosterman – for his work on 'Search and scrape' API; all students of Cold Case Minor course – for their contributions to data collection and feedback on developed tools. We also thank volunteer organization Bureau Dupin for the support and knowledge exchange in the various steps of this research.

References

- Adcock, J.M. & Chancellor, A.S. (2016) *Death Investigations, The 2nd Edition*. 2nd edn. CreateSpace Independent Publishing Platform.
- Adcock, J.M. & Stein, S.L. (2015) *Cold cases: An evaluation model with follow-up strategies for investigators*. 2nd edn. CRC Press, Taylor & Francis Group. doi:10.1201/b10204.
- CBS (2021) *Minder moorden in 2020, wel meer jongeren vermoord*.
  Available at: https://www.cbs.nl/nl-nl/nieuws/2021/39/minder-moorden-in-2020-wel-meer-jongeren-vermoord#:~:text=Onder
- de Kock, P.A.M.G. (2014) *Anticipating criminal behaviour: using the narrative in crime-related data*. 1st edn. WLP.
- Devlin, J. *et al.* (2019) 'BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding', in *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*. Minneapolis, Minnesota, pp. 4171–4186. doi:10.48550/arxiv.1810.04805.
- Ganpat, D.S. *et al.* (2011) 'Homicide in Finland, the Netherlands and Sweden: A first study on the European Homicide Monitor Data', Homicide Studies 17(1) 75 –95

- Liem, M. *et al.* (2013) 'Homicide in Finland, the Netherlands, and Sweden: First Findings From the European Homicide Monitor', *Homicide Studies*, 17(1), pp. 75–95. doi:10.1177/1088767912452130.
- Mali, B., Bronkhorst-Giesen, C. & den Hengst, M. (2017) *Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot*. Apeldoorn: Politieacademie.
- Politie (2020) *Nieuwe coldcasekalender ook in tbs-instellingen*.
  Available at: https://www.politie.nl/nieuws/2020/januari/17/00-nieuwe-coldcasekalender-ook-in-tbs-instellingen.html
- Schipperheyn, R. (2021) *Scenario's van moord en doodslag: Exploratief onderzoek naar samenhangende kenmerken van kapitale delicten*. Politieacademie.
- Soon, W.M., Lim, D.C.Y. & Ng, H.T. (2001) 'A machine learning approach to coreference resolution of noun phrases', *Computational Linguistics*, 27(4), pp. 521–544. doi:10.1162/089120101753342653.
- van Brakel, R. (2016) 'Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing', in *Exploring the Boundaries of Big Data*. Amsterdam: Amsterdam University Press, pp. 117–141. doi:10.2139/ssrn.2772469.
- van de Mortel, M.E.J. (2020) *In hoeverre kan de (soort) relatie tussen de dader en het slachtoffer van dodelijk geweld binnen Nederland, worden voorspeld aan de hand van slachtofferkenmerken en de modus operandi?* Universiteit Leiden.
- van der Veur, I. (2021) *De mogelijke bepaling van de aard van een levensdelict aan de hand van de sociaaleconomische, geografische en demografische kenmerken van het plaats delict*. Hogeschool van Amsterdam.

AI-Potential to Uncover Criminal Modus Operandi Features

Ana Isabel Barros

Dutch Police Academy TNO Defence, Safety and Security Institute for Advanced Study, University of Amsterdam

Koen van der Zwet

Computational Science Lab & Institute for Advanced Study, University of Amsterdam TNO Defence, Safety and Security

Joris Westerveld

TNO Defence, Safety and Security

Wendy Schreurs

Dutch Police Academy

Abstract

Technological innovations such as digitalisation have an increasingly important role in our society. This development is also reflected in police work. In particular, the access to information on a global scale has increased the international character, adaptivity, and fluidity of criminal organisations. As such, there is a pressing need to better understand the evolving nature of these organisations and their associated modus operandi. While digitalisation enables access to lots of information and yields information overload challenges, developments in Artificial Intelligence (AI) offer new opportunities to tackle these challenges. In particular, they provide support in the automatic extraction and analysis of unstructured sources of information to efficiently make sense of large amounts of textual information sources. In this paper, we will explore the potential and challenges of various AI methods to extract criminal modus operandi from unstructured open text sources, like law court sentences. Such open text sources are reliable information sources that include detailed validated information on the criminal activities and the modus operandi evolution in a given country. The application of this approach offers an alternative to the examination of classified police information and it also facilitates cross-country comparisons. The inherent complexity of modus operandi and the unstructured character of law court sentences yield the need to align and structure the modus operandi question with particular text mining methods. Specifically, we propose a step-wise approach to analyse automatic extraction of modus operandi-related problems via exploration, detection, and categorisation analysis. This decomposition enables to align these problems to specific functions of text-mining or machine learning methods, such as similarity detection, clustering, or named entity recognition. Using practical examples we demonstrate how this approach enables to automatically extract relevant information from court cases sentences for analysing modus operandi evolution in time.

Keywords: Artificial Intelligence, Modus Operandi, Intelligence analysis

Introduction

Technological innovations have found their way into society. For instance, the incorporation of digital technologies into business and social processes (digitalisation) provides new possibilities for services and business and also easy access to information and new forms of communication. Criminal organisations also profit from these technological advances as they enable, among others, to enlarge the illicit market in an efficient and anonymous manner (Bird et al., 2020). Moreover, criminal organisations are also able to quickly adopt new technology (Allison, 2017) and adapt to change or counter strategies (Ayling, 2009: 182). For instance, digitalisation enables sharing information (how to avoid law enforcement efforts, to exploit the potential of new technology) and as such it accelerates this adaptation capability. These adaptations are reflected in the methods of operations taken by criminal organisations to achieve their criminal goal, the so-called Modus Operandi, MO. As the analysis of the MO supports the detection of criminal activities (Fosdick, 1915), it is important to develop a process to acquire more insight into MO features and their evolution in order to strengthen the police intelligence position.

Developments in Artificial Intelligence (AI) and particular text analytics and natural language processing (NLP) methods, provide support in this process as they enable automatic extraction and analysis of unstructured sources of textual information. For instance, Shabata, Omar, & Rahem (2014), have used AI to extract nationalities, weapons, and crime locations from online crime documents. Li & Qi (2019) have used a natural language processing method to extract the MO features from crime process information and Birks, Coleman, and Jackson (2020) introduce an Artificial Intelligence framework to identify different crime types in unstructured crime reports data, as these are often classified as a single crime category for administrative purposes.

In this paper, we will build on existing research in order to explore the potential and challenges of the application of AI methods to extract criminal modus operandi features from unstructured open text sources, like law court sentences. As often, these court sentences are available online and form an accessible and reliable information source that contains validated information on criminal activities. The exploration of these open sources offers an alternative to the examination of classified police information and it also facilitates cross-country comparisons.

The use of natural language processing (NLP) techniques for the analysis of court cases narrative texts enables the exploration of large volumes of these unstructured text documents, the extraction of relevant information, and the uncovering of patterns. For instance, the potential of these techniques to support sentencing is discussed by Stobbs, Hunter, & Bagaric (2017). Medvedeva, Vols & Wieling (2020) demonstrate the potential of NLP techniques to support the prediction of judicial decisions of the European Court of Human Rights. On the other hand, Wenger et al. (2021) have applied NLP for automated punishment extraction in sentencing decisions from criminal court cases sentences in Hebrew, which poses extra challenges due to the less availability of tooling for other languages. Das & Das (2017) proposed a two stage approach for the automated analysis of a large number of crime reports against women in India. The first phase focuses on the extraction from online newspaper articles of crime reports and its exploration in order to identify most frequent observed entities, like names of cities, etc. They also show that a second stage of processing is required in order to further categorise the identified basic entities in order to extract unique and relevant modus operandi features. This short literature overview shows the importance of the development of a framework with various AI approaches to extract modus operandi features from unstructured textual data. As such we propose a step-wise approach to analyse automatic extraction of modus operandi-related features via exploration, categorisation, and detection analysis. This decomposition enables to align these problems to specific functions of text-mining or machine learning methods, such as similarity detection, clustering, or named entity recognition. Using practical examples we demonstrate how this approach enables to automatically extract relevant information from court case sentences for analysing modus operandi evolution in time.

Methodology

Vijay Gaikwad, Chaugule & Patil (2014) underline the importance of articulating the goal of text analysis with the appropriate technique functionality. Moreover, Das & Das (2017) point out that modus operandi extraction is a challenging task specifically due to the complex-

ity of organised crime. In order to create insights into the evolution of the synthetic drugs trade very specific details of the criminal process, like the precursors used to produce synthetic drugs (which will also influence the production process), need to be extracted and analysed. On the other hand, other types of crimes may require less specific information in order to reveal adaptation in the MO. For instance, focusing on the type of weapon used in murders can provide insight into the trends in murder MO. Therefore, different MO questions may require different text analysis technique functionalities given the available data at hand. As such we propose a step-wise text analytical approach for automated extraction of MO features from criminal court sentences. This approach uses different NLP methods to extract and understand information from textual data. Some of the methods in our approach are based on supervised machine learning, while others are based on unsupervised machine learning. An unsupervised learning approach uses machine learning algorithms to analyse and cluster unlabelled data sets. These algorithms discover hidden patterns in data without the need for human intervention, which yields the term "unsupervised". An example of an unsupervised learning method is topic modelling as it automatically analyses text data to determine cluster "topics" that occur in the set of documents. On the other hand, a supervised learning approach uses labelled datasets that have been designed to train or "supervise" algorithms into classifying data or predicting outcomes accurately. Using labelled inputs and outputs, the model can measure its accuracy and learn over time. As an example, a supervised method can be trained to perform Named Entity Recognition (NER). NER is the method of locating and categorizing important nouns and proper nouns in a text (like the name of a city or organisation) (Mohit, 2014).

Although supervised methods are prone to bias (due to the selection and labelling process), the analysis of large bodies of data without support is also prone to biases as one usually explores the data based on predefined keywords yielding a less objective analysis (Birks, Coleman and Jackson, 2020).

Our stepwise approach consists of three main steps that focus on different facets of MO extraction: *Exploration, Detection,* and *Categorisation*.

The *Exploration step* aims at getting a grip on the available data. In this step, broad MO questions can be addressed like what are the relevant terms in court sentences? Do these terms change over the years? Unsupervised methods are well suited for this step. Application of such methods is usually preceded by a process of tokenisation (separating a given text into smaller text pieces, tokens), sentence segmentation, parsing and other pre-processing tasks like lemmatization (a process that analyses words according to their root lexical components). Topic modelling techniques are often used to filter and identify the semantic structure (Landauer, Foltz, & Laham, 1998). Topic models are probabilistic methods that aim to discover latent themes that are the hidden structure that characterise the unstructured text. Depending on the parameter setting, which controls the number of categories, methods search for global themes or salient local themes. The Latent Dirichlet Allocation (LDA) method and Latent Semantic Analysis (LSA) method are conventional tools used to extract the various topics from the text (Blei, Ng & Jordan 2003). The LDA method applies a generative process in which the Dirichlet distribution is used to draw random samples from the data. With this procedure, a topic can be drawn from each word, and each word can be associated with a topic. By limiting the number of topics, each word is assigned to the most likely topic. Similarly, LSA provides contextual meaning to text (Landauer, Foltz, & Laham, 1998) as follows. First, a document-to-term matrix is generated, which is then used to decompose the text into different dimensions based on the parameter setting of the algorithm. In terms of modus operandi questions, unsupervised methods provide a general overview of available terms and a nonspecific overview of the underlying structure of the available information, in some sense, they offer the possibility of zooming out.

The results of the exploration step provide insight into the potential of the available data and also input for the Detection and Categorisation steps.

In the Detection step, a further deepening of the analysis of the available data takes place to identify specific MO features and possible links between these features. Supervised methods are particularly well suited to address these questions (Shabata, Omar, & Rahem, 2014). This is particularly of interest when quick and nuanced information is required of specific modus operandi types. Supervised methods usually require a pipeline of annotation (process of labelling text so that it can be used by a model), model training, and model evaluation. By training the model using the labelled exam-

ples, it can learn the capability to distinguish and classify specific information. Models that perform NER are very popular and efficient. In particular, the application of a supervised model that is trained to perform NER requires an existing pre-trained model (for example BERT; Devlin et al 2018) or self-trained models. However, due to the level of quality (these models are trained and require a large corpus of text) of the pre-trained models and the number of models that are publicly accessible on the internet, using a pre-trained model is usually more efficient to perform NER. Moreover, it is even possible to add your own entities to the pre-trained models which could tune the model to a specific domain. This is especially useful in order to extract relevant information about the modus operandi.

The identification process of entities enriches the analysis with additional information, such as the identification of persons, organisations, locations, or modus operandi specific information such as weapon and drug-related information. Therefore, validated supervised models performing NER are a powerful tool to quickly enable users to detect and extract specific information on modus operandi types and search for specific information in large data sets.

The *Categorisation step*, brings further deepening to the analysis by focusing on the detection of modus operandi features and their differences and types (for instance, which trends in the synthetic drugs modus operandi can be identified in a given period?). It can be executed when the dataset and more specifically the modus operandi question is sufficiently structured, and the necessary context (subject matter expertise) is available. In this step, a pipeline is formalised in which different types of methods are combined. This ranges from data transformation techniques like the Term Frequency-Inverse Document Frequency (TF-IDF), a numerical statistic that demonstrates how important a word is in the available data (Ramos, 2003), or the classic K-means clustering (unsupervised machine learning method that aims to derive a partition of the data occurrences into k clusters (Hartigan & Wong, 1979) and supervised machine learning which uses the labels identified by the K-means clustering.

Finally, and as a picture is worth a thousand words, several AI algorithms can be used to support the analysis and interpretation of the results of the above applications.

Results

In order to illustrate the potential of the proposed step-wise approach, we have conducted some experiments based on the published court case sentences on the website of the Dutch Judicial System (www.rechtspraak.nl). We focused on the sentence indictment component "Tenlastelegging", which summarises the reasoning behind the sentencing based on the evidence. As these open sources do not contain personal information (this data has been blurred) the data set does not pose ethical and/or privacy challenges. It should be noted that the data set is on itself biased as it focuses only on published court sentences and thus does not cover fully the reality of the criminality.

Exploration step

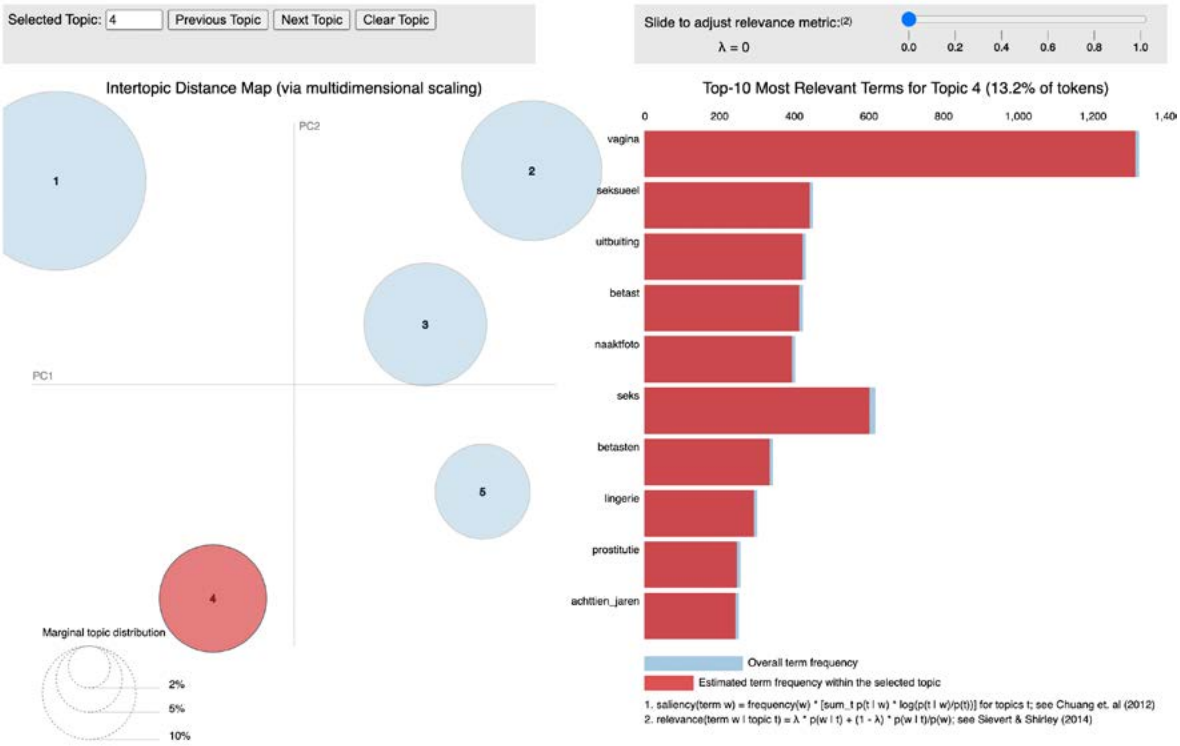
A first data set was extracted by considering available criminal law (in Dutch: strafrecht) verdicts between 2018 and 2021. This data set was further refined in order to include sentences that contained indictment or evidence, which resulted in 19.976 sentences (Jung et al., 2022).

In order to gain insight into this large data volume the exploration step was conducted. LDA (and a visualisation package pyLDAvis) was applied to uncover topics in the data set, see figure below.

In this figure, the identified topics for sexual offences are displayed on the left-hand side (topic modelling). This can be further analysed by clicking on the topic in the top-left corner. When selecting a topic, the ten most relevant terms of that topic are displayed on the right-hand side in decreasing importance order. As the above figure shows, the use of topic modelling supports the exploration of large sets in order to get an overview of the semantic structure in the textual information.

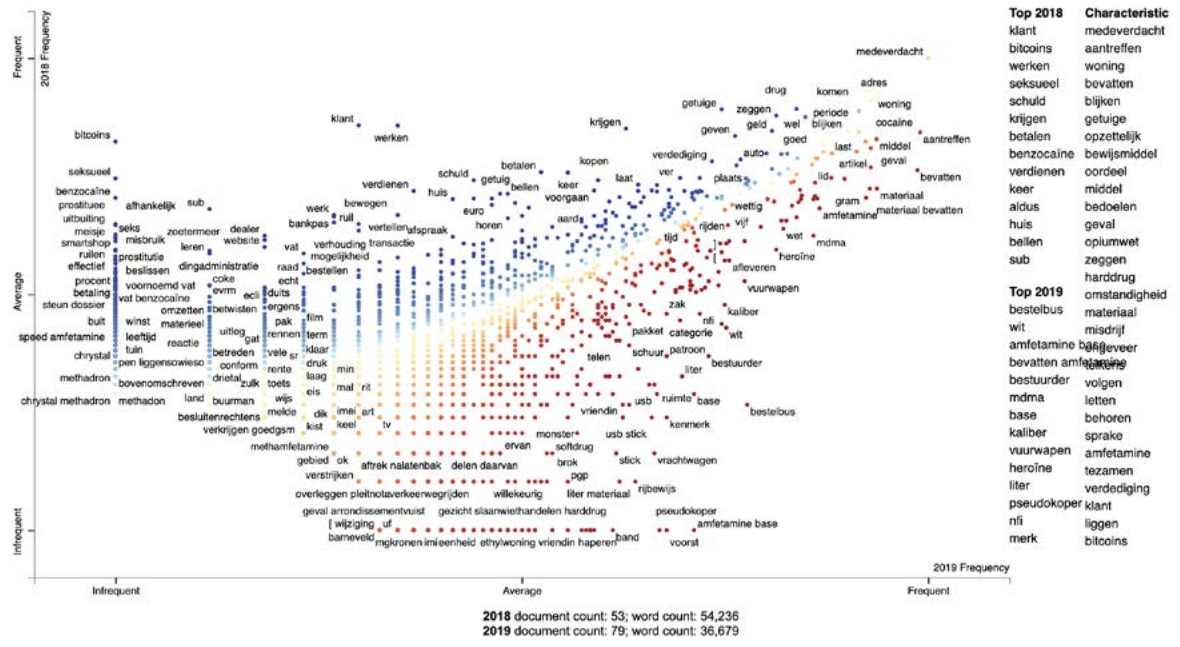
The potential of visualisation to aid the exploration is shown by the application of Scattertext (Python package to visualise the differences between two categories of text according to the term frequencies within each class), see Figure 2. This figure displays the comparison in frequency of all the words found in the used data set (available criminal law verdicts) between the years 2018 (X-axis) and 2019 (Y-axis). Each dot represents a word found in the data set court sentences of 2018 or 2019. A dot closer to the top of the plot indicates that this word occurred more frequently in 2018, while a dot

Figure 1: Example of topic modelling



further to the right of the plot shows that this word occurred more frequently in 2019. At the top-left corner "bitcoin" appears which indicates that Bitcoin occurred often in court sentences in 2018 but not in 2019. On the other hand, 'amphetamine' (bottom-right corner) occurred more often in 2019 and not in 2018

Figure 2: Example of data visualisation

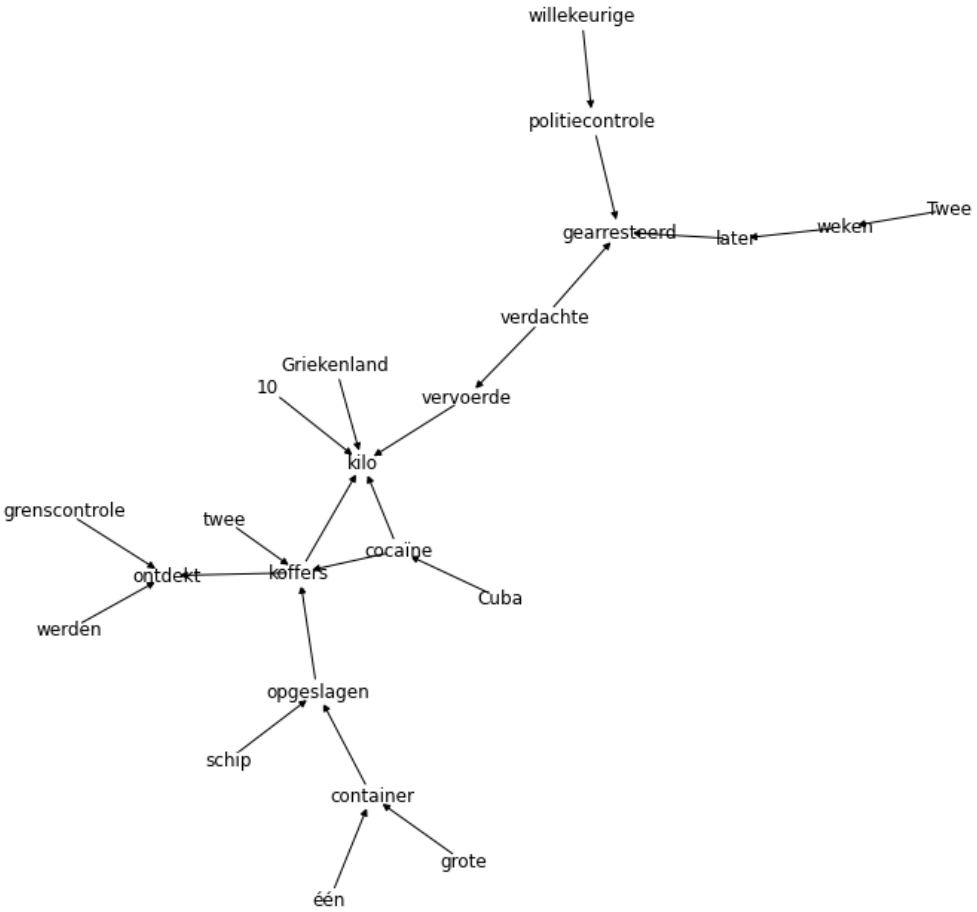


This exploration of the data using unsupervised methods quickly provides insight into the similarities and differences in the data and enables analysis across different time horizons, without requiring labelling of data. On the other hand, the topic clusters found might be too similar or too many.

Detection step

In order to illustrate this step, we will focus on court sentences related to a more complex type of crime, drugs trade, and in particular cocaine trade. As such the court sentences related to *Strafrecht* (Criminal Law) ranging from the 1930s to 2022 and containing the words cocaine and *tenlastelegging* (indictment) were selected (Dijkstra et al. 2022). In order to identify specific characteristics of modus operandi of cocaine trading in the court sentences and possible relations, NER was applied (from the open-source library SpaCy). Although the models available have been pre-trained for different languages including Dutch, the library model was not able to identify entities related to crime, like different types of drugs, weapons, and storage spaces. Therefore, it was necessary to retrain the model to identify these entities. The entities from the NER are used in *SpaCY displayCy dependency visualiser* to find relevant sentences and keywords, which are then exploited to create a graph, summarizing the relation between the MO cocaine features as shown in the figure below.

Figure 3: Possible relations between cocaine modus operandi features

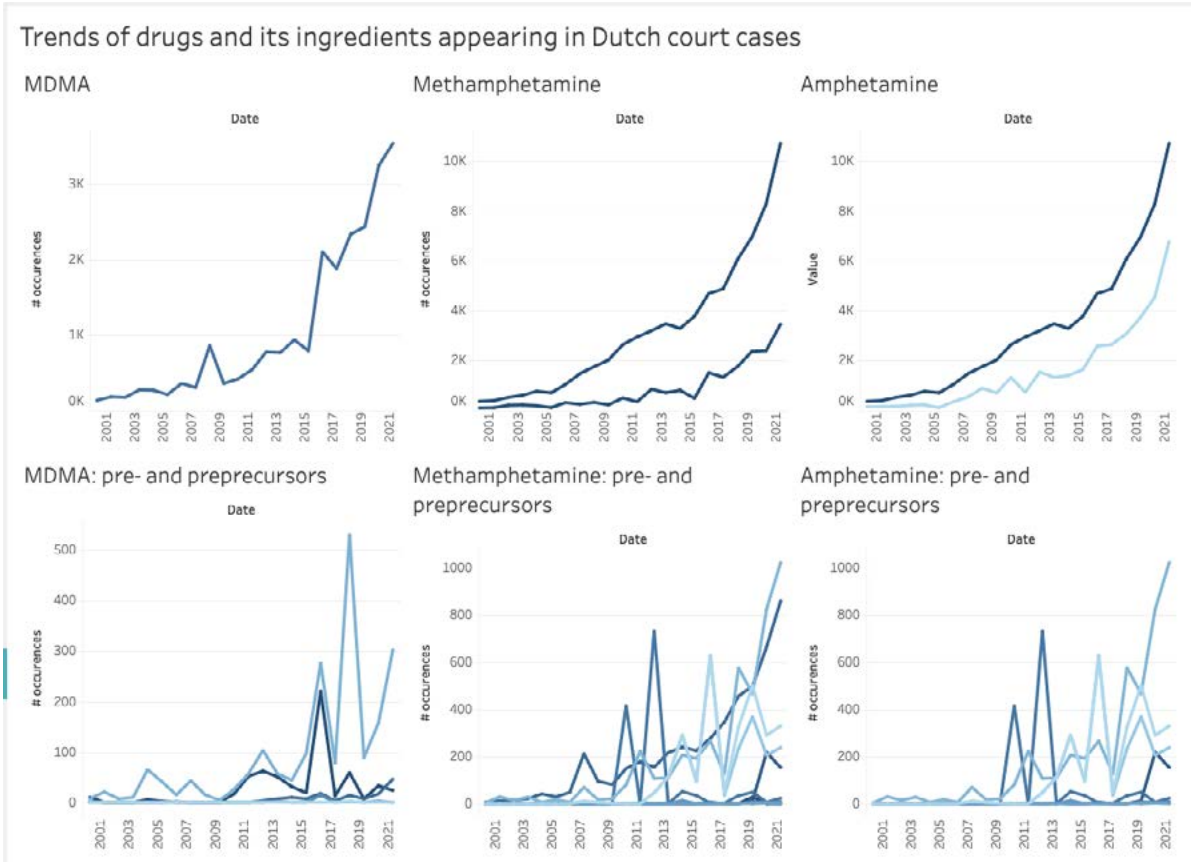


This experimental application of SpaCY NER was able to detect specific elements of modus operandi in the cocaine trade (means for transport, locations, etc). Moreover, the SpaCY displayCy dependency visualiser enables visualisation of these entities and their relationships creating extra insights. Nonetheless, the application of NER does require annotation of the data by experts in order to increase its performance, and also the development of dedicated training data sets as well as validation procedures.

Categorisation step

To illustrate this step court sentences related to synthetic drugs were considered as this has a rather intricate modus operandi. In order to address the research question regarding the evolution of synthetic drugs MO in the Netherlands, the court sentences related to *Strafrecht* (Criminal Law) up to 2022 and containing the words drugs and *tenlastelegging* (indictment) were selected which resulted in 17.714 drug-related court cases sentences (Bertrams et al, 2022). In this preliminary experiment, the textual data were transformed using the TF-IDF analysis. Using the TF-IDF on itself can already reveal interesting patterns. The figure below shows the trend of synthetic drugs and required precursors that appeared in Dutch court cases in the last years.

Figure 4: Synthetic drugs and required precursors trends in Dutch court cases

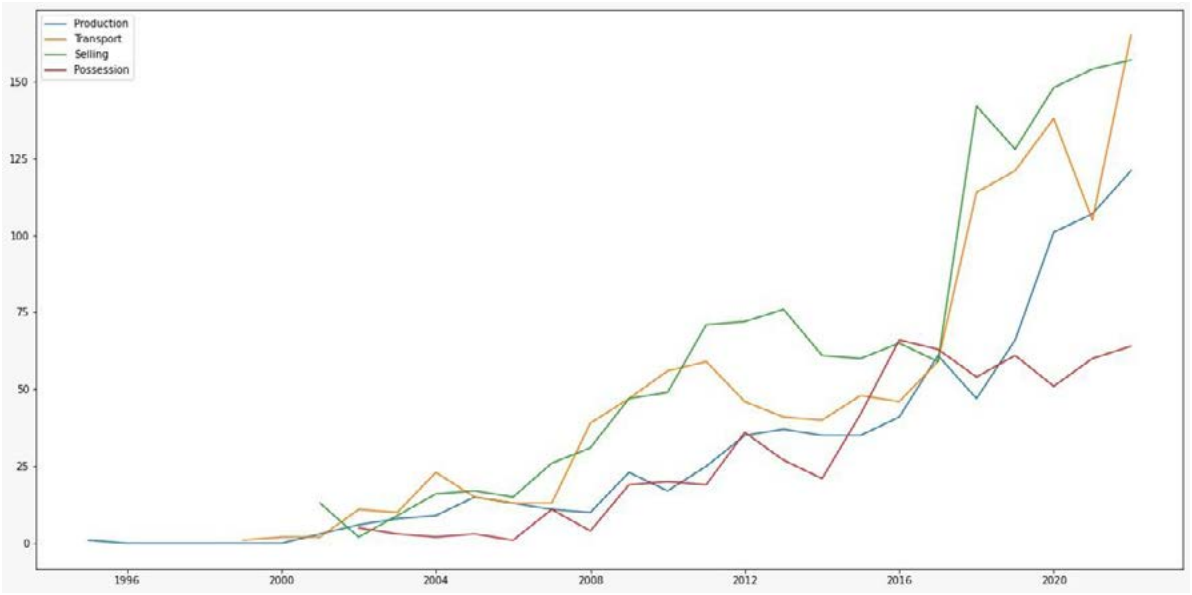


The first row of graphs shows the prevalence of the end product is mentioned over time in court cases. The second row shows the prevalence of synthetic drugs and the precursors and pre-precursors over time.

After the TF-IDF transformation, K-means clustering was used to generate several clusters. After examination of these clusters (and the words that were part of the cluster), 4 categories were identified (Production, Transport, Selling, and Possession). Using the court cases sentence dates the evolution over time of these categories can be observed, see figure below. In particular, an increased prevalence of court cases related to Production is visible around 2017.

These experiments show that the applications of categorisation methods does enable identifying differences and similarities between specific modus operandi characteristics. Moreover, they also support the analysis of the evolution of specific modus operandi features over time. However, the application of these methods require pre-identified specific modus operandi features that yield different modus operandi types. Such specific features need to be significant in order to be detected. Moreover, like other supervised methods it does require manual annotation and training process as well as validation.

Figure 5: Evolution over time of the occurrences of four synthetic drugs MO feature categories



Conclusions

The quick pace of technological innovations poses increasing challenges and opportunities to policing. As criminal organisations profit from these technological advances and quickly adopt new technology there is a pressing need to acquire insight into adaptations in the used criminal methods of operations, Modus Operandi (MO), and their evolution over time.

In this paper, we build on existing research in order to explore the potential and challenges of the application of AI methods to extract criminal modus operandi features from unstructured open text sources, like law court sentences. Court sentences provide an accessible (as they are often available online) and reliable information source that contains validated information on criminal activities, although not complete. Nonetheless, they form a solid basis for MO analysis and offer an alternative to the examination of classified police information. Moreover, the use of court case sentences also facilitates cross-country comparisons. The automatic analysis of court cases narrative texts using natural language processing (NLP) techniques enables the exploration of large volumes of court sentences, the extraction of relevant information and the uncovering of patterns. Consequently, it reduces the effort and time spent by crime analyst resources and it also supports an objective extraction process as the manual extraction of MO features by different crime analysts is more prone to errors and biases.

The inherent complexity of modus operandi and the unstructured character of law court sentences yield the need to align and structure the modus operandi questions with the appropriate methodologies. In fact, different MO features–related questions demand different approaches that vary from exploration, detection, and categorisation analysis. Therefore, the proposed stepwise approach offers support when tackling different MO features-related questions.

The preliminary experiments conducted show the potential but also highlight the caveats to its application in policing practice. In particular, they emphasise the need to consider the criminal context when applying AI and suggest the importance of establishing multi-disciplinary teams and stimulating a stronger cooperation between data scientists and IA specialists with crime analysts. Moreover, the experiments also reveal the importance of developing transparent data annotation schemes in order to support the development of unbiased supervised methods as well as creating training sets for the AI methods as also mentioned by Gumusel et al (2022).

Finally, more research is needed to further explore this initial effort in practice and to analyse its potential for cross-national comparisons.

References

- Allison, P. (1997) *Organised Crime Exploiting New Technology*. [online] ComputerWeekly.com. Available at: https://www.computerweekly.com/feature/Organised-crime-exploiting-new-technology [Accessed 24 June 2022]
- Ayling, J. (2009) Criminal Organizations and Resilience. *International Journal of Law, Crime and Justice*, *37*(4), pp.182-196.
- Bertrams, C., Hofstee, R., Malfa, I. & Miner, L. (2022) 'Mapping Synthetic Drug Production: Using Text Analysis to Track and Identify Precursor Prevalence'. *Data System Project 2021-2022 report*. University of Amsterdam. Amsterdam
- Bird, L., Hoang, T., Stanyard, J., Walker, S. & Haysom, S. (2020) *Transformative Technologies. How Digital is Changing the Landscape of Organized Crime*. 2020 Global Initiative Against Transnational Organized Crime, Switzerland.
- Birks, D., Coleman, A. & Jackson, D. (2020) Unsupervised Identification of Crime Problems from police free-text data. *Crime Science,* 9(1), pp.1–19.
- Blei, D. M., Ng, A. Y. & Jordan, M. I. (2003) Latent Dirichlet Allocation. *Journal of machine Learning research*, 3(Jan), pp.993-1022.
- Das, P. & Das, A.K. (2017) A Two-stage Approach of Named-entity Recognition for Crime analysis. In *2017 8th International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pp.1-5. IEEE.
- Devlin, J., Chang, M.-W., Lee, K., Google, K. & Language, A. (2018) BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. Available at: https://arxiv.org/pdf/1810.04805.pdf
- Dijkstra, S., Cheirmpos, G., Schipper, M. & Menarini, E. (2022) 'Graph Representation of Modus Operandi from Court Sentences'. Data System Project 2021-2022 report. University of Amsterdam. Amsterdam.
- Fosdick, R. (1915) The Modus Operandi System in the Detection of Criminals. *Journal of the American Institute of Criminal Law and Criminology*, 6(4), pp.560-570.
- Gumusel, E., Malic, V. Q., Donaldson, D. R., Ashley, K., & Liu, X. (2022) An Annotation Schema for the Detection of Social Bias in Legal Text Corpora. In International Conference on Information. pp.185-194. Springer, Cham.
- Hartigan, J.A. & Wong, M.A. (1979) Algorithm AS 136: A K-means Clustering Algorithm. *Journal of the royal statistical society* - series c (applied statistics), 28(1), pp.100-108.
- Jung, D., Kalff, E., da Rocha Bazilio, L., Rink L. & Mokkenstorm, M. (2020) 'Uncovering Modus Operandi: Using Unsupervised NLP algorithms to Identify Patterns in Unstructured Crime Data'. Data System Project 2021-2022 report. University of Amsterdam. Amsterdam
- Landauer, T. K., Foltz, P. W., & Laham, D. (1998) An introduction to latent semantic analysis. *Discourse processes*, 25(2-3), pp.259-284.
- Li, Y. S., & Qi, M. L (2019) An approach for understanding offender modus operandi to detect serial robbery crimes. *Journal of Computational Science*, 36, pp.101024.
- Medvedeva, M., Vols, M., & Wieling, M. (2020) Using Machine Learning to Predict Decisions of the European Court of Human Rights. *Artificial Intelligence and Law*, 28(2), pp 237-266.
- Mohit, B. (2014) Named Entity Recognition. In: Zitouni, I. (ed): Natural language processing of semitic languages, pp.221-245. Springer, Berlin, Heidelberg.
- Ramos, J. (2003) Using tf-idf to Determine Word relevance in document queries. In Proceedings of the first instructional conference on machine learning, 242(1), pp.29-48.
- Shabat, H., Omar, N., & Rahem, K. (2014) Named Entity Recognition in Crime using Machine Learning Approach. In Asia Information Retrieval Symposium (pp. 280-288). Springer, Cham.
- Stobbs, N., Hunter, D., & Bagaric, M. (2017) Can Sentencing be Enhanced by the Use of Artificial Intelligence? *Criminal Law Journal*, 41(5), pp.261-277.
- Vijay Gaikwad, S., Chaugule, A. & Patil, P. (2014) Text Mining Methods and Techniques. *International Journal of Computer Applications*, 85(17), pp.42-45.
- Wenger, M., Kalir, T., Berger, N., Chalamish, C., Keydar, R. & Stanovsky, G. (2021) Automated Extraction of Sentencing Decisions from Court Cases in the Hebrew Language. In Proceedings of the Natural Legal Language Processing Workshop 2021, pp.36-45.

The Potential of AI and Data Science in Reducing the Vulnerability of Ports to Undermining Crime

Nienke de Groes

Dutch Police Academy & Leiden University[1]

Willem-Jan van den Heuvel

Jheronimus Academy of Data Science

Pieter Tops

Jheronimus Academy of Data Science, Dutch Police Academy & Leiden University

Abstract

The port of Rotterdam is an important gateway to Europe and an important logistic hub for global trade. However, factors that ensure the competitive position of the port of Rotterdam are also attractive for drug criminals. In this paper the findings of an empirical study on the potential of AI and data science in securing ports against undermining crimes are presented. The study consisted of a qualitative research, which was conducted through semi-structured interviews, in-depth interviews, and an expert meeting. The findings of this research show that developments in Data Science and AI at ports could have a strong effect on reducing the vulnerability of ports against illegal activity. With the advent of smart technologies, the vulnerable human factor (in the context of undermining crime) in port processes could, gradually, become less important and be replaced by technology. However, new vulnerabilities may arise in the field of data ownership and cybersecurity. To realise the potential of AI and Data Science to protect ports from undermining crime, attention must be paid to these vulnerabilities, as well as ensuring the acceptance of the new (automated) technologies and adopting a systems approach.

Keywords: data science, artificial intelligence, undermining crime, seaports

1 Corresponding author's email: nienkedegroes@gmail.com

Introduction

In this contribution[2], we describe the possibilities that technological developments (in data science and Artificial Intelligence) at ports could offer for reducing the vulnerability of ports to undermining crime. In addition, we consider what would be required to realise this potential of data science and AI in the short and long term and what new vulnerabilities may arise. This contribution is based on international academic literature and the results of our own exploratory research[3], which focused on the relationship between technological developments in seaports (the movement towards Twin Harbours) on the one hand, and the vulnerability of ports to undermining criminal activities (particularly the import of drugs) on the other (see Tops, P., van den Heuvel, W., de Groes, N., & Gravenberch, V., 2021).

Seaports play an important role in world trade and are also a major hub in the international drugs trade. Incidentally, it is not only about drug trafficking (although that is a very important category), but also about arms trafficking, human trafficking, and trade in counterfeit products. The intrinsic interconnection between the legal and illegal world plays a major role in the daily reality of ports. This also applies to the Dutch seaports, with the port of Rotterdam in the lead (see also Staring et al., 2018). Rotterdam is the gateway to Northwest Europe and an important logistics hub for world trade (Port of Rotterdam 2019; Jacobs 2000, in Roks, Bisschop & Staring, 2021). The quality of the port facilities and the logistical efficiency of the Port of Rotterdam are not only beneficial for the legal economy, such as excellent accessibility by water, rail and road; high-quality port infrastructure and the efficient handling of containers and cargo (Port of Rotterdam, 2019; Van der Horst et al., 2019; in Roks, Bisschop & Staring, 2021), but also for undermining crime. This has led, among other things, to the port of Rotterdam becoming the main gateway for cocaine for Europe (UNODC, 2018, in Staring et al., 2019). With a certain regularity, reports on new 'record drugs seizures' appear in the Dutch media. In September 2021, an enormous quantity of cocaine of 4,022 kilos was intercepted in the port of Rotterdam, with a probable street value of more than 301 million euros (Public Prosecutor, 2021). In the same month, the police removed nine suspects from a container in the port of Rotterdam. These persons had broken into the container to take drugs out of the container and called the police after they had trouble breathing in the container (NOS, 2021). In 2020, over 40.000 kilos of cocaine were detected in containers in the port of Rotterdam. This was approximately 7.000 kilos more than in 2019 when 33.732 kilos of cocaine were intercepted. The total street value of cocaine seized was over EUR 3.5 billion. There is a trend in the interceptions towards increasingly large shipments: in 2020, 12 consignments above 1.000 kilos were intercepted (HARC team, 2021). It is assumed that the above figures of drug seizures in the port of Rotterdam are just the tip of the iceberg, as only a small proportion of the 7.5 million containers that pass through Rotterdam annually are checked (NOS, 2021).

The most vulnerable factor at ports from an organised crime perspective is the human factor (Hiemstra & de Vries, 2021). After all, there are tens of thousands of people working in the ports who – given their relatively low incomes – can 'easily' be bribed or threatened (Tops et al., 2021). The consequences of undermining crime at seaports are great:

- The corruption of organisations, such as security companies, customs, transhipment companies (see Nelen & Kolthoff, 2017; Bisschop et al., 2019);
- The attraction to young people in particular, who for example take the drugs out of the containers (see Verseput & de Haan, 2021; Ghosen, 2021)
- The use of violence, in the form of liquidations, mistaken murders, shooting incidents (see, among others, Meeus, 2019).

Interestingly, the vulnerable human factor (in the context of undermining crime) is likely to disappear from the ports as the role of technology increases and gradually takes over human activities. Digitalisation means that the human factor could be removed from the process. For example, crane operators could be replaced by automated cranes, border police could be replaced by smart containers, truck drivers could be replaced by self-driving cars and harbour masters could be replaced using smart ships that contact docks directly to check availability and make reservations without the need for human intervention (Van den Heuvel & Tops, 2021). These technological developments can potentially play an important role in securing ports against undermining crime. For example, the development of

2 The authors wish to thank dr. Vlad Niculescu-Dincă (Institute of Security and Global Affairs, Leiden University) for his stimulating comments on an earlier version of this contribution.

3 Throughout the text this research is referred to as Tops et al. (2021) or short *the study*.

'smart containers' will probably make it considerably more complicated to use containers for criminal purposes. Smart containers can only be opened at specific geographical endpoints, so-called 'geofencing', and accurately record (permanently and in real time) the contents, weight (and changes in weight) and transport movements of the container. These technological developments could make the criminal exploitation of containers for criminal purposes less attractive, as criminals choose the path of least resistance (Tops et al., 2021).

This contribution explains, from a long-term perspective, how vulnerabilities in seaports could be reduced through the application of Data Science and AI. This contribution addresses an important gap in the scientific literature; the lack of literature about the use of digitisation and Data Science to reduce the vulnerability of ports to criminal (drugs) activities. A literature review by Van den Heuvel and Tops (2021) on (improved) security of (smart) ports, revealed that the vast majority of the analysed scientific literature relates to potential (new) technologies, tools and methodologies, while the number of actual experience reports, longitudinal studies, empirical experiments and case studies is limited. Only a few papers explicitly address the relationship between ports and security (e.g. Lokulaluge et al., 2012; Poikonen, 2021). However, the role that digitisation and Data Science can play in reducing the vulnerability of ports to criminal (drug) flows has not been studied yet. As one of the main pioneers in the application of Data Science and AI technology in ports, and also a location where a lot of drug-related crime takes place, the Port of Rotterdam serves as a good case study to explore the potential of Data Science and AI in securing ports against undermining crime. Furthermore, this contribution emphasises that strong attention should be paid to the human factor – even in an automated and very digitalised future of seaports. This strong suggestion is highlighted by proposing that the leading model in studying acceptance and usage of new technologies – the Technology Acceptance Model, which assumes an active user and close proximity to the technology – should be reviewed for automated environments in which the user could have a more supervisory and distant role in the interaction with the technology.

Content

This contribution begins with an explanation of the methods used in the research and with a further explanation of the Technology Acceptance Model. We outline the trend of smart ports that could increasingly operate autonomously using the example of a smart container (Container 42). We then discuss the potential of Data Science and AI in reducing the vulnerability of ports to undermining crime using the findings of our own research, after which we consider important conditions to realise the potential and new vulnerabilities that might arise. We conclude this contribution by presenting a conclusion and recommendations.

Methods

This article draws mainly on the exploratory research of Tops et al. (2021). This practical exploration of the potential of Data Science and AI in reducing the vulnerability of ports to undermining crime consisted of two phases. The first phase consisted of an exploratory phase where relevant stakeholders were interviewed using semi-structured interviews with a topic list, which also included relevant questions related to the acceptance of automated technologies in order to discover new factors that might be of relevance to adjust the Technology Acceptance Model for automated technologies. The interviewees were selected based on their involvement in and knowledge of the issue of undermining crime at seaports. Amongst them were security professionals from the port of Rotterdam and the port of Moerdijk, the seaport police of Rotterdam and a senior researcher on port economics. In the second phase, the conclusions and observations from the interviews of the previous phases were presented to a broader forum of experts during an expert meeting and were tested against their experience and expertise, using the Delphi method.

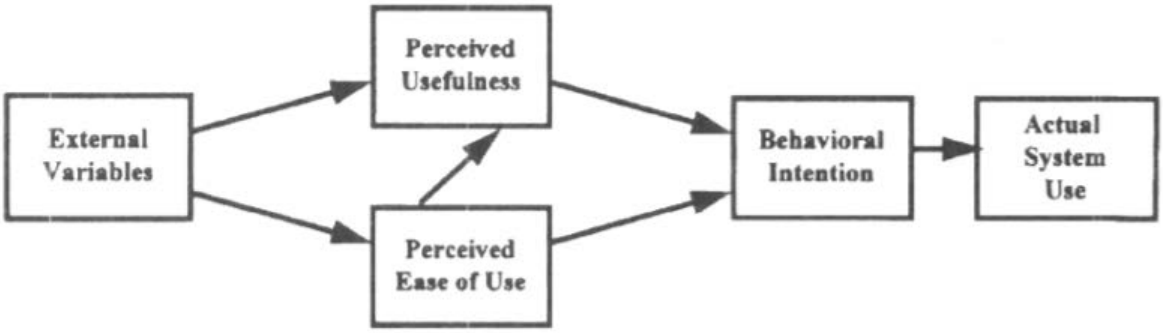
Technology Acceptance Model

While a wide range of models exist that focus on the acceptance of new technologies by the active user, few if any models focus on the acceptance of automated technologies – where the role of the human (the user) is tending to decline. Technology-acceptance models, like the *Technology Acceptance Model* (TAM) (Davis, 1986), focus on the acceptance of technologies where a user has an active role. However, in the case of smart ports, the role of the user could gradually be-

come smaller, more passive or could even disappear completely in the long run. Therefor it is important to reconsider the factors that stimulate acceptance and usage of the new automated technologies in the TAM and consider a new acceptance model for automated technologies. In the research of Tops et al. (2021), the TAM was used as guideline to discover and analyse if and what new factors could be of relevance for the acceptation and usage of automated technologies in future smart seaports.

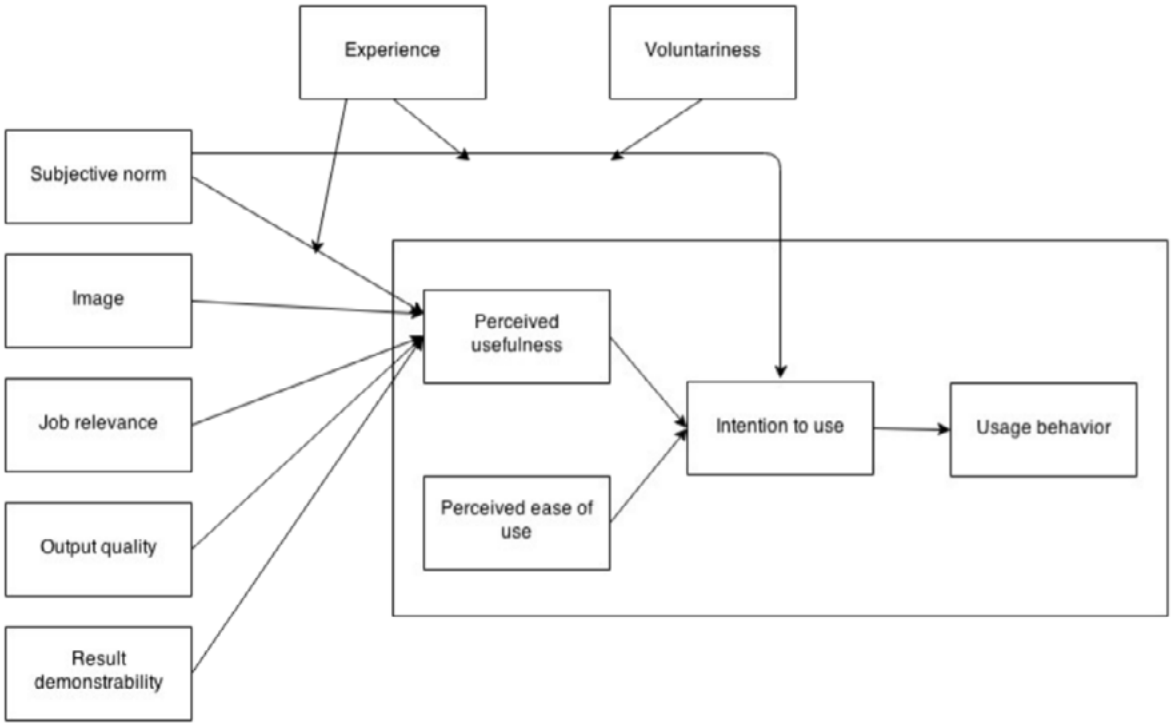
The TAM (Davis, 1986) is a leading model for explaining or predicting individual technology acceptance. This model illustrates how users come to accept and use technology. The TAM states that users' behavioural intention to use technology is influenced by the perceived usefulness and perceived ease of use of the technology (Venkatesh & Davis, 2000). According to Davis (1989), perceived usefulness – the belief that using the new system will increase performance – and perceived ease of use – the extent to which a person believes that using a particular system will be effortless – are the two main indicators that influence the use of technological systems. Davis, Bagozzi and Warshaw (1989) stated that the ability of TAM to explain individuals' attitudes and behaviour towards technological systems also depends on external variables. These external variables simultaneously influence perceived ease of use and perceived usefulness. What these external variables are, depends on the environment in which the research is conducted. Colvin and Goh (2005) validated the TAM for police officers and showed that the findings of the TAM were empirically supported in law enforcement environments.

Figure 1. Technology Acceptance Model (TAM) (Venkatesh & Davis, 1996, p. 453).



Venkatesh and Davis (2000) extended the original TAM by including subjective norms and cognitive processes, resulting in TAM2 (Lin et al., 2004). Social influence processes, subjective norms, voluntariness, image, cognitive processes, job relevance, output quality, demonstrability of results and perceived ease of use are included as factors in TAM2.

Figure 2. Technological Acceptation Model 2 (TAM2) (Venkatesh & Davis, 2000).



The trend towards 'digital twins' and 'smart ports'

Digital Twins are a digital reflection of a physical or cyber-physical object and were developed in the Smart Industry (Industrie-4.0), also known as the fourth industrial revolution. The fourth (and current) revolution is characterised by new technologies that increasingly influence social, industrial, economic, and governmental disciplines, such as big data applications, artificial intelligence, robotics, 3D printers, autonomous vehicles, mobile internet, Internet of Things (IoT) and Cloud technology (Ernst et al., 2019). According to Schwab (2016), with the advent of big data and technological innovations, a fourth revolution has begun that, more than previous industrial revolutions, is unique in scope, complexity and speed. Digital twin technology is applied in the domain of smart cities, but this technology has also made its appearance in the domain of seaports (Van den Heuvel & Tops, 2021).

The ambition of the Port of Rotterdam is to become the 'smartest port' in the world (Port of Rotterdam, 2019) and to this end, it has joined forces with several global IT players (IBM; CISCO) to develop a digital twin of the port; Twin Harbour. The development of digital twins aims to go beyond what is possible in the physical world using traditional processes. This approach is made possible by recent advances in IoT technologies, including sensors, wireless connectivity, and artificial intelligence. In theory, digital twins enable a holistic digitisation of harbour objects within their spatial-temporal context, going beyond simple automation and digitisation of traditional human processes. The Twin Harbour forms a system-of-systems in which every object in a harbour, ranging from building, dock to bollard, can be imitated, observed, and controlled by means of a digital twin. In a Twin Harbour, physical objects will – in theory – be digitally available and interact with each other in an automated way without human intervention. This means *de facto* that the need to exchange (electronic) documents through human actors could gradually disappear and make way for direct communication between the digital 'smart' objects in a Twin Harbour through automated messages. This could lead to 'smart harbours' that are increasingly populated by autonomous smart objects, ranging from 'static' smart containers to dynamic vehicles including trucks and ships.

A crucial part of (smart) seaports, are containers. Approximately 90% of all trade is conducted via maritime containers, of which more than 500 million are shipped annually in the supply chain. This incredible quantity of containers travelling by sea from country to country and continent to continent makes them a prime target for individuals or organised groups involved in illicit drug trafficking, arms

trafficking, or human trafficking and for those involved in the production and supply of counterfeit products (Tops et al., 2021). Both customs and other authorities were surprised during the 1980s with the use of containers by international drug cartels and smugglers. The latter made clever use of the anonymity, relative concealment, reliability, and efficiency of containers to transport drugs (Levinson, 2016). For example, essential raw materials for synthetic drugs, the so-called precursors, are mainly produced in China. From China they are transported to the Netherlands, often via containers, to be converted here into the desired end product, i.e., ecstasy, amphetamine and methamphetamine. A large proportion of these end products are then distributed around the world. Without a sophisticated international logistics system, none of this would be possible; containers play a crucial role here (Tops, van Valkenhoef, van der Torre, & van Spijk, 2018). This has allowed local drug producers to grow into international players where the location of customers is of minor importance, given the low costs of transport. After all, containers proved to be just as efficient for transporting legal as illegal products, including drugs, immigrants, counterfeit products, and weapons/munitions. The global dependence on maritime trade, combined with sophisticated methods of concealment by drug traffickers or product counterfeiters and diverse smuggling routes, make successful interception and intervention a difficult task. Previously, the focus was mainly on the physical security of containers; the demarcation of container storage areas and access controls. However, this focus is broader nowadays, due to the many possibilities offered by AI and Data Science. For example, container security is increasingly equipped with 'smart' automated systems, for example biometric access controls that use computer vision technology, resulting in 'smart containers'.

A concrete example of a smart container can be found in the port of Rotterdam under the heading of 'Container 42'. The 'Container 42' project is a good example of the digital transformation that the Port of Rotterdam is pursuing, as the port has the ambition to become the smartest port in the world (Port of Rotterdam, 2019). The 'Container 42' project, which started in 2019, is committed to developing a smart container equipped with dozens of sensors to detect vibration, temperature, GPS position, noise, and air pollution, among other things. The data generated by these sensors will enable the container to make decisions autonomously to a certain extent. An essential part of the smart container is a 'smart lock' that can determine exactly where and when a container was opened and can indicate in advance where a container may be opened by applying 'geofencing' technology (Van den Heuvel & Tops, 2021). Thanks to the smart lock, containers can be used less easily for criminal purposes (such as the illegal transport of drugs). Containers are an essential part of seaports, and thus also of the concept of 'smart ports', and could potentially make the port system less vulnerable to criminal exploitation.

Figure 3. Container 42 (Onze Haven, 2020).

The potential of AI and Data Science in reducing the vulnerability of ports to undermining crime

In this section, we explain the potential of AI and Data Science in reducing the vulnerability of ports to undermining crime. We do this by using relevant literature and findings from our own research (Tops et al., 2021). This section focuses on the following argumentation, which will then be discussed step by step.

1. Recent years have shown increasingly better physical security at ports (e.g. through better surveillance, access passes, smart fencing);

2. As a result, criminal attention has shifted to the human factor (bribing people to gain access to the port area); Therefore,

3a. On the short term, we need to pay more attention to the human factor because this risk is not likely to disappear soon.

3b. On the long term, we could reduce these vulnerabilities by investing in promising technological developments (Twin Ports, Container 42, AI, Data Science) which announce amongst others to diminish the importance of the human factor.

Step 1. Recent years have seen an increase in the physical security of ports (e.g. through better surveillance, access passes, smart fencing)

Seaports constitute logistical infrastructures that are vulnerable to international drug trafficking; it is a phenomenon that has been extensively documented (Staring et al., 2019; Sergei et al., 2021; Noordanus et al., 2020; Tops & Tromp, 2021) and also acknowledged in government documents (BOTOC, 2018). In recent years, there has been significant investments in the physical security of ports, including the deployment of entrance gates, guards, surveillance vehicles and extensive camera surveillance (Roks, Bisschop, & Staring, 2020). Based on interviews, Nelen and Kolthoff (2017) found that stakeholders in the port have succeeded in using combined efforts to significantly raise the threshold for criminal activities in the port area through risk analysis and stricter supervision.

In this and other ways, ports have worked on improving their physical security in recent years. They all have in common that they try to make it more difficult for 'unauthorised persons' to gain access to port areas.

Step 2. As a result, criminal attention has shifted to the human factor (bribing people to gain access to the port area)

However, the downside of success in improved security is that criminals increasingly rely on contacts within the port area to secure and relocate drugs or other illegal goods (Nelen & Kolthoff, 2017). With the improvement of physical border gates to the port, the focus from the criminal organisations has shifted to trying to influence the human factor (Roks, Bisschop & Staring, 2020). Hiemstra and de Vries (2021) therefore conclude in their report that the greatest vulnerability, exploitation, and risk associated with any port processes is the human factor. After all, a wide range of port employees have physical access to port sites, insight into the refinement of port logistics and detailed knowledge of container numbers and -locations, security measures and supervision (Roks, Bisschop & Staring, 2020). They represent the human vulnerabilities at ports, as they can be corrupted or coerced by criminals into involvement in drug trafficking. These workers range from port workers (including crane operators, security staff) to police officers and customs officials (Nelen & Kolthoff, 2017; Meeus, 2019).

Both the literature consulted, and the experts interviewed in the research of Tops et al. (2021) underline the development that better physical security has led to a shift in criminal attention to the human factor at the port.

Step 3a. However, on the short term, we need to pay more attention to the human factor because this risk is not likely to disappear soon

The ambition of ports such as Rotterdam and Moerdijk to operate as 'smart ports' within ten years may have major consequences for the required human workforce, which is expected to diminish. The vulnerability of ports in terms of undermining crime could therefore decrease. However, the exploratory study by Tops et al. (2021) shows that the human factor at ports will not disappear completely in the short term, the redundancy of the human factor as a result of technological developments at ports might only be realistic in the long term. In the current phase (and in the near future) of smart ports, human resources still have an important role to play. First of all, for data analysis. In the long run, it may be possible for technology itself to inter-

pret data from dashboards by training AI technologies, without the need for human analysts. However, the experts interviewed in our own research do not see this happening in the near future. Moreover, some physical functions will remain reserved for humans – at least in the near future – such as lashers, rowers, pilots and steersmen. Lashers are people who secure all kinds of cargo in ships, also known as cargo-lashing. A rower is someone who helps seagoing vessels to dock and undock in ports. Pilots advise the captain or helmsman when entering or leaving the port. Helmsmen have the task of ensuring that all tasks on board are carried out properly and safely. They are an essential link between the skipper (or captain) and the rest of the crew and must be able to replace the skipper if necessary. The experts interviewed in the study strongly agree that these functions will still be performed manually in the near future and will not be replaced by technology soon. Even if the consultation for entering and leaving the port takes place remotely instead of physically on board, this must – because of the possible dangerous consequences of an error – still be done by people, according to a port expert.

Step 3b. On the long term, we could reduce these vulnerabilities by investing in promising technological developments ((Twin Ports, Container 42, AI, Data Science) which announce amongst others to diminish the importance of the human factor

Digital Twins at ports seems a (distant) prospect, but developments are already underway. Digital twins can be defined as "the right data available at the right time and place, anytime and anywhere", according to an interviewed employee of the Port of Rotterdam (Tops et al., p. 81). For example, a container ship in 'the smart port of the future' can be considered as "a large amount of data on the move, bundled in many thousands of intelligent containers on the ship" (Kuipers, Koppenol, Paardenkooper, & van Driel, 2018, p. 167). Interestingly, the vulnerable human factor (in the context of undermining crime) could disappear from ports as the role of technology increases and gradually takes over human activities in the smart ports of the future. These technological developments can potentially play an important role in securing ports against undermining crime. A concrete example of the development of Digital Twins at ports is Container 42. The development of 'smart containers' is likely to make it significantly more difficult to use containers for criminal purposes, due to technological security mechanisms (such as geofencing) and accurate recording of the container's movements, weight and temperature (and deviations within these factors). Container 42 illustrates that a solution to securing logistic hubs, such as ports, against undermining crime does not lie in Data Science alone, but in a combination of Data Science with physical modifications of (objects of) the port. Container 42 is a physical development coupled with data and is therefore an example of the vision of a digital twin (a data development) reduced to one object (a physical development).

How to realise the potential of AI and Data Science to make ports less vulnerable to undermining crime

The findings of Tops et al.'s (2021) research show that it might be worthwhile to continue to monitor technological developments at ports, with an eye to what it can deliver in the fight against undermining. Indeed, the discussed technological developments at ports, and thus the trend towards smart ports in the future, may have several positive effects in the long term:

- Making it physically more difficult to enter ports and containers.
- Detecting contraband.
- Provide detection information using smart sensors on the container.
- Reducing human actions in the process of container transport.

However, the technological developments should not be taken for granted or considered a silver bullet solution in themselves. To realise the potential of AI and Data Science to protect ports from undermining crime, attention must be paid to the following aspects:

a) ensuring the acceptance of the new (automated) technologies.

b) adopting a systems approach.

Ensuring the acceptance of the new (automated) technologies

As described in step 3a (section 5), the human factor is still here to stay; in the short term for physical processes in the port, but also in the long term for the design of algorithms. The study enabled the exploration of factors that port experts consider relevant for the acceptance and usage of these new technologies. The Technology Acceptance Model (TAM) was used as a guiding model to explore these factors.

First of all, the results of the interviews with port experts show that a socio-technical approach is desirable when discussing the potential of these new technologies. The majority of the experts talked about the technological innovations in a rather deterministic way, for example "The technology *will lead* to better security" or "The obligation of smart containers *will lead* to more stakeholders making use of it" (personal communication, 29 November 2021). However, as the field of Science and Technology Studies (STS) points out, it is important to consider *the interaction* between the technology and practitioner (e.g. Tromp, Hekkert & Verbeek, 2011; Mali et al., 2017; Meijer et al., 2021). For example, in studies about the use of algorithms in policing it is shown that human employees still have the task to enrich the data from algorithms to come to meaningful insights to act on the output when performing their working tasks (Mali et al., 2017) and that the outcome of the process of organizational rearrangement around the use of an algorithm is not determined by the technological features itself but by social norms and interpretations of the facilities of algorithmic systems (Meijer et al., 2021).

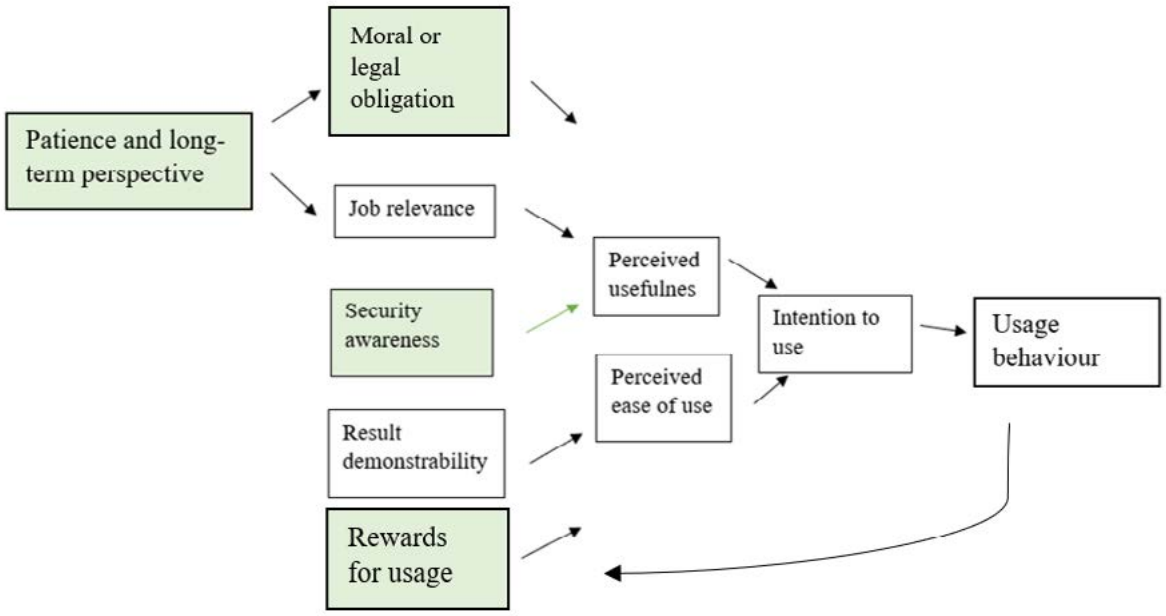
Keeping that in mind, the interviews from the study by Tops et al. (2021) gave a first impression of new factors that might be relevant for the acceptance and usage of new automated technologies. Two factors were considered by the experts to have a positive influence on the external factor 'job relevance' of the TAM. The experts stated that ports (and their stakeholders) must be prepared to accept that some technological innovations will not have an impact within ten years but may have an extremely positive impact in the longer term. This underlines the importance of patience in the acceptance and use of new technologies in smart ports. Innovation is often accompanied by frustration, as organisations need to see technological innovations in a long-term perspective and consider the long-term relevance of innovations. Patience and long-term perspective relate to job relevance.

The factor 'result demonstrability' from the TAM was considered to remain relevant in smart ports. In the study, this is illustrated by the programme manager of the Port of Rotterdam: "People see objections in things that may not matter, such as solar panels of containers being blocked when stacking containers. But that is not the point: for example, you can spray the container with special paint that extracts energy from sunlight. People are surprised by the world suddenly changing." (personal communication, 27 September 2021). Resistance is an unintended effect that can occur when using new technology (Manning, 1992). Knowledge of the underlying reasons why a new system may or may not be beneficial has a positive effect on the intention to use new technology.

According to expert statements in the study, there must be a sense of urgency among port employees to secure the port against undermining crime. The perceived usefulness of technology is expected to be influenced by security awareness. Security awareness among port employees and stakeholders could be an important factor to have a positive effect on the perceived usefulness of new technologies at smart ports.

In the study, interviewed experts suggested that the voluntary factor in the TAM could be replaced by moral or legal obligation in the case of smart technologies; transport services and users of container transport should be mobilised to use smart containers to ensure the safe transport of goods with little or no opportunity for undermining crime. For example, by introducing a so-called fast lane in which organisations receive a discount for the use of safe containers. Another possibility is to legally require the use of safe (smart) containers. Another solution suggested in the study is to reward the use of smart containers (or other smart technologies); a form of moral obligation. However, replacing voluntariness with obligations does not necessarily mean a greater acceptance and usage of the technologies. Here again it should be stressed that a socio-technical approach is needed that takes into account the interaction between the practitioner and technology.

Figure 4. An adjusted TAM for automated technologies in smart ports, with in green the factors found to be relevant by port experts (based on TAM2 (Venkatesh & Davis, 2000), adjusted by the authors).



Adopting a systems approach

The expert meeting that took place in the study confirms that technological developments in the field of Data Science and AI have the potential to reduce the vulnerability of ports to undermining crime. However, this potential could only be realised when stakeholders feel responsible to invest in the developments. The stakeholders involved, however, face the dilemma of who can be held responsible for undermining crime within the container transport chain. Because of the many different stakeholders involved – shipping companies, ports, cargo owners, etc. – each with their own interests, the question of responsibility is one that is often wrestled with. The stakeholders involved are dependent on each other in the logistics chain; "We are all part- and moral owners... No one feels ownership to solve it either." (Tops et al., 2021, p. 84). The dilemma of responsibility is of great importance in the context of tackling undermining crime, because a shared sense of responsibility can drive new (technological) innovations. There is an awareness among those involved that several stakeholders must be mobilised to achieve technological developments in container transport and that technological developments must therefore be viewed from a systematic approach and with a long-term perspective.

The expert meeting revealed the need for an exchange of knowledge and expertise between the parties. On the one hand, to learn from each other's issues – and the projects currently being carried out in this area – and, on the other, to prevent a waterbed effect in which criminals move to ports that are technologically less developed. Since criminals also continue to develop (technologically), it is important to join forces and work together. "Alone you go faster, together you get further" (ibid., p. 86). The experts in the study make two recommendations in the context of this desired cooperation. First of all, they recommend to create a joint agenda with projects in the field of undermining crime and technology at ports. This can help to prioritise and distinguish between the fragmentations of projects in this area. The second recommendation relates to benchmarking: establishing a lower limit and making effects measurable. Establishing a lower limit for minimum performance can help in addressing other ports, also at the European level. In addition, benchmarking can possibly contribute to measuring the effects of technological implementations.

Possible new vulnerabilities at smart ports

To realise the potential of Data Science and AI in protecting ports from undermining crime, it is necessary to consider possible new vulnerabilities that may arise as a result of digitalisation. One potential new vulnerability consists of digital attacks that can lead to the interruption of port processes. The interviews in the study by Tops et al. (2021) outline the expectation that in the future the context of ports – or the digital infra-

structure – will be attacked, so that from that context the port becomes vulnerable; "In the future, you will not be attacked yourself, but digitally, without damaging the physical object" (ibid., p. 82). For example, you only need to attack one terminal to bring down the whole system. The 2017 Russian cyber-attack victimising the Maersk container company demonstrates the dependence on digital infrastructure. Russian military hackers spread the ransomware NotPetya via vulnerabilities in Ukrainian accounting software, which they had previously hacked into. The spread of the ransomware was not limited to Ukraine and affected various companies and organisations worldwide, causing damage estimated at many billions of euros. The Rotterdam branch of the container company Maersk was also a victim. Container transport via the port, motorway and railway came to a stop, resulting in traffic jams (Scientific Council for Government Policy, 2019). Another example comes from the port of Antwerp. In the port of Antwerp, hackers manipulated the terminals of two large container handling companies on behalf of a Dutch drug gang. The IT specialists used malicious software that was sent by e-mail. They also broke into offices to get information. This enabled the gang to get to the containers before the carrier did (Van Maanen, 2019). These examples underline the importance of cyber security in ports, a necessity that is also increasing with the increasing digitalisation of ports.

Not only the technology itself, but also the people behind the technology can become targets for criminal purposes, what – again – stresses the need for a socio-technical approach when monitoring the technological developments of smart ports (e.g. Niculescu-Dinca, 2021). Although technological progress can be seen as reducing the opportunities for illicit trafficking by fragmenting chains of authorities and creating shared information storages, it also brings new challenges and shifts certain risks (Sergi, 2020b). By making technologies more secure, people who have access to them may themselves become targets. Since it can be difficult for most criminals to remotely access computer systems, this can lead to attempted corruption of back office personnel rather than port workers at terminal sites (Easton, 2020, in Tops et al., 2021).

Conclusion and recommendations

This contribution shows that Dutch ports have both the ambition and the potential to operate as 'smart ports' within ten years and to minimise the vulnerable human factor in ports in terms of undermining crime. The developments of smart ports are promising, for example smart containers. How relevant these technologies are going to be 'tomorrow' is constructed today. We can do that by carefully studying and building knowledge about their potential and in this way working towards fulfilling their potential. Tops et al. (2021) recommend that the undermining domain, much more than now, take this development into account in the process of developing different types of approaches to undermining.

However, the technologies should not be taken for granted or considered a silver bullet solution in themselves. Therefore, based on this study and arguments, we call attention to the following aspects:

1) To realise the potential of AI and Data Science to protect ports from undermining crime, two things are important:

a) ensuring the acceptance of the new (automated) technologies. The fact that the human factor is for now and in the near future still here to stay, calls for a socio-technological approach when monitoring the practitioner-technology interaction with the automated technological innovations in smart ports.

b) adopting a systems approach. The long-term goal is system change; container 42 is a metaphor for this and a concrete starting point. In this case, Container 42 should not be seen as a separate project, but as a fundamental realisation of a change strategy.

2) Even if fully implemented, criminals may find a different modus operandi (therefore the importance of cybersecurity in ports). Not only the technology itself, but also the people behind the technology can become targets for criminal purposes. What calls for the continued need to pay attention to the human factor (security partitioners and their interaction with technologies) also in the future?

So, in light of all these insights, we make a couple of concrete recommendations:

- Keep a good eye on AI and Data Science developments at ports. This applies to professionals active in the undermining domain, ranging from academics as well as law enforcement practitioners. Herein also lies a task for the government to provide insight and overview in how these developments will evolve. This does not only apply to developments in large ports such as Rotterdam, but also in smaller ports. The government could for example be of assistance in the alignment of various projects and the development of policy for smaller ports.
- Discussing of data governance between the stakeholders – who owns the data, who is allowed to use the data, what is the quality of the data and what possibilities do investigative bodies have for accessing this data? These discussions are gaining new inputs as a result of developments – including trustworthy AI. The insight into data is shifting towards insight into the AI models that underpin the new generation of digital technology with which ports will be managed, using the Twin Harbour metaphor. This calls for new policies and regulations regarding the sharing of data and models.
- Developing a common and orchestrated strategy on Data Science and AI at ports and its connection to undermining crime at ports, on a national and international level. The consequences and significance for not only the Port of Rotterdam but also other (smaller) ports in the Netherlands will have to be closely monitored and the knowledge (including the technology) will have to be transferred, also in an EU context, to prevent a waterbed effect.
- The entire chain (logistics, justice and production) will have to be included in a holistic system approach. Try to develop technology or standards together with the other partners in the chain (e.g. for improved sharing of (big) data and/or AI models); so-called smart logistics. The chain should also be approached in a European or even an international context. After all, the Netherlands could take the responsibility and lead the way, but we need to get everyone on board on an international scale to bring about real change, and to continue to lead as the Netherlands' trade and distribution country.

References

- BOTOC (2018) Uitwerking breed offensief tegen georganiseerde ondermijnende criminaliteit. Available at: https://open.overheid.nl/repository/ronl-b27340ea-ce38-4e07-aa61-765a1f530cfa/1/pdf/tk-uitwerking-breed-offensief-tegen-georganiseerde-ondermijnende-criminaliteit.pdf
- Colvin, C. A., & Goh, A. (2005) Validation of the technology acceptance model for police. *Journal of Criminal Justice*. 33, 89-95.
- Davis, F. D. (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*. 12 (3), 319-40.
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989) User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*. 35 (8), 982-1003.
- Ernst, S., Ter Veen, H., Lam, J., & Kop, N. (2019) Leren van technologisch innoveren: "De techniek is niet zo spannend". Apeldoorn, Police Academy.
- Ghosen, D. (2021) Danny's Wereld; Onveilige haven. Available at: https://www.npostart.nl/dannys-wereld/04-11-2021/VPWON_1332342
- HARC-team. (2021) HARC-team onderschept ruim 40.000 kilo cocaïne in 2020. Available at: https://www.om.nl/actueel/nieuws/2021/01/13/harc-team-onderschept-ruim-40.000-kilo-cocaine-in-2020
- Hiemstra & de Vries. (2021) Quick scan aanpak criminele stromen zeehavens. Commissioned by the Ministry of Justice and Security.
- Jussi, P. (2021) AI for smart ports, part 2: Optimizing vessel schedule predictions using machine learning. Available at: https://www.awake.ai/post/ai-for-smart-ports-port-call-prediction-part2
- Kuipers, B., Koppenol, D., Paardenkooper, K., & van Driel, H. (2018) Rotterdamse container kopstukken. Rotterdam, Promedia group.
- Levinson, M. (2016) The Box. How the Shipping Container Made the World Smaller and the World Economy bigger. New Jersey, Princeton University Press.
- Lin, C., Hu, P. J., & Chen, H. (2004) Technology implementation management in law enforcement: COPLINK system usability and user acceptance evaluations. *Social Science Computer Review*. 22 (1), 24-36.
- Mali, B., Bronkhorst-Giesen, C., & den Hengst, M. (2017) Predictive policing: lessen voor de toekomst. Apeldoorn, Police Academy.

- Manning, P. K. (1992) Information technologies and the police. In: Tonry, M. & Morris, N. (Eds.), Modern Policing: Crime and Justice, A Review of Research. 15, 349–398. University of Chicago Press.
- Meeus, J. (2019) De Schiedamse cocaïnemaffia. Amsterdam, Nieuw Amsterdam.
- Meijer, A., Lorenz, L., & Wessels, M. (2021) Algorithmization of Bureaucratic organizations: Using a Practice Lens to Study How Context Shapes Predictive Policing Systems. *Public Administration Review*. 81, 837-846. https://doi.org/10.1111/puar.13391
- Nelen, H., & Kolthoff, E. (2017) Schaduwen over de rechtshandhaving. Georganiseerde criminaliteit en integriteitsschendingen van functionarissen in de rechtshandhaving. The Hague, Boom Criminologie.
- Niculescu-Dinca, V. (2021) Theorizing technologically mediated policing in smart cities. An ethnographic approach to sensing infrastructures in policing practices. In M. Nagenborg, T. Stone, G. Woge, & P. Vermaas (Eds.), Technology and The City: Towards a Philosophy of Urban Technologies. New York: Springer, pp.75-100.
- Noordanus, P., van der Torre, E., Tops,P., & Kester, J. (2020) Een pact voor de rechtsstaat; een sterke terugdringing van drugscriminaliteit in tien jaar. The Hague, Aanjaagteam ondermijning.
- NOS (2021, oktober 29) Tussen frituurvet en ananassen: meer dan 1500 kilo coke onderschept in haven Rotterdam. Available at: https://nos.nl/artikel/2403484-tussen-frituurvet-en-ananassen-meer-dan-1500-kilo-coke-onderschept-in-haven-rotterdam
- NOS (2021, september 13) Negen mensen in ademnood uit container op maasvlakte gehaald. Available at: https://nos.nl/artikel/2397655-negen-mensen-in-ademnood-uit-container-op-maasvlakte-gehaald
- Onze Haven (2020) Reisverslag van de slimste container. Available at: https://onzehaven.nl/2020/01/03/reisverslag-van-de-slimste-container/
- Perera, L., Oliveira, P., & Soares, C. (2012) Maritime Traffic Monitoring Based on Vessel Detection, Tracking, State Estimation, and Trajectory Prediction. *Institute of Electrical and Electronics Engineers*. 13 (3), 1188-1200.
- Public Prosecutor's Office. (2021, september 17) Douane onderschept 4022 kilo cocaïne tussen hout. Available at: https://www.om.nl/actueel/nieuws/2021/09/17/douane-onderschept-4022-kilo-cocaine-tussen-hout
- Roks, R.A., Bisschop, L.C.J., & Staring, R.H.J.M. (2021). Getting a foot in the door. Spaces of cocaine trafficking in the Port of Rotterdam. *Trends in Organized Crime*. 24, 171–188.
- Schwab, K. (2016) The fourth industrial revolution. New York, Penquin Random House.
- Sergei, A., Reid, A., Storti, L., & Easton, M. (2021) Ports, Crime and Security. Governing and Policing Seaports in a Changing World. Bristol, Bristol University Press.
- Staring, R., Bisschop, L., Roks, R., Brein, E., & van de Bunt, H. (2019) Drugscriminaliteit in de Rotterdamse haven. Aard en aanpak van het fenomeen. The Hague, Boom Criminologie.
- Tops, P., van Valkenhoef, J., van der Torre, E., & van Spijk, L. (2018) Waar een klein land groot in kan zijn; Nederland en synthetische drugs in de afgelopen 50 jaar. The Hague, Boom Criminologie.
- Tops, P., van den Heuvel, W., de Groes, N., & Gravenberch, V. (2021). Hoe zeehavens veranderen door Artificial Intelligence en Data Science en wat dat kan betekenen voor de aanpak van ondermijning. Een praktijkverkenning. Centrum voor de studie van ondermijning, Jheronimus Academy of Data Science.
- Tops, P., & Tromp, J. (2021) Nederland drugsland. Amsterdam, Balans.
- Tromp, N., Hekkert, P., & Verbeek, P. (2011) Design for socially responsible behavior: A classification of influence based on intended user experience. *Design Issues*. 27 (3), 3–19.
- Van den Heuvel, W. & Tops, P. (2021) AI en data science in de haven. Hoe Artificial Intelligence en Data Science een hefboom kunnen zijn voor Slimme(re) Havenbeveiliging. Jheronimus Academy of Data Science, Tilburg University.
- Van Maanen, M. (2019) De aansprakelijkheid van de zeevervoerder voor pincode fraude bij aflevering. Available at: https://www.vantraa.nl/media/2128/mma-de-aansprakelijkheid-van-de-zeevervoerder-voor-pincode-fraude-bij-aflevering.pdf
- Vankatesh, V. & Davis, F. D. (2000) A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*. 46 (2), 186-204.
- Verseput, S., & de Haan, M. (2021) De drugsuithalers hebben nu bijna vrij spel in de Rotterdamse haven. NRC. Available at: https://www.nrc.nl/nieuws/2021/09/22/de-drugsuithalers-hebben-nu-bijna-vrij-spel-in-de-haven-a4059311
- Wetenschappelijke Raad voor het Regeringsbeleid (2019) Voorbereiden op digitale ontwrichting. Available at: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

Evidential Validity of Video Surveillance Footage in Criminal Investigation and Court Proceedings

Ksenija Butorac
Hrvoje Filipović
Police University College[1], Ministry of the Interior, Zagreb

Abstract
The paper analyzes several aspects of the video surveillance system application, starting from the prevention of misdemeanors and crime according to the Council Decision on the establishment of the European Crime Prevention Network. The second aspect relates to the use of video surveillance systems in the misdemeanors and crime investigation, and the third one relates to the evidential value of video surveillance systems in court proceedings. For this purpose, the case law analysis of the highest level was made, namely of the High Misdemeanor Court, the Supreme Court of the Republic of Croatia and of the European Court of Human Rights through case studies. The paper discusses the evidential value of the footage important for criminal investigation. However, the central issue is a question whether digital evidence in the form of video surveillance can be decisive in court proceedings or not, since no court order is required for it as for other evidentiary actions. The paper proposes solutions de lege ferenda given that video surveillance systems are becoming more widespread and have proven to be very effective in criminal investigation, but, contextually speaking, also in procedural terms. The respective contextual approach requires the interpretation of current case law emphasizing that the content and significance of the footage in court proceedings must be perceived as a whole and that, besides the right of defense, the public and the victim's interests are to be taken into account.

Keywords: video surveillance; protection of human rights and fundamental freedoms; appropriateness test; necessity test; proportionality test.

Introduction

A fair procedure is in the interests of the public, the media, and the bodies conducting criminal proceedings. The values related to this process, as well as to human rights in general, have been actively contributed by the European Court of Human Rights and the European Convention for the protection of Human Rights and Fundamental Freedoms. The principle of fair procedure, as Roxin (2012) states, is a supreme principle, and two functions stand out in the procedure: the protection of society from crime; and the protection of human rights.

Thus, video surveillance can be viewed in the context of the principle of protection of citizens' rights and the principle of effectiveness. It is against these two different

1 Co-authors' emails: kbutorac@fkz.hr; hfilipovic@fkz.hr

contexts where dubious interpretations occur, even at the highest court levels. Video surveillance is no longer the exception but the rule in the protection of persons and property. Accordingly, there is no important institution that is not covered or protected by video surveillance.

The aim of this paper is to determine the probative value of video surveillance and related institutes, which are sometimes problematized when evaluating evidence. Our research is based on case studies of judgments of the European Court of Human Rights, the Supreme Court and county courts of the Republic of Croatia. The following issues will be particularly problematized:

- When applying video surveillance, is it a violation of Art. 8. European Convention for the Protection of Human Rights and Fundamental Freedoms[1].
- When applying video surveillance, is it legal evidence that has sufficient probative force or must it be supported by other evidence, such as, for example, the questioning of the defendant, temporary confiscation of objects, questioning of witnesses and other evidentiary proceedings?
- When applying video surveillance, should the appropriateness test, necessity test and proportionality tests be applied.

Video surveillance in general

It has already been emphasized that video surveillance should be seen in the context of protecting society from crime, which, on the one hand, nevertheless limits the rights of citizens, and, on the other hand, protects the same citizens from possible threats. The crucial importance of video surveillance is that it has a preventive as well as a revealing role in the criminal investigation of misdemeanors or criminal acts. Gold (2004) states that video surveillance is closed circuit television as a generic term (CCTV), and it is the use of video cameras to transmit video signals to a central control computer in order to monitor the obtained footage in real time or store it for subsequent review and analysis (Gold, 2004, according to Butorac et al., 2016, 102).

When video surveillance was introduced, there were concerns on their impact on individual rights and freedoms that evaporated subsequently when their role in detecting serious crimes became evident. A criminal event that, even on a global level, brought changes in the understanding of the value of video surveillance took place on February 12, 1993, when two perpetrators J.V. (10 years old) and R.T. (10 years old) kidnapped and tortured two-year-old J.B., whom they eventually killed. The perpetrators were discovered, and later convicted too, by using surveillance cameras recordings that revealed the perpetrators taking the toddler away (see Levine, 1999; Maguire, Morgan & Reiner, 2007; Easton & Piper, 2016).

In the last ten years, video surveillance has not only been accepted, but has also been demanded in public places because their presence makes the citizens feel safer. Moreover, research has shown a reduction in both misdemeanors and criminal offences in such a places. The research conducted by Filipović and Šneperger (2012, 850) in Vodnjan near Pula (Croatia) shows the effectiveness of video surveillance in preventing crime at the main square of a small town. The aim of this research was to determine the number of criminal offences by comparing the number of incidents four years before the introduction of video surveillance with the number of respective cases four years after such a system was installed. There was a decrease in criminal offences by 31 percent, and misdemeanors by 32 percent. Butorac et al. (2016, 104) state that the advantages of video surveillance are multidimensional and manifest in reducing the fear of crime in the local community, providing emergency medical care, managing the scene, gathering information, added value to this surveillance and assisting in criminal investigations.

Regarding video surveillance, Usher (2003) states that it is a surveillance technique aimed at preventing punishable behavior with increasing the perceived risk for being detected when committing a criminal offence. The main purpose of video surveillance is to deter potential criminals from committing criminal acts in areas under video surveillance, provided they are aware of the existence of such surveillance. In cases where the existence of cameras is publicly known, potential perpetrators, as a rule, perceive and evaluate situations in which the increased risk of arrest outweighs the possible benefit of the criminal act, and most often give up their original intention.

1 Available at https://www.echr.coe.int/Documents/Convention_ENG.pdf.

Application of video surveillance over financial institutions, public areas, workplaces and residential buildings

The use of new technologies should also be seen in the context of several important sources, namely, first of all, the EU Charter of Fundamental Rights (2016/C 202/02), which determines the protection of privacy and family life, home and communication (Article 7). Protection of personal data from Art. 8. is determined in more detail, so the first paragraph refers to the protection of personal data, the second paragraph requires that several conditions be cumulatively met: the data must be processed fairly for established purposes and based on the consent of the person in question, or on some other legitimate basis established by the law. The third paragraph states that the protection of personal data is subject to the supervision of an independent body.

In the EU Charter of Fundamental Rights, and the Treaty on the Functioning of the European Union (2016/C 202/1) in Art. 16. the protection of personal data is defined, as well as the rules on the protection of individuals with regard to the processing of personal data in the institutions, bodies, offices and agencies of the EU, when they perform their activities in the area of application of EU law and the rules on the free movement of such data (Art. 16, para. 2, UFEU). Consequently, it can be concluded that the protection of personal data is subject to numerous normative sources.

Video surveillance is most commonly used in financial institutions, public areas, workplaces and residential buildings. There are several normative sources in force in Croatia that regulate the application of video surveillance, namely the Act on the Protection of Financial Institutions (Official Gazette 56/15, 46/21) and the Act on the Implementation of the General Data Protection Regulation (Official Gazette 42/18), which implemented Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Independent supervision, in addition to criminal prosecution bodies, is carried out by the Personal Data Protection Agency according to the aforementioned acts. It is important to emphasize that the processing of personal data through video surveillance can only be carried out for a purpose that is *necessary and justified* for the protection of persons and property, and recordings obtained through video surveillance can be kept for a maximum of six months (Article 26, paragraph 1 of the Act on the Implementation of the General Data Protection Regulation). It is important to emphasize that if, during the implementation of the supervision, information is obtained or objects are found that point to the commission of a criminal offence for which there is *ex officio* prosecution, the authorized persons shall notify the competent police station or the state attorney as soon as possible (Article 38 of the Act on the Implementation of the General Data Protection Regulation).

The Act on the Protection of Financial Institutions (Official Gazette 56/15, 46/21), financial institutions, branches of the Financial Agency, the Croatian Monetary Institute, bank branches, central vaults, ATMs, residential savings banks, post offices, betting shops, slot machines, jewelry stores, and casinos requires protective measures, one of which is a continuous video surveillance system inside and outside the facility with video storage in digital form. There are numerous examples in Croatia, and only a few will be singled out in the following, from which the effectiveness of video surveillance in detecting the perpetrators of criminal offences is the most notorious, because the afore mentioned legislative solution has networked cities with cameras that are also used by the police in case of criminal offences.

Video surveillance of public areas

Video surveillance of public areas is permitted only for public authorities, legal entities with public authority, and legal entities performing public service, and it is permitted only when it is prescribed by law as being necessary for the execution of the business and tasks of public authorities or for the protection of life and health of people and property (Article 32 of the Act on the Implementation of the General Data Protection Regulation). Offenders have often, and still do, filed appeals that video surveillance footage is illegal evidence, but, as research into numerous case studies displays, such appeals have been rejected as unfounded. This is also the case in the judgment of the County Court in City of Split (Business number: Kžmp-7/2021-5, Split, March 9, 2021), in which it is stated that surveillance camera footage of public places such as streets, squares, and the like do not constitute illegal evidence, since every person who appears in a public space must be ready and reckon with the fact that they can be recorded by a surveillance camera.

Video surveillance of residential buildings

The establishment of video surveillance in residential or business-residential buildings requires the consent of the co-owners, who make up at least 2/3 of the co-owned parts, and video surveillance can only include access to entrances and exits from residential buildings and their common rooms. The use of video surveillance to monitor janitors, cleaners and other persons working in a residential building is prohibited (Article 31 of the Act on the Implementation of the General Data Protection Regulation).

Perpetrators of criminal offences problematize and call into question court decisions regarding the legality and evidentiary use of video surveillance recordings of commercial companies and residential buildings. Thus, in the following example of the decision of the Supreme Court of the Republic of Croatia (SCRC), it is evident that it is, contrary to the allegations of the appeal, and according to the assessment of the SCRC as a second-instance court, the correct conclusion of the first-instance court that the minutes on the temporary confiscation of items and certificates on the temporary confiscation of items refer to video surveillance recordings, and, consequently, specific video surveillance recordings, as well as the expert report and opinion of expert V. M. are not illegal evidence, and that there is no place for their separation, as suggested by the defendant. From the cited certificates and minutes on the temporary confiscation of objects, the video surveillance footage was exempted by the police in the pre-investigation procedure related to the investigation of the criminal offence referred to in Article 110 in connection with Article 34. Criminal Code/11 (attempted murder) committed to the detriment of the victim K. R. Therefore, contrary to the appellant's position, the data processing, which unquestionably includes the viewing of recordings, and which has the purpose of discovering criminal offences and their perpetrators, in this particular case was carried out by the competent authorities, and not by the compiler of the disputed video surveillance, so it is not illegal evidence (SCRC, Number: I Kž 680/2020-4, Zagreb, December 14, 2021).

Video surveillance of workplaces

The processing of the employee's personal data through the video surveillance system can only be carried out if the conditions established by the regulations governing safety at work are met and if the employees were adequately informed in advance about such a measure and if the employer informed the employees before making the decision to install the video surveillance system. Video surveillance of work premises must not include rooms for rest, personal hygiene and changing clothes (Article 30 of the Act on the Implementation of the General Data Protection Regulation).

There are frequent complaints for illegal recording. In one separate judgment of the County Court it was pointed out that video surveillance at the DM – drogerie markt d.o.o. shopping center in the City of Zagreb, was installed in accordance with legal regulations in public space and with the aim of preventing criminal acts. Namely, as the first-instance court correctly concluded, in this particular case it is not illegal evidence because a warning that the area is under video surveillance, was displayed in a visible place in the area of the shopping center (Zagreb County Court, 7 Kž-706/2020-3 dated October 19, 2020).

Video surveillance in recent decisions of the European Court of Human Rights

Video surveillance appears in the context of several provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms, and it is certainly worth highlighting: "The right to respect for private and family life" (Article 8) and "The right to a fair trial" (Article 6).

Article 8, paragraph 1 of the Convention reads: " Everyone has the right to respect for his private and family life, his home and his correspondence", and Art. 8, paragraph 2 of the Convention reads: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

In the introductory part, it was already said that there is a conflict between the *principle of protection of citizens' rights and the principle of effectiveness*, which can also be applied to Art. 8, paragraph 1 of the Convention, because on the one hand, respect for one's private and family life, home and correspondence is ensured, but not unconditionally, because already Art. 8. paragraph 2 stipulates that the public authority (police) shall not in-

terfere in the exercise of this right, except in accordance with the law and if in a democratic society it is necessary in the interest of state security, public order and peace, or the economic wellbeing of the country, and prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. The example of video surveillance in the workplace has already been mentioned, but it should be viewed through Art. 8, paragraph 1 and paragraph 2 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The legal doctrine of the application of video surveillance according to Art. 8. is not completely uniform, but additional criteria have been given in several judgments, so it is evident in the recent separate case study *Bărbulescu v. Romania* (application no. 61496/08 of January 12, 2016) that the European Court of Human Rights has determined the principles that must be applied in cases of employee supervision at the workplace.

In order to ensure the proportionality of surveillance measures, i.e. to achieve a fair balance between conflicting interests, domestic courts must take into account the following factors:

- Whether the employee had been notified of the possibility of video-surveillance measures being adopted by the employer and of the implementation of such measures;
- The extent of the monitoring by the employer and the degree of intrusion into the employee's privacy;
- Whether the employer had provided legitimate reasons to justify monitoring and the extent thereof;
- Whether it would have been possible to set up a monitoring system based on less intrusive methods and measures;
- The consequences of the monitoring for the employee subjected to it;
- Whether the employee had been provided with appropriate safeguards (*Bărbulescu v. Romania*).

Video surveillance in the shopping center

The European Court for the Protection of Human Rights and Fundamental Freedoms has also discussed the application of video surveillance in numerous recent decisions. In the judgment of *López Ribalda et. al. v. Spain* (ECHR, 1847/13, January 9, 2018) it is evident that *"the applicants were employed in the Spanish supermarket chain M. as cashiers and sales assistants, and after the manager noticed the economic losses in the supermarket business, he decided is to install* visible *and* invisible *cameras to confirm suspicions about potential thefts" (*§ 12*.).* The applicants claimed that the decision by which their employer fired them was based on video surveillance that was carried out in violation of their right to respect for their private life guaranteed by Art. 8 of the Convention and that domestic courts have not fulfilled their obligation to ensure the protection of that right *(§ 3).* Furthermore, according to Art. 6. of the Convention they complained about the inclusion in evidence of recordings obtained by video surveillance during the procedure. According to the same provision, the third, fourth and fifth applicants further appealed against the acceptance of the settlement agreement they signed with their employer by the domestic courts *(§ 3).* The court made a decision that there was a violation of Art. 8., and that there was no violation of Art. 6 of the Convention. On October 17, 2019, the Grand Chamber made another decision that is different from the decision of January 9, 2018, that is, it considered that there was no violation of the Convention.

It is worth noting that in this case too the court points out in an ambiguous way that the court should not act as a court of fourth instance and therefore will not question the judgments of national courts unless their findings can be considered arbitrary or manifestly unreasonable *(§ 149).* In the judgment of *López Ribalda et. al. v. Spain*, an opinion was expressed that is significant and even far-reaching, and indeed when some authors say that the Convention is a "living organism", this is confirmed in the following statement: "New technologies have dramatically changed the ease with which video surveillance can be carried out and transmitted, thereby significantly multiplying the potential violation of the right to privacy under Article 8 of the Convention". It is precisely for this reason that there is a need, at the national level, for the legislative framework to be clear and predictable in relation to cases concerning electronic surveillance (p. 51 and 52. *López Ribalda et. al. v. Spain*), and such a notion repeated is also in the case of *S. and Marper v. the United Kingdom* ([VV], no. 30562/04 and 30566/04, ECHR 2008), where the court concluded that "detailed rules governing the scope and application of measures" are necessary to ensure sufficient guarantees against the risk of abuse and arbitrariness.

From the judgment of *López Ribalda et. al. v. Spain* are the visible criteria that the national courts have estab-

lished for the measure to be considered acceptable, namely that it should pass a threefold test, the first relates to a legitimate aim (appropriateness test), the second measure should be necessary (necessity test) and proportional (proportionality test). In other words, the courts had to determine whether a fair balance had been established between the interference with the fundamental right and the importance of the legitimate aim achieved (López Ribalda et. al. v. Spain, ECHR, 1847/13, January 9, 2018).

Thus, all three criteria must be met when evaluating the video surveillance in order not to resort to more difficult means to achieve the goal, which would constitute a violation of human rights. The fact that in the judgment *López Ribalda et. al. v. Spain Proportionality test* was highlighted 28 times, *Necessity test* 5 times and *Appropriateness test* 4 times, speaks of their relevance.

Video surveillance in the faculty lecture halls

The judgment Antović and Mirković (*Case of Antovic & Mirkovic v. Montenegro*, 70838/13, 28.11.2017, 28.2.2018) is in focus because many, who deal with legal doctrine, can find themselves in such a situation that they are recorded when they have presentations in front of students, whether they are permanently employed at the faculties or are guest lecturers. This judgment is also interesting because there were separate opinions of the judges questioning whether it is really a violation of Art. 8 of the Convention.

It is evident from the circumstances of the judgment that the dean of the Faculty of Science and Mathematics informed the professors who teach there (including the applicants) at the session of the Faculty Council that video surveillance has been introduced in seven lecture theatres (§ 6). The decision stated that the aim of the measure is to ensure the safety of property and people, including students, and to supervise the performance of teaching activities. The decision stated that access to the collected data was protected by codes that were known only to the dean, and the data was to be kept for one year (§ 7).

It is evident from the judgment that on January 19, 2012, the applicants filed a claim for damages against the University of Montenegro, the Agency for the Protection of Personal Data and the State of Montenegro, due to the violation of their right to private life, especially through the unauthorized collection and processing of data about them. In particular, they argued that such interference in their private lives, without any possibility of controlling that process, was not foreseen by any law and therefore was not in accordance with the law, in the sense of Article 8 §. 2 of the Convention. They also argued that it did not pursue any legitimate goal and was not needed in a democratic society. They referred to the relevant provisions of the Personal Data Protection Act, Art. 8. of the Convention and relevant case law of the Court (§ 13).

On December 27, 2012, the basic court in Podgorica established that the term private life certainly includes activities in the business and professional sphere. However, judgment stated that the University is a public institution that performs activities of public interest, including teaching, and that, therefore, it is not possible for the use of video surveillance in lecture halls as public places to violate the applicant's right to respect their private life. It is concluded that the installation and use of video surveillance and the collection of data did not violate the applicant's right to privacy and, therefore, did not cause them mental pain (§ 13).

Nevertheless, the European Court of Human Rights reiterates that "private life" is a broad concept that is not subject to exhaustive definition and that it would be too restrictive to limit the concept of "private life" to the "inner circle" in which an individual can live one's personal life as one chooses and to completely exclude from it the external world that is not covered by that circle (§ 41.). The court has already ruled that the term "private life" can include professional activities or activities that take place in a public context. Therefore, there is a zone of interaction of a person with others, even in a public context, which can fall within the scope of "private life", and professional life is part of it (§ 42).

The European Court of Human Rights pointed out that university lecture theatres are the workplaces of teachers where students are taught, but communication with them is also achieved, developing mutual relations and constructing their social identity (§ 55). The court notes that the domestic courts did not examine the question of whether the actions were in accordance with the law, given that they did not consider that the contested video surveillance was an interference in the applicant's private life at all (§ 56), but the Agency for the Protection of Personal Data of Montenegro expressly determined that this is not in accordance with the law, especially Ar-

ticles 10, 35 and 36 of the Personal Data Protection Act (see previous paragraph 11).

In this regard, the Court notes that Art. 35 of the Personal Data Protection Act stipulates that public institutions, like universities, can conduct video surveillance of access areas to official premises. However, in this particular case video surveillance was carried out in lecture threatre (§ 58).

Furthermore, Art. 36 of the Personal Data Protection Act stipulates that video surveillance equipment can also be installed in official or business premises, but only if the goals provided for in that article, especially the safety of people or property or the protection of confidential data, cannot be achieved in any other way. The court notes that video surveillance in this case was introduced to ensure the safety of property and people, including students, and to monitor classes.

It should be noted that one of these goals, namely the supervision of teaching, is not provided by law as a basis for video surveillance. Furthermore, the Agency expressly considered that there was no evidence that property or people were endangered, which is one of the reasons for justifying the introduction of video surveillance, and the domestic courts did not deal with this issue. The government, for its part, has not provided any evidence to the contrary in this regard, nor has it shown that it even previously considered any other measure as an alternative (§ 59).

Given that the relevant legislation expressly provides for the fulfillment of certain conditions before resorting to camera surveillance, and that in this particular case these conditions were not met, and taking into account the Agency's decision in this regard (in the absence of any examination of the issue by domestic courts), the Court cannot but conclude that the interference in question was not in accordance with the law, and this is a fact that is sufficient to constitute a violation of Art. 8. Bearing in mind the previous conclusion, the Court does not consider it necessary to examine whether the other requirements from paragraph 2 of Art. 8. fulfilled (see Amann v. Switzerland [GC], no. 27798/95, § 81, ECHR 2000-II, and Vukota-Bojić v. Switzerland, Application no. 61838/10; § 78).

In the judgment Antović and Mirković v. Montenegro, there are two separate opinions of the judges, in the first, judges Vučinić and Lemmens fully agree with the determination of the violation of Art. 8 of the Convention, but they believe that greater importance should be given to the nature of the activity that is under supervision and that Art. 8 of the Convention guarantees the development, without external interference, of the personality of each individual in his or her relations with other human beings and that therefore there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life (see Peck v. United Kingdom, No. 44647/98, § 57, ECHR 2003-I et al.). (Joint concurring opinion of judges Vučinić and Lemmens, *Case of Antovic & Mirkovic v. Montenegro*, 70838/13, 28.11.2017, 28.2.2018).

These interactions are, of course, not exclusively of social nature. In the classroom, the professor can allow himself to act ("perform") in a way that he might never do outside the classroom, and that, at least in an academic environment, where both teaching and learning activities are covered by academic freedom, the aforementioned expectation of privacy should be considered "reasonable".

This does not mean that video surveillance in the hall is not possible. There may be good reasons for putting the auditorium under video surveillance. This means, among other things, that there must be an appropriate legal basis, that the scope of supervision must be limited and that there are guarantees against abuse (*A. and M. v. Montenegro*, 70838/13, 28.11.2017, 28.2.2018).

In the same case, the judges of the European Court of Human Rights Spana, Bianku and Kjølbro issued a joint unanimous opinion and voted against declaring the request admissible and establishing a violation of Art. 8 of the Convention because they believe that the judgment expands the scope of Art. 8, paragraph 1 of the Convention and can have significant implications because it interprets the term "private life" very extensively and broadly (Joint dissenting opinion of judges Spano, Bianku and Kjølbro, *Case of Antovic & Mirkovic v. Montenegro*, 70838/13, 28.11.2017, 28.2.2018). The judges state that the teachers held classes in the university lecture theatre, which meant that they were fully engaged in their professional activities, and not, for example, in their offices. Because they were informed of the video surveillance in it, their reasonable expectation of privacy in that particular context, if any, was very limited. In conclusion, the mere fact that the lecture theatres are monitored cannot, according to the interpretation of the already mentioned judges, include Art. 8, paragraph

1 of the Convention without proven further elements and that it is not sufficiently supported by convincing legal arguments.

From the aforementioned recent judgment, it is evident that there is a disagreement first between the Agency for the Protection of Personal Data of Montenegro and the Basic Court in Podgorica (Montenegro), where the Agency is of the opinion that the introduction of video surveillance in the faculty's lecture theatres is against Article 8 of the Convention, which was ultimately concluded by the European Court for Human Rights[2]. The Court held that covert video surveillance of employees at their workplace must be considered, as such, as a considerable intrusion into their private life, entailing the recorded and reproducible documentation of conduct at the workplace which the employees, who were contractually bound to work in that place, could not evade. There was no reason for the Court to depart from that finding even in cases of non-covert video surveillance of employees at their workplace. Furthermore, the Court had also held that even where the employer's regulations in respect of the employees' private social life in the workplace were restrictive they could not reduce it to zero. According to Art. 8, paragraph 2, respect for private life continued to exist, even if it might be restricted in so far as necessary. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Conclusion

The issue of video surveillance, as can be seen from recent decisions, is complex and there are still doubts, especially regarding the application of Art. 8. European Convention for the Protection of Human Rights and Fundamental Freedoms. It is a good circumstance that, at the level of the Council of Europe, there are control, and even supervisory, mechanisms that ensure uniform application and that do not deviate from the most important principles, and that only in the case of extremely serious criminal offences can there be justification for the use of new technologies as the only or decisive evidence.

A new normative framework will definitely have to be prepared for new technologies, which will definitely contain provisions related to artificial intelligence, because these are all challenges that the world will face in the near future. However, there is no need to deviate from the fundamental human values that are contained precisely in a superior legal source such as the European Convention for the Protection of Human Rights and Fundamental Freedoms.

We should definitely go back to the opening remarks of the article, in which the two principles of protecting the rights of citizens and the principle of effectiveness are problematized, and the question was which of them will prevail. The answer to the last mentioned question certainly depends on the case by case, that is, there should be a balance as a guide that we encountered in history inspired by Greek and Roman mythology such as *Themis and Iustitia* were.

From the research of judicial practice, case studies were selected that best indicate the problem that can arise with the application of new technologies such as video surveillance, and this is confirmed by the quote from the judgment of *López Ribalda et al. v. of Spain*:

"New technologies have dramatically changed the ease with which video surveillance can be carried out and transmitted, thereby significantly multiplying the potential violation of the right to privacy under Article 8 of the Convention" (Joint dissenting opinion of judges De Gaetano, Yudkivska and Grozev, *López Ribalda et. al.* v. *Spain* (ECHR, 1847/13, January 9, 2018), § 4).

Therefore, it is important that there is a clear and unambiguous legal basis, that the scope of duration must be limited in time and that there are control mechanisms of supervision. In addition, there must be a legitimate, necessary and proportional goal.

We can conclude from the judgments that the jurisprudence of the European Court of Human Rights is also changing and that it is noticeable that when things are similar or identical, part of the "balance" is still tilted towards the protection of citizens' rights. This is an aspiration that should continue to be guided because if there were no such efforts, the question is what level of intrusion into human rights would occur with the further development and application of new technologies.

2 See https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-183012%22]}

References

- Act on the Implementation of the General Data Protection Regulation (2018) Official Gazette 42/18.
- Act on the Protection of Financial Institutions (2021) Official Gazette 56/15, 46/21.
- Amann v. Switzerland [GC], no. 27798/95, § 81, ECHR 2000-II.
  Available at: https://hudoc.echr.coe.int/eng?i=001-58497
- Bărbulescu v. Romania, Application no. 61496/08 of January 12, 2016.
  Available at: https://hudoc.echr.coe.int/eng?i=001-177082
- Butorac, K., Cajner-Mraović, I. & Filipović, H. (2016) Učinkovitost video nadzora u smanjenju kriminaliteta – pregled istraživanja. *Proceedings of the 5th International Scientific-Professional Conference – Research Days of the Police College in Zagreb "Improving the security role of the police by applying new technologies and methods"*, pp. 100-113.
- Case of Antovic & Mirkovic v. Montenegro, 70838/13, 28.11.2017, 28.2.2018.
  Available at: https://hudoc.echr.coe.int/eng?i=001-178904
- Decision of the European Court of Human Rights in the case of López Ribalda et. al. v. Spain, 1847/13, January 9, 2018.
- Decision of the European Court of Human Rights in the case of Antović and Mirković v. Montenegro, 70838/13, November 28, 2017. and February 28, 2018.
- Decision of the European Court of Human Rights in the case of Bărbulescu. Romania, Application no. 61496/08, January 12, 2016.
- Easton, S. & Piper, C. (2016). *Sentencing and Punishment: The Quest for Justice*. Fourth Edition. New York: Oxford University Press.
- European Convention of Human Rights and Fundamental Freedoms
  Available at https://www.echr.coe.int/Documents/Convention_ENG.pdf
- EU Charter of Fundamental Rights (2016/C 202/02)
- Filipović, H. & Šneperger, D. (2012) Prevencija kriminaliteta primjenom sustava video nadzora, *4th International Expert-Scientific Meeting,* Zadar, Croatia, p. 845-853.
- Gold, B. J. (2004) *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*. Oxford: Oxford University Press.
- Levine, M. (1999) Rethinking bystander nonintervention: Social categorization and the evidence of witnesses at the James Bulger murder trial. *Human Relations*, 52(9), 1133-1155.
- López Ribalda et. al. v. Spain, ECHR, 1847/13, January 9, 2018.
  Available at https://hudoc.echr.coe.int/eng?i=001-197098
- Maguire, M., Morgan, R. & Reiner, R. (2007). *The Oxford Handbook of Criminology*. Fourth Edition. Oxford: Oxford University Press.
- Peck v. United Kingdom, No. 44647/98.
  Available at https://hudoc.echr.coe.int/eng?i=001-60898
- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Roxin, C. (2012) Kriminalpolitik und Strafrechtssystem. In: *Kriminalpolitik und Strafrechtssystem*.. Schriftenreihe der Juristischen Gesellschaft zu Berlin, 39, Berlin: de Gruyter.
- S. and Marper v. the United Kingdom ([VV], No. 30562/04 and 30566/04, ECHR 2008.
  Available at https://www.refworld.org/pdfid/4a7a91032.pdf
- Supreme Court of the Republic of Croatia, No: I Kž 680/2020-4, Zagreb, December 14, 2021.
- Treaty on the Functioning of the European Union, 2016/C 202/1.
- Usher, N. (2003) Video Surveillance Comes to Big Easy. *San Diego Union-Tribune,* 24, 14.
- Vukota-Bojić v. Switzerland, Application No. 61838/10.
  Available at https://hudoc.echr.coe.int/eng?i=001-167490
- Zagreb County Court, 7 Kž-706/2020-3, October 19, 2020.

Authors

Contributors' professional profiles

Please Note: This list only includes authors who spoke in person or were present at the Vilnius conference.

Alexa, Noemi

EU Law Enforcement Training Needs on Digital Skills and the Use of New Technologies

Being the Head of Exchange, Research and Analysis Sector at CEPOL Noemi Alexa`s main responsibility is supporting the design of law enforcement training by coordinating training needs assessment and analyses. Prior to joining CEPOL she worked as an assistant professor at the Central European University teaching at MBA and Executive MBA courses with research focusing on leadership and business integrity. Before her academic carrier she was the Executive Director of the Hungarian chapter of Transparency International. In this position, she coordinated and conducted several applied research activities linked to the anticorruption field. She holds a PhD in Multidisciplinary Social Sciences from Budapest Corvinus University.

Contact: noemi.alexa@cepol.europa.eu

Apolozan, Nicoleta

Children on the Internet – Law Enforcement Challenges

Police officer (sociologist), works with The Research and Crime Prevention Institute within the General Inspectorate of the Romanian Police.

Nicoleta Apolozan graduated from the National School of Political and Administrative Studies (2005). She also graduated with a Master's degree in Public Policy and European Integration (2007) from the same university, as well as a Master's degree in International Police Cooperation (2013) from the "Alexandru Ioan Cuza" Police Academy. She is currently a PhD student at the School of Advanced Studies of the Romanian Academy, in the field of Sociology.

She has participated in numerous studies on the aetiology of crime and its specific forms of manifestation, including "Risks and vulnerabilities of students in the online environment" (2021), a study conducted within the RO Cyberex Project – Improving, cooperating and preventing in the fight against cybercrime (2021). Her areas of interest for research include studies on the perception of public safety, police authority and public confidence in this institution.

Contact: nicoleta.apolozan@politiaromana.ro

Barros, Ana Isabel

AI Potential to Uncover Criminal Modus Operandi Features .

Ana Isabel Barros currently works as applied research professor at the Dutch Police Academy. In this role she coordinates and conducts research in the field of intelligence in close cooperation with police stakeholder and international partners and actively contributes to the Police Academy intelligence educational program. She is also Principal Scientist at TNO where she is responsible for encouraging innovation, knowledge sharing and ensuring technical quality of projects and research programs in the areas of intelligence analysis, complex systems and operational analyses. As external fellow at the Institute for Advanced Study (IAS) of the University of Amsterdam, she conducts research in complexity & resilience of organised crime systems. Her involvement in several international (cooperation) projects and activities, together with her large international network, academic experience and strong communication skills facilitate the establishment of links between practice and theory in an international environment.

Contact: ana.barros@politieacademie.nl

Bosisio, Antonio

Investigating High-Risk Firms

Antonio Bosisio is Senior Researcher at Transcrime and Data Analytics Manager at Crime&tech. His research focuses on organised crime, corruption, money laundering and financial crime. In this domain, he has participated in numerous research projects at national and international level, and he is currently coordinating the EU-funded project DATACROS II. He holds a Master's degree in Economics and Social Sciences at Università Commerciale Luigi Bocconi in 2016. In his previous experiences, he worked at the European Commission (DG COMP), and at the Competition and Markets Authority in the UK.

Contact: antonio.bosisio@unicatt.it

Butorac, Ksenija

Evidential Validity of Video Surveillance Footage in Criminal Investigation and Court Proceedings

Ksenija Butorac obtained her MSc degree in Criminal Investigation after a Law degree, as well as her PhD in Criminology at the University of Zagreb, Croatia. She has been working as a Full Professor of Criminology, Drug-Related Crime and Addictions at the Croatian Police University College of the Ministry of Interior, also teaching at the Military Studies and at the Faculty of Education and Rehabilitation Sciences, University of Zagreb. She was a visiting professor in Law Enforcement at the Police College in Lower Saxony, Germany and at the Faculty of Public Security, Mykolas Romeris University, Vilnius, Lithuania. Her areas of research include phenomenology and aetiology of the modern crime and perpetrator's profile. She has published over 70 peer-reviewed academic papers and book chapters. She is a member of the European Society of Criminology, and of the Forensic Social Sciences Association, USA.

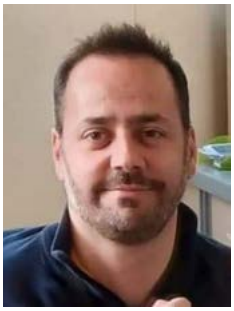
Relevant publications:

- Butorac, K., Gracin, D., Dešić, I. (2020). Enhanced Surveillance of Citizens During SARS-Cov-2 Coronavirus Pandemic (COVID-19). Journal of Forensic Sciences & Criminal Investigation. 14(3), 45-54. doi:10.19080/JFSCI.2020.14.555888
- Constantinou, A.G., Butorac, K. (2018). An attestation of the spatiality and saliency of police culture: A cross comparison study of Croatian and Cypriot law enforcers. Police Practice and Research: An International Journal, 20(1), 48-63, ISSN: 1477-271X (online) doi:10.1080/15614263.2018.1500281
- Butorac, K., Mikšaj-Todorović, Lj., Žebec, M.S. (2016). Missing Persons in Croatia: Incidence, Characteristics

and Police Performance Effectiveness. In: Morewitz, S. & Sturdy-Colls, C. (Eds.) Handbook of Missing Persons. New York: Springer Science+Business Media LLC, 207-231. doi:10.1007/978-3-319-40199-7-2

Contact: kbutorac@fkz.hr

Carré, Cédric



The Challenges of E-Learning in the French Police Nationale

Currently working as a Training and E-learning expert specialised in languages for the French Police Nationale Training and Recruitment Department (DCRFPN), my mission is to build, organise and implement national online curriculums. Formerly, he spent 8 years as an English teacher at Limoges University (France) and spent 10 years as a high school teacher before that, always trying to combine the teaching of languages with new technologies and encourage e-learning possibilities.

Coman, Iulian

EU Law Enforcement Training Needs on Digital Skills and the Use of New Technologies

Iulian Coman is currently analyst/training officer – seconded national expert at the European Union Agency for Law Enforcement Training from 'Alexandru Ioan Cuza' Police Academy Bucharest, with a broad experience in law enforcement training, international cooperation, public relations and analysis. Formerly a border police investigator dealing with cross-border criminality at the Romanian Coast Guard, international relations officer, trainer, spokesperson and PhD candidate in public order and national security with the 'Alexandru Ioan Cuza' Police Academy Bucharest.

Contact: iulian.coman@cepol.europa.eu

Constante Orrios, Agustín

Open Source Intelligence and Cultural Property Crimes

20 years of policing experience, with specific focus on investigation, intelligence and collaboration with civil society. Agustín has a longstanding experience in criminal investigation, with collaborations with other police forces and agencies. He has worked for different local police forces and held briefly a position at FRONTEX as AST-4. He has participated as a speaker at the European Institute for Crime Prevention and Control (HEUNI) on the police response to undocumented migrants in Spain and on a project on the detention of people with learning disabilities. He has delivered several trainings for police on OSINT, tactics and other subjects. Agustín is currently studying Criminology and is passionate about OSINT and intelligence..

de Groes, Nienke

The Potential of AI and Data Science in Reducing the Vulnerability of Ports to Undermining Crime

Nienke de Groes is affiliated with the Dutch Police Academy as a researcher/PhD student.

el Rahwan, Amr

Artificial Intelligence and Interoperability for Solving Challenges of OSINT and Cross-Border Investigations

Amr el Rahwan is experienced in supporting international organizations, border security, and police in solving

issues related to physical security and public safety by studying the security gaps in the information systems, building capacities, applying standards & regulations and converting them into technologies, providing feasibility studies & roadmaps, and providing exceptional global solutions for preventing, detecting, and investigating terrorism & serious crime.Amr is based in the Netherlands and studying MSc in Cybersecurity at the International Hellenic University. Affiliated Member of "Secure Identity Alliance" for Interoperability for Law Enforcement & Border Security, and was a former Police Officer Engineer in Egypt.

Contact: amr.rahwan@secureidentityalliance.org

Elias, Luís Manuel André

Policing in a Digital Age

Luís Manuel André Elias is Superintendent of Police and a Professor at the Higher Institute of Police Sciences and Internal Security in Lisbon, Portugal. Currently he is the Liaison Officer at the Portuguese Bureau at Europol. Before he served as the Director of Operations Department at the National Headquarters of Police (2018-2021), as Security Advisor to the Prime Minister (2015-2018), and in leading positions at the Metropolitan Police of Lisbon (2010-2015).

Relevant publications:

- Elias, Luís, Gestão de Crises e a Pandemia de COVID-19 in Segurança em Tempo de Crise, revista do IDN Nação e Defesa n.º 156, 2020
- Elias, Luís, Terrorismo Transnacional Contemporâneo: Segurança, Justiça e Cooperação in Terrorismo e Violência Política, revista do IDN Nação e Defesa n.º 152 de 2019
- Elias, Luís (2019). A Cooperação Policial Europeia: a Dimensão Externa e Interna da Segurança in JANUS 2018-2019. Conjuntura Internacional. A Dimensão Externa da Segurança Interna. Lisboa. OBSEVARE. Universidade Autónoma de Lisboa.
- Elias, Luís (2018). Crises management in international context: the role of the police in the European Union Crises management in international context: the role of the police in the European Union in Studies on international relations and security / edited by José Francisco Lynce Zagallo Pavia. Lisboa. Universidade Lusíada Editora

Contact: lmelias@psp.pt

Fuchs, Micha

The Influence of Digital Devices on Learning Interest, Engagement and Academic Performance in Basic Police Training

Since 2018, M.A. Micha Fuchs has been working in training and life-long training at the headquarters of the Bavarian Riot Police. His main areas of interest are the methodical development of basic police training as well as evaluation of training, especially in the fields of digitalisation, test performance and teacher training. In addition, Micha Fuchs is currently pursuing a PhD in educational science at the University of Bamberg.

Relevant publications:

- Fuchs, M. & Enkling, G. (2022). How to successfully use a learning management system in police training. Southeast Asian Regional Police Training Conference in Phuket, Thailand, 07.-12.03.2022.
- Fuchs, M. (2022). Challenges for police training after COVID-19. European Law Enforcement Research Bulletin, (SCE 5), 205-220. doi:10.7725/eulerb.v0iSCE%205.480.
- Fuchs, M., Becker, S., Muff, A. & Pfost, M. (2021). Empirische Befunde zur Akzeptanz von Multiple-Choice-Prüfungsformaten in der Ausbildung der Bayerischen Polizei. In: Polizei & Wissenschaft, Nr. 2, 2021, S. 44-69.

Contact: micha.fuchs@polizei.bayern.de

Giardiello, Gerardo

Developing a Judicial Cross-Check System for Case Searching and Correlation Using a Standard for the Evidence

Gerardo Giardiello holds a Master Degree in Computer Science from the University of Florence in 2004. From

2007 he worked as researcher or collaborator at a spin-off of the Italian CNR (National Research Council), at the Institute of Legal Information Theory and Techniques of the CNR and, currently, at the Institute of Legal Informatics and Judicial Systems of the CNR. He conducts research and software implementation in the fields of legislative drafting, ontologies and knowledge representation, legal document classification and metadata extraction for legal texts analysis and consolidation, analysis of the quality of legal texts and implementation of e-justice services and tools.In his current assignment, he is working on a piloting of the exchange of digital evidence across Member States by using the Evidence Exchange Standard Package Application, within the EXEC-II European project.

Contact: gerardo.giardiello@igsg.cnr.it.

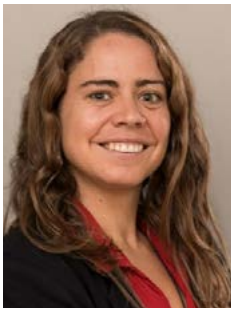
Haberfeld, Maria (Maki)

American Policing in the Digital Age

Dr. Maria (Maki) Haberfeld is a Professor of Police Science, at John Jay College of Criminal Justice in New York City and Chair of the department of Law, Police Science and Criminal Justice Administration. She holds a PhD in Criminal Justice from City University of New York. She served in the Israeli Defense Forces in a counter-terrorist unit and left the army at the rank of a Sergeant. Later she served in the Israel National Police and left the force at the rank of Lieutenant. She is one of the co-creators of Police Leadership Program for the NYPD sworn officers and the Academic Director of this program since its creation in 2001. In addition, she has created the Law Enforcement Leadership Institute for Police Chiefs in NY State and created an on-line Law Enforcement Leadership Certificate. She has trained police forces around the country and the world including, the Dominican Republic, Czech Republic, Poland, India, China, Cyprus, Turkey, Mongolia, Taiwan and conducted research in over 70 police departments in the US and in 35 countries. She has published 22 academic books on policing and over 50 book chapters and journal articles in peer reviewed publications. Her books were translated into three languages and are used by police departments around the country and around the world.

Contact: mhaberfeld@jjay.cuny.edu

Jofre, Maria



Investigating High-Risk Firms

Maria Jofre is a postdoctoral research fellow at Transcrime working on several EU-funded project in the field of security. Maria is an expert in criminal data analytics, risk assessment and machine learning. Her main expertise and interests lie in the development of analytical solutions for practitioners and other stakeholders aimed to improve the assessment of transnational crimes, including money laundering, terrorist financing, organized crime, illicit trafficking, human smuggling and cybercrime. Maria holds a PhD in Business Analytics (The University of Sydney), a Master in Operations Management (University of Chile) and a degree in Industrial Engineering (University of Chile).

Relevant publications:

- Jofre, M. (2022) Network analysis for financial crime risk assessment: the case study of the gambling division in Malta, Global Crime, 23:2, 148-170, doi:10.1080/17440572.2022.2077330
- Aziani, A., Bertoni, G.A., Jofre, M. et al. (2021) COVID-19 and Organized Crime: Strategies employed by criminal groups to increase their profits and power in the first months of the pandemic. Trends in Organized Crime (2021). https://doi.org/10.1007/s12117-021-09434-x
- Jofre, M., Aziani, A. & Villa, E. (2022) Terrorist Financing and the Use of Traditional and Emerging Financial Technologies. Available at SSRN: https://ssrn.com/abstract=4223469

Contact: maria.jofre@unicatt.it

Johansson, Ylva

Commissioner's Welcome Address

Ms Ylva Johansson was appointed European commissioner for home affairs in December 2019. From Sweden, she was minister for employment in the Swedish government from 2014 to 2019, minister for welfare and elderly healthcare from 2004 to 2006 and minister for schools from 1994 to 1998. Johansson was educated at Lund University and the Stockholm Institute of Education.

Kafteranis, Dimitrios

Art of Money Laundering with Non-Fungible Tokens: A myth or reality?

Dimitrios is an Assistant Professor of Law at the CFCI, Coventry University. He has studied English Language and Literature and then Law. He holds a Master of Arts in Innternational Studies and an LLM in European Economic and Financial Criminal Law. He completed his PhD at the University of Luxembourg on the legal protection of whistle-blowers in the EU banking and financial sector. He worked at the Court of Justice of the European Union prior to joining the CFCI.

Contact: dimitrios.kafteranis@coventry.ac.uk

Kovács Szitkay, Eszter

Race, Ethnicity, Biotechnology and the Law .

Eszter Kovács Szitkay is a PhD student at Ludovika University of Public Service, Doctoral School of Law Enforcement (Hungary, Budapest) and a junior research fellow at (formerly Hungarian Academy of Sciences) Centre for Social Sciences, Institute for Legal Studies (Hungary, Budapest). Her research interest includes access to justice, law enforcement, and the conceptualization of race and ethnicity.

Relevant publications:

- Kovács Szitkay, E., & Pap, A. (2022) Populist Pressures, Policing and the Pandemic. European Law Enforcement Research Bulletin, (SCE Nr. 5), 279-288.
- Kovács Szitkay, E. (2021). Egy lépéssel közelebb az igazságszolgáltatáshoz való teljesebb hozzáféréshez [One step closer to a fuller access to justice]. In: Harmati, B.; Kovács Szitkay, E.; Pap, A. L.; Papp, B. (eds.): Honestas, Humanitas, Humilitas. Budapest, Magyarország : L'Harmattan Kiadó, pp. 115-125.

Contact: kovacs.szitkay.eszter@tk.hu

Kuznecova, Tatjana

Cold Case – Solved & Unsolved: Use of digital tools and data science techniques to facilitate cold case investigation

Tatjana Kuznecova holds a double Master's degree in Environmental Sciences and Environmental Technology acquired in Riga Technical University (Latvia) and Vilnius Gediminas Technical University (Lithuania). Her past professional experiences include research and educational work in Riga Technical University (Latvia) and University of Twente (Netherlands), and participation in various local and international projects.

She is a senior researcher and project leader at Saxion University of Applied Sciences. She specializes in applications of data science, data mining and geo-spatial data processing. As a coordinator and project leader, she has been leading projects 'Cold Case: Solved and Unsolved' (TechForFuture subsidy) and 'NarcoView' (EU ISF-P subsidy).

Contact: t.kuznecova@saxion.nl

Leese, Matthias

Digital Data and Algorithms in Law Enforcement

Matthias Leese is a professor at the Center for Security Studies at the ETH Zurich, Switzerland. As a social scientist he is interested in the use of new and emerging technologies in law enforcement and border control. He conducted a multi-year project on predictive policing in Germany and Switzerland and has begun a new five-year research program, funded by the European Research Council, on data quality in European police and border control cooperation.

Relevant publications:

- Egbert, S. & Leese, M. (2021) Criminal Futures: Predictive Policing and Everyday Police Work. London/New York: Routledge.
- Leese, M. (2020) Predictive Policing: Proceed, but with Care. CSS Policy Perspectives, Vol.8 /14. December.
- Kaufmann, M., Egbert, S. & Leese, M. (2019) Predictive Policing and the Politics of Patterns. British Journal of Criminology 59(3): 674-692.

Contact: mleese@ethz.ch.

Linden, Ruth

AP4AI – Accountability principles for artificial intelligence in the internal security domain t

Ruth works as a policy advisor for the Europol Innovation Lab. Under the umbrella of the EU Innovation Hub for Internal Security, she contributes to the "Accountability Principles for AI" (AP4AI) project, run in partnership with five EU JHA Agencies and their academic partner CENTRIC, aiming at developing accountability principles for the use of AI in the field of internal security.

Contact: ruth.linden@europol.europa.eu

López Carral, Héctor

An Assistive System for Transferring Domain Knowledge to Novice Officers

Predoctoral Researcher at the Synthetic Perceptive Emotive and Cognitive Systems (SPECS) group, Barcelona, Spain.

Contact: hlopez@ibecbarcelona.eu.

Lygeros, Georgios

The Identification of Invalid Information about the COVID-19 Coronavirus Pandemic on a Social Networking Platform

Georgios Lygeros was born in Patras in Western Greece. Working as a police officer he is currently in charge of the Regional Department investigating trafficking in human beings-sexual exploitation. At the same time, through his role as Regional Coordinator for internet-based crime, he works in close collaboration with the Central Division of Cyber Crime, focusing on related cases through internet. He is also a certified member of the Crises Negotiation Team of the Hellenic Police, responsible for the region of Western Greece. He holds a master's degree in communication and information systems from the University of the Aegean and a master's degree in crisis management from the Kapodistrian University of Athens.

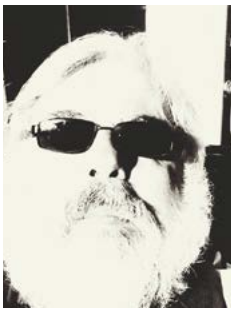
Marín López, Montserrat

Executive Director's Welcome Address?

María Montserrat Marín López is the Executive Director of CEPOL, the European Agency of Law Enforcement Training. She has held various leading operational and strategic roles for 26 years in a wide range of policing areas such as forensics, public safety, money laundering, drug trafficking, and irregular migration. She had been serving as Commissioner of Police since 2017. Ms. Marín López, who has broad experience in police training and education, studied Psychology and graduated with honours from the CEPOL European Joint Master Programme in 2019.

Contact: montserrat.marin-lopez@cepol.europa.eu

Nogala, Detlef



Preparing Law Enforcement for the Digital Age – Editor's reflection

Research and Knowledge Management Officer, European Union Agency for Law Enforcement Training (CEPOL).

Dr Detlef Nogala has worked at CEPOL for almost 20 years, first as a scientific advisor, then as RKMO until the end of October 2022, and has been Editor-in-Chief of the Bulletin since its launch. He holds diplomas in psychology and criminology from the University of Hamburg and earned his PhD in political science from the Free University of Berlin. Research, project and teaching activities at the University of Hamburg, the Hamburg Police Academy and the Max Planck Institute for Foreign and International Criminal Law at Freiburg i.Br., Germany. He now occasionally works as a freelance consultant and author.

Relevant publications:

- Nogala, D. (2021) 'Von der Policey zur PolizAI - Vorüberlegungen zur weiteren Aufklärung eines zukunftsfesten Polizeibegriffs', in R. Haverkamp et al. (eds) Unterwegs in Kriminologie und Strafrecht - Exploring the World of Crime and Criminology. Festschrift für Hans-Jörg Albrecht zum 70. Geburtstag. Berlin: Duncker & Humblot, pp. 391–412.
- Nogala, D. and Schröder, D. (2019) 'Innovations in Law Enforcement – Introduction to the Special Conference Edition', in D. Nogala et al. (eds) Innovations in Law Enforcement – Implications for practice, education and civil society. Luxembourg: EU Publication Office (European Law Enforcement Research Bulletin, Nr. 4), pp. 7–17.
- Konze, A. and Nogala, D. (2018) 'Higher Police Education in Europe: Surveying Recent Developments', in C. Rogers and B. Frevel (eds) Higher Education and Police - An International View. Palgrave Macmillan, pp. 155–177.

Contact: dr.detlef.nogala_exCEPOL@gmx.net

Ott, Kristina

The Influence of Digital Devices on Learning Interest, Engagement and Academic Performance in Basic Police Training

Senior staff for the implementation of the digitalisation strategy in the Department training and further education, Headquarters of the Bavarian Riot Police..

Contact: kristina.ott@polizei.bayern.de

Pap, Andras L.

Race, Ethnicity, Biotechnology and the Law

Research Professor and Head of Department for Constitutional and Administrative Law at the Eötvös Loránd Research Network (formerly Hungarian Academy of Sciences) Centre for Social Sciences Institute for Legal Studies.

Professor of Law at the Institute of Business Economics at Eötvös University (ELTE) and at the Law Enforcement Faculty of Ludovika University

Research Affiliate at CEU Democracy Institute, Rule of Law Research Group in Budapest, Hungary. Adjunct (Recurrent Visiting) Professor in the Nationalism Studies Program at the Central European University in Vienna.

His research interest includes comparative constitutional law, human rights, law enforcement, in particular hate crimes, discrimination and the conceptualization of race and ethnicity. He worked as rapporteur, consultant, senior expert, project manager and lead researcher in various project commissioned by the European Union (the Commission as well the Parliament and the Agency for Fundamental Rights), the Council of Europe and the UN. He is a recurrent evaluator for research grants for the EU and agencies in the Czech Republic Netherlands, Russia, Slovakia and Switzerland and serves as expert witness for courts in the UK and the US. He habitually works with international NGO's and think tanks like Freedom House, Transparency International, the Open Society Institute, Scholars at Risk, the Centre for European Policy Studies, International Centre for Democratic Transition, and for many years had been trainer at the International Law Enforcement Academy. He is a member of the Hungarian Helsinki Committee. He is the author of multiple publications in English and frequent conference presenter.

Relevant publications:

- Academic freedom: A test and a tool for illiberalism, neoliberalism and liberal democracy, The Brown Journal of World Affairs, Spring/Summer 2021 • Volume XXVI, Issue II.
- Piecemeal Devourment: Academic Freedom in Hungary, UIC John Marshall Law Review, January 5th, 2021, https://lawreview.jmls.uic.edu/piecemeal-devourment-academic-freedom-in-hungary/.
- Neglect, marginalization and abuse: hate crime legislation and practice in the labyrinth of identity politics, minority protection and penal populism, Nationalities Papers, The Journal of Nationalism and Ethnicity, Volume 49 Issue 3. (2020)

Papadoudis, Nikolaos

Mobile Forensics and Digital Solutions

Police Lieutenant, Digital Evidence Examiner at the Hellenic Police Forensic Science Division / Digital Evidence Department. Postgraduate Student, Department of Computer Science and Engineering – MSc in Artificial Intelligence, European University Cyprus.

Contact: n.papadoudis@astynomia.gr

Raffaele, Luigi

Technology Foresight on Biometrics for the Future of Travel

Luigi Raffaele is a Research Senior Assistant in the Frontex Research and Innovation Unit, where he supports the development and implementation of research studies and R&I projects in the field of border security. He joined the Research and Innovation Unit in 2019 as seconded national expert from the Ministry of Interior – Central Anticrime Directorate of the Italian National Police – Italy. Luigi previously served in the microelectronics and optoelectronics industries for 15 years. He holds a MSc degree and a PhD in Electronics, and a Master's Degree in Engineering Management for Public Security.

Contact: luigi.raffaele@frontex.europa.eu

Rufián Fernández, Francisco José

Open Source Intelligence and Cultural Property Crimes

Archaeologist and Police Officer in the Municipal Police of Madrid. Currently, finishing a PhD in Law, at the Autonoma University of Madrid and researching heritage protection by local policies.

Relevant publications:

- Sanz Domínguez, E., Rufián Fernández, F.J., Sabrine, I. (2023). New Security Challenges at Museums and Historic Sites: The Case of Spain. In: Oosterman, N., Yates, D. (eds) Art Crime in Context. Studies in Art, Heritage, Law and the Market, vol 6. Springer, Cham. https://doi.org/10.1007/978-3-031-14084-6_7
- Isber Sabrine, Francisco José Rufián Fernández (2021) Tráfico ilícito de antigüedades: una visión internacional del problema En: Tutela de los bienes culturales: una visión cosmopolita desde el derecho penal, el derecho internacional y la criminología / coord. por Juan Periago Morant; Cristina Guisasola Lerma (dir.), pp. 597-612.
- Rufián Fernández, F J; M Fernández Díaz; Sabrine, I; Ibáñez, J J; Claramunt-López, B; et al. (2020) The documentation and protection of cultural heritage during emergencies. The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences; Göttingen Tomo XLIV-M-1-2020, Göttingen: Copernicus GmbH, pp. 287-293. doi:10.5194/isprs-archives-XLIV-M-1-2020-287-2020.

Schreurs, Wendy

AI Potential to Uncover Criminal Modus Operandi Features

Wendy Schreurs works as a scientific researcher at the Dutch Police Academy. She is also the program director of the Master of Science in Policing, which is a collaborative programme between Canterbury Christ Church University and the Dutch Police Academy. She has a background in social psychology and public administration and received her PhD in 2019 on Citizen Participation in the police domain. Currently she is mainly working on research on the topic of intelligence.

Relevant publications:

- Schreurs, W., Franjkić, N., Kerstholt, J. H., De Vries, P. W., & Giebels, E. (2020) Why do citizens become a member of an online neighbourhood watch? A case study in The Netherlands. Police Practice and Research, 21(6), 687-701.
- Schreurs, W., Kerstholt, J. H., de Vries, P. W., & Giebels, E. (2018) Citizen participation in the police domain: The role of citizens' attitude and morality. Journal of community psychology, 46(6), 775-789.
- Zebel, S., Schreurs, W., & Ufkes, E. G. (2017) Crime seriousness and participation in restorative justice: The role of time elapsed since the offense. Law and human behavior, 41(4), 385.

Contact: Wendy.Schreurs@politieacademie.nl

Sousa-Silva, Rui

Forensic Linguistics: The potential of language for Law Enforcement in the Digital Age

Rui Sousa-Silva is assistant professor of the Faculty of Arts and researcher at the Linguistics Centre (CLUP) of the University of Porto, where he conducts his research into Forensic Linguistics, especially in the areas of authorship analysis, plagiarism detection and analysis and cybercrime. He has a first degree in Translation and a Masters in Terminology and Translation, both awared by the Faculty of Arts of the University of Porto, and a PhD in Applied Linguistics from Aston University (Birmingham, UK), where he submitted his thesis on Forensic Linguistics. He has also authored and co-authored several articles on (computational) authorship analysis, plagiarism detection and analysis of cibercriminal communications. He is co-editor of the international bilingual journal Language and Law / Linguagem e Direito (with Malcolm Coulthard) and of the 2nd edition of 'The Routledge Handbook of Forensic Linguistics', published by Routledge (with Malcolm Coulthard and Alison May). He is chair of the 'Compu-

tational Linguistics' working group of the COST Action LITHME – Language in the Human-Machine Era.

Relevant publications:

- Sousa-Silva, R. (2022) Fighting the Fake: A Forensic Linguistic Analysis to Fake News Detection. International Journal for the Semiotics of Law – Revue Internationale de Sémiotique Juridique. https://doi.org/10.1007/s11196-022-09901-w
- Coulthard, M., May, A., & Sousa-Silva, R. (Eds.). (2021) The Routledge Handbook of Forensic Linguistics (2nd ed.). London and New York: Routledge.
- Sousa-Silva, R., Laboreiro, G., Sarmento, L., Grant, T., Oliveira, E., & Maia, B. (2011) 'twazn me!!! ;(' Automatic Authorship Analysis of Micro-Blogging Messages. In R. Muñoz, A. Montoyo, & E. Métais (Eds.), Lecture Notes in Computer Science 6716 Springer 2011: Vol. Natural La (pp. 161–168). Berlin and Heidelberg: Springer – Verlag.

Contact: rssilva@letras.up.pt.

Turchi, Fabrizio

Developing a Judicial Cross-Check System for Case Searching and Correlation Using a Standard for the Evidence

Fabrizio Turchi is the Technological Director at Institute of Legal Informatics and Judicial Systems of the National Research Council of Italy (CNR-IGSG). His research activities are the applications of IT to legal domain, legal standard and legal drafting, and use of the XML technologies to devise legal documents models. He has been designing and developing Web applications, formal parsers to identify parts and structures that exist inside textual documents and natural language processing techniques applied to legal documents for knowledge extraction, such as automated text classification and anonymity processes based on Named Entity Recognition (NER). He has been involved in several European projects:

- Evidence (European Informatics Data Exchange Framework for Courts and Evidence – March 2014/August 2016), as leader of the WP4 (Standard Issues);
- Evidence2e-Codex (Linking Evidence into e-CODEX for EIO and MLA procedures in Europe – February 2018 /January 2020), as leader of the WP3 (Matching Evidence into e-CODEX)
- EXEC-II (Electronic eXchange of e-Evidences with e-CODEX – October 2020/September 2022), as leader of the WP6 (Piloting of the exchange of digital evidence across Member States by using the Evidence Exchange Standard Package Application)
- INSPECTr (Intelligence Network & Secure Platform for Evidence Correlation and Transfer (INSPECTr, as leader of the WP2 (Provide a Reference Framework for the Standardisation of Evidence Representation & Exchange (SERE) to be implemented in the INSPECTr platform)

Contact: fabrizio.turchi@igsg.cnr.it

Turksen, Umut

Art of Money Laundering with Non-Fungible Tokens: A myth or reality?

Umut Turksen is a Professor in law at the Centre in Financial and Corporate Integrity, Coventry University, United Kingdom. He leads the EU-funded TRACE Project (https://trace-illicit-money-flows.eu) and the Law, Risk and Compliance Cluster at the Research Centre for Financial and Corporate Integrity, Coventry University. He is interested in the practical application of the law in innovation, societal security and development. He has published several books and articles on energy, financial crime and international trade and economic law. He has provided consultancy and training to prestigious international businesses and government projects, including technical assistance programmes for multinational corporations (e.g., France Telecom, Equas Ltd, Wilmington Plc) and international organisations (e.g., Commonwealth, NATO, EUROPOL); and professional development training for practitioners and EU-funded projects (e.g., SecuCities, MUTRAP III, COFFERS, PROTAX, VIRTEU). Umut is also a member of the UK Innovation Caucus.

Contact: umut.turksen@coventry.ac.uk

Whelan, Michael

Law Enforcement Agency Capacity Building as a Driver for the Adoption of European Resear

Michael is an experienced cyber analyst at UCD Centre for Cybersecurity and Cybercrime Investigation. He engages with a wide range of sectors including financial services, national government and international law enforcement communities, contributing to the fields cybersecurity and cybercrime investigations. In particular, he works closely with law enforcement officers from across Europe, coordinating and implementing the stages of the software development lifecycle, developing open-source tools for cybercrime investigations. He is passionate about innovation and education, with a demonstrated history of working in the higher education sector. He has prepared and delivered many modules for Programming for Investigators, Digital Forensics and Online Investigator training courses.Michael holds a BSc and Research MSc from University College Dublin.

Contact: michael.whelan@ucd.ie

Conference Programme

Day 1: Wednesday 8th June 2022

Speakers[1]	Contribution	Room
Inga Žalėnienė	Welcome Address by Rector of Mykolas Romeris University	Auditorium (Plenary)
Ylva Johansson	Welcome Address by EU Commissioner Home Affairs (per video)	Auditorium (Plenary)
Montserrat Marín López	Welcome Address by CEPOL Executive Director	Auditorium (Plenary)
Juan Fernando López Aguilar	Welcome Address by Chair of the LIBE Committee of the European Parliament (per video)	Auditorium (Plenary)
Arunas Paulauskas	Welcome Address – Deputy Police Commissioner Lithuanian Police	Auditorium (Plenary)
	Coffee Break I	Lobby
Andy Higgins	Redesigning Policing and Public Safety for the Digital Age: an example for Europe?	Auditorium (Plenary)
Ruud Staijen	The Importance of Forensic Speed in Crime Fighting – making things digital	Auditorium (Plenary)
	Lunch Break I	Lobby
Iulian Coman, Noemi Alexa	EU law enforcement training needs on digital skills and the use of new technologies	Panel Room III
Ana Isabel Barros, Wendy Schreurs	AI Potential to Uncover Criminal Modus Operandi	Panel Room I
Cédric Carré	Challenges of E-learning in the French Police Nationale	Panel Room II
Niklas Hamann	UNCOVER – Towards an efficient framework for uncovering hidden data in digital media	Panel Room III
Micha Fuchs, Kristina Ott	The influence of digital devices on learning interest, engagement and academic performance in basic police training – Experiences and findings	Panel Room II

1 Names in bold are contributors of this volume.

Speakers[1]	Contribution	Room
Maj Lenaršič	AI model building for data analysis in LEAs: A practical example	Panel Room I
Markianos Kokkinos	Challenges and Perspectives on the Digitalization of Education at the Cyprus Police Academy	Panel Room II
Maria Eleni Vardaki	Predicting crime in Athens, Greece: A Machine Learning Approach	Panel Room I
Theodora Tsikrika	CONNEXIONs H2020 project: crime scene investigation and training through 3D reconstruction and VR	Panel Room III
	Coffee Break II	Lobby
Tor Damkaas	E-learning Community Policing for International Police Advisors	Panel Room II
Umut Turksen, Thomas Havranek	The Human Factors and AI in Countering Financial Crime and Tracing Illicit Money Flows	Panel Room I
Andras L. Pap, Eszter Kovács Szitkay	Race, Ethnicity, Biotechnology and the Law: Potentiality and Challenges for Law Enforcement in the Digital Age	Panel Room III
Héctor López Carral	An Assistive System for Transferring Domain Knowledge to Novice Officers	Panel Room II
Nienke de Groes	The Potential of Artificial Intelligence and Data Science in Securing Ports against Undermining Crimes	Panel Room I
Vesa Huotari	The police – a tool, machine or technical ensemble?	Panel Room III
Anita Hazenberg	Innovation and Digitalization in Global Policing: a roadmap for action	Auditorium (Plenary)
Maria Haberfeld	American Policing in the Digital Age	Auditorium (Plenary)
	"Learning and Education in the Digital Age – What to look out for?" (Panel)	Auditorium (Plenary)

Day 2: Thursday 9th June 2022

Speakers[2]	Contribution	Room
Jesús Gómez	Increasing Efficiency in the Fight against Hate Crimes in Spain using Artificial Intelligence	Panel Room I
Francisco Rufián Fernández, Agustín Constante Orrios	OSINT and Cultural Property Crimes.	Lecture Room 1
George Kokkinis	Implementing the THOR Methodology in Security projects: Lessons learnt on the interplay of technological, human-related, organisational, and regulatory challenges	Panel Room II
Georgios Lygeros	Identification of invalid information about the Covid-19 coronavirus pandemic on a social networking platform	Lecture Room 2
Jorn van Rij	Cyber ethnographic policing as a step forward to success: A Human Trafficking example	Panel Room III

2 Names in bold are contributors of this volume.

Patrick Perrot	Generative Adversarial Network for LEA: Dr Jekyll or Mr Hyde ?	Panel Room I
Rui Sousa-Silva	Forensic Linguistics: The potential of language for Law Enforcement in the Digital Age	Panel Room II
Sigute Stankeviciute, Evaldas Bruze	Innovative NAAS ecosystem to fight desinformation and related online threats	Lecture Room 2
Ashwinee Kumar	e-Evidence: Collection, Analysis, and Sharing: An evidence-based policy perspective by the EU funded research projects LOCARD, ROXANNE & FORMOBILE	Panel Room III
Krunoslav Antoliš	Cross-border Access to Digital Evidence at Internet and Cloud	Lecture Room 1
Nestor Garcia-Barcelo, Marta Rivero	"SER – DesVi: developing a predictive system for the risk assessment of missing persons' harm and fatal-violent outcomes".	Lecture Room 1
Juan Arraiza	EACTDA presentation – a new exploitation path for security research results	Panel Room II
David Wright	Clustering and other measures to improve information sharing and cooperation between LEAs and the private sector	Panel Room III
Amr el Rahwan	Artificial Intelligence and Interoperability for Solving Challenges of OSINT and Cross-Border Investigations	Panel Room I
	Coffee Break III	Lobby
Luís Elias	Policing in a Digital Age: a balance between community-based strategies and technological intelligence	Auditorium (Plenary)
Sirpa Virta	Digital Meets Political: Strategic Preparedness of the Police for AI and Hybrid Threats	Auditorium (Plenary)
	Lunch Break II	Lobby
Roger von Laufenberg	Intelligence Led Policing and the Risks of Artificial Intelligence	Panel Room III
Luigi Raffaele	Technology Foresight on Biometrics for the Future of Travel	Lecture Room 1
Fabrizio Turchi, Gerardo Giardiello	Developing of a Judicial Cases Cross-Check System for Case Searching and Correlation Using a Standard for the Evidence	Panel Room II
Nikolaos Papadoudis	Mobile Forensics, Big Data and Artificial Intelligence: Current Status, Challenges and Future Directions	Panel Room I
Maria Jofre, Antonio Bosisio	Investigating High-Risk Firms through the Application of a Machine Learning-based Approach to Cross-Border Ownership Data	Panel Room I
Michael Whelan	LEA Capacity Building as a Driver for the Adoption of European Research	Panel Room III
Tiina Koivuniemi	Developing Law Enforcement Agencies Online – Challenges and Opportunities in International Development Cooperation	Panel Room II
Costas Kalogiros	The ROXANNE platform for supporting Law Enforcement practitioners in criminal investigations by analysing multi-modal data	Lecture Room 1

Zaneta Navickienė, Mindaugas Bilius	Whether Traditional Didactic Tools Are Appropriate for Methodics of Modern Crime Investigation?	Panel Room II
Umut Turksen, Dimitrios Kafteranis	Non-Fungible Tokens (NFTs) in the art market: A new medium for money laundering?	Panel Room I
Rashel Talukder	CYCLOPES – Cybercrime Law Enforcement Practitioners Workshop	Lecture Room 1
	Coffee Break IV	Lobby
Ruth Linden	Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain – Europol Innovation Lab	Auditorium (Plenary)
Matthias Leese	Digitization: Proceed with care	Auditorium (Plenary)
	"Artificial Intelligence in and for Law Enforcement: Panacea or Hype?" (Panel)	Auditorium (Plenary)

Day 3: Friday 10th June 2022

Speakers	Contribution	Room
Ksenija Butorac	Evidential validity of video surveillance footage in criminal investigation and court proceedings	Panel Room III
	Project Technical Demonstrations	Lecture Room 1
Tatjana Kuznecova	Use of digital tools and data science techniques to facilitate cold case investigation	Panel Room II
Jose L. Diego	RESPOND-A Project: How Digital Tools Can Help LEAs Managing Emergencies	Panel Room I
Ruben Fernández Bleda	Overview of CC-DRIVER and RAYUELA projects: investigate, identify, understand and explain drivers of juvenile cyberdelinquency	Panel Room I
Nicoleta Apolozan	Children on the Internet – Law Enforcement Challenges	Panel Room III
Marion Johanna Neunkirchner	Digitalization in penal system changes workflows and daily decision makings in prisons	Panel Room II
José L. Diego	DARLENE project: Enhancing LEA decision-making by employing AR and ML capabilities	Panel Room I
Paul Caruana	Burning bridges – understanding participant typologies and behaviours of Live Distant Child Abuse (LDCA) as a contributor towards response calibration.	Panel Room III
Michael Whelan	INSPECTr: Intelligence Network and Secure Platform for Evidence Correlation and Transfer	Panel Room II
	Coffee Break V	Lobby
Joanna Goodey	Embedding Respect for Fundamental Rights in Artificial Intelligence for Policing and Law Enforcement	Auditorium (Plenary)
Olivier Onidi	Looking Ahead: Preparing Law Enforcement for the Digital Age (per video)	Auditorium (Plenary)
Montserrat Marín López	Conclusion of Conference	Auditorium (Plenary)
	Farewell Lunch – Departure of Participants	Lobby

QR-AG-22-001-EN-C

EUROPEAN LAW ENFORCEMENT RESEARCH BULLETIN

Special Conference Edition Nr. 6

Preparing Law Enforcement for the Digital Age

Conference in cooperation with Mykolas Romeris University, 8-10 June 2022, Vilnius, Lithuania

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