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 an-

thropoid 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].

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).

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".
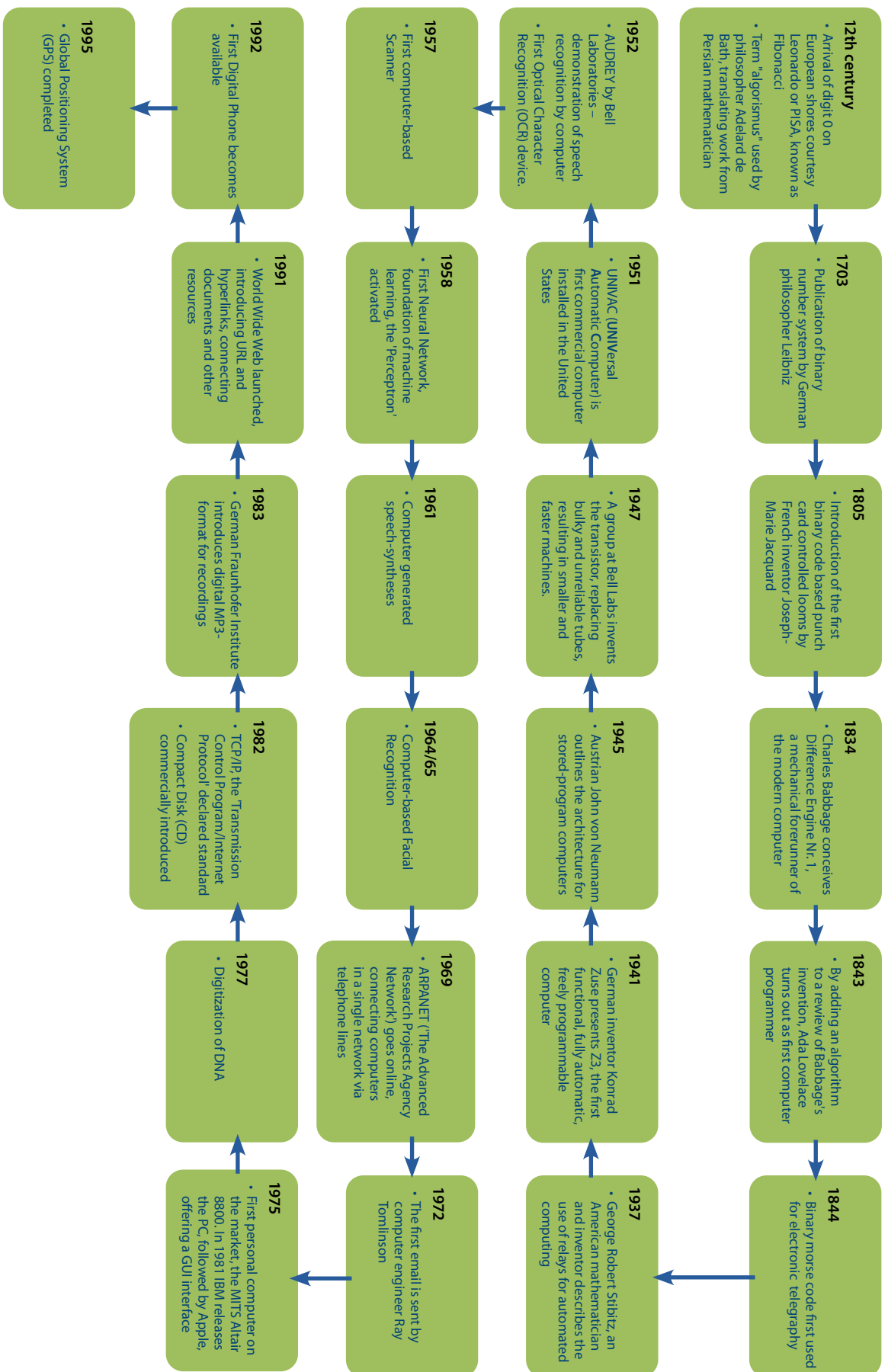
Digitisation – Computerisation – Digitalisation

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.

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

12th century
- Arrival of digit 0 on European shores courtesy Leonardo or PISA, known as Fibonacci
- Term "algorismus" used by philosopher Adelard de Bath, translating work from Persian mathematician

1703
- Publication of binary number system by German philosopher Leibniz

1805
- Introduction of the first binary code based punch card controlled looms by French inventor Joseph-Marie Jacquard

1834
- Charles Babbage conceives Difference Engine Nr. 1, a mechanical forerunner of the modern computer

1843
- By adding an algorithm to a rewiew of Babbage's invention, Ada Lovelace turns out as first computer programmer

1844
- Binary morse code first used for electronic telegraphy

1952
- AUDREY by Bell Laboratories – first demonstration of speech recognition by computer
- First Optical Character Recognition (OCR) device.

1951
- UNIVAC (**UNIV**ersal **A**utomatic **C**omputer) is first commercial computer installed in the United States

1947
- A group at Bell Labs invents the transistor, replacing bulky and unreliable tubes, resulting in smaller and faster machines.

1945
- Austrian John von Neumann outlines the architecture for stored-program computers

1941
- German inventor Konrad Zuse presents Z3, the first functional, fully automatic, freely programmable computer

1937
- George Robert Stibitz, an American mathematician and inventor describes the use of relays for automated computing

1957
- First computer-based Scanner

1958
- First Neural Network, foundation of machine learning, the 'Perceptron' activated

1961
- Computer generated speech-syntheses

1964/65
- Computer-based Facial Recognition

1969
- ARPANET ("The Advanced Research Projects Agency Network") goes online, connecting computers in a single network via telephone lines

1972
- The first email is sent by computer engineer Ray Tomlinson

1992
- First Digital Phone becomes available

1991
- World Wide Web launched, introducing URL and hyperlinks, connecting documents and other resources

1983
- German Fraunhofer Institute introduces digital MP3-format for recordings

1982
- TCP/IP, the Transmission Control Program/Internet Protocol) declared standard
- Compact Disk (CD) commercially introduced

1977
- Digitization of DNA

1975
- First personal computer on the market, the MITS Altair 8800. In 1981 IBM releases the PC, followed by Apple, offering a GUI interface

1995
- Global Positioning System (GPS) completed

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 au-

thorities 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

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.

CEPOL

- 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.