Crime prevention policy

EU- priority	Cybercrime; • Child sexual exploitation • Payment card fraud • Cyber-dependent crimes
Country	Finland
Year	2018

1. Overview of the field

Definition of cybercrime

There is no established definition for cybercrime In Finland. Traditionally cybercrime has referred to crime targeted at information networks and related services.

It is acknowledged that majority of crimes can be committed by using computers. For example property crime is one of the most common cybercrimes. Most such crimes are fraud and means of payment offences, money laundering, extortion, Sexual abuse of children and young persons. Also individuals with ties to violent extremism and terrorism use the internet to distribute propaganda and terrorist material, recruit new members, and engage in violent radicalisation. Terrorists also use the internet to exchange messages and plan activities such as terrorist acts.

Assessment of trends and developments

General view is that cybercrime is growing rapidly. However, it is hard to estimate the exact development since much of it is not detected by citizens/organisations or reported to the authorities or they are recorded as part of traditional crimes like fraud.

In recent years a substantial increase in both credit card and other frauds has been observed, the latter reflecting new forms of fraud connected with the use of the Internet.
In 2017 the police recorded 121 credit card frauds and 425 other frauds per 100,000 in population (absolute figures 6,678 and 23,380), with credit card frauds decreasing by 56 % and other frauds decreasing by 7 % in comparison to year before. The rates of fraud by the population size of the region follow the same pattern as the rates of theft and embezzlement. They are clearly higher in big cities than in rural regions.

Recent overview of statistics and research

The trends in Cybercrime are also monitored as part of annual study: "Crime Trends in Finland" carried out by the Institute of Criminology and Legal Policy.

- According to statistics on crimes reported to police the most common cybercrime are cracking, interference with communications system, and interference with Information system and identity theft. There is very little statistics about cybercrimes since these crimes are usually recorded as part of traditional crimes.
- The amount of online bank fraud (e-banking malware fraud) has declined; there have

been only few isolated cases within last two years. However, there is significant increase in the amount of online payment card frauds since last year (1Q 2016 174,6% increase compared to 1Q 2015).

- Phising campaigns have become constant and in addition more carefully planned and executed than before. Social engineering in its various forms is more common nowadays than it was few years ago. As a rather new phenomenon we have seen quite a few CEO frauds recently.
- Malware, especially ransomware, have become more severe than before in terms of its capability to cause damage.
- In 2015, 6 percent of trade sector and 8 percent of industrial businesses had been targets of cybercrime. In terms of computed aided cybercrime, harassment, cyberbullying, fraud, illegal downloading and phishing are among the most common forms of cybercrime.

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

2. Crime strategy and coordination

Objectives of the crime strategy

The aim of Finland's national cyber security strategy is to respond to cyber threats, strengthen the overall security of society and ensure the smooth functioning of the cyber domain in all circumstances.

The Strategy presents ten objectives that, when implemented, provide Finland with the capability nationally to control the intentional and unintentional adverse effects of the cyber domain as well as to respond to and recover from them.

1. In line with the Government decree on the tasks assigned to ministries matters, which relate to cyber security as a rule fall within the remit of the Government. Each ministry is in its sector responsible for preparing cyber security related matters and appropriate arrangement of administrative matters.

2. As cyber security is an essential part of the comprehensive security of society, the approach for its implementation follows the principles and procedures established in the Security Strategy for Society.

3. Cyber security relies on the information security arrangements of the whole society. Cyber security depends on appropriate and sufficient ICT and telecommunication network security solutions established by every actor operating in the cyber world. Various collaborative arrangements and exercises advance and support their implementation.

4. The approach for the implementation of cyber security is based on efficient and wide-ranging information-collection, an analysis and gathering system as well as common and shared situation awareness, national and international cooperation in preparedness. This

requires the establishment of a Cyber Security Centre as well as the development of 24/7 information security arrangements for the entire society.

5. Cyber security arrangements follow the division of duties between the authorities, businesses and organisations, in accordance with statutes and agreed cooperation. Rapid adaptability as well as the ability to seize new opportunities and react to unexpected situations demand strategic agility awareness and compliance from the actors as they keep developing and managing the measures which are aimed at achieving cyber security.

6. Cyber security is being constructed to meet its functional and technical requirements. In addition to national action, inputs are being made into international cooperation as well as participation in international R&D and exercises. The implementation of cyber security R&D and education at different levels does not only strengthen national expertise, it also bolsters Finland as an information society. Cyber security development will heavily invest in cyber research and development as well as in education, employment and product development so that Finland can become one of the leading countries in cyber security.

8. In order to ensure cyber security development, Finland will see to it that appropriate legislation and incentives exist to support the business activities and their development in this field. Basic know-how in the field is gained through business activity.

STRATEGIC GUIDELINES:

1. Create an efficient collaborative model between the authorities and other actors for the purpose of advancing national cyber security and cyber defence.

2. Improve comprehensive cyber security situation awareness among the key actors that participate in securing the vital functions of society.

3. Maintain and improve the abilities of businesses and organisations critical to the vital functions of society as regards detecting and repelling cyber threats and disturbances that jeopardise any vital function and their recovery capabilities as part of the continuity management of the business community.

4. **Make certain that the police have sufficient capabilities to prevent, expose and solve cybercrime**. The police are the competent authority for carrying out investigations related to cybercrime. The police will generate an analysed, high-quality cybercrime situation picture and disseminate it as part of the combined situation picture detailed in guideline 2. The police will closely cooperate with the Cyber Security Centre. It must be ensured that the police have sufficient powers, resources and motivated personnel for cybercrime prevention, tactical police investigations as well as for processing and analysing the digital evidence. International operational cooperation and the exchange of information will be continued and intensified with the EU and with other countries’ corresponding law enforcement officials, such as Europol.

5. The Finnish Defence Forces will create a comprehensive cyber defence capability for their statutory tasks. A military cyber defence capacity encompasses intelligence as well as cyber-attack and cyber defence capabilities. The Defence Forces will protect their systems in such a manner that they are able to carry out their statutory tasks irrespective of the threats in the cyber world. Guaranteeing capabilities, intelligence and proactive measures in the cyber world will be developed as elements of other military force. Under the leadership of the Ministry of Defence the required provisions on powers will be prepared for the Defence Forces to facilitate the implementation of the aforementioned tasks. Any identified short-comings in the provisions will be corrected through legislation. Cyber defence will be exercised and developed together with the key authorities, organisations and actors in the business community, both nationally and internationally. The Defence Forces will provide executive assistance within the constraints of legislation.

6. Strengthen national cyber security through active and efficient participation in the

activities of international organisations and collaborative fora that are critical to cyber security.

7. Improve the cyber expertise and awareness of all societal actors.

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

A working group was assigned in May 2018 to draft an Action plan for preventive measures in cyber-crime. Ministry of Interior coordinates this work. Action plan will be ready by the end of the year 2018.

Several NGOs and governmental institutions aim to prevent child sexual exploitation

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

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

The Security Committee monitors the implementation of Finland's Cyber Security Strategy. The Security Committee assists the Government and ministries in broad matters pertaining to comprehensive security. The Committee follows the development of Finnish society and its security environment and coordinates proactive preparedness related to comprehensive security. The Security Committee comprises a total of 19 members and 5 experts from a number of administrative branches, authorities and the business community.

Finnish Communications Regulatory Authority develops and monitors the operational reliability and security of communications networks and services. It produces and publishes situational awareness of cyber security and acts as the National Communications Security Authority. The National Cyber Security Centre Finland is situated in the Finnish Communications Regulatory Authority. It was established in 2014 and the main duties include solving information security violations and threats against network, communications and value-added services. The Centre also gathers information on such incidents and disseminates information on information security matters.

The new Cyber Crime prevention Centre in the National Bureau of Investigations began operations on April 1 in 2015. It is geared towards improvement of police capacity to prevent serious crimes and investigate. In addition to prevention of Cyber Crimes, the new Centre is involved in internet intelligence as well as conducting treats assessments. The Cyber Crime prevention Centre generates and maintains an analysed cybercrime situation picture.

Participation in European/ international networks, working groups, etc.

Because cyber threats do not respect the borders between states, international cooperation above all is needed in order to strengthen cyber security. One of the Finland's Cyber Security Strategy's objectives is that Finland shall strengthen its national cyber security by participating actively and effectively in international discussions and cooperation on cyber security. The Foreign Ministry coordinates this international activity.

As concerns cyber security, particularly increasing confidence between states is a key issue. Efforts to this end are pursued by intensifying the discussion of cyber domain related issues between states multilaterally, regionally and bilaterally.

Discussion of the cyber domain takes place, among others, within the scope of the United Nations, the OSCE, the EU, the Council of Europe, the OECD, NATO, the Organization of American States (OAS) and the ASEAN Regional Forum (ARF).

The Foreign Ministry coordinates Finland's participation in international cooperation and takes an active part in global, regional and bilateral discussion of the cyber domain.

To Finland, especially the EU is a central player in cyber security issues. The EU has formulated a number of common policies on cyber issues, among them the Council Conclusions on Cyber Diplomacy adopted by the Council of the European Union in February 2015.

The EU's objective is to promote the realisation of core values (including human rights and fundamental rights) also in the cyber domain. In international cooperation the EU stresses openness, respect for freedom of expression and the protection of privacy, as well as the multi-stakeholder model where stakeholders are also included in the global dialogue.

In the international dialogue Finland promotes the consistent implementation of the open dissemination of information and freedom of expression, and emphasises non-discrimination. Finland, together with the other EU countries, considers that the agreements and standards pertaining to international law are also applicable to the cyber domain, and that their interpretation in this regard shall be deepened.

Furthermore, both Nordic cooperation and cooperation among the Nordic and Baltic countries in cyber security issues is close. As a NATO Partnership for Peace country, Finland also conducts cooperation with NATO in cyber security issues.

Important global issues include for instance the application of international law and human rights, such as freedom of expression and the protection of privacy, in the cyber domain, confidence-building measures, management of the Internet, the development of cyber capabilities as well as increasing security in the cyber domain.

One key challenge is to find a balance between the freedom and transparency of digital networks, on the one hand, and their security on the other hand.

3. Good practices

Overview of recent good practices, prevention programs, etc.