RAND EUROPE

The Future of Cybercrime in Light of Technology Developments

Jacopo Bellasio, Erik Silfversten, Eireann Leverett, Anna Knack, Fiona Quimbre, Emma Louise Blondes, Marina Favaro, Giacomo Persi Paoli

For more information on this publication, visit www.rand.org/t/RRA137-1

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

RAND Europe is a not-for-profit research organisation that helps to improve policy and decision making through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

www.rand.org

www.randeurope.org

Study context

Digital systems and Information Communication Technology (ICT) have become critical in all sectors of economic activity in Europe and beyond. The uninterrupted flow of information and access to the internet now undergird many businesses and the day-to-day functioning of societies. Cybersecurity incidents, either intentional or accidental, can severely disrupt essential services as well as economic and societal activities. One significant and growing threat to digital systems and to the secure functioning of digital institutions and economies is cybercrime.

The Government of Estonia has requested support from the European Commission under Regulation (EU) 2017/825 to analyse new and emerging technological developments and identify their potential application in cybercrime. In May 2019, RAND Europe was commissioned by the European Commission Structural Reform Support Service (SRSS) to conduct a study (ref: SRSS/C2018/092) aimed at:

1. Conducting an analysis of future technologies and identifying those that could be used to commit cybercrimes;
2. Analysing the effect of changes in ICT on cybercrimes, including both cyber-dependent and cyber-enabled crimes;
3. Proposing possible ways to prevent future technologies from being exploited by criminals for these purposes.

Study methodology

To meet the study objectives, RAND Europe conducted the following activities:

1. Initiate the project through kick-off and scoping meetings to ensure a clear, agreed, and common understanding of the research scope, objectives and approach (Task 1).
2. Take stock of current knowledge of and policy on cybercrime, and conduct horizon scanning activities to identify technologies that may have an impact on cybercrime (Task 2).
3. Engage with stakeholders and experts to elicit their views on current and future cybercrime and technology trends, review existing cybercrime classifications, and validate initial findings (Task 3).
4. Design and deliver a table-top exercise to identify possible policy and legislative initiatives to be adopted to prevent the exploitation of technologies for cybercrime purposes (Task 4).
5. Report the key study findings in a final study synthesis report, and produce adequate communications materials, inclusive of a research brief and infographics (Task 5).
6. Deliver a final presentation to the Estonian authorities (Task 6).

Certain limitations, caveats, and assumptions underpinning the study methodology and the results of the work discussed should be noted. The purpose of the study conducted is to identify future trends, challenges, and opportunities for cybercrime and harm reduction over a ten-year timeframe from 2020. The study team employed a futures methodology designed to ascertain future possibilities and formulate recommendations to inform decision making in a context of uncertainty. Given the current speed and magnitude of change in many of the different technology areas considered, the findings and results of this study should not be taken as an exact prediction of future advances and scenarios. Rather, the study aims to offer an analysis designed to identify the main drivers,

trends and opportunities likely to materialise in the next decade, and to facilitate the adoption of flexible, forward-looking policies and investment strategies.

Understanding the context

There is no clearly articulated and globally accepted definition of cybercrime. However, many different definitions have been proposed by experts, industry, academia, law enforcement, governments, and international organisations. However, it is widely recognised that cybercrime crosses both the physical and the virtual worlds.

The virtual aspect of cyberspace allows cybercriminals to disregard national borders and to target victims around the world at range and at scale, making it challenging to combat, investigate and prosecute. Nevertheless, most cybercrime has real-world implications despite its virtual context. Therefore, it is useful to distinguish between two broad categories of cybercrime:

- **Cyber-enabled crime** refers to existing crimes that have been transformed in scale or form by the use of the internet, such as online fraud and forgery.
- **Cyber-dependent crime** refers to crimes that employ a digital system as the target as well as the means of the attack, such as the spreading of viruses or other malware and hacking.

This bipartite definition reflects the fact that certain forms of crime in the virtual world have their counterpart in the real world, as the internet's relative anonymity, ease of use, and transnational and borderless character are all features that create new opportunities for old crimes. At the same time, certain crimes are unprecedented in their ways and means compared to the pre-digital era.

Figure 1 provides an overview of some of the key characteristics, drivers, actors, motivations, and costs associated with cybercrime.

New and emerging technologies of interest

The study identified seven new and emerging technology clusters expected to have a significant impact on cybercrime and related phenomena over the next decade. The technology clusters included in the study were shortlisted from a broader list of technologies on the basis of their expected:

- **Likelihood of adoption** (i.e. the extent to which a given technology cluster is expected to be widely used and adopted, or not, for cybercrime purposes in the next decade).
- **Impact** (i.e. the extent to which a technology cluster is expected to change or influence cybercrime in the timeframe considered, either from a defender or criminal perspective).
- **Relevance to Estonia** (i.e. the extent to which a technology cluster is expected to bear implications for the Estonian context specifically in the next decade).

The technology clusters considered and included in the study were identified as a result of horizon scanning, desk research, and expert and stakeholder consultation activities. These include:

- **Artificial intelligence and machine learning**
- **Autonomous devices and systems**
- **Computing and data storage technologies**
- **Telecommunications infrastructure**
- **Internet of Things**
- **Privacy-Enhancing Technologies**
- **Blockchain and Distributed Ledger Technologies**

Figure 1: Overview of cybercrime

CYBERCRIME

No clearly articulated and globally-accepted definition of cybercrime, a complex phenomenon influenced by many different actors and technological and socio-economic drivers

Europol defines cybercrime as *criminal acts that are committed online by using electronic communications networks and information systems*

Cyber-enabled crime refers to existing crimes that have been transformed in scale or form by the use of the Internet

Cyber-dependent crime employs a digital system as the target as well as the means of the attack

CLASSES OF INCIDENTS

Malware
Software designed to perform undesirable operations.

Intrusion attempt
Attempts to intrude by exploiting vulnerabilities in a system, component or network, or to log in to services or authentication/ access control mechanisms.

Fraud
Misuse or unauthorised use of resources, as well as false representation, which results in a loss of property caused with fraudulent or dishonest intent.

Availability
Attacks designed to disrupt the processing and response capacity of systems and networks in order to render them inoperative.

Intrusion
Actual intrusions that exploit vulnerabilities in a system, component or network, or achieved by compromising a user or administrator account.

Abusive content
Distribution of so-called SPAM messages, as well as of copyright-protected content or of content forbidden by law.

Information gathering
Active and passive gathering of information on systems or networks, unauthorised monitoring and reading of network traffic, and attempts to gather information through phishing.

Information security
Unauthorised access to, change, or elimination of a particular set of information.

Other
Unclassified or undetermined incidents not represented in other categories.

DRIVERS

Technological change
Leveraging of technological advances and increased connectivity

Social and economic drivers of crime
Poverty, lack of social cohesion, lack of access to housing, employment, education and health services

Environmental factors
Opportunities to commit crimes including connected and global aspect of the Internet, prevalence of exploitable vulnerabilities, ease of anonymity, speed of offending

Lack of criminal justice responses
Law enforcement challenges in investigating cybercrime, difficult in prosecution, lack of cross-border cooperation and international responses

ACTORS AND MOTIVATIONS

Individuals
Individual interest
Personal gain
Fame
Challenge

Hacktivists
Ideology

Organised Crime
Financial gain
Access to other systems

Nation state and state-sponsored actors
Espionage
Exploitation

COST

Challenging to estimate costs

Limited data collection due to concentrated losses, unverified self-reported numbers

Can have severe realised costs and damage and disrupt functioning and operations of contemporary societies

NotPetya affected government agencies, hospitals; power companies, shipping companies; airports; banks; ATMs

Other technology clusters expected to have an impact on cybercrime in the future were considered but ultimately not included in study's in-depth assessments due to their being perceived in the literature and by experts consulted as (i) comparatively less relevant to, and potentially impactful on, cybercrime than other clusters; and/or (ii) being more than ten years away from reaching a sufficiently mature level of development and readiness for use. These secondary technology clusters include: quantum computing, bio-technologies, human-machine interfaces, and advanced manufacturing.

Figure 2 provides an overview of new and consolidating technology clusters considered, as well as of their uses, applications, and potential implications for cybercrime.

Conclusions

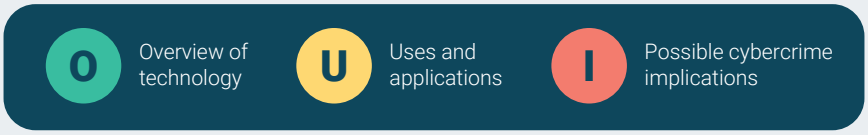
Recent decades have seen a revolution occurring in ICTs and in the use of IT in contemporary societies. ICTs and IT technologies have seen a growing uptake among individuals, enterprises and institutions, becoming intimately embedded in all aspects of human life. Technological advancements provide significant opportunities and have had wide-ranging effects on contemporary societies, affecting economy, education, health, politics, security, defence, private life, and society at large.

Technological developments identified in this study are expected to have similar effects in the coming decade on contemporary societies, including on Estonia. Furthermore, technological change and development may occur at such a pace, and have such wide-ranging impact, that society and institutions both in the public and private sectors could struggle to cope with these changes.

This study highlights some of the implications that may stem from developments in the next decade within individual technology clusters considered (see Figure 2). Crucially, however, technologies will not operate in silos, but rather build on and interact with one another in ways that will result in additional, broader trends, opportunities, and challenges. From a cybercrime perspective, an array of cross-cutting trends and implications for cyber-enabled and cyber-dependent crimes should therefore be highlighted and considered. Relevant trends and implications include:

- **Exacerbation of current trends and grey swan scenarios**. Advances in new and emerging technologies are likely to contribute to a continuation and exacerbation of current cybercrime trends and activities. The increasing availability of more powerful, easier to use, and less expensive technologies is likely to further stimulate the conduct of cybercrime activities by a wide array of individuals with an interest in making quick financial gains. In addition, the development of new, complex technological solutions and capabilities may enable cybercrime professionals, organised groups, and state-sponsored actors to conduct complex attacks and activities, resulting in higher criminal returns and, potentially, nefarious impacts on the stakeholders and individuals targeted.
- **Increased speed and coverage of connectivity.** In light of expected technological developments, particularly in telecommunications infrastructure and IoT, the next decade will likely see an increase in the speed of connectivity. These advances will contribute to reducing even further the impact that geographical distances have on telecommunications. This trend will be compounded by an increase in the volume of connected devices in the world in light of the growing availability and use of personal and IoT

Figure 2: Overview of new and emerging technologies of interest



Artificial Intelligence (AI) / Machine Learning (ML)

O AI is a science that aims to develop intelligent machines and to find methods for solving complex problems that can only be solved based on large amounts of data and human-like perception, conversation and/or decision-making capabilities.

O ML is the science of creating intelligent computer programs that can automatically improve their performance through experience.

U AI/ML is used in many fields to make systems more efficient and scalable, and for tasks that exceed the capabilities of humans.

I AI/ML could increase the automation, speed, frequency, and efficiency of attacks and increase the potential for these to be flexibly tailored to target different individuals, groups, or institutions.

I AI/ML could increase the speed of cyber detection, prevention and recovery systems or be used to fill vacant domain specialist positions or replace specialists in certain areas of cybersecurity.

Autonomous Devices and Systems

O Autonomous systems combine intelligent software-based systems with hardware devices and can achieve their goals independently, requiring limited to no external control and supervision.

U Autonomous systems are value-adding systems that can replace or reduce human engagement to help increase productivity, reduce costs and enhance safety, penetrate spaces that were previously inaccessible to humans, or assist humans in carrying out complex tasks thereby expanding human capabilities.

I Autonomous systems may be employed to carry out disguised criminal acts, develop new criminal modi operandi, or conduct large-scale and automated attacks. Autonomous systems may increase complexity of forensic investigations and attribution issues for crimes or incidents caused by autonomous devices.

Computing and Data Storage Technologies

O Computing power and data storage technologies are fundamental enablers which allow the capture, manipulation, and storage of data by IT devices. Computing and data storage technology advancements comprise a variety of solutions including miniaturised supercomputers and smart dusts, AI computing, cloud data storage systems, holographic data storage, and others.

U Computing and data storage technologies are fundamental enablers for the day-to-day functioning of contemporary societies and economies, from powering IT devices employed by individuals to enabling the performance and management of complex operations by transnational companies and governments alike.

I The development and ubiquity of computing and data storage technologies could facilitate the exfiltration of data, storage and dissemination of non-consensual recordings and illicit data, as well improve and automate the detection of financially motivated but nonviolent crimes.

Telecommunication Infrastructure

O Telecommunication infrastructure comprises the physical and digital infrastructure that enables information to flow across the Internet and between devices.

U Advances in technology in the context of telecommunication infrastructure aim to increase bandwidth, decrease latency, and increase spectral efficiency of telecommunications, accelerating the process of making the world connected and digitalised.

I Technological advances could be leveraged to enhance the anonymity, speed and capacity of criminal activities or to exfiltrate personal and sensitive data. Telecommunication infrastructure could also be targeted to cause large-scale disruption.

Internet of Things (IoT)

O IoT encompasses a set of applications, capabilities, services and infrastructure that collectively provide the intelligence needed to enable the connectivity and enhance the utility of new connected objects and devices.

U IoT encompasses a wide range of models, devices and applications such as wearable technologies, smartphones, and domestic appliances designed to increase connectivity and efficiency of traditional devices.

I Growing volumes of data collected by IoT devices could become vulnerable to theft, corruption, destruction, extortion, or sale. IoT devices are also likely to increase the attack surface for cyber-dependent crimes and introduce new vulnerabilities in complex IT systems and environments.

Privacy-Enhancing Technologies (PETs)

O PETs aim to minimise data collection and secure personal information circulating online, enabling data sharing through telecommunication structures while ensuring that these remain anonymised or concealed.

U PETs can enhance online privacy and help businesses and service providers comply with applicable laws and regulations. PETs could also be leveraged to securely and legally collect large amounts of data to conduct large scale analysis and investigations.

I PETs could be leveraged by malicious actors to pursue illicit activities anonymously and secretly, making it increasingly difficult to detect, monitor and investigate criminal activity. PETs could also be targeted by malicious actors to access confidential or private information.

Blockchain and Distributed Ledger Technologies (DLTs)

O The blockchain and DLTs cluster refers to decentralised public ledgers that record all transactions occurring across a peer-to-peer network and which do not require a trusted central authority to authorise transactions but rely on peer group according to consensus protocols.

U DLTs are reportedly more efficient, secure and transparent than traditional financial tools and may be used to transfer ownership of assets, including digital assets, financial assets, property assets and public registries.

I As transactions become digitalised and processed through DLTs, these technologies could be manipulated for malicious purposes for instance by preventing transactions from being processed or by hacking its consensus. DLTs could also be leveraged to store disruptive or inappropriate content making it difficult to be removed.

devices, including also in developing countries. This trend is expected to contribute to an overall increase in the volume and speed with which different types of cybercrime are conducted.

- **Increased attack surface and vulnerabilities.** An additional trend expected to stem from the proliferation of autonomous devices and systems, IT and IoT devices, as well as different ICT-enabled services and products, pertains to an increase in the attack surface and vulnerabilities that could be leveraged by malicious actors. This is project to have significant repercussions both in the physical and cyber domains. The development and adoption of devices and products with poor security standards and safeguards, particularly as regards IoT and autonomous devices and system, are expected to expand the existing landscape of vulnerabilities that can be leveraged by malicious actors.
- **Increased ability to record, generate, store, access, and manipulate data.** Developments in the fields of computing and data storage technologies, paired with a proliferation of devices, are expected to result in an increased ability to record, generate, store, access and manipulate data. The proliferation of existing sensors across a growing number of devices, as well as the development and use of new sensors, for example in the context of IoT and autonomous devices and systems, will expand data collection capabilities and contribute to the development and collection of new data types. This trend is expected to be compounded by advances in data storage technologies which should result in increased data storage capabilities and in a quasi-ubiquitous accessibility of data through technologies such as cloud storage. This trend is expected to contribute to an increase in the variety of criminal and malicious activities that could be conducted, including the development of new techniques and modi operandi.
- **Increased ability to process and analyse data.** Advances in computing power, accompanied by developments in the fields of AI and ML, are expected to contribute to a growing ability to process and analyse data, allowing to infer from these new insights and results which are currently beyond the reach of human and IT analytical capabilities. The impact of advances in analytical capabilities through growing computing power and stronger AI/ML capabilities is expected to be exacerbated by advances in the overall data capture and storage capabilities. These advances are expected to contribute to the development of new forms of cybercrime and malicious activities, as well as to an increase in the volume of already existing ones.
- **Increased difficulty in attributing and tracking criminal and malicious activities.** Advances in the fields of AI/ML, autonomous devices and systems, and telecommunications, are expected to result in increasing complexity as regards the tracking and attribution of criminal and malicious activities. This is expected to contribute to an increase in the attractiveness and perceived clout of unaccountability of cybercrime, putting increasing strains on law enforcement agencies and prosecution services.
- **Consolidation of the internet economy and growing reliance on limited proprietary technologies.** A small number of companies operate some of the most popular services on the internet and are now developing and offering a number of enabling technologies and services. The consolidation of the internet economy around a limited number of

key players, and an increasing societal reliance on their products and services, may raise significant challenges. First, this could contribute to the widespread embedding of vulnerabilities with the potential to yield large-scale systemic effects when leveraged. Further, reliance on technologies, products and services stemming from companies located outside the EU raises questions as to Estonian or European ability to investigate cybercrime conducted in or through these services, as well as influence these companies to improve their cybersecurity posture or regulatory compliance.

- **Eroding trust in technology and associated products and services.** The degree of penetration and pervasiveness that new and consolidating technologies will reach in the next decade is expected to expand the scope of crimes and malicious activities with a cyber component. Within the span of a decade, a growing degree of illicit and criminal activities are likely to embed a cyber-enabled or cyber-dependent tactic or component. Furthermore, as discussed above, greater dependence of critical infrastructure and of the general day-to-day functioning of societies on such technologies is expected to increase the volume and impact of any vulnerabilities and disruptions associated with them. These vulnerabilities may also have cascading effects, which may be difficult to predict or mitigate in increasingly complex and non-linear systems. In this context, individual failures or potentially inconspicuous instances of crime may result in a much broader impact due to previously unforeseen linkages and embedded co-dependencies. These trends, compounded by a potential lack of institutional safeguards and regulations pertaining to the security of ICT products and services, may lead to a growing feeling of distrust towards new technologies and public institutions from different stakeholder groups (e.g. private sector; general public).

Lastly, it should be noted that while this study focuses on the impact that technological advances may have on cybercrime, a wide variety of other non-technical drivers and factors are expected to influence this phenomenon over the coming decade. In particular, policy- and decision-makers should consider the expected impact of factors such as:

- **Social and economic drivers of crime.** These include for instance motive and opportunity stimulated by issues of poverty, lack of social cohesion and opportunities, or limited access to education, employment, health services and housing.
- **Environmental factors.** These include opportunities to commit cybercrimes and other illicit activities stemming from permissive environments with limited cyber-related laws and regulations in place or with structural limits in their ability to prevent and tackle cybercrime.
- **Challenges with criminal justice responses.** These include challenges and limits in criminal justice responses associated with criminal investigation and difficulties in prosecution, as well as lack of or limits to cross-border cooperation and international responses.

Recommendations for policy action and investments

In light of findings identified through study activities, the study team formulated recommendations for Estonian authorities to consider for implementation. The study team sought to develop recommendations

Figure 3: Overview of strategic recommendations

Source: RAND Europe analysis

that address the perceived change driven by technological developments, as well as perceived weaknesses or opportunities for action in the Estonian context.

While these recommendations build on the outputs of the study, neither the Estonian authorities nor the RAND study team have yet conducted further analysis of their practical implementation or associated resource requirements. Each of these recommendations emphasises a distinct type of intervention required to create a more holistic approach to combatting cybercrime, and presents options for Estonia to engage with, either on its own or in collaboration with other actors. Figure 3 provides an overview of the three strategic recommendations formulated.

In addition to the individual recommendations, the study team emphasises four overarching factors to consider when pursuing future cybercrime policy and associated interventions:

- **Stakeholders desire for a broad range of initiatives.** Regardless of which technologies ultimately have the largest impact on Estonia in the future, it is likely that the Estonian authorities need to engage in a wide range of strategic and policy measures to adequately address the future of cybercrime. None of the recommendations provided are mutually exclusive, nor are any of them sufficient on their own. In contrast, it is likely that the most meaningful progress can be achieved through a combination of options and mutually-reinforcing policy interventions.
- **An emphasis on technology-agnostic approaches.** While the study has highlighted a small number of technology areas as potentially more challenging than others, most policy options are relatively

technology-agnostic. There is a need to strike a balance between targeted interventions aimed at specific technology developments (e.g. AI, autonomy or IoT technologies) and more general resilience-building measures aimed at cybercrime and technological change more broadly (e.g. public awareness and education initiatives).

- **The importance of multi-stakeholder solutions.** As with other areas of cybersecurity, cybercrime affects all parts of society and requires the government, law enforcement agencies, private sector organisations, academia and civil society to work together to design, implement and operate appropriate interventions. This does not mean that the Estonian government should rely on other actors to take the lead, but rather that Estonian authorities should focus on finding the way forward that best leverages its partnerships, both nationally, in the EU, and globally, to meet the challenges posed by the future of cybercrime and technological change.
- **The need for prioritisation of resources.** Technology trends discussed in this study may have a profound impact on cybercrime and society at large, as well as presenting significant challenges to the Estonian authorities. While there is a plethora of policy directions that Estonian authorities could pursue, resources are finite, which means that choices and trade-offs are inevitable. Any further action by the Estonian authorities should therefore be preceded by a period of analysis and reflection as to which direction is best to pursue – and in which areas the Estonian government should take the lead or otherwise.

With these considerations in mind, Figures 4, 5 and 6 provide a more detailed overview of each of the recommendations and their supporting actions to help inform future Estonian decision making.

Figure 4: Overview of Recommendation 1

Recommendation 1: Pursue broad cybercrime capacity building in light of technological development

Strengthen the overall cybersecurity resilience of Estonia through awareness, education and capacity building.

Supporting actions:

- Development and implementation of a nation-wide cybersecurity and cybercrime awareness programme
- Further invest in integrating cybersecurity into primary and secondary education
- Strengthen higher education and research on emerging technologies
- Explore the need for targeted professional development for cybercrime professionals

Figure 5: Overview of Recommendation 2

Recommendation 2: Seek legal, regulatory and organisational agility

Prepare the Estonian legal, regulatory and organisational environment to adequately respond to cybercrime challenges resulting from technological change.

Supporting actions:

- Explore the need for regulatory or legal intervention in relation to technologies of interest
- Explore the relevance of a national cybersecurity competence centre
- Further develop Estonia's contribution and participation in international cooperation to counter cybercrime and strengthen cybersecurity resilience

Figure 6: Overview of Recommendation 3

Recommendation 3: Invest in technologies relevant to the Estonian context

Ensure that Estonia has sufficient technological expertise, skills and research in relation to high-priority emerging technologies.

Supporting actions:

- Identify the technology investment needs for Estonian law enforcements and justice systems
- Identify technology investment opportunities to improve Estonia's technological readiness