How could technological developments influence the future of cybercrime?
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.

RAND Europe was commissioned by the European Commission Structural Reform Support Service (SRSS) to conduct a study requested by the Government of Estonia (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 technological change on cybercrime, including both cyber-dependent and cyber-enabled crimes.
3. Proposing possible ways to prevent future technologies from being exploited by criminals for these purposes.

To meet the study objectives, the research included:

1. Policy and literature review
2. Technology horizon scanning
3. Expert and stakeholder consultations
4. Table-top exercise
5. Reporting and dissemination
Study results

There is no clearly articulated and globally accepted definition of cybercrime. 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. Most cybercrime has real-world implications despite its virtual context. The cost of cybercrime is difficult to estimate or calculate, but actual realised costs of cyber incidents can be severe.

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 and expected impact in the next decade, as well as of their expected relevance for Estonia.

Artificial Intelligence (AI) / Machine Learning (ML)

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.

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

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.

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

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

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

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.

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

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 advances comprise a variety of solutions including miniaturised supercomputers and smart dusts, AI computing, cloud data storage systems, holographic data storage, and others.

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.

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

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

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.

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)**

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.

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.

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)**

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.

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.

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)**

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.

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.

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.
Technologies analysed 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 be considered:

**Exacerbation of current trends and grey swan scenarios.**
Technological advances are likely to contribute to a continuation and exacerbation of current cybercrime trends and activities, as well as to the development of new, complex technological solutions and capabilities.

**Increased speed and coverage of connectivity.**
The next decade will likely see an increase in the speed of connectivity. This will contribute to reducing even further the impact that geographical distances have on telecommunications.

**Increased attack surface and vulnerabilities.**
The proliferation of existing devices as well as different ICT-enabled services and products will lead to an increase in available attack surface and vulnerabilities that could 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. This could contribute to an increase in the variety of criminal and malicious activities conducted.

**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. This could result in an ability to infer from available data new insights and results which are currently beyond the reach of human and IT analytical capabilities.

**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.

**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 offer enabling technologies and services. The consolidation of the internet economy around a limited number of key players may raise challenges by embedding vulnerabilities with the potential to yield large-scale systemic effects when leveraged.
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 that address the perceived change driven by technological developments, as well as perceived weaknesses or opportunities for action in the Estonian context.

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.

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.

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.

Source: RAND Europe analysis

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.

• **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.

• **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.

• **The need for prioritisation of resources.** Technology trends discussed may have a profound impact on cybercrime and society at large. 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.