DO CRIMINALS DREAM OF ELECTRIC SHEEP?

How technology shapes the future of crime and law enforcement

EUROPOL

DO CRIMINALS DREAM OF ELECTRIC SHEEP?
HOW TECHNOLOGY SHAPES THE FUTURE OF CRIME AND LAW ENFORCEMENT

The title of this report is a reference to the 1968 science fiction novel "Do Androids Dream of Electric Sheep?" by American author Philip K. Dick, which reflects on questions of the impact of new technologies on humanity and the unintended consequences and complexities that introducing these technologies can entail for the individual and society at large. Europol seeks to explore the potential consequences of emerging and upcoming technologies to work with our partners towards a future less bleak than the one painted by Philip K. Dick.

www.europol.europa.eu

Contents

Foreword

Europol's strategy 2020+ sets out our ambition to establish Europol as an innovator in the European law enforcement community. Encouraging this innovation and remaining at the forefront of this complex crime landscape requires a deep understanding of the environment in which we operate.

Europol is therefore developing its foresight analysis capabilities. As a proactive EU agency, Europol identifies the challenges and opportunities new technologies present and anticipates changes in serious and organised crime. As we have seen time and again, it is no longer good enough to be reactive when contending with such rapid evolutions in technology and criminality. Our agency's ability to predict which emerging technologies criminals will turn to next is instrumental to our mission of keeping EU citizens safe.

I am therefore proud to present this forward-looking report on emerging and developing technologies. In this report, we identify the profound impact of technological change and disruptive technologies have on the dynamic security environment in the EU. To remain relevant and effective, law enforcement authorities must invest in and seek out new, innovative solutions. They must also embrace organisational change and challenge established business models to access the potential locked within these new technologies.

I look forward to Europol's continued cooperation with law enforcement agencies in the EU on this complex and ever-changing issue.

"It is no longer good enough to be reactive… our agency's ability to predict which emerging technologies criminals will turn to next is instrumental to our mission of keeping EU citizens safe."

Catherine De Bolle
Executive Director of Europol

Technology fundamentally shapes security challenges and responses in the EU.

KEY JUDGMENTS

Technology fundamentally shapes security challenges and responses in the EU. Law enforcement must engage in foresight activities to understand emerging challenges, formulate innovative countermeasures and, where necessary, challenge established business models and embrace organisational change to keep pace with technological developments.

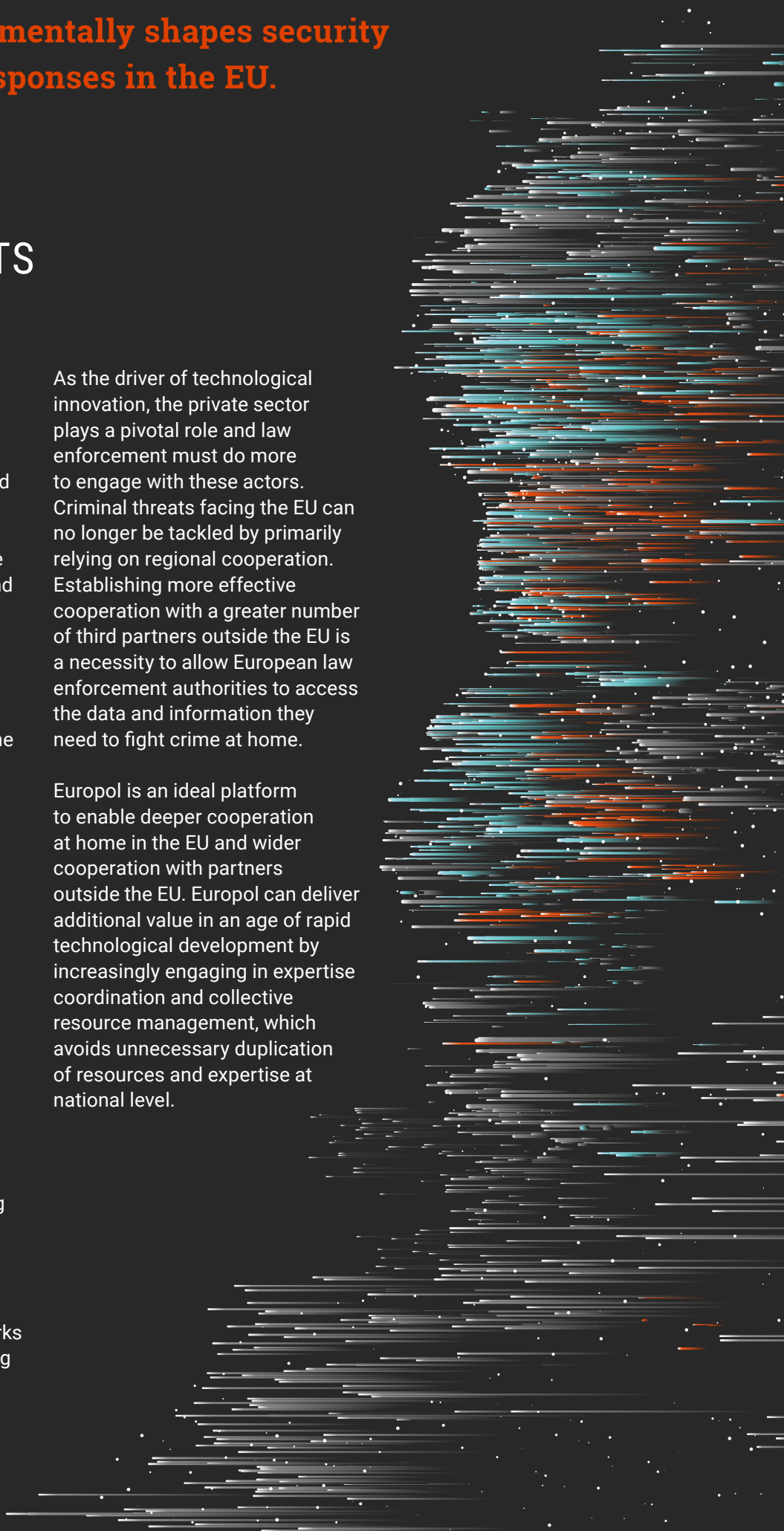
Disruption trough technological progress occurs as a result of the convergence of new emerging technologies, and the ways they challenge existing legal and regulatory frameworks with previously unseen applications.

Disruption through new technologies presents both challenges and opportunities for law enforcement authorities through the emergence of new or significantly altered criminal activities as well as through the potential exploitation of these technologies by law enforcement authorities.

Some of the disruptive emerging technologies with an impact on law enforcement and crime include Artificial Intelligence (AI), quantum computing, 5G, alternative decentralised networks and cryptocurrencies, 3D printing and biotech.

As the driver of technological innovation, the private sector plays a pivotal role and law enforcement must do more to engage with these actors. Criminal threats facing the EU can no longer be tackled by primarily relying on regional cooperation. Establishing more effective cooperation with a greater number of third partners outside the EU is a necessity to allow European law enforcement authorities to access the data and information they need to fight crime at home.

Europol is an ideal platform to enable deeper cooperation at home in the EU and wider cooperation with partners outside the EU. Europol can deliver additional value in an age of rapid technological development by increasingly engaging in expertise coordination and collective resource management, which avoids unnecessary duplication of resources and expertise at national level.



1.0 NAVIGATING THE DIGITAL ERA

Technology has been a key driver in the evolution of crime and terrorism over recent years. Technological developments and the way they transform the criminal landscape present new, emerging challenges for law enforcement authorities. Developments in Artificial Intelligence, quantum computing and 5G, among others, are set to have a profound impact on the criminal landscape and the ability of law enforcement authorities to respond to emerging threats. Making incremental changes to existing solutions has proven insufficient in the fight against serious security challenges. To remain relevant and effective, it is necessary to invest in understanding and actively pursuing new, innovative solutions.

Europol has already shown its capacity to be innovative with the launch of the European Cybercrime Centre (EC3), and the EU Internet Referral Unit (EU IRU) within the European Counter Terrorism Centre (ECTC), in response to a changing security environment. The organisation has also embraced innovative solutions and emerging technologies as it develops its information infrastructure, analytical capabilities and agile operational support models.

More recently, the Europol Strategy 2020+ set out for the organisation to support the Member States by becoming "a central point for law enforcement

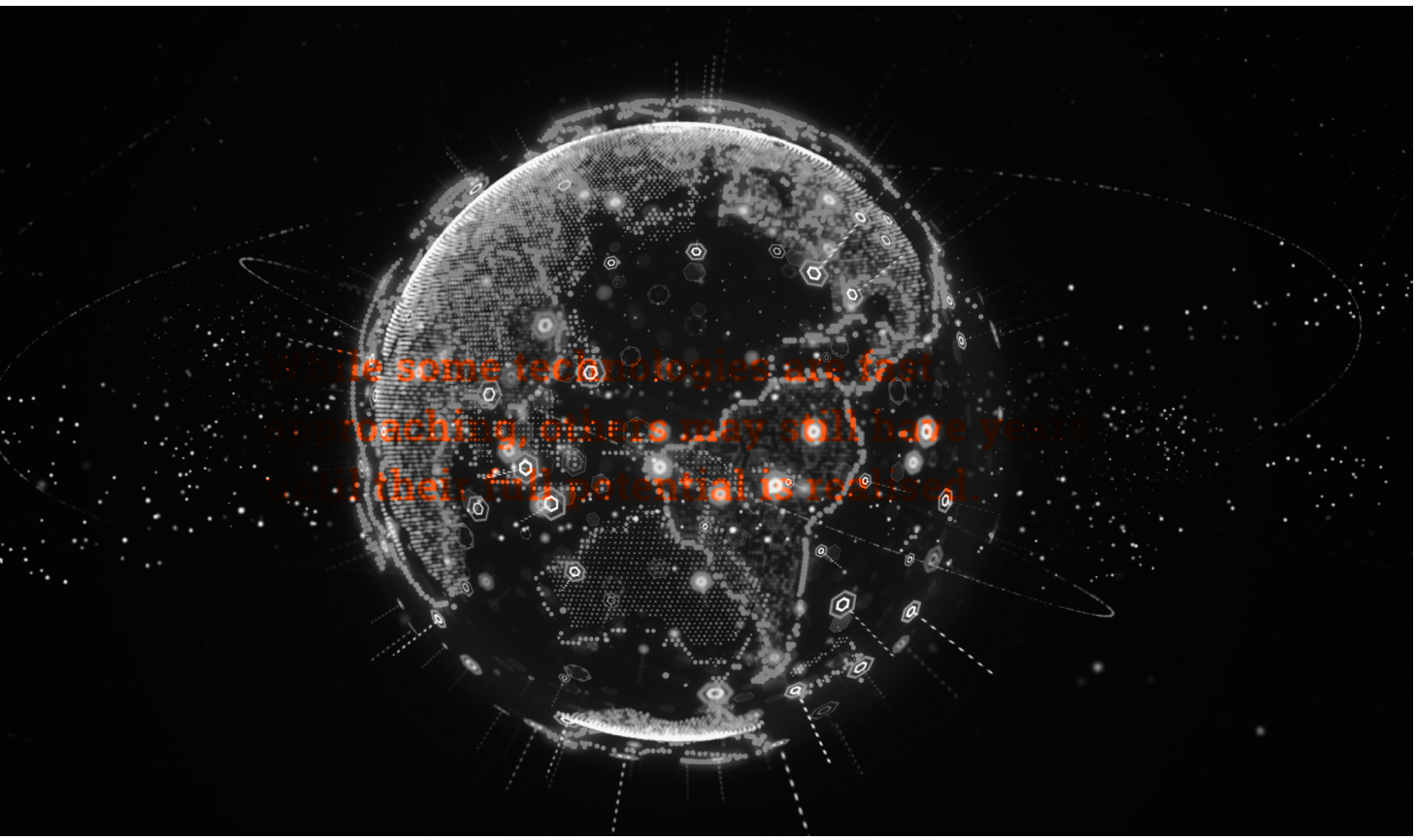
To remain relevant and effective, it is necessary to invest in understanding and actively pursuing new, innovative solutions.

innovation and research.[1]" Identifying emerging challenges to EU law enforcement and shaping the way we collectively respond to them is central to the vision of ensuring "an effective EU response to the threats of serious international and organised crime, cybercrime and terrorism in the EU, by acting as the principal information hub, delivering agile operational support and providing European policing solutions in conjunction with our network of partners.[2]" The strategy envisions Europol as a leading innovator and key platform for advanced EU policing solutions covering the full spectrum of the organisation's core service offerings from information management to the delivery of operational support.

2.0 EXPLORING FUTURE THREATS

This report aims to identify the security threats associated with emerging and disruptive technologies, and the challenges that need to be addressed in order to effectively counter these threats. It also points to ways for law enforcement to use the opportunities brought by the advent and development of new technologies. The report does not intend to provide an exhaustive analysis of the impact of emerging technologies on the work of law enforcement, nor does it provide a clear-cut roadmap for addressing the challenges they pose. Instead, it serves as a basis for future discussions that Europol hopes to have with its main stakeholders, the law enforcement authorities of the Member States, in support of its main mission of making Europe safer for citizens, businesses and other stakeholders.

While some of the technologies presented in this report are fast approaching, others may still have years until their full potential is realised. Recognising them early on and understanding their implications is key to developing a strategic response.



3.0 THE ROLE OF DISRUPTIVE TECHNOLOGIES IN A DYNAMIC SECURITY ENVIRONMENT

Technological innovation has driven profound changes in all areas of society over the past decades. The speed of recent breakthroughs has led some to suggest that we are currently witnessing a Fourth Industrial Revolution (4IR), characterised by the development of technologies that blur the lines between the physical, digital, and biological spheres[3]. This advent of so-called 'disruptive technologies' – those that fundamentally alter the way we live, work, and relate to one another – has significant implications on our security environment. It provides criminals with new ways to pursue their nefarious goals, but also equips law enforcement with powerful tools in the fight against crime.

In recent years, technology has acted as a driver of innovation across the whole spectrum of criminality, with criminals quickly adopting new modi operandi and activities enabled by advanced technologies. The emergence of the online trade in illicit goods and services has created entirely new criminal markets.[4] Virtual currencies and alternative banking platforms are enabling the rapid flow of criminal finances, and new communication technologies, including the use of encrypted communications, have enabled criminals and terrorists to connect and interact covertly.

As technologies develop even further, it becomes increasingly evident that disruption is not solely the result of technological advancement, but rather an outcome of the convergence of various disruptive technologies, challenging established legislative or regulatory frameworks with previously unknown applications.

This new landscape is challenging the traditional definition of organised criminal group (OCG). Since the year 2000, the United Nations Convention against Transnational Organized Crime has provided an internationally shared definition of an organised criminal group as "a group of three or more persons existing over a period of time acting in concert with the aim of committing crimes for financial or material benefit." This definition was also adopted in the EU Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime and continues to reflect law enforcement authorities' conceptualisation of organised crime across the world. However, this definition does not adequately describe the complex and flexible nature of modern organised crime networks in the digital era. The ability of criminals to operate and interact anonymously and the emergence of the crime-as-a-service (CaaS) model across the spectrum of cyber criminality have enabled organised crime networks to become increasingly complex, flexible and opportunistic.

At the same time, disruptive technologies present a set of opportunities and challenges for law enforcement in countering this new criminal threat landscape. Due to technological innovation, law enforcement authorities now have a greater and more impactful set of tools at their disposal to fight crime. To use the full potential of disruptive technologies, and stay ahead of technologically advanced criminals, law enforcement authorities will need to address challenges related to the implementation and regulation of new technologies and realise their potential by also adapting their respective organisational cultures.

4.0 KEY DEVELOPMENTS AND THEIR IMPACT ON CRIME AND TERRORISM

4.1 Artificial Intelligence (AI): super-smart policing vs supervillains

Artificial Intelligence (AI) refers to a system, machine or algorithm that is capable of observing its environment, learning, and based on the insights and experience gained, take actions or propose decisions. These actions include a certain degree of autonomy, while retaining a human-centric approach to ensure trustworthiness and respect for fundamental rights[5].

AI technology is developing at an unprecedented rate. Recent developments in AI technology have allowed for a number of beneficial applications including machine translation, speech and facial recognition, medical diagnostics and many more. However, AI and Machine Learning (ML) technology are also steadily transforming the security landscape and, as they become more easily available, can be exploited by malicious actors.

In the field of cybersecurity, AI is a double-edged sword: it can be greatly beneficial to increase the security of devices, systems and applications, but can also empower those who seek to attack systems and networks and thus become an advanced tool in the arsenal for cyber-attacks. Malicious actors may deploy AI to customise and automate the distribution of malicious contents, such as social engineering attacks or phishing emails[6]. They may also deploy tailored AI algorithms to automate the process of discovering new attack vectors or vulnerabilities. AI technology can also be deployed to support target selection and prioritisation, or respond to changes in a target's behaviour[7].

The exposure of citizens to large-scale disinformation, including misleading or outright false information, is a major challenge for Europe. The use of AI may further exacerbate the impact of hybrid threats, as the mass production of false information can be automated by malicious actors with little to no required technical expertise. The recent development of deepfake technology[i] raises further concerns about the ability of malicious actors to open up new methods of spreading disinformation and impersonating others. Criminals are already reported to have used deepfake audio impersonating chief executives in an attempt to defraud organisations[8].

AI technology is also likely to have implications for traditional organised crime and terrorist threats. The use of unmanned vehicles which rely on AI planning and autonomous navigation technologies could increase the success rate of trafficking activities[9]. They may also be used by terrorist actors to carry out attacks, either by delivering explosives or by using self-driving vehicles as weapons[10]. Researchers have also found that social bots based on ML technology can be used to advertise and sell illicit goods and services, as well as to interact with customers[11].

Law enforcement authorities need to invest in understanding AI technology and its implications to properly detect and contain these emerging threats. Law enforcement should equally explore the opportunities that AI presents for actively countering these threats. This is particularly relevant in the area of cybersecurity where AI can help make defences more effective and scalable.

i Deepfake is a technique for human image synthesis based on artificial intelligence. The term is largely used for videos that have been digitally altered with the intent to deceive viewers.

The exposure of citizens to large-scale disinformation, including misleading or outright false information, is a major challenge for Europe.

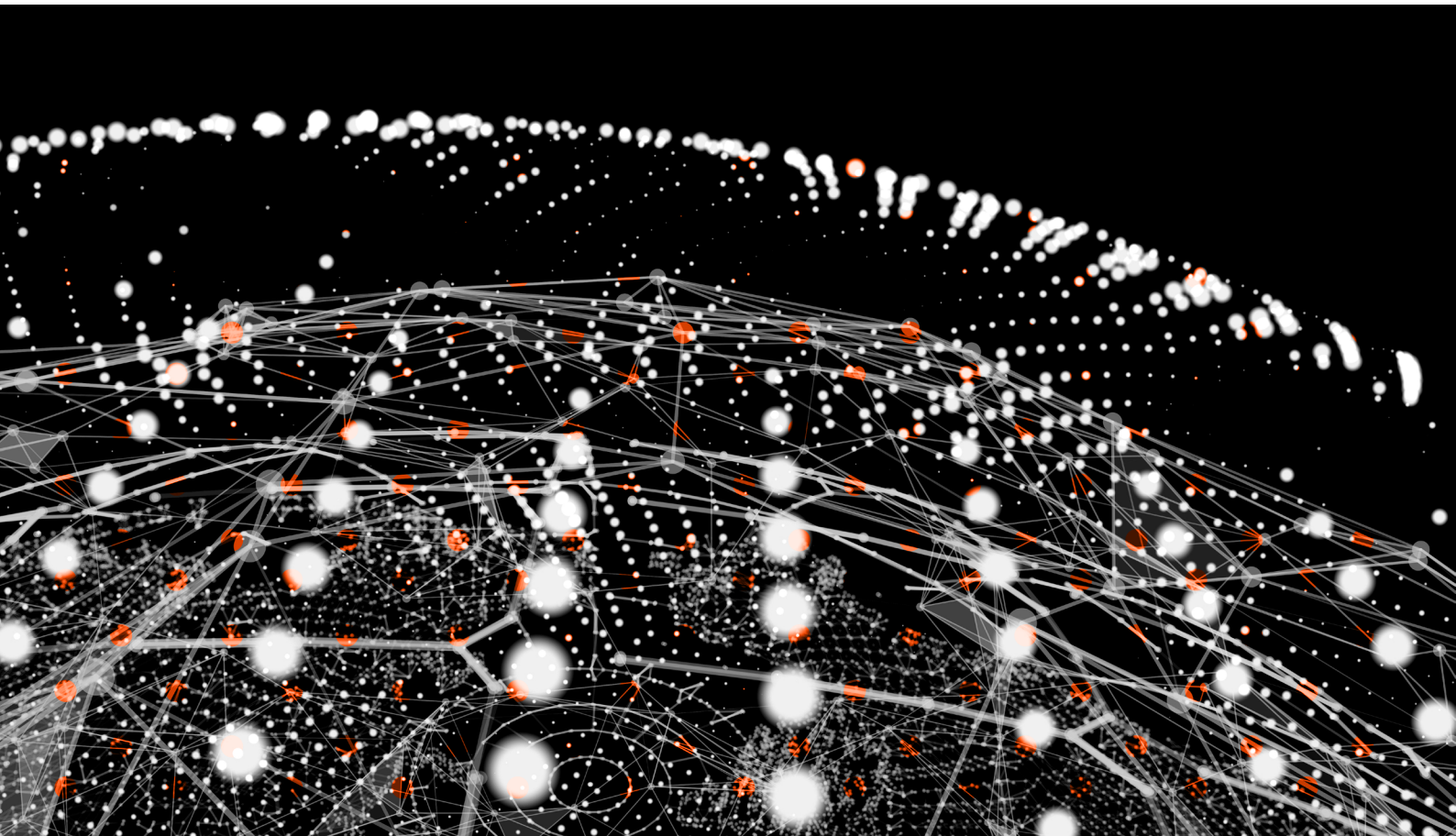
4.2 Quantum computing and encryption: Quantum-capabilities – for whom?

Quantum computers are expected to deliver an unprecedented increase in computer processing power and help reach significant breakthroughs in science, medicine and other fields. Quantum computing has been heralded as one of the next great security risks, although opinions vary on the level of concern this should attract. There is, however, a broader consensus that the advent of the quantum computer is likely to introduce a revolution in the areas of information security and encryption. This is because many security and encryption standards used today depend on the complexity of tasks that classical computers cannot complete in any reasonable time. Given that quantum computers will overcome some of these limitations, it is naturally expected that the technology will prompt a radical rethinking of cybersecurity[12].

One of the principal threats of the application of quantum computers is their ability to break current encryption standards. Theoretically this would grant the first actor with a quantum computer of necessary computing power with the ability to render current standards in the area of encryption obsolete. Malicious actors in possession of a quantum computer would have the opportunity to break traditional security standards, orchestrate far more sophisticated cyber-attacks or decrypt information and communications. Quantum computers may also be used to develop new ways of encrypting communications, making them impervious to interception.

Prototype quantum computing is still at a research stage and practically usable quantum computers are still some years away. The complexity and tremendous costs involved in the development of quantum computers make the prospects of any immediate danger coming from non-state actors such as criminals or terrorists unlikely.

Researchers have already started preparing. The area of post-quantum cryptography, an area of research focusing on the development of cryptographic systems that are secure against both quantum and classical computers[13], is already far ahead. EU-based research projects, such as the one based at KU Leuven's Quantum Center, are also making progress with research into the practical applications of quantum computing[14]. Law enforcement authorities should ensure their involvement in discussions around the regulation and use of quantum-enabled computing completing the private sector view, which is not necessarily informed by security and public safety considerations. This is particularly true in the area of quantum cryptography, which will likely have a significant impact on the work of law enforcement.



4.3 Taking the mobile leap: 5G enabled crime and policing

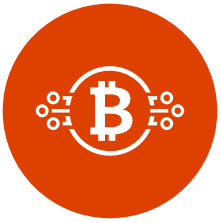
The fifth generation of telecommunication systems, or 5G, is considered to be one of the most critical building blocks of our digital economy and society over the next decades. 5G will enable significantly faster data connections, exceptionally low latency and will be able to handle the increasing number of connected devices. The technology is thus going to form the basis for a number of innovative business models across multiple sectors.

Despite the many anticipated benefits, 5G poses a number of challenges for law enforcement. The first set of challenges pertains to the potential impact of 5G developments with respect to the ability of law enforcement to identify and locate users. 5G technology will complicate the use of the unique mobile phone card identifiers that allow law enforcement to identify and locate devices. As a result, it may no longer be possible to carry out legally permissible, technical investigation and surveillance measures. One of the most important tactical operational and investigation tools would therefore become obsolete.

On the other hand, certain characteristics of 5G technology would also limit the availability and accessibility of information needed when conducting lawful interception. The set-up of 5G networks would mean that information is fragmented, and may not be either available or accessible for law enforcement. Law enforcement would therefore require the cooperation of numerous network providers both at home and abroad. Other features of 5G technology would mean devices communicate directly with each other, without having to use the operator's core network, which would further complicate law enforcement's ability to retrieve communication data. Finally, end-to-end (E2E) encryption protocols may be included as obligatory standards during the upcoming standardisation process (Release 16). An alternative is that terminal manufacturers will (voluntarily) implement this function. Either way, E2E would make it impossible to carry out content analysis of communications within the framework of lawful interception.

An additional challenge that 5G technology presents for law enforcement comes as a result of the virtualisation of physical parts of the network, known as network functions virtualisation (NFV). Existing special personnel and infrastructural security measures to protect the confidentiality of surveillance measures by the providers, for example spatial security measures, access checks etc., will be nullified. This means criminals can employ or execute attacks to access and even alter telephone numbers (target lists) which are to be monitored.

The potential challenges for law enforcement as a result of developments within the area of 5G do not appear to be a priority for developers. Therefore, keeping track of 5G developments and ensuring that lawful interception by design becomes (and stays) part of that evolution will require significant effort. Law enforcement must continue to engage with providers and contribute to developments in the area of 5G through stronger representation of law enforcement interests in the international standardisation bodies (in particular 3GPP) and in the EU institutions (e.g. the European Commission, the JHA Council, the European Parliament) in order to communicate the views and concerns of European law enforcement authorities and their partners.



4.4 Dark web networks and cryptocurrencies: a plethora of islands in the digital sea

As technologies are becoming easier to access and use, criminals are increasingly able to commit crimes and move illicit funds anonymously, to communicate covertly and hide their identity to avoid law enforcement detection. The Darknet and cryptocurrencies have become vital instruments for criminals in that regard and have been consistently identified[15] as key enablers of crime in the 21st century.

The Darknet is a key facilitator for the trade in illicit goods and services and has become an enabler for criminals to conceal their identity and the hosting location of illicit forums, websites and markets. Since 2017, law enforcement agencies shut down some of the largest Darknet markets: AlphaBay, Hansa, RAMP, Valhalla and Wall Street Market. Other illicit markets closed after their administrators fled with the markets' stored funds. This has prompted the migration of users towards other existing or newly established markets, or to other platforms entirely. The volatility of the Darknet market ecosystem may lead to the proliferation of alternative decentralised markets which would overcome the weakness and vulnerability of being hosted in a specific location.

Cryptocurrencies are a key enabler of criminality as they enable vendors and customers to carry out transactions anonymously. Criminals are also increasingly abusing cryptocurrencies to fund crime or launder the proceeds of illicit activities[16]. These activities are increasingly facilitated by new developments such as decentralised exchanges with less stringent Know-Your-Customer (KYC) requirements, which allow users to register and exchange virtual currencies without revealing their true identity. The increase in value and use of cryptocurrencies has also led to the emergence of new forms of cyber criminality, such as cryptocurrency mining, which has increased significantly since 2017[17]. The expanding criminal use of high-privacy cryptocurrencies and decentralised cryptocurrency exchanges frustrate the efforts of law enforcement authorities to detect and recover criminal assets as well as to prevent fraudulent transactions. The future of cryptocurrencies and the extent to which criminals and terrorists will use them will depend on factors such as anonymity, future regulation, law enforcement activities and security of the systems[18].

Researchers and technology leaders are already working on new decentralised computing technologies that are expected to revolutionise the cyber world as we know it today. Decentralised systems have grown in prominence over the past few years, not least in part due to the rising popularity of blockchain technology and cryptocurrencies. Decentralised networks are a type of distributed system where no entity is in control of the underlying infrastructure[19].

Considering the trends observed in illicit activities on the Darknet and the increased criminal use of privacy-based virtual currencies, criminals and terrorists will likely seek to abuse decentralised computing technologies to be able to operate with a greater degree of anonymity and avoid law enforcement detection. The very design of the current centralised networks enables governments to pressure technology companies into enforcing rules and laws on their platforms. In a decentralised web, no single entity is responsible for operating or storing data and can be held accountable for the criminal abuse of their networks.

Researchers and technology companies are already running various projects and are developing applications that are beginning to function. Law enforcement authorities must ensure they keep pace with the developments in this area and invest into a better understanding of the challenges that decentralised networks may entail for investigations and digital forensics. Privacy concerns largely drive innovation in this field. Without law enforcement engagement in discussions on regulation, it is unlikely that law enforcement concerns will be taken into account. Cooperation with the private sector and intensified efforts of forming public-private partnerships would enable law enforcement to promote a safer and healthier digital environment for the general public.

As IoT devices find applications in industry and infrastructure, and as IoT technology provides the building blocks for smart cities, cyber-attacks may become an increasingly physical threat

4.5 The Internet of All Things

The Internet of Things (IoT) refers to the ever-growing network of interconnected physical devices enabled by internet connectivity and the communication that occurs between them. IoT devices are developed for consumer, commercial, industrial and infrastructural use, and are finding applications in a wide range of environments. IoT devices increasingly benefit from the convergence and integration of technologies, such as ML and real-time analytics[20]. The next generation mobile network (5G) is expected to further enable IoT technology by providing faster and more reliable connections for all devices[21].

There are a number of cybersecurity implications particular to IoT devices, which have been consistently highlighted by researchers and law enforcement authorities. IoT devices allow for the proliferation of attack vectors. Insecure IoT devices may become an easier target for criminals aiming to distribute attacks, infiltrate or infect networks. For instance, 2016 saw the emergence of a threat that had been predicted by Europol since 2014 – Distributed Denial of Service (DDoS) attacks originating from botnets of compromised Internet of Things (IoT) devices. There is also a growing number of cases involving malware-infected IoT devices, which exploit software vulnerabilities or weak authentication settings. The vulnerability of IoT devices may be exploited by criminals seeking to collect personal data, compromise user credentials or even spy on people or organisations[22] [23].

IoT devices may also pose a threat that goes beyond the digital world. As IoT devices find applications in industry and infrastructure, and as IoT technology provides the building blocks for smart cities, cyber-attacks may become an increasingly physical threat[24]. For instance, attacks on critical infrastructure enabled by IoT technology, such as industrial control systems across the energy and water industries, have the potential to disrupt power and water supply operations[25]. More recently, a number of companies and national space agencies have been exploring IoT applications in space (e.g. in satellites and space ships)[26]. Although we are still some way from IoT in space becoming a mainstream technology, the spread of IoT devices to space may provide further opportunities for malicious actors to target satellite infrastructure, to either manipulate or disrupt their operations.

Law enforcement authorities need to put an emphasis on understanding the implications of the fast-developing IoT environment to keep pace with the evolution of its applications and recognise the emerging threats that this may pose. In this context, Europe's IoT policy and concrete initiatives such as the Alliance for Internet of Things Innovation (AIOTI) and strategies aiming at advancing the IoT in Europe, looking specifically at security, liability, privacy and data protection, will play a key role in addressing these challenges. In this context, Europol can act as law enforcement's voice in ongoing discussions at EU-level. In addition, Europol and ENISA co-organise the annual IoT Security Conference, which aims to raise awareness on the security implications of the Internet of Things (IoT) and enable a broad discussion by bringing together experts from cybercrime units, Computer Security Incident Response Teams (CSIRTS), international organisations, private industry, regulatory agencies, and academia.

4.6 Manufacturing profits for crime through 3D printing

3D printing, also known as additive manufacturing, comprises a variety of processes used to create three-dimensional structures out of various materials from a digital model[27]. The technology has been around since the 1980s, but experienced an explosion in interest and use over the past ten years, when many patents on parts of the technology expired and prices for 3D printers began to drop[28].

The technology is promising for its versatility and new opportunities opened up by 3D printing can be found in diverse fields, including supply chain management, health care and others[29] [30]. However, the increasing availability of 3D printing technology also creates opportunities for criminal abuse. While the proliferation of 3D printed firearms has often been cited as a main concern in the past, this has not materialised as a large-scale threat to law enforcement. However, the technology offers other avenues for criminal use: 3D printing is already being used to manufacture ATM skimming devices[31]. In the near future, it could also be used to increase the production of counterfeit goods[32].

Another threat associated indirectly with the proliferation of 3D printing in various industries is the potential of hackers infiltrating machines and altering digital blueprints[33]. In an experiment to demonstrate this threat, a group of university researchers hacked into a desktop computer and altered the 3D digital blueprint for a drone's propeller. While the microscopic changes were invisible to the observer, it led the propeller to malfunction, resulting in the crashing of the drone[34]. The potential effects of such sabotage are wide-reaching, especially considering the increasing use of 3D printing in security-relevant fields, such as the aerospace, military, and health industries.

The potential criminal abuses of 3D printing technology can take an even more complex shape with the development of programmable matter (PM) technology and its use in 4D printing. The term PM has been described as the "science, engineering, and design of physical matter that has the ability to change form and/or function (shape, density, moduli, conductivity, colour, etc.) in an intentional, programmable fashion"[35] . PM would enable 3D printed objects to be customisable by the user or programmable for other post-fabrication changes in shape and function, including adapting to changing environments. PM technology, and its use in 4D printing, is still in development stages and it is yet to overcome a series of technical challenges before it becomes mainstream. However, it holds enormous disruptive potential for global commerce, geopolitics and security, as the technology is expected to completely transform the way materials are produced and utilised in a range of industries[36, 37]. Law enforcement authorities and other security actors need to keep abreast of developments in 3D printing, programmable matter (PM) and 4D printing technology to better asses their disruptive capacity and potential misuse by malicious actors, such as criminals or terrorists.

4.7 One microbe makes all the difference: the implications of biotech for security

Unprecedented technological progress has been made in the fields of molecular biology and genetics over the past 20 years. Central to this is the development of genome editing: technologies allowing genetic material to be added, removed or altered at particular locations in the genome[38]. The technology is advancing as the price of DNA sequencing has fallen rapidly since 2008, far outpacing Moore's law, according to which processing power doubles or its price halves every two years[39]. As a result, genetic engineering is becoming more accessible to a wider group of people: a growing movement of do-it-yourself biohackers is experimenting with genetic editing on themselves and on bacteria in the confines of their own homes, with kits starting from $159[40]. Researchers at the University of Alberta have used mail-order DNA to recreate from scratch an extinct relative of smallpox, horsepox, for about $100,000[41]. The potential for misuse of biotechnology and genetic engineering for criminal purposes is evident.

Law enforcement and security agencies have long been worried about biological agents as weapons of choice for terrorists. Although terrorists in the past were certainly motivated to do so, operational capability to use such agents was limited.

However, biological terrorism may be witnessing a resurgence: in recent years, terrorist organisations have increasingly included references to biological weapons in their online propaganda material. The impact of those publications is visible in two foiled 2018 plots using the same suggested modus operandi: using ricin in homemade explosive devices to commit a biological attack[42]. With biological engineering becoming more commonplace, more people will have the knowledge and skills to synthesise pathogens and carry out such an attack. While governments stockpile select agents in secure sites, their DNA codes are often publicly available, thus opening up the potential for non-state actors to design new bioweapons. The lack of a global system for monitoring biological agents in public areas compounds this vulnerability[43].

As DNA is increasingly used for a wide range of identification and authentication methods, criminal actors may try to steal, analyse, or even replicate someone's genetic data.

In a broader security context, biological weapons may feature more prominently in a developing hybrid threat landscape. Pathogens could target large populations at frequencies too low to be immediately detected and difficult to be attributed to a state or non-state actor, and would thus be a prime example of an unconventional weapon that damages an adversary while remaining below the threshold of all-out warfare.

Beyond using biological substances as weapons for terrorist purposes, developments in biotechnology can be used by criminal actors for monetary gain. Combined with more traditional cybercriminal means, actors could hack corporate and government databases to steal genetic codes and use it to replicate biologically produced drugs. As the field of synthetic biology progresses, new and potentially expensive treatments and therapies for infectious diseases and cancers will become available, a market which criminal actors can exploit by producing cheaper counterfeits.

Advances in biotechnology may also enable identity-related crimes. As DNA is increasingly used for a wide range of identification and authentication methods, criminal actors may try to steal, analyse, or even replicate someone's genetic data. Accessing someone's DNA – found on everyday items, such as cups, cutlery, or hotel beds – will be facilitated by cheaper and more accessible DNA sequencing tools. This opens up the potential for planting false DNA evidence at crime scenes to frame someone, or to falsify genetic tests to establish paternity or ancestry for the purpose of establishing inheritance rights.

As a wide range of products and services become digitalised and interconnected, law enforcement may exploit new avenues for detecting criminals' digital traces.

5.0 CHANGING THE GAME - LAW ENFORCEMENT READINESS AND RESPONSES

As technological developments provide new opportunities for crime, law enforcement will itself need to adapt its response to a new and more complex threat landscape. Success in doing so will be based on how well it can make use of new technologies to keep up with the threats posed by criminal actors. However, exploiting the full potential presented by technological innovation is only possible if several underlying parameters are fulfilled. These include the presence of necessary technical infrastructure and expertise, a legal framework and regulations supportive of new policing technologies, and an organisational culture that promotes innovation, flexibility and quick responses to emerging threats.

5.1 Opportunities

Developing technologies provide law enforcement with invaluable opportunities to carry out investigations and identify suspects. As a wide range of products and services become digitalised and interconnected, law enforcement may exploit new avenues for detecting criminals' digital traces. Big data analysis can reveal or anticipate crime patterns, as well as links between previously unconnected events or actors, helping law enforcement target resources where they are most likely to be effective[44]. As cellular network technology improves, more data can be transmitted faster, which can be processed more efficiently by artificial intelligence algorithms. Quantum computing may provide for easier access to encrypted data, facilitating the collection of digital evidence.

Many forthcoming technological opportunities for law enforcement promise more efficient ways to collect and analyse increasingly large and diverse amounts of data, thereby significantly alleviating the resource burden on operational and technical analysis. AI and ML play a central role in this: promising new law enforcement technologies that rely on these mechanisms include predictive policing, multimedia analytics, automated number plate recognition (ANPR) and natural language processing.

Predictive policing refers to the usage of mathematical, predictive analytics and other analytical techniques in law enforcement to identify potential criminal activity[45]. This enables law enforcement to shift from a traditionally reactionary approach to crime fighting to one that is more proactive and preventative in character. Crime data collected by law enforcement, such as the type, date and location of past crimes, are processed by algorithms that then anticipate where and when future crimes are most likely to occur. Similarly, predictions can be made about an individual's likelihood of reoffending. While several EU countries have already begun to implement predictive policing solutions, many such projects have recently attracted public scrutiny due to ethical and data protection concerns[46].

Multimedia analytics is another area where law enforcement can benefit from advances in technology, with facial and object recognition having undergone rapid developments in recent years. Innovate projects that are being developed or trialled in different countries include software that analyse images and communication patterns on a suspect's electronic devices able to cross-match faces from databases or other devices, or recognise weapons, drugs, cars, nudity in images[47]. Such software is also being used to find images of child sexual exploitation in large image datasets. Similarly, natural language processing algorithms have been developed to crawl the open and dark web for clues pointing to human trafficking activity. Already widely used in the U.S. for that purpose, it has now been trialled for use in narcotics, weapons smuggling and counterfeiting investigations[48]. Social media companies have also started using algorithms to detect harmful content, whether to spot terrorist speech, graphic violence, nudity, hate speech, or material promoting self-harm[49]. These include applications screening images and videos, text, and even text within images[50] for such material. There is a great potential for law enforcement to make use of such technologies, for instance, to detect terrorist or child sexual exploitation content online.

Collectively, such applications have the potential to reduce human bias in processing and analysing large data sets and thus achieving a higher level of accuracy and precision. They also help law enforcement make better use of existing resources – both human and financial – by achieving a larger degree of automation of selected processes within the intelligence management cycle. In relation to collecting e-evidence, artificial intelligence applications may present a more efficient solution to the challenge of investigating cases that involve an ever-increasing amount of data.

Taking advantage of these and other technology-enabled opportunities will require law enforcement to adapt both in terms of adjusting existing job profiles and in creating entirely new roles previously unfamiliar to a law enforcement environment. Law enforcement authorities will need to increasingly work with data scientists and other technical experts to handle mass data including crowd-sourced data. Handling these data streams will require law enforcement to move away from business models based on data input to data evaluation. This will require robust and reliable information management structures that encompass all aspects of the data handling chain from data collection to handling, evaluation, exploitation and data security.

5.2 Operational implementation: technical infrastructure and specialist expertise

Many promising new policing technologies rely on being able to collect and process increasingly high volumes of unstructured data. Examples of such new trends in policing include the increased use and interconnectedness of law enforcement databases; real-time identification systems, such as automated license plate readers, facial and voice recognition systems; and predictive policing technologies, such as predictive mapping of crimes and predictive identification of suspects[51].

While some of these data-driven policing technologies are already in use by some national law enforcement authorities, the adoption and integration by others is still piecemeal, with pilot programmes being implemented across the EU[52]. Current limitations exist with regard to the high technical requirements of data analytics. As the complexity of data evolves both in terms of volume and structure, organisations are faced with an information management challenge, particularly with regards to storing and processing data at the rate at which it is being collected[53].

Similarly, increasing technological progress in policing raises the need for up-skilling and re-skilling the workforce, as well as attracting new talents with highly specialist skillsets, while competing for these human resources with the private sector. Training and recruitment may be particularly challenging in the face of budget cuts that many law enforcement agencies have been facing across Europe. Increased cooperation with the private sector, already established within the area of cybercrime, may need to become more widespread, also in crime areas previously not associated with private sector involvement[54]. In the case of some Member States, additional legal mechanisms will need to be implemented to allow for a deeper private sector involvement in law enforcement tasks.

Within law enforcement organisations, formal training measures should be taken to bring staff on board when new technologies are implemented, so as to elicit staff buy-in and ensure that implementation of new systems translates into operational activity[55].

There is also a need to adapt procurement procedures to reduce the time it takes to implement new products and solutions to match, or ideally outpace, the speed at which disruptive technologies change the criminal landscape.

5.3 Regulatory and legal framework: law enforcement's voice must be heard

The digital revolution has led to an increased public awareness of the importance of data privacy and security. Recent years have seen increasing regulatory activity in the EU and Member States in order to construct a legal framework tailored to new technological realities. This includes the implementation of the General Data Protection Regulation (GDPR)[56], the e-evidence package, and more recently, the proposal for an ePrivacy Regulation[57], which is currently being negotiated at EU level.

As new technological developments can significantly improve law enforcement's capabilities to carry out surveillance and collect and analyse data, addressing data privacy concerns will likely be a priority for legislators. It is of paramount importance that the voice of law enforcement is heard when legislative and regulatory frameworks are being discussed and developed, in order to have an opportunity to address their concerns and needs, particularly with regards to the accessibility of data and lawful interception.

Beyond data privacy concerns, a further need for international legal and regulatory cooperation concerns the collection, retention, and exchange of data and electronic evidence. Given that technologically-enabled crime often involves several jurisdictions and stakeholders, different data retention regulations and reliance on mutual legal assistance treaties complicate and lengthen the investigation and prosecution of such crimes. The European Commission has taken several steps to mitigate this and, most recently, proposed on 5 February 2019 to start international negotiations on cross-border access to electronic evidence, with two negotiating directives now pending approval by the Council[58].

5.4 Organisational culture: promote innovation and strategic foresight

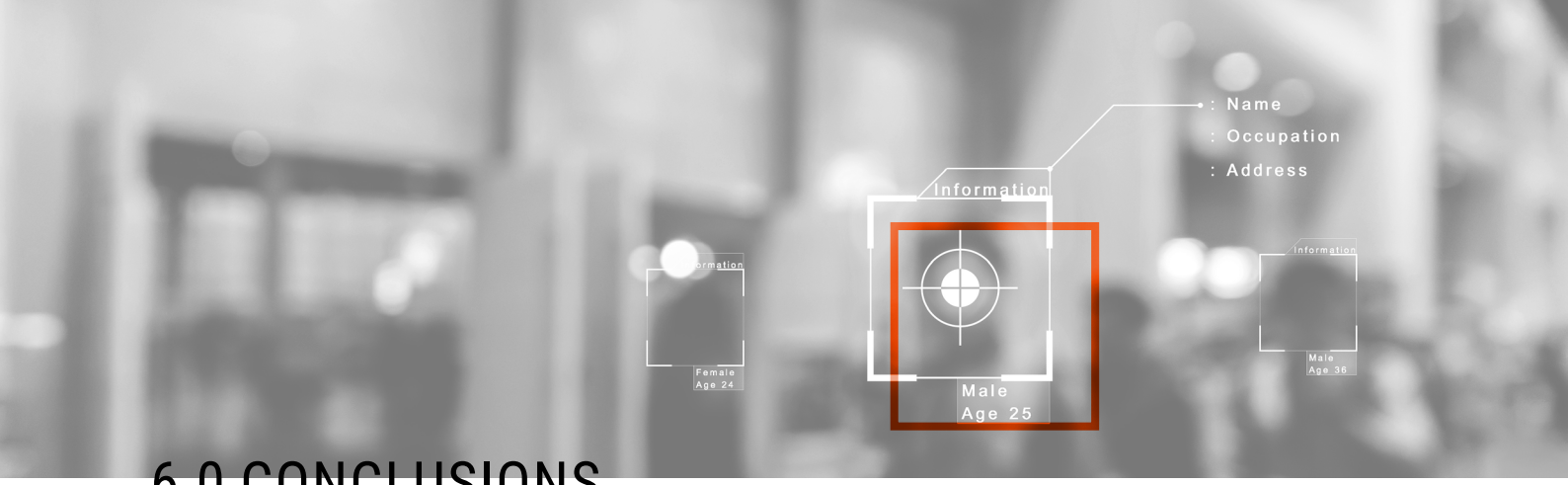
Traditional 'command and control' organisations like law enforcement are often reliant on hierarchical structures and bureaucracy and may thus find it difficult to adapt quickly to changes in the threat environment. Yet, in order to proactively tackle the threats posed by new technologies, law enforcement organisations will need to create an organisational culture that promotes innovation and strategic foresight.

A key measure identified to increase innovation within law enforcement is to institute a culture that welcomes new ideas and challenges on their own merit, regardless of rank[59]. Good ideas from the bottom need to be able to reach the top without passing through lengthy chains of command that tend to delay or even block an idea if it reaches one disapproving link in that chain. Once an idea has been shut down, perhaps without good explanation, it can cause disillusionment among lower-ranking officers and staff and inevitably discourage future attempts at innovation.

Law enforcement organisations have also pointed out that it is important to manage traditionally high levels of risk aversion in order to promote innovation[60]. As innovation, by definition, involves trying new things without always knowing the consequences, it can be at odds with a desire to minimise risk[61]. Organisations will need to shift from a "culture of blame" to a "culture of learning from mistakes"[62], in order to create an environment that contributes to the proactive sharing of new ideas.

Innovation, especially in the area of new, highly specialised technologies, also requires a culture that embraces cooperation with external partners to broaden the expertise at hand. Much of the developments in this area have been led by academia and the private sector. To benefit from their expertise and to ensure a seat at the table when new technologies are conceptualised and developed, law enforcement culture will need to move toward an organisational mindset that rewards information-sharing and proactively engages with partners outside the law enforcement community.

To keep abreast of new technological developments and to be able to proactively shape a response, law enforcement organisations will also need to allocate more resources to strategic foresight. This involves creating institutionalised structures and opportunities for strategic thinking and analysis as well as research and development, with staff assigned to these functions on a full-time basis, rather than next to their day-to-day jobs.



6.0 CONCLUSIONS

The profound impact of technological change on law enforcement has been highlighted repeatedly over the last decades. However, the pace and scale of technological innovation confronting law enforcement authorities in the EU and beyond is now becoming increasingly apparent.

The opportunities for law enforcement in harnessing these technologies are as great as the challenges and their potential utility to criminal actors. Law enforcement authorities must employ foresight and embrace organisational change challenging established business models in order to access the potential held by these technologies.

The list of technological innovations with an impact on law enforcement and crime mentioned in this report is not exhaustive and is not necessarily surprising, but it may provide a starting point to a discussion on how to mitigate risks and utilise the capabilities of these technologies.

First and foremost, it is clear that in an era of resource scarcity in public sector cooperation, resource sharing and maximising efficiencies are key to effective law enforcement work in a highly dynamic security environment shaped by rapid technological change.

This requires joint approaches at national and European level, not only in terms of operational delivery, but also in terms of aligning legislation to enable even more far-reaching and deep cooperation among law enforcement authorities.

As the driver of technological innovation, the private sector plays a pivotal role and law enforcement must do more to engage with these actors. It is also becoming increasingly clear that criminal threats facing the EU can no longer be tackled by primarily relying on regional cooperation. Establishing more effective cooperation with a greater number of third partner countries and organisations is necessary to allow European law enforcement authorities to access the data and information needed to fight crime at home, which is increasingly held outside the EU. This flexible approach to cooperation needs to be enabled by a robust legal framework that carefully balances the needs of law enforcement authorities and other security actors and fundamental rights of EU citizens.

Europol is an ideal platform to enable deeper cooperation at home in the EU and wider cooperation with partners outside the EU. Europol can deliver additional value in an age of rapid technological development by increasingly engaging in expertise coordination and collective resource management, which avoids unnecessary duplication of resources and expertise at national level. Europol can ensure expertise available in one Member State is accessible to law enforcement authorities in need of support in another Member State.

As set out in Europol's Strategy 2020+, Europol is committed to further establishing its role as a driver for innovation in law enforcement. This will involve exploring new ways of supporting Member State law enforcement authorities enabled by some of the technologies set out in this paper. Crucially, Europol's key role in connecting Member States will require the organisation to continue developing its approach to information management by exploring cutting-edge technologies for faster information sharing and processing as well as generating deeper insights from the data held in European databases.

This report is only the beginning of a conversation Europol hopes to have with its main stakeholders, the law enforcement authorities of the Member States, in support of its mission of making Europe safer for citizens, businesses and other stakeholders.

References

1 Europol, 2019, Europol Strategy 2020+, accessible at https://www.europol.europa.eu/publications-documents/europol-strategy-2020

2 Europol, 2019, Europol Strategy 2020+, accessible at https://www.europol.europa.eu/publications-documents/europol-strategy-2020

3 World Economic Forum, 2018, The Fourth Industrial Revolution, by Klaus Schwab, accessible at https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab

4 Europol, 2017, EU Serious and Organised Threat Assessment (SOCTA 2017), accessible at https://www.europol.europa.eu/newsroom/news/crime-in-age-of-technology-%E2%80%93-europol%E2%80%99s-serious-and-organised-crime-threat-assessment-2017

5 Russell, S., Norvig, P., 1995, Artificial Intelligence: A Modern Approach; EU Joint Research Centre 2018, Artificial Intelligence: A European Perspective, accessible at https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/artificial-intelligence-european-perspective

6 World Economic Forum, 2019, 3 ways AI will change the nature of cyber-attacks, accessible at https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/

7 University of Oxford, 2018, The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, accessible at https://static.rasset.ie/documents/news/2018/02/ai-report.pdf

8 BBC, 2019, Fake voices "help cyber-crooks steal cash", accessible at: https://www.bbc.com/news/technology-48908736

9 Europol, 2017, EU Serious and Organised Threat Assessment (SOCTA 2017), accessible at https://www.europol.europa.eu/newsroom/news/crime-in-age-of-technology-%E2%80%93-europol%E2%80%99s-serious-and-organised-crime-threat-assessment-2017

10 King, T.C., Aggarwal, N., Taddeo, M. et al. Sci Eng Ethics (2019). https://doi.org/10.1007/s11948-018-00081-0

11 University of Oxford, 2018, The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, accessible at https://static.rasset.ie/documents/news/2018/02/ai-report.pdf

12 Europol and Eurojust, 2019, First report of the observatory function on encryption, accessible at https://www.europol.europa.eu/publications-documents/first-report-of-observatory-function-encryption

13 Chen, L., Stephen, J., Yi-Kai, L., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D., National Institute of Standards and Technology, 2016, "Report on Post-Quantum Cryptography", accessible at: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

14 Quantum Center, https://fys.kuleuven.be/qc/about for more information about the pan-European collaborative research project connecting universities in Amsterdam, Delft, Leuven and Munich

15 Europol, 2017, EU Serious and Organised Threat Assessment (SOCTA 2017), accessible at https://www.europol.europa.eu/newsroom/news/crime-in-age-of-technology-%E2%80%93-europol%E2%80%99s-serious-and-organised-crime-threat-assessment-2017; Europol, 2017, Internet Organised Crime Threat Assessment (IOCTA) 2017, accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017; Europol, 2018, Internet Organised Crime Threat Assessment (IOCTA) 2018, accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018; Europol, 2015, Exploring tomorrow's organised crime, accessible at https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime

16 Europol, 2017, Internet Organised Crime Threat Assessment (IOCTA) 2017, accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

17 Cyber Threat Alliance, 2018, The Illicit Cryptocurrency Mining Threat, accessible at https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf

18 RAND Corporation, 2019, Terrorist Use of Cryptocurrencies, accessible at https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf

19 Blockstack, 2019, Blockstack Technical Whitepaper v2.0, accessible at https://blockstack.org/whitepaper.pdf

20 Wigmore, I., 2014 "Internet of Things (IoT)", TechTarget, accessible at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

21 Europol, 2018, Internet Organised Crime Threat Assessment (IOCTA) 2018, accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

References

22 Bastos, D., Shackleton, M, El-Moussa, F, 2018 "Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments" Living in the Internet of Things: Cybersecurity of the IoT – 2018. Institution of Engineering and Technology: 30.

23 Stelnberg, J., 2014, Forbes, These devices may be spying on you (even in your own home), accessible at: https://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-your-own-home/#5a1a20a3b859

24 Clearfield, Christopher (26 June 2013). "Rethinking Security for the Internet of Things". Harvard Business Review Blog.

25 Trend Micro, 2018, Critical Infrastructures Exposed and at Risk: Energy and Water Industries, accessible at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries

26 Fredric, P., 2018 Network World, Is the IoT in space about to take off?, accessible at: https://www.networkworld.com/article/3315736/is-the-iot-in-space-about-to-take-off.html

27 RAND Corporation, 2018, Additive Manufacturing in 2040, accessible at https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE283/RAND_PE283.pdf

28 RAND Corporation, 2018, Additive Manufacturing in 2040, accessible at https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE283/RAND_PE283.pdf

29 DHL, 2016, 3D Printing and the Future of Supply Chains, accessible at https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/dhl-trendreport-3dprinting.pdf

30 EY, 2016, If 3D printing has changed the industries of tomorrow, how can your organization get ready today?, accessible at https://www.ey.com/Publication/vwLUAssets/ey-3d-printing-report/$FILE/ey-3d-printing-report.pdf

31 Fruehauf, J., Hartle, F., Al-Khalifa, F., 2016, 3D Printing: The Future Crime of the Present, accessible at https://www.researchgate.net/publication/312042613_3D_Printing_The_Future_Crime_of_the_Present

32 Europol, 2015, Exploring tomorrow's organised crime, accessible at https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime

33 Harvard Business Review, 2017, 3D Printing Gives Hackers Entirely New Ways to Wreak Havoc, accessible at https://hbr.org/2017/10/3d-printing-gives-hackers-entirely-new-ways-to-wreak-havoc

34 Belikovestky, S., Yampolskiy, M., Toh, J., Gatlin, J.,Elovici, Y., 2017, dr0wned – Cyber-Physical Attack with Additive Manufacturing, accessible at https://www.usenix.org/system/files/conference/woot17/woot17-paper-belikovetsky.pdf

35 Campbell, A., Tibbits, S., Garrett, B., Atlantic Council, 2014, The Next Wave: 4D printing: Programming the Material World, accessible at: https://www.atlanticcouncil.org/images/publications/The_Next_Wave_4D_Printing_Programming_the_Material_World.pdf

36 Campbell, A., Tibbits, S., Garrett, B., Atlantic Council, 2014, The Next Wave: 4D printing: Programming the Material World, accessible at: https://www.atlanticcouncil.org/images/publications/The_Next_Wave_4D_Printing_Programming_the_Material_World.pdf

37 Akenburg, C., 2013, "Cities of the Future: Built by Drones, Bacteria, and 3D Printers,", available at: http://www.fastcoexist.com/1681891/cities-of-the-future-built-by-drones-bacte¬ria-and-3-d-printers

38 US National Library of Medicines, 2019, What are genome editing and CRISPR-Cas9?, accessible at https://ghr.nlm.nih.gov/primer/genomicresearch/genomeediting

39 Wetterstrand, K.A., 2019, DNA Sequencing Costs: Data from the NHGRI Genome Sequencing Program (GSP), accessible at https://www.genome.gov/about-genomics/fact-sheets/DNA-Sequencing-Costs-Data

40 The New York Times, 2018, As D.I.Y. Gene Editing Gains Popularity, 'Someone Is Going to Get Hurt', accessible at https://www.nytimes.com/2018/05/14/science/biohackers-gene-editing-virus.html

41 Noyce, R.S. & Lederman S. & Evans D.H., 2018, Construction of an infectious horsepox virus vaccine from chemically synthesized DNA fragments, accessible at https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0188453#sec018

42 Reuters, 2018, France foils possible ricin plot by Egyptian-born student, accessible at https://www.reuters.com/article/us-france-security/france-foils-possible-ricin-plot-by-egyptian-born-student-idUSKCN1IJ0SR; Deutsche Welle, 2018, Cologne ricin plot bigger than initially suspected, accessible at https://www.dw.com/en/cologne-ricin-plot-bigger-than-initially-suspected/a-44319328

References

43 Wired.co.uk, 2013, DNA hacking is the biggest opportunity since cyber-attacks, accessible at https://www.wired.co.uk/article/the-bio-crime-prophecy

44 Europol, 2015, Exploring tomorrow's organised crime, accessible at https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime

45 CEPOL, 2019, Webinar 35/2019 'Predictive policing', accessible at https://www.cepol.europa.eu/education-training/what-we-teach/webinars/webinar-352019-predictive-policing

46 The Guardian, 2019, Ethics committee raises alarm over 'predictive policing' tool, accessible at https://www.theguardian.com/uk-news/2019/apr/20/predictive-policing-tool-could-entrench-bias-ethics-committee-warns

47 The Guardian, 2018, Police trial AI software to help process mobile phone evidence, accessible at https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence; Incibe, 2017, Nadal y Zoido presiden la entrega de los equipos de detección de delitos electrónicos, accessible at https://www.incibe.es/sala-prensa/notas-prensa/nadal-y-zoido-presiden-entrega-los-equipos-deteccion-delitos-electronicos

48 Szekely, P., Kejriwal, M., 2018, Domain-specific Insight Graphs (DIG), 433-434. 10.1145/3184558.3186203, accessible at https://www.researchgate.net/publication/324639857_Domain-specific_Insight_Graphs_DIG; Computer.org, 2018, Update on the Crime-Fighting AI Tool Called "DIG": An Interview with Developer Mayank Kejriwal about his Research, accessible at https://www.computer.org/publications/tech-news/research/interview-with-mayank-kejriwal

49 CNET.com, 2018, How Facebook uses artificial intelligence to take down abusive posts, accessible at https://www.cnet.com/news/heres-how-facebook-uses-artificial-intelligence-to-take-down-abusive-posts-f8/ Facebook Newsroom, 2018, Hard Questions: What Are We Doing to Stay Ahead of Terrorists?, accessible at https://newsroom.fb.com/news/2018/11/staying-ahead-of-terrorists/

50 Facebook Code, 2018, Rosetta: Understanding text in images and videos with machine learning, accessible at https://code.fb.com/ai-research/rosetta-understanding-text-in-images-and-videos-with-machine-learning/

51 Jansen, F, 2018, Data Driven Policing in the Context of Europe, accessible at https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf

52 Jansen, F, 2018, Data Driven Policing in the Context of Europe, accessible at https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf

53 Royal United Services Institute for Defence and Security Studies (RUSI), 2017, Big Data and Policing, accessible at https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf

54 Europol, 2015, Exploring tomorrow's organised crime, accessible at https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime

55 Royal United Services Institute for Defence and Security Studies (RUSI), 2017, Big Data and Policing, accessible at https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf

56 Royal United Services Institute for Defence and Security Studies (RUSI), 2017, Big Data and Policing, accessible at https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf

57 UK Parliament, 2018, Policing for the future, accessible at https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/51512.htm

58 European Commission, 2019, E-evidence - cross-border access to electronic evidence, accessible at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

59 Involvement & Participation Association (IPA), 2019, Forces of Change: Innovation and Engagement in UK Policing, accessible at https://www.ipa-involve.com/Handlers/Download.ashx?IDMF=f3242899-cc18-46e3-a3c3-2abd75a8173c

60 UK Parliament, 2018, Policing for the future, accessible at https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/51512.htm

61 Involvement & Participation Association (IPA), 2019, Forces of Change: Innovation and Engagement in UK Policing, accessible at https://www.ipa-involve.com/Handlers/Download.ashx?IDMF=f3242899-cc18-46e3-a3c3-2abd75a8173c

62 UK Parliament, 2018, Policing for the future, accessible at https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/51512.htm