CYBERSECURITY EDUCATION IN ESTONIA: BUILDING COMPETENCES FOR INTERNAL SECURITY PERSONNEL

Piret Pernik, MA
NATO CCD COE
Researcher

Keywords: cybersecurity and cybercrime curriculum, cybersecurity and cybercrime knowledge, skills, and abilities of law enforcement, the internal security sector

ABSTRACT

Currently there is no formal cybersecurity education for internal security first-responders in Estonia. The Estonian Academy of Security Sciences (EASS) does not provide this education at basic (all students) and advanced (cybercrime investigators) levels. The Estonian government has highlighted the need to improve the cybersecurity competence of mid-level and senior civil servants in the administrative area of the Ministry of the Interior.

In this context, this article gives an overview of cybersecurity formal education and extra-curricular initiatives in Estonia, including those supported by the Ministry of Defence. It further gives a snapshot of the state-of-the-art cybersecurity education in the police academies of Finland, Germany, the Netherlands, and Norway, as well as of other international competence building frameworks. The author recommends several policy solutions in order to improve digital skills, cybersecurity and cybercrime competences of future internal security personnel. The following aspects should be considered in competence building: the existing frameworks, best practices from foreign police universities and academies, and developing closer cooperation with the Estonian Defence Academy, TalTech, and the Ministry of Defence.

INTRODUCTION

The functioning of the Estonian economy and society depends to a large degree on the digital environment. Estonia is a leading country in Europe in public e-services, and is also considered a leader in digital transformation and e-governance. In cybersecurity Estonia ranks fifth globally (International Telecommunication Union, 2018). Digitisation brings to public administrations and private sector companies great socio-economic benefits. It brings efficiencies and cost savings, enhances business transactions. Digital tools that increase transparency and accountability also support the strengthening of democracy by reducing opportunities for corruption.

Emerging technologies, such as artificial intelligence (AI) narrowly defined, bring great opportunities to governments and militaries, as well as for law enforcement agencies. The European law enforcement agencies have begun to use AI systems in order to reinforce their investigative capabilities and strengthen digital evidence (Craglia et. al., 2018). For example, machine learning tools enable more proactive policing to be conducted and improve data analysis and identity checks (European Commission, 2019a).[1] They can aid police to prevent crimes and send out patrols to urban districts where there is more crime, track illicit money flows, predict criminal and terrorist action, identify suspicious behaviour, persons of interest and stolen vehicles, discover criminal patterns, and detect, target and interdict crimes (Ibid, 2019). In Norway and Poland the law enforcement agencies use machine learning tools in order to identify online child exploitation material and monitor disinformation campaigns (Skattor, 2019).

On the flip side, digitisation of almost every aspect of society brings greater cybersecurity risks. Negative tendencies of new technologies

[1] According to the definition provided by the European Commission AI refers to a machine or algorithm that observes and learns from its environment, and based on this knowledge and experience, can take intelligent actions or propose decisions. Common AI technologies are machine learning, data science, robotics, internet of things and use of big data (European Commission, 2019a). The term AI refers to a constellation of AI-related technologies of which four are the most crucial: more narrowly defined AI, machine learning, big data and Internet of Things (Wright, 2018).

illustrated by the growth of cybercrime and more complex, coercive and destructive cyber-attacks that have in recent years inflicted costs worth billions of euros (for example notPetya malware in June 2018). Cyber-attacks threaten national security and public order. For example, in September 2019 Iran used a swarm of drones to attack an oil refinery in Saudi-Arabia, which caused loss of production and affected global oil prices (Kirkpatrick and Hubbard, 2019). Drone exploit toolkits and malware for smart home devices are already traded on the digital dark market, while designer psychedelic drugs, which are not designated as illegal, are sold in internet forums (McAfee, 2018; Silberglitt, et. al., 2015). Criminals will be able to hack personal medical devices (such as pacemakers, heart rate and blood glucose monitors among others) and produce guns with 3D printers (Silberglitt, et. al., 2015). Drones can also be used for smuggling and espionage, autonomous cars can be hijacked or used for launching cyber-attacks, and automated tools are used for software vulnerability scanning.

AI tools will enable cybercriminals to become more agile and better in circumventing protections (McAfee, 2018). Technological development and digitisation (for example employment of 5G and Internet of Things) will expand both cyber-attack vectors and surface. New vulnerabilities have already emerged from storing huge amounts of data in clouds and from Internet of Things devices which commonly lack cybersecurity standards. The complex ICT supply chain with third-party-dependencies is increasingly difficult to secure against software and hardware vulnerabilities, and cyber-attacks through a long chain of vendors and subcontractors. Many scholars and industry experts have assessed that in the coming years cybercriminals and adversary nation states and groups supported by them will use various emerging technologies to commit new crimes with the aim to impair national security.[2]

[2] Game-changing (also called emerging and disruptive) technologies include autonomous devices and systems, artificial intelligence and machine learning, advanced robotics, virtual and augmented reality, blockchain/distributed ledger technologies, Internet of Things, additive manufacturing (also called advanced manufacturing and 3D printing), quantum computing, data storage technologies such as cloud, human-machine interface, telecommunication technologies such as 5G, biotechnologies, privacy-enhancing and anonymisation technologies, etc.

In this context this article discusses introducing digital skills, cybersecurity and cybercrime study themes into the internal security formal education system. The main research questions are the following:

- What is the status of formal (primary, secondary and tertiary level) cybersecurity education and extra-curricular training in Estonia?
- How can the internal security personnel's competences be efficiently and effectively increased by the existing extra-curricular activities? How can the EASS cooperate with other education providers in Estonia in order to benefit from the existing formal and extra-curricular offer?
- What can Estonia learn from best practices in other countries and international organisations in order to develop a basic and advanced formal education curriculum for internal security personnel?
- What type of courses should the EASS develop on its own and which international courses are available for EASS cadets and students, as well as the internal security personnel?

The central research objective is to identify, based on the document analysis and expert opinions, a number of study themes to be included as of autumn 2020 into vocational and bachelor study programmes of the Estonian Academy of Security Sciences (EASS). In order to achieve this research objective and answer the above research questions the author conducted desk-research comprising of academic and specialist literature reviews, existing curricula, competence building frameworks and other relevant documentation. The author conducted several face-to-face and email interviews with domestic and foreign subject matter experts. Insights were also gathered from two working meetings with subject matter experts in Estonia, and an international working meeting in Finland.[3]

[3] Two working meetings were held and face-to-face and email interviews were conducted by the author between February and September 2019. Three in-person interviews were conducted with teaching personnel from police academies in Finland and Germany, and from TalTech in Estonia, which were followed up by a number of email interviews. The author took notes from discussions at the working meetings with experts from the Police and Border Guard Board and the EASS, and incorporated these insights into research results. The best practices from Finland, Germany, the Netherlands and Norway were collected from a literature review, during the interviews and in a working meeting in April 2019 in Tampere.

The article gives a snapshot of the existing cybersecurity education in the police academies of Finland, Germany, the Netherlands and Norway.[4] It does not aim to present representative research results of the current best practices in Europe, but rather it outlines the Estonian approach comparing it with other countries and international-level activities in Europe.[5]

[4] The police academies in the four countries were chosen because they had recently introduced cybersecurity into the curriculum, and the Estonian Academy of Security Sciences had close working relationships with them. This enabled the author to learn from recent experience and gave access to subject matter experts who were responsible for the matter. In the future research, best practices from other police academies (for example, in the UK, US, other Nordic countries, Latvia and Lithuania) could be analysed as the current overview four countries are not representative of the trans-Atlantic, European or Nordic-Baltic best practices. The scope of the current research did not enable including more countries.

[5] This article presents only preliminary results from a longer research project. At this stage of the project data was gathered with qualitative methods (literature and document reviews, interviews and meetings) and results have not been validated with other qualitative and quantitative research methods (such as questionnaires, focus groups). The following phases of the research project should include validation.

1. CYBERCRIME PHENOMENA AND CYBERCRIME COMPETENCE OF CIVIL SERVANTS

First responders at a crime scene must have basic knowledge of cybercrime investigations in order to be able to detect, target and interdict crimes.[6] Cybercrime phenomena can be divided for legal discussion purposes into two categories: cyber-enabled and cyber-dependent crime. However, it is expected that in the near future most crime investigations will have some digital component and for the day-to-day police work of first responders this distinction may no longer be relevant.[7]

Cyber-enabled crimes are those criminal acts that are committed by the use of ICT. The European Commission distinguishes between three types of cybercrime:

- Crimes specific to the internet, such as attacks against information systems or phishing (for example, fake bank websites to solicit passwords enabling access to victims' bank accounts).

- Online fraud and forgery – large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.

- Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia (European Commission, 2019b).

Cyber-dependent crimes are traditional crimes that have greater impact and volume in the digital environment (for example, cryptomining and

[6] In this article internal security sphere personnel denotes all personnel working in the administrative area of the Ministry of the Interior, as well as cadets, students and staff of the Estonian Academy of Security Sciences.

[7] With the adoption of new technology, the boundaries between traditional crimes committed through ICT and so called pure cybercrimes have become blurred.

ransomware, attacks against critical infrastructure, and data breaches) (European Union Agency for Law Enforcement, 2018).[8]

The most common types of cyber-attacks are distribution of malware (especially ransomware), denial of service attacks, phishing, unauthorised access, intrusion by exploitation of vulnerability, fraud and abusive content (Europol, 2017). Also, data breaches have been growing exponentially in the last decade. This is a concern for law enforcement agencies who collect and transit large data bulks (for example, images, videos, geospatial intelligence, communication data, traffic data and data on financial transactions, etc.). The confidentiality, availability and integrity of data and ICT systems and networks must be protected not only against outsiders, but also against unintentional insider threats and technical mishaps.

The European Commission has recognised that criminals have greatly benefitted from technological development, but unfortunately measures for countering cybercrime are lagging behind (European Commission, 2019b). Moreover, this negative situation is exacerbated by a lack of cybersecurity specialists in Europe and North-America, as well as a low level of cybersecurity awareness in society as a whole. For example, by 2021 the lack of unfilled cybersecurity jobs will grow worldwide to 13,5 million (Cybersecurity Ventures, 2019a). By 2022 Europe will face an estimated skill gap of 350 000 cybersecurity professionals (European Union Institute of Security Studies, 2019). Estonia will need by 2023 up to 870 cybersecurity professionals more than it has today – which means that the current cybersecurity workforce should be increased by 86% (Melesk, 2019). In addition to the specialist cybersecurity workforce, cybersecurity competence of civil servants in public administrations must be enhanced, and the requisite study subjects must be included into the formal curriculum of public administration schools and universities at all three education levels (primary, secondary and tertiary).

[8] The Council of Europe's Convention on Cybercrime defines cybercrime based on four types of offences committed: offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference and system interference); computer-related offences (computer-related forgery and computer-related fraud); content-related offences (offences related to child sexual abuse and exploitation); offences related to infringements of copyright and related rights (Council of Europe, 2001).

1.1 THE ESTONIAN EDUCATION SYSTEM, DIGITISATION AND CYBERSECURITY

According to Linnar Viik (2019), a recognised visionary who works as a programme director of the Estonian e-Governance Academy, in Estonia digital competence development has become a normal part of the education system. The same confidence cannot be expressed in regard to cybersecurity competence. The education system in the internal security sphere offers only one study programme at the master's level, which includes an elective cybersecurity and cybercrime course in scope of 3-6 academic credit points (EASS, 2019). There are no cybersecurity courses taught within the vocational and bachelors programmes.

In other Estonian vocational schools and universities technical cybersecurity-related courses have already been integrated in science, mathematics, engineering, technology (STEM) disciplines and in some public administration study programmes (for example, e-governance and technology policy programmes in TalTech). There are ICT-related non-technical courses available in the faculties of law and social sciences at Tartu University (for example, the information technology law and international relations study programmes). In some other faculties (humanities, medicine, earth sciences), however, no cybersecurity or ICT-related study courses have been included, even though the Estonian health care system is almost fully digitised (Melesk, 2019). Likewise, in the Estonian Defence Academy which provides formal education for the Estonian defence forces, cybersecurity subjects are currently present to a small extent in a few further specialisation areas such as communications.

1.2 CYBERSECURITY CHALLENGES OF THE ESTONIAN INTERNAL SECURITY SPHERE

In Estonia, internal security is considered part of a comprehensive defence principle, which consists in addition to upholding the internal security itself from other activities in four areas:

- Military defence
- Civilian support to military

- International action
- Government functioning, including the protection of essential services; and strategic communications (Government Office, 2017).

Cybersecurity is essential in ensuring the functioning of the government, society and economy as cyberspace permeates these four activity areas of a comprehensive defence approach. Whereas the Estonian Defence Forces have created advanced cyber capabilities such as cyber command, cyber range, and the Cyber Defence Unit of the Estonian Defence League, cybersecurity investments in the internal security sphere are lagging behind.

As a rule, law enforcement agencies in Europe are responsible for the prevention and response to cybercrime, curbing online disinformation and child abuse, as well as tracking and countering extremist activities in cyberspace. In Estonia, law enforcement is also responsible for issuing digital/electronic identity (e-ID) for citizens, residents and e-residents.[9] In the Estonian digital ecosystem a secure e-ID is a key component without which most of the essential services cannot be provided.

The Digital Agenda 2020 for Estonia includes the National Cybersecurity Strategy 2019-2022. The strategy assesses that in the next four years online criminal malevolence and economic loss resulting from it will further increase (Ministry of Economic Affairs and Communications, 2018a). A dramatic rise in cybercrime is predicated to cost $6 trillion annually worldwide, whereas costs from ransomware are predicted to exceed $20 billion by 2021 (Cybersecurity Ventures, 2019b). Globally the five most attacked industries are healthcare, manufacturing, financial services, government and transportation (Cybersecurity Ventures, 2019b). In Estonia, for example, tax, healthcare and financial services are almost exclusively digitised and thus especially vulnerable to cybercrime attacks. Since the early 2010s cybercrime has been growing in Estonia and the cost of cybercrime has doubled since the mid-2010s. For example, the number of digital fraud cases have doubled when compared to 2014. In 2017, malware, including ransomware attacks made up 70% of the registered cyber incidents (Ministry of the Interior, 2019).

[9] In Estonia e-ID is issued to all citizens and residents, as well as e-residents. It is based on an electronic identification document that can be an ID-card, SmartID, mobile-ID, digi-ID, or e-resident digi-ID. About 3000 e-services are provided by public administration authorities and about 2000 e-services by private sector companies. Almost all bank transactions are conducted online.

Essential services – in particular critical services such as financial systems, transportation, energy, telecommunications and healthcare – have become key targets of state and non-state cyber threat actors. Indeed, private cyber threat intelligent companies report that state-affiliated adversary groups regularly target critical services, especially the financial and energy sectors, as well as the defence industry and government. It has been disclosed that state threat actors have had an intention to cause physical damage to the equipment, which could cause longer power disruptions and physical harm to humans (Greenberg, 2019).

In addition to malicious cyber-attacks conducted by state-affiliated and cybercrime actors, technical failures and unknown vulnerabilities in the supply chain can cause interruptions in the provision of essential services. For example, in 2017 Czech computer scientists discovered a critical firmware vulnerability that affected almost 800 000 Estonian ID-cards and the government had to replace them (Information System Authority, 2017). This example illustrates how vulnerable the Estonian information society is on individual components of the digital ecosystem, which is made up of various digital infrastructures, web platforms, registers as well as third party suppliers and service providers, while the exact interdependencies between these components are difficult to determinate. This in turn complicates effective risk analysis and management. Thus, even if only one component fails the impact on the continuous operation of essential services and the functioning of the government, economy and society can be serious.

Indeed, in Estonia almost all essential services depend on ICT components almost totally. The majority of services are connected to the internet at least to an extent. As of today, there are almost 5000 electronic-services (e-services) accessible for users, whereas the majority of public services are digital and paper back-up copies are not provided (Härma, 2018). E-ID provides secure digital authentication and signature through which the end-user can use e-services such as declaring taxes, signing contracts, performing online banking transactions, accessing medical record, etc. The end-user can also encrypt documents and transmit and receive encrypted documents. Thus, e-ID is a central component of Estonia's digital ecosystem and as such it is designated in national regulations as a critical service that is subject to stronger cybersecurity risk management measures (Emergency Act, 2017).

There are four key stakeholders (three in the public sector and one in the private sector) who are responsible for e-ID management. It is essential that their requisite roles and responsibilities are clearly defined in regulations and well understood by all stakeholders, including law enforcement agencies. The Police and Border Guard Board that itself lacks technical capacity in E-ID development issues (digital and physical) identification documents. The Estonian Information System Authority, in the administrative area of the Ministry of Economic Affairs and Communications, is responsible for e-ID software development. The third stakeholder is a private company SK ID Solutions who provides trust service that enable the use of e-ID. The Ministry of Economic Affairs and Communications is moreover responsible for organising continuity of e-ID authentication and digital signature services (Emergency Act, 2017). The Ministry of the Interior together with other authorities in its administrative area (the Police and Border Guard Board, the Internal Security Service, and the Rescue Board) is responsible for three areas of internal security activity that pertain to ensuring safety in cyberspace:

- Crime prevention and criminal investigation (including cyber-enabled and cyber-dependent crime).
- Counterintelligence.
- Investigation of national security incidents.

Considering these responsibilities cybercrime knowledge and skills, as well as personal digital safety skills are essential competencies for first-responders. In the administrative area of the Ministry of the Internal Affairs dozens of specialist information systems and registers are used daily. For example, the e-police digital solution gives each police patrol car a real-time online connection to numerous national databases and the EU's Schengen information systems (e-Estonia, 2019). First-responders must be able to use national and international ICT systems and registers safely, including Estonian personal identification registers. Digital safety skills need to be trained from entry level jobs to senior leadership as a lack of these skills may cause sensitive and personal data leaks that can have serious national security implications.

Also, the application of disruptive technologies such as machine learning is actively pursued in the internal security sphere. For example, the Police and Border Guard Board uses a machine learning solution that enables the location of police patrols to be predicted (Government Office, 2019). The Estonian government adopted in May 2019 a strategy, which in July 2019 was followed by an action plan, to accelerate AI implementation in the public and private sectors. As of today, 13 projects have been implemented in the public sector. The government will invest 10 million euros in the next three years (Government Office, 2019).

A study by the Estonian Academy of Security Science (2017) evinces that in the opinion of civil servants and the EASS cadets the latter's digital skills for using internal security information systems and databases are sufficient. However, the cadets are not confident in using the systems and cannot understand how data is created and transmitted between different databases, and what are the links and interdependencies between databases. This can lead to data corruption caused by human error, for example, if incorrect data is unintentionally inserted into one register that is replicated in or accessed from other registers. Moreover, the study determined that the cadets lack practical experience in using police information systems and registers (Estonian Academy of Security Science, 2017). Thus, even if the cadets believe their digital skills are sufficient, the lack of exposure to using police IT-systems and registers conceals the possible lack of digital safety skills. Most likely cadets' digital skills are better than their digital safety skills – a trend that is also prevalent in the general public. The study recommended that the EASS should give cadets a comprehensive view on interdependencies and links between police IT-systems and registers in a way that more general IT-knowledge will be linked to a work process (Ibid.). For example, the first-responder should understand how data is created and transmitted between the systems and how reliable it is.

In the area of data protection, EASS cadets had little knowledge about personal data protection regulations and encryption methods of data, as well as about processes and requirements for designating documents for official use (Ibid.). According to a recent opinion survey among the Estonian youth, 90% of young people use legacy digital authentication methods such as PIN codes instead of secure methods such as e-ID (Tarros, 2019). This illustrates that even though young people are considered digitally savvy, cybersecurity considerations tend to be an afterthought. In addition, the opinion survey identified that primary and secondary level education should give pupils more information about

Estonian e-services (Ibid.). This indicates that pupils and students alike would benefit from a better understanding of the Estonian digital ecosystem, including public and private sector e-services and e-solutions in order to enhance their digital skills and digital safety skills.

1.3 STRATEGIC GUIDELINES FOR COMPETENCE BUILDING IN THE ESTONIAN INTERNAL SECURITY SPHERE

The Estonian government has recognised that e-governance/e-state, the information society and e-services rely on strong cybersecurity, which is impossible to harness without an adequate number of quality specialised cybersecurity workers. The National Cybersecurity Strategy 2019-2022 sets out an objective of educating more technical cybersecurity experts. It also calls for developing cybersecurity competence across society, and all public servants (central government, municipal and local authorities) must possess a degree of cybersecurity competence (Ministry of Economic Affairs and Communications, 2018b).

The strategy highlights a need to provide cybersecurity formal education and in-service training for the defence forces and internal security workforce (Ministry of Economic Affairs and Communications, 2018b). The previous iteration of the strategy (National Cybersecurity Strategy 2014-2017) focused on cybercrime prevention in key activity areas. During that period, in July 2016 a new cybercrime prevention bureau at the Central Criminal Police of the Police and Border Guard Board was founded. During the present strategy period 2019-2022 the focus is on improving digital skills across the internal security workforce. In order to do so, cybersecurity study subjects need to be integrated into formal education and additional training provided to mid and senior level leadership.

In conjunction with these objectives set out in the National Cybersecurity Strategy 2019-2022, the Estonian government endorsed in September 2019 a Proposal for Updating the Internal Security Action Plan for 2020-2030. This strategic guideline recognises that the increasing number of cyber-attacks and emerging technologies will have a negative impact on internal security. The guideline recommends that the forthcoming Internal Security Action Plan for 2020-2030 must design ends, ways and means to offer solutions to the following security challenges in the area of cybercrime and e-ID management:

- How to build capacity in the internal security sphere for responding to challenges stemming from the development of disruptive technology.

- How to establish capacity of situational awareness about cyber incidents in the area of internal security.

- How to improve capacity to remove illegal content from the internet.

- How to ensure adequate deterrence against cybercrime (Ministry of the Interior, 2019).

Given that these are the most important challenges for the internal security workforce, the following cybersecurity competences should be emphasized in formal education and additional training:

- Enhancing the understanding of the cybercrime phenomena and its current trends, as well as preventative and response measures (including digital evidence);

- Enhancing the understanding of regulations, procedures and technical tools in removing illegal online content.

In summary, in order to implement the strategic guidelines as set out in the National Cybersecurity Strategy, the Proposal for Internal Security Action Plan, and the EU policies, the EASS must introduce cybersecurity courses in all curriculums (vocational, bachelor, master's programmes). In addition, extra-curricular activities and additional training initiatives for mid and senior leadership and technical cybercrime investigators should be created.

1.4 CYBERSECURITY FORMAL EDUCATION IN THE ESTONIAN INTERNAL SECURITY SPHERE

The EASS provides vocational, bachelor and master's programmes for internal security employees (police officers, rescue service officers, prison officers, and tax and custom officers). As of September 2020, the EASS plans to integrate cybersecurity subjects into two programmes: the vocational curriculum "Police Service" and bachelor curriculum "Police Officer".

The majority of EASS graduates begin their professional careers at the Police and Border Guard Board in the following positions: border guard, patrolling police officer, traffic police officer, district police officer, youth police officer, and crime investigator. Whereas each of these positions has few unique duties, basic digital safety and cybersecurity skills for first-responders largely overlap. For example, youth police officers should have a good understanding of online privacy and security. Crime investigators should be competent in acquiring and handling digital evidence. Therefore, the basic competences that should be developed at EASS are related to e-ID management, cybercrime and data protection. As discussed earlier, every civil servant must have requisite knowledge about the Estonian digital ecosystem and its interdependencies (e-state, e-governance, e-services, etc.). Employees of internal security must understand what are the roles and responsibilities of different public and private actors in maintaining e-ID. In addition, the entry-level civil servants must be aware of the government strategic cybersecurity objectives and policies, cyber threats, and impact of disrupting technologies to cybersecurity. Everyone should receive requisite knowledge on digital evidence and challenges posed to crime investigation by the use of encryption applications (for example, WhatsApp, Signal, Telegram).

2. BEST PRACTICE FROM INTERNATIONAL ORGANISATIONS AND OTHER COUNTRIES

A. NATO

NATO and the Partnership for Peace (hereinafter NATO) cybersecurity reference curriculum for military officers and public servants provides an example of the cybersecurity topics that could be included into the curriculum of national defence and police academies for non-technical mid-level professionals (Costigan and Hennessy, 2016). The recommended teaching methods include interactive components (examining case studies, practical exercises and demonstrations). Four themes of the NATO curriculum are considered relevant to internal security employees:

- Cyberspace and the Fundamentals of Cybersecurity.
- Risk vectors.
- International cybersecurity organisations and standards.
- Cybersecurity management in the national context (Ibid.).

For example, cybersecurity management in the national context includes a sub-theme of digital forensics that covers methods and tools for analysing data acquired from computers, networks, mobile devices, databases and sensors. These competences are necessary for all internal security employees.

B. THE EU

In February 2019 Europol developed a *Cybercrime Training Competency Framework* targeting law enforcement personnel who deal with cybercrime, including first-responders. The framework includes required knowledge and skills at basic and expert levels across three dimensions: management, technical and investigation skills. The framework is recommended to be used by EU member states for defining education and training requirements and the development of curricula (Sobusiak-Fischanaller and Vandermeer, 2019).

The EU has also created a *Cyber Competencies Career Path Matrix* in order to educate and train all military and civilian personnel who conduct Common Security and Defence Policy (CSDP) operations and missions. The training requirement analysis was conducted in 2019. The report of the training requirement analysis identifies tasks to be performed by civilian and military personnel, and respective competencies and skills required for performing them. It further identifies gaps in the existing training offer of the member states and EU education and training bodies, and proposes solutions to fill these gaps (including a list of new courses). The list of the suggested courses include the following areas of study: digital forensics, cybercrime investigation, and protection of critical infrastructure (European External Action Service, 2019).

Both documents (the framework and training requirement analysis) should be used by the EASS for developing cybersecurity curricula at a national level. The EU framework and analysis provides an overview of CSDP military and civilian personnel tasks and competencies (defined as knowledge, skills and abilities) that enable individuals to perform these roles as proficiently as possible. Similar assessment methodology could be used for developing competence frameworks and to design respective education and training courses at the national level.

C. THE UNITED STATES

The US has developed a nationwide NICE Cybersecurity Workforce Framework that “aims to codify cybersecurity talent; define the cybersecurity workforce in common terms; and tie the workforce’s various jobs, competencies, and responsibilities into a common architecture (Paulsen, et.al. 2012). Organisations in the public and private sector can use the NICE framework as a reference source from which to develop training that meets their needs. However, the NICE framework is suitable for education, training, recruitment and retaining of the technical cybersecurity workforce, while the non-technical internal security workforce needs a more social science based curriculum. To fill this gap, Kessler and Ramsay (2014) proposed a number of such cybersecurity courses. For example, a baseline course *Foundations of Information Security* targets all internal security students. The course includes a definition of information security, the need for this field of study, ethical and legal issues, risk management and planning, and information security technology (Ibid.).

D. FINLAND, GERMANY, THE NETHERLANDS, AND NORWAY

In Finland, Germany, the Netherlands, and Norway police academies teach basic cybersecurity and cybercrime knowledge at vocational and bachelor levels.

The Finnish Police University College (POLAMK) has integrated the secure use of IT and the use of a digital environment for crime investigation into bachelor and master's programmes (Toiviainen, 2019). POLAMK relies on cybercrime study materials of the European Cybercrime Training and Education Group, and cooperates in cybercrime advanced training with the European Union Agency for Law Enforcement Training (CEPOL) and the European Cybercrime Centre of EUROPOL (EC3). POLAMK runs several long-term education and training projects in the area of cybersecurity and cybercrime in cooperation with the Jyväsküla University of Applied Sciences. In 2018 a four-year €1.1 million project CYBERDI was initiated in the area of cybercrime prevention, awareness raising and capacity building in cooperation with the Jyväsküla University of Applied Sciences and several other domestic stakeholders (POLAMK, 2019a). A bachelor programme "Bachelor of Police Services" teaches cybersecurity and cybercrime themes as part of professional studies that provide the student with the vocational core competences required in policing. A course entitled "pre-trial investigation" includes the topics of cybersecurity environment, cybercrime, digital evidence, and the use of open source information and databases in police investigation (POLAMK, 2019b). POLAMK also provides education on open source intelligence (OSINT) as part of formal education and non-degree additional training. This type of training for employed internal security professionals covers three themes: digital forensics, OSINT and tactical investigation methods (Toiviainen, 2019).

As part of elective studies an English language e-course "First Responders E-learning Course on Cybercrime" offered by the European Cybercrime Training and Education Group can be chosen. In this course a student learns about cybercrime, the internet, encryption, dark web and virtual currencies, and acquires skills to identify and seize potential digital evidence. The course includes topics such as open source intelligence, cyber-enabled and cyber-dependent crimes, seizure of digital evidence, and technical knowledge of software and technology (POLAMK, 2019c).

In Germany the Federal University of Applied Administrative Sciences has integrated cybercrime subjects at bachelor and master's levels. A bachelor programme "Criminal Police Officer at the Bundeskriminalamt" includes several ICT, cybersecurity and cybercrime subjects as part of a mandatory module that focuses on the gathering and use of information by the police and the cybercrime phenomena. The module consists of 240 study hours and accredits 8 ECTS credit points. The key subjects are basic principles of ICT, gathering and use of information, cybercrime and requisite police tasks and action in this field. It includes knowledge on the German legal framework in this field, for example, covert surveillance (Federal University of Applied Administrative Sciences, 2019a).

Also, a master's programme "Public Administration Police Management" includes a module on police information gathering (150 study hours and 5 ECTS credit points), which has ICT and cybercrime subjects. In addition, as part of the programme, master's students can choose an elective course about cybercrime (150 study hours and 5 ECTS credit points).

The Federal University of Applied Administrative Sciences offers a formal education diploma-programme "Police service in the Federal police (Diploma in Public Administration)," which includes a small amount of cybercrime related subjects (in total 24 study hours) such as international cooperation in cybercrime prevention, digital evidence and police tasks concerning online fraud (Federal University of Applied Administrative Sciences, 2019b).

The Dutch Police Academy, which provides formal education at vocational, bachelor and master's level, offers a two-year master's level programme - Criminal Investigator for police cybercrime investigators.

The Norwegian Police University College runs several advanced digital forensics e-courses in English for cyber investigators that are open to partners from other Nordic countries (Norwegian Police University College, 2019). Since 2014 it also runs an English language master's programme on digital forensics and cybercrime investigation.

In addition to incorporating the cybersecurity subject to compulsory courses in formal education, several police academies offer in cooperation with domestic and international partners additional advanced cybercrime training for cybercrime investigators.

3. BEST PRACTICE IN ESTONIAN SECONDARY AND TERTIARY FORMAL EDUCATION

There are several extra-curricular activities in primary and secondary schools starting from grade four to twelve.[10] For example, a digital competence pilot test was introduced in 2018 for 1400 pupils and a model for assessing pupils' digital competencies is available (Innove, 2018). The Information Technology Foundation for Education (HITSA) supports schools in developing digital competencies and digital safety of pupils and teachers, and offers a wide range of IT-related courses. Another example is the ProgeTiger progamme that includes courses on programming, 3D design, mechatronics, robotics, etc. In addition, HITSA offers a Safer Internet initiative for children, pupils, youth, teachers and parents with learning and teaching materials (HITSA, 2019). Currently there are some elective courses on cyber security in upper secondary level and the Põltsamaa municipal gymnasium has an elective cyber security course. The syllabus of the Põltsamaa municipal gymnasium could serve as a reference curriculum for integrating cybersecurity to the EASS curriculum.[11] Study materials include both technical and non-technical subjects about the information society and digital safety.[12] However, elective courses, student competitions and exercises in high schools are not coordinated, and access is random rather than systematic (Meleski, 2019).

In tertiary education the IT College of Tallinn University of Technology offers an English language Bachelor of Science programme "Cybersecurity Engineering". TalTech and the University of Tartu offer a joint Master of Science program "Cybersecurity", which includes digital forensics courses.

[10] For an overview of IT and cybersecurity education in Estonia see Lorenz, Kikkas, Sõmer, and Laugasson, 2019.

[11] The syllabus is available at https://onedrive.live.com/view.aspx?resid=7B5915FDC0CD4BE4!9609&ithint=file%2cdocx&authkey=!AGo9f4nh7CguAjI

[12] The syllabus is available at https://drive.google.com/drive/folders/0B431U6eEm9oVY081WEhMaENQSFk

The University of Tartu has also integrated cybersecurity subjects to several non-technical programmes, for example, an elective course in the Master of Arts programme "International Law and Human Rights." Likewise, in the Faculty of Social Sciences programmes, cybersecurity is designated as one of the study objectives; however, at the Faculty of Arts and Humanities, the Faculty of Medicine and in Earth Sciences, cybersecurity-related study subjects have not been introduced (Praxis, 2019).

The TalTech master's programme "Law of Technology" has elective courses for cyber defence and law, e-governance, digital evidence and e-state IT solutions. Mandatory cyberspace-related subjects are regulations pertaining to the protection of ICT infrastructure, human rights, ethics and technology, as well as law on intellectual property. In addition, a master's programme "European Union and International Law" includes courses on cyber defence and law, legal aspects of e-governance, and the rights of internet users.

The TalTech master's programme "Technology Governance and Digital Transformation" focuses on various IT-subjects, and has an elective course on the fundamentals of information security. The "International Relations and European-Asian Studies" master's programme includes an elective course on cybersecurity, and the Faculty of Economics master's programmes include technology courses such as big data and registers. Also, the public sector leadership and innovation master's programme includes technology, big data, e-governance, and e-democracy courses. The TalTech master's programme on International Relations and European Studies, as well as the EASS master programme on Internal Security include an elective cybersecurity course.

Finally, TalTech has launched it's "TalTechDigital" initiative with an e-course "DigiWisdom" covering basic digital safety skills, which was piloted for academic and administrative staff in 2018 (Lorenz, Kikkas, Sõmer, and Laugasson, 2019).

3.1 BEST PRACTICE OF THE MINISTRY OF DEFENCE AND THE NATIONAL DEFENCE ACADEMY

The National Defence Academy does not provide cybersecurity courses as part of a master's programme. Both vocational and bachelor programmes contain few ICT-related subjects in only one specialisation area of the curricula (communications). For example, as part of specialisation in communications, the curricula of a vocational programme "Military leadership for Senior Non-commissioned Officers" includes subjects such as IT and cybersecurity foundations, and methods to ensure cybersecurity. Also, bachelor programmes provide to those students who specialise in communications tactical level knowledge on ICT and cybersecurity foundations. The bachelor programme also includes themes of cyber hygiene and cyber threats. However, those students who choose other areas of specialisation do not currently receive any cybersecurity education (The National Defence Academy, 2019).

The Ministry of Defence has launched a Cyber Olympic programme for young talent. It includes a CyberCracker competitions for two age groups at primary and secondary education level and a CyberSpike competition at secondary and tertiary level for ages 14-24 (Taltech, 2019a). Estonian youth teams participate at the annual European Cybersecurity Challenge competition.

Since 2015 the Ministry of Defence also supports a 35-hour advanced cybersecurity course in a Põltsamaa municipal gymnasium, as well as the integration of cybersecurity into national defence courses in gymnasiums and vocational schools. The national defence course gives an overview of cyber defence in the military, and a study book published by the Ministry of Defence includes a chapter on cybersecurity (Kaas, 2019).

As part of compulsory military service for male citizens (in Estonia, conscription is voluntary for females) a pilot cyber conscription programme was launched in 2016. There are plans to extend the current eleven-month duration of the cyber conscription service to twelve months (Err, 2018). Sõmer, Ottis, and Lorenz (2019) have suggested that cyber training of the conscription service should include subjects relevant for cybercrime investigators (digital forensics, open source and signal intelligence). According to these scholars, conscripts could receive a certificate of training after completion of service. They propose that such on-the-job training could be transferred to academic credit points or diplomas at IT and cybersecurity programmes in universities and vocational schools (Ibid.). Against this background, if cyber conscription will provide know-how on digital forensics and digital evidence, as well as open source and signal intelligence, the conscription service could be used as a recruitment base for cybercrime investigators of the Central Criminal Police.

The Cyber Defence Unit of the Estonian Defence League is a public-private and civil-military cooperation model that pools cybersecurity talent and skills from the public and private sector in order to support national level cybersecurity. The unit can be assigned a task of assisting public and private sector companies in protecting essential services, as well as municipal and local authorities where the level of cybersecurity tends to be lower. The members come from diverse technical and non-technical (legal, policy, academic, etc.) backgrounds and contribute voluntarily without receiving any pay. The members of the unit assist upper secondary schools in introducing cybersecurity subjects to pupils (Sõmer, Lorenz, Kikkas, and Laugasson, 2019).

The Ministry of Defence in cooperation with other domestic partners supports an annual high-level e-state and cybersecurity course. The training audience includes top opinion leaders as well as mid and senior level leadership from the media, business, public administration, civil society, and other areas of societal and economic activity. It is a non-technical course that presents views of senior experts about technology, cyber threats, cybercrime, adversary activity, legal and strategic communication issues, as well as strategies, policies and measures of cybersecurity in NATO, the EU and Estonia.

4. DISCUSSION AND POLICY RECOMMENDATIONS

The article revealed that enhancing general cybersecurity and cybercrime competence of internal security public servants is an important objective of the Estonian government. Many countries in Europe and beyond struggle with finding enough resources to support cybersecurity education and training, as well as cybersecurity workforce development. In order to enhance cybersecurity competences of internal security employees the government of Estonia and the Ministry of the Interior should allocate substantial funding to support the EASS initiatives. The ends, ways and means for doing so should be determined with the Internal Security Action Plan 2020-2030. The EASS should pursue cooperation and partnerships with national and international partners for greater synergy and cost efficiency in developing programmes for specific training audiences.

In summary, this article discussed cybersecurity and cybercrime education and training efforts of foreign police universities, the NATO reference curricula and syllabus of Põltsamaa municipal gymnasium. Based on the comparative analysis, a number of common themes across countries was identified. It is suggested that the same themes should be integrated into the EASS programmes given they are adapted to the context of an Estonian digital ecosystem. In addition, the EASS curricula should address in depth those digital safety and cybersecurity issues that pertain to tasks of first-responders. For example, e-ID and data protection are subjects that pertain directly to first-responders on-job responsibilities and tasks, and the previous research and expert opinion indicates that the knowledge on these issues among police cadets and employed first-responders is insufficient.

Therefore, future first-responder job descriptions should include requirements for skills required for the secure use of internet and information systems, as well as about more general cybersecurity and cybercrime knowledge. In addition, the EASS curriculum should provide knowledge and practical experience to students about the secure and safe use of police information systems and state registers, in particular about data protection regulations and methods. As the previous research has shown the EASS students do not understand how data is created and transmitted in and between different information systems and what are the implications for data protection.

Lastly, the impact of new courses and study subjects, as well as appropriate teaching methods and tolls should be periodically assessed (and amended as needed), and student and teachers feedback collected. The content and teaching methods and tools should be updated regularly so that they correspond to real life problems that professionals at the Police and Border Guard Board encounter, and that teachers are using the same software and IT systems that are used by employed professionals.

Given that the National Defence Academy has integrated to date only a few subjects about cybersecurity fundamentals and cyber defence in the Estonian Defence Forces to its own curricula, it could cooperate with the EASS and HITSA to develop a joint cybersecurity curriculum and attractive digital study materials.

For example, HITSA has made available e-textbooks and study videos for primary and secondary school pupils and teachers. Interactive video games could be developed for defence and police cadets. Teachers for technical subjects should be recruited from technical universities (IT college, TalTech, etc.) and among cybercrime prevention professionals working at the Police and Border Guard Board, whereas general knowledge subjects could be taught by the Cyber Defence Unit of the National Defence League.

In the longer-term cybersecurity courses should be integrated into all programmes of the EASS, including the rescue service, correction and prison officials, and customs and tax officials. A cyber hygiene e-learning course developed by an Estonian company is employed in many government authorities and Estonian universities. The e-course is mandatory for public servants of the Police and Border Guard Board. The Estonian Information System Authority likewise uses this tool to improve cyber hygiene of public servants and family physicians. It is recommended the e-course should be compulsory for EASS teaching personnel, administrative staff, and police and border guard cadets in order to improve their cyber hygiene skills.[13] The EASS could cooperate with other domestic partners, such as the Cyber Defence Unit of the Estonian Defence League to provide non-formal activities such as student camps, competitions, and hackathons to the cadets. The Cyber Defence Unit could also regularly brief EASS students and staff on how to improve cyber hygiene.

As part of elective studies EASS students should be able to choose advanced ICT and cybercrime investigation courses provided by other universities (TalTech, IT college) and through the Erasmus student exchange in the police academies of Nordic countries. Advanced level cybercrime training for cybercrime investigators (cyber criminalists) should be conducted in cooperation with technical universities and other educational institutions. International cooperation with Nordic countries and European partners could offer study opportunities with minimal costs (for example, the Norwegian offers digital forensics e-courses in English).

First-responders working at the Police and Border Guard Board should pass the e-course for first responders provided by the European Cybercrime Training and Education Group.[14] In addition, a new e-learning course that targets all law enforcement officers, prosecutors and judges who deal with cybercrime, including first responders is under development. The course includes topics such as identifying, preventing and investigating cybercrime, conducting first response, the legal framework, etc.[15]

All first-responders must have a profound understanding of judicial and security implications of the inappropriate use of e-ID in Estonia. For example, people may not fully acknowledge that by entering PIN codes digitally they will be subject to legally binding obligations because a digital signature is equivalent to a hand-written signature. Likewise, there have been fraud cases where the elderly may not fully comprehend the reasons why sharing their ID-card and PIN codes with third persons is equivalent to transferring their digital identity. In case of doing so for

[13] Description of the course is available at the company website https://cybexer.com/cyber-hygiene-e-learning-course/.

[14] The course description is available at https://www.ecteg.eu/running/first-responders/.

[15] The draft version as of October 2019 of the course description is available through national representatives.

internet voting will violate a principle of secrecy and in their case result in unwanted financial obligations. Therefore, first-responders should be able to explain to less tech-savvy e-ID users the legal framework and reasons why digital identity is only for personal use. First-responders should also have an understanding on how to protect personal data in police registers, how the data is created and how it is used for the identification of persons of interest (Kirch, 2019). Both of these aspects are specific to the Estonian digital infrastructure, thus if a foreign reference curriculum will be used it should be complemented by basic knowledge about the Estonian system. There is a need to provide basic cyber security skills for all cadets and focus on more specialised training for cybercrime investigators.

In addition to students, cyber security and digital competences need to be part of teacher training. HITSA could provide basic and additional training for teachers, involving cyber security experts, trainers in companies, public sector and potentially also talented students, as well as support the development of a support network for teachers, education technologists and science schools for more interested students (Melesk, 2019).

Students who will complete the cyber conscription service in the Estonian Defence Forces and who do not wish to work for the military could be encouraged to study at the EASS and join the cybercrime investigation team at the Central Criminal Police after completion of their studies. The cyber conscription training prepares conscripts not only in defending military networks, but also provides skills on gathering digital evidence as part of digital forensics, OSINT and signal intelligence. Those conscripts who do not start working as active duty military should be encouraged to join law enforcement. As proposed earlier in this article, extra-curricular cybersecurity activities for EASS students should be initiated in order to find and develop cybersecurity talent for the law enforcement workforce and existing programmes (competitions, summer camps) should be extended to the internal security sphere.

The extra-curricular cybersecurity training initiatives of the Ministry of Defence should be further analysed with a view to extend benefits to the internal security sphere by creating joint projects. The EASS should initiate similar extra-curricular activities (student competitions and exercises) and cooperate with the Ministry of the Defence in finding synergy between each other's extra-curricular programmes and initiatives.

The Ministry of the Interior proposed in September 2019 the creation of a 700-person armed internal security reserve force that would be deployed in the case of a public order crisis. According to him the force can be deployed in internal security scenarios such as mass riots and evacuations, protection of state borders and of objects of essential services. The cost for training and equipment are estimated about 20 million euros during the next four years, and it would be composed of graduates of the EASS, former police officers and members of military reserve who have competed their conscription service, including military police training (Tooming, 2019). In order to support a response to a cyber emergency and day-to-day protection of cyberspace a voluntary civilian cyber team could be created composed of students, staff and alumni of the EASS as well as professionals from the internal security sphere. Previous research shows that cyber security skills are mainly acquired outside of formal education, through hobby groups or self-learning and these possibilities should be created for the cadets of EASS.[16] The main objectives of a voluntary cyber team could be twofold:

- Supporting cybersecurity in the internal security sector by raising awareness and conducting training.

- Supporting the response to a cyber emergency.

For example, in October 2019 the EASS organised a non-technical hackathon where teams of EASS students were tasked to come up with innovative ideas on how to apply simulation, virtual reality and other high-tech tools in to the study process. Such competitions, camps and other activities could be organised by a voluntary cyber team in order to raise cybersecurity awareness and interest in ICT and cybersecurity among students, staff and professionals. The team could participate in national and international cybersecurity competitions (for example, Garage48 Cybersecurity Hackathon organised by the University of Tartu), and organise training events (summer camps, competitions) for EASS students and staff.

[16] For example, see Sõmer T., et. al., 2019.

In case of a serious cyber-attack or incident that has national security implications, members of the team could support response activities of internal security authorities, the government Computer Emergency Response Team of the Estonian Information System Authority, and the Cyber Defence Unit of the Estonian Defence League. During an armed conflict the team would not become a part of the wartime structure of the Estonian Defence League. A civilian voluntary organisation may attract additional members including women who may not consider the military nature of the Cyber Defence Unit appealing. The organisation can serve as a focal point to establish and maintain joint projects with the industry, such as Estonian companies developing AI and cybersecurity solutions. Stronger cooperation with the industry is necessary to implement AI and digitisation solutions to analyse large datasets such as drone and satellite data.

Based on the research presented in this article the author recommends the EASS to integrate in the vocational and bachelor level programmes the following main themes from autumn 2020:

- Introduction to and fundamentals of cybersecurity and cyber threats.
- The impact of disruptive technologies on cybercrime, government and law enforcement.
- Introduction to cybercrime.
- National and EU regulations in cybersecurity and data protection as well as international regulations (for example, the Budapest convention).
- Key international organisations pertaining to cybercrime prevention and response.
- Principles and foundations of secure e-government and digital infrastructure (e-ID, e-services, etc.) in Estonia.
- Cybercrime prevention, response and investigation, including gathering and handling of digital evidence.
- The use of ICT for police investigations and gathering information.
- National and international cooperation in cybercrime prevention.

These subjects can be divided to several courses, and the descriptions of courses must include the purpose of the course, learning objectives, competences and qualifications acquired by students. Study methods should include classroom and individual study, group and individual assignments, written papers and presentations, a list of mandatory readings, interactive workshops, demonstrations, and practical exercises. New learning paradigms and attractive learning materials (demonstrations, simulations, computer-game-based learning), digital materials (videos, e-courses, -tests, -books, etc.) and cybercrime incident analysis computer software programmes should be used. Cybersecurity and cybercrime study subjects could be integrated into the existing modules first as pilot courses, and after collecting students and teachers feedback the content could be reviewed and updated regularly.

It should be noted that the findings within this article are subject to a number of limitations. It is not possible to assess the impact of teaching cybersecurity study subjects to the actual competences of first responders employed in law enforcement agencies. Introduction of cybersecurity subjects into the curriculum of police academies has been a recent initiative in most countries and assessing the impact of these models to improve job-related tasks can be performed after the graduates of these courses have started their professional careers. Cybersecurity education and training is a rapidly evolving discipline and all curricula should be reviewed and updated regularly. The scope of this study dictates that this is not a full or comprehensive review of the existing best practices, and does not examine the application of the cybersecurity workforce building frameworks in the Estonian context. The article provides an overview of current cybersecurity education initiatives in Estonia, and in some other countries, as well as the EU and NATO. The article does not capture the full perspectives of all subject matter experts in the field, but the author reviewed relevant documents and conducted interviews to produce a review of cybersecurity education in the Estonian internal security sector. In the course of future research the proposed study themes should be specified at two or four levels of proficiency (basic and advanced or basic, intermediate, advanced and expert).

CONCLUSION

The article described strategic guidelines of the Estonian government for cybersecurity competence building in the internal security sphere. It gave an overview of the existing cybersecurity education in Estonia and of cybersecurity formal education in police universities in Finland, Germany, the Netherlands and Norway.

The current deficit of digital skills, shortness of cybersecurity and cybercrime knowledge, skills and abilities of the internal security personnel are risks to national security and public order. Currently EASS students do not have a clear understanding of the Estonian digital ecosystem and interdependencies of its components, and enough knowledge about data protection principles, regulations, and measures. There is also no training provided to improve digital safety skills such as an e-learning course and test. The author recommended study subjects to be included as a pilot project to the EASS curriculum from the autumn semester of 2020. A closer cooperation with the Ministry of Defence, which has initiated and supports a number of initiatives for cybersecurity competence building through extra-curriculum activities, is also recommended.

Contact:

Piret Pernik
E-mail: piretpernik@icloud.com

REFERENCES AND SOURCES

Costigan S. S. and Hennessy, M. A. eds. (2016) *Cybersecurity. A Generic Reference Curriculum.* [Online source] Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-curriculum.pdf.

Council of Europe. (2001) Budapest Convention: Convention on Cybercrime, Budapest, 23 November 2001. [Online source] Available from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

Craglia M. (Ed.), Annoni A., Benczur P., Bertoldi P., Delipetrev P., De Prato G., Feijoo C.,

Fernandez Macias E., Gomez E., Iglesias M., Junklewitz H., López Cobo M., Martens B., Nascimento S., Nativi S., Polvora A., Sanchez I., Tolan S., Tuomi I., Vesnic Alujevic L. 2018. Artificial Intelligence - A European Perspective, EUR 29425 EN, Publications Office, Luxembourg, 2018, ISBN 978-92-79-97217-1, doi:10.2760/11251, JRC113826.

Cybersecurity Ventures. (2019a) Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics. [Online source] Available from: https://cybersecurityventures.com/cybersecurity-almanac-2019/.

Cybersecurity Ventures. (2019b) Cybercrime Damages $6 Trillion By 2021. [Online source] Available from:

https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

EASS [Estonian Academy of Security Science]. (2017) *Information Systems Training of Cadets of the Police and Rescue College of the Estonian Academy of Security Science.*

EASS [Estonian Academy of Security Science]. (2019) *Internal Security Master Programme. Curriculum.* [Online source] Available from: https://www.sisekaitse.ee/sites/default/files/inline-files/Sisejulgeoleku%20magistri%20%C3%B5ppekava_0.pdf.

e-Estonia. (2019) *Security and Safety, e-Police.* [Online source] Available from: https://e-estonia.com/solutions/security-and-safety/e-police/.

Emergency Act. (2017) *State Gazette.* [Online source] Available from: https://www.riigiteataja.ee/en/eli/525062018014/consolide.

European Union Agency for Law Enforcement Cooperation. (2018) *Internet Organised Crime Threat Assessment.* Available from: European Union Agency for Law Enforcement Cooperation 2018.

European Union Institute of Security Studies. (2019) *EUISS Yearbook of European Security.*

[Online source] Available from: https://www.iss.europa.eu/sites/default/files/EUISSFiles/YES_2018.pdf.

Err. (2018) *New EDF commander favours extending conscription for some fields*. 6 December 2018. [Online source] Available from: https://news.err.ee/882577/new-edf-commander-favours-extending-conscription-for-some-fields.

European Commission. (2019a) *Horizon 2020. Programme 2018-2020.* [Online source] Available from: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf.

European Commission. (2019b) *Cybercrime.* Migration and Home Affairs. [Online source] Available from: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en.

Europol. (2017) *Common Taxonomy for Law Enforcement and CSIRTs.* Europol EC3 European Cybercrime Centre. Version 1.3. [Online source] Available from: https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts.

Federal University of Applied Administrative Sciences. (2019a) *Criminal Police Officer at the Bundeskriminalamt*. Module 10.

Federal University of Applied Administrative Sciences. (2019b) *Police Service in the Federal Police (Diploma in Public Administration).*

Government Office. (2017) *National Defence Development Plan 2017-2026.* [Online source] Available from: https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/rkak_2017_2026_avalik_osa.pdf.

Government Office. (2019) *AI Implementation Report of Estonia* [Eesti tehisintellekti kasutuselevõtu aruanne]. [Online source] Available from: https://www.riigikantselei.ee/sites/default/files/riigikantselei/strateegiaburoo/eesti_tehisintellekti_kasutuselevotu_eksperdiruhma_aruanne.pdf.

Greenberg, A. (2019) New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction. *Wired*. [Online source] Available from:

https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/).

Information System Authority. (2017) *ROCA Vulnerability and eID: Lessons Learned*. [Online source] Available from: https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf.

Innove. (2019) Täna algab pilootprojekt, mis annab esimest korda võimaluse mõõta õpilaste digioskusi. [Online source] Available from: https://www.innove.ee/uudis/tana-algav-tasemetoo-annab-esimest-korda-voimaluse-moota-opilaste-digioskusi/.

International Telecommunication Union. (2018). The Global Cybersecurity Index 2018. Available from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

HITSA [The Information Technology Foundation for Education]. (2019) ProgeTiigri koolitused. [Online source] Available from: https://www.hitsa.ee/ikt-hariduses/koolitused/progetiigri-koolitused.

Härma, K. (2018) Kuu pärast tuleb olla e-teenustega valmis uueks ID-kaardiks. Äripäev. [Online source] Available from: https://www.aripaev.ee/uudised/2018/11/08/kuu-parast-tuleb-olla-e-teenustega-valmis-uueks-id-kaardiks.

Kaas, K. (2019) *Riigikaitseõpik gümnaaasiumitele ja kutseõppeasutusele.* Ministry of Defence. Avita publishing, Tallinn. [Online source] Available from:

https://drive.google.com/file/d/1cY6MzkbJeFmZ3-60XHoESXH5h7ZPkkLY/view.

Kessler G., and Ramsay J. (2014) *A Proposed Curriculum in Cybersecurity Education Targeting Homeland Security Students.* 47th Hawaii International Conference on System Sciences, 2014. DOI: 10.1109/HICSS.2014.605.

Kirkpatrick D., Hubbard, B. (2019) Attack on Saudi Oil Facilities Tests U.S. Guarantee to Defend Gulf. *The New York Times.* 19 September 2019. [Online source] Available from: https://www.nytimes.com/2019/09/19/world/middleeast/saudi-iran-attack-oil.html.

Kirch, K. (2019) Email communication with the author. September, Tallinn.

McAfee (2018) 2019 Threats Predictions. [Online source] Available from: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions/.

Melesk K., Mägi E., Koppel K., Michelson A. (2019) *Labor force and skills need in cyber security.* Praxis. [Online source] Available from: http://www.praxis.ee/wp-content/uploads/2018/04/K%C3%BCberturbe-uuring_aruanne-23_04_2019.pdf

Ministry of the Interior. (2019) *The Internal Security Action Plan 2020-2030* [Siseturvalisuse arengukava 2020-2030].

Ministry of Economic Affairs and Communications. (2018a) *Digital Agenda 2020 for Estonia. Updated 2018.* [Online source] Available from: https://www.mkm.ee/sites/default/files/digital_agenda_2020_estonia_engf.pdf.

Ministry of Economic Affairs and Communications. (2018b) *National Cybersecurity Strategy 2019-2022.* [Online source] Available from: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

National Defence Academy. (2019) *Military Leadership for Land Force. Curriculum.* [Online source] Available from: https://www.kvak.ee/

files/2019/05/S%C3%B5jav%C3%A4eline-juhtimine-maav%C3%A4es-rakendusk%C3%B5rgharidus%C3%B5pe.pdf.

Norwegian Police University College. (2019) *Studies in English.* [Online source] Available from: https://www.phs.no/en/studies/post-graduate-studies/.

Paulsen, C., Newhouse W., McDuffie, E., Toth, P. (2012) NICE: Creating a Cybersecurity Workforce and Aware Public. IEEE Security and Privacy. May-June 2012, pp. 76-79, vol. 10. DOI: 10.1109/MSP.2012.73.

POLAMK [The Finnish Police University College]. (2019a) *CYBERDI.* [Online source] Available from: https://jyvsectec.fi/2018/10/cyberdi/.

POLAMK [The Finnish Police University College]. (2019b) *Bachelor of Police Services. Curriculum 2018-2020.* [Online source] Available from: https://www.polamk.fi/instancedata/prime_product_julkaisu/intermin/embeds/polamkwwwstructure/61434_Curriculum_Bachelor.pdf?1180e46df085d688).

POLAMK [The Finnish Police University College]. (2019c) *Poliisi (AMK) -tutkinto Vapaasti valittavat opintojaksot, jotka eivät ole opetussuunnitelmassa Lukuvuosi 2018 – 2020.* [Online source] Available from: https://www.polamk.fi/instancedata/prime_product_julkaisu/intermin/embeds/polamkwwwstructure/84011_Poliisi_AMK_opsin_ulkopuoliset_vapaasti_valittavat_opintojaksot_2019_2020.pdf?c5ec6b44fa31d788).

Silberglitt R., Chow B., Hollywood J., Woods, D., Zaydman M., Jackson B. (2019), Visions of Law Enforcement Technology in the Period 2024-2034

Report of the Law Enforcement Futuring Workshop, Rand Corporation. [Online source] Available from: https://www.rand.org/pubs/research_reports/RR908.html.

Sobusiak-Fischanaller M., and Vandermeer Y., (2019) *Cybercrime Training Governance Model. Cybercrime Training Competency Framework.* European Cybercrime Training and Education Group. [Online source] Available from: https://rm.coe.int/3148-2-3-ecteg-16-cy-train-module/1680727f34.

Skattor, B. (2019) Trust & Security: building trust for use of AI by law enforcement. [Presentation] Tallinn Digital Summit 2019, Tallinn, 16 September 2019.

Sõmer T., Ottis R, Lorenz B. (2019) *Developing Military Cyber Workforce in a Conscript Armed Forces: Recruitment, Challenges, and Options.* ICCWS 2019: International Conference on Cyber Warfare and Security. 28 February - 1 March, South Africa.

Sõmer T., Lorenz B., Kikkas K., and Laugasson A. (2019) *Cybersecurity within the Curricula of Informatics: The Estonian Perspective.* 12th International Conference on Informatics in Schools (ISSEP 2019). 18-19 November 2019, Larnaca. To be published in Lecture Notes on Computer Science conference proceedings.

TalTech. (2019a) *About the project.* [Online source] Available from: https://sites.google.com/view/kyberolympia/eng/about-the-project.

Tarros, M. (2019) [Presentation] *Digital Agenda For Estonia 2021+.* Tallinn, 16 September 2019.

Toiviainen, T. (2019) Interview with the author. April, Tampere.

Tooming, M. (2019) Sisekaitse reservi loomine nõuab nelja aastaga 20 miljonit eurot. *Err.* [Online source] Available from: https://www.err.ee/981248/sisekaitse-reservi-loomine-nouab-nelja-aastaga-20-miljonit-eurot.

Viik, L. (2019) *Exclusive overview of the story of e-Estonia and will zoom into the future plans to push e-Estonia even further into the future.* [Discussion] Digital Agenda For Estonia 2021+, Tallinn, 16 September 2019.

Wright, N. (2018) *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives. A Strategic Multilayer Assessment (SMA) Periodic Publication.* Department of Defense, Joint Chiefs of Staff. December 2018, pp. 1-2. [Online source] Available from: https://nsiteam.com/social/wp-content/uploads/2018/12/AI-China-Russia-Global-WP_FINAL.pdf.