Crime prevention policy	
EU- priority	Cybercrime; • Child sexual exploitation • Payment card fraud • Cyber-dependent crimes
Country	Estonia
Year	2018

1. Overview of the field

Definition of cybercrime

In 9.05.2018 entered into force the Cybersecurity Act, which provides for the requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities' network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents.

Cybercrime offences are stipulated in the Penal Code as follows (list includes crimes committed using computer/ computer-related crimes, marked with):

§ 157^1. Illegal disclosure of sensitive personal data
§ 157^2. Illegal use of another person's identity
§ 206. Interference in computer data*
§ 206^1. Unlawful removal and alteration of means of identification of terminal equipment*
§ 207. Hindering of operation of computer system*
§ 213. Computer-related fraud*
§ 216^1. Preparation of computer-related crime*
§ 217. Unlawful use of computer system*
§ 217^1. Use of terminal equipment with unlawfully removed or altered means of identification*

In the time-frame of transposition of Directive 2016/1148/EU (Network and Information Security Directive), Estonia has taken a broader scope in updating its cyber security related legislation, which is coordinated by the Ministry of Economic Affairs and Communications. Estonia's first "Cybersecurity Act" came into force 23.05.2018.

Assessment of trends and developments

Annual Cyber Security Assessment is conducted by the Estonian Information System Authority (EISA). Report for year 2018: https://e-estonia.com/cyber-security-report-2018/ states that last year, the Incident Response Department of EISA recorded about 10,923 cyber security cases – one third more than in 2016. Only 122 incidents had a direct impact on a service vital to the functioning of the state and society – the lowest figure in the last three years. Last year, 32 known cyber incidents took place in the Estonian healthcare sector, and ten of these cases had a direct influence on the work of hospitals and general practitioners. 61% of the cyber security incidents recorded were malware, 8% ransomware and 1% DDoS attacks.

The number of computer-related frauds recorded by police has gone up from 470 in 2013 to 650 in 2017, an almost 50 per cent increase.

Recent overview of statistics and research

Annual crime statistics (registered crimes) is collated by the Ministry of the Justice and published (in Estonian) on the web page of the Ministry of Justice: http://www.kriminaalpoliitika.ee/et/statistika-ja-uuringud/kuritegevus-eestis.

Overview of cybercrimes is as follows:

Penal Code §		2013	2014	2015	2016	2017	2018 until 17.9.2018
§ 206	Interference in computer data	12	7	32	33	31	14
§ 206¹	Unlawful removal and alteration of means of identification of terminal equipment	0	1	0	0	0	0
§ 207	Hindering of functioning of computer systems	6	9	16	15	9	3
§ 213	Computer-related frauds	470	486	494	608	650	391
§ 216¹	Preparation of computer-related crime	13	37	15	8	10	14
§ 217	Illegal obtaining of access to computer systems	31	22	85	71	81	113
§ 217¹	Use of terminal equipment with unlawfully removed or altered means of identification	1	3	0	3	0	5

Other national priorities besides child sexual exploitation, payment card fraud and cyber-dependent crimes?

The Estonian Presidency of the Council of the EU in second half of 2017 focused on renewing the EU Cyber Security Strategy as a priority. Within this priority the Presidency agreed on specific steps for making the EU better protected against cyber-attacks and strengthening the fight against cybercrime. Cybercrime is a real and growing threat that impacts the EU´s internal security as digitalising society unavoidably becomes more vulnerable to new cyber threats. As cybercrime is cross-border and international, efficient cooperation between the law enforcement agencies in preventing and investigating crime is crucial.

2. Crime strategy and coordination

Objectives of the crime strategy

The Cyber Security Strategy 2014-2017 is the basic document for planning Estonia’s cyber security and a part of Estonia’s broader security strategy. The strategy highlights

important recent developments, assesses threats to Estonia's cyber security and presents measures to manage threats. This strategy continues the implementation of many of the goals found in the Cyber Security Strategy 2008-2013.
Estonia is currently drafting its third national Cyber Security Strategy 2019 – 2022, which will be completed by December 2018, and replace the current strategy from January 2019. Cybercrime related strategic planning for the upcoming period will partly be addressed in the new Cyber Security Strategy and partly in the new Estonian Internal Security Strategy 2020-2030.

Role of prevention in the crime strategy on state/regional/local level

Prevention is one of the key components of ensuring cyber security and reducing the damage done by cybercrime. Preventive activities are implemented in cooperation of Estonian Ministry of Economic Affairs and Communications, EISA, Ministry of the Interior and the Police and Border Guard Board.

Implementation of the policy (which level is responsible for the implementation and how is the implementation coordinated?)

The implementation of Estonian Cyber Security Strategy is coordinated by the Ministry of Economic Affairs and Communications in cooperation with other relevant ministries, including the Ministry of Interior. Implementation of the Internal Security Strategy is coordinated by the Ministry of Interior, this includes activities to tackle cybercrime. Ministries, authorities and institutions are responsible for the implementation within their respective competences.

Stakeholders (working groups, specialised agencies, partners, etc)

In 2009, the Cyber Security Council was established at the Security Committee of the Government of the Republic. The task of the Council is to contribute to smooth co-operation between various institutions and conduct surveillance over the implementation of the goals of the Cyber Security Strategy. The Council is chaired by the Secretary General of the Ministry of Economic Affairs and Communications. In 2010, by a decision of the Government of the Republic, the Estonian Informatics Centre was given government agency status.

The Ministry of Economic Affairs and Communications implements cyber defence policies in close co-operation with the following partners:

1) Estonian Defence League Cyber unit is a voluntary organisation aimed at protecting Estonian cyberspace. The Cyber Unit's mission is to protect Estonia's high-tech way of life, including protection of information infrastructure and supporting broader objectives of national defence.
2) International Centre for Defence Studies **(**ICDS) aims to advance the transatlantic community's strategic thinking on the security challenges facing the Baltic-Nordic region, from armed or cyber attacks to threats against social cohesion and energy security.
3) Estonian Information System's Authority (EISA) coordinates the development and administration of information systems ensuring the interoperability of the state's information system, organises activities related to information security, and handles security incidents in Estonian computer networks.
4) Information Technology Foundation for Education (HITSA), formerly known as the Tiger Leap Foundation is the main provider of training and awareness-raising of the cyber security.

Participation in European/ international networks, working groups, etc.
Europol, incl EC3, ENISA, EMPACT

3. Good practices

Overview of recent good practices, prevention programs, etc.
The **cyber defence field of study at Põltsamaa Coeducational gymnasium** (winner of ECPA 2017): https://eucpn.f2w.fedict.be/sites/default/files/content/download/files/gp_ecpa_2017_ee_the_cyber_defence_field_of_study_at_poltsamaa_coeducational_gymnasium.pdf **The cyber defence field of study at Põltsamaa Coeducational Gymnasium (PÜG) started with the first cohort in the school year 2015/2016. A total of 64 students (grades 10-12) are studying cyber-security at the moment. The first cohort graduated this spring. A record number of students - 27 - is studying cyber defence in the 10th grade.** **PÜG continues educate students in the field of cyber-security by sharing knowledge about cyber hygiene and safe use of the Internet and the dangers on the Internet. In addition, they learn how to protect themselves and their loved ones by raising their awareness.** **PÜG has invested in teaching materials in order to better pass on practical knowledge in cyber defense. Thanks to the European Crime Prevention Award (ECPA) and prize, the school was able to acquire desktop computers, which enable cyber defense classes to virtualize, configure, and program drones. In addition, the PCs have also been used in networking tutorials and allow students to use various simulation, drawing and 3D modelling programs.** **Secure use of the Internet is an area that the school wishes to introduce more widely in all school settings by integrating the subject into different subjects. The school wants to do its utmost to raise students' awareness. The knowledge gained in a timely manner helps to avoid any future problems in the Internet world.** **We have also developed cooperation with Tallinn University of Technology (TalTech), in the form of guest lectures. We are also planning an annual hackathon for cyber defense students. We want to share our knowledge and experience with others, and therefore, we cooperate with the Jõhvi State High School where our teacher will teach the foundations of secure networking.** **There has also been specific interest in our activities is from outside Estonia. The Center for Expertise Cyber Security have inquired about in our curriculum and experience, and we have shared this information with them. One of their research groups (Cyber Security & Safety with dr. Marcel Spruit) is working on a project to improve cyber defence skills of primary- and secondary school students in the Netherlands. Our school was also visited by Alyazia Rashed, a Master's student in the Institute of International and Civil Security at Khalifa University in the United**

Arab Emirates. Currently, she is conducting research about cyber-security-based study resources in the UAE and whether these materials are tailored to the local culture and context. Her research approach is to compare and contrast these resources in 3 different countries, which are Estonia, Singapore and Australia.

In conclusion, PÜG is making steady progress in developing our curriculum and sharing our know-how. We are also always open to new opportunities to cooperate in the field of teaching cyber defence.

One of the main high level meetings of the EU Estonian Presidency was **Tallinn Digital Summit** taking place on 29 September 2017, which provided a platform for the heads of EU institutions and member states to launch discussions about the digital future of Europe:
https://www.eu2017.ee/digitalsummit

The Digital Safety Game, DSG (entry of ECPA 2015):
https://eucpn.f2w.fedict.be/document/digital-safety-game-dsg
http://www.dsg.onu.ee/

Estonian web-constables (awarded entry of ECPA 2012):
http://eucpn.org/document/web-constables

Safer Internet Centre in Estonia - Targalt internetis (comprehensive project in the field with participation of national organisations, led by NPO Estonian Union for Child Welfare and co-financed by the European Commission):
http://www.targaltinternetis.ee/en/