2014–2017

Cyber Security Strategy

Ministry of Economic Affairs and Communication

2014

TABLE OF CONTENTS

INTRODUCTION

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; however, new threats and needs which were not covered by the previous strategy have also been added.

1. ANALYSIS OF CURRENT SITUATION

1.1. Sectoral progress

In 2009, a Cyber Security Council was added to the Security Committee of the Government of the Republic, whose main task is to support strategic level inter-agency co-operation and oversee the implementation of Cyber Security Strategy objectives.

In 2010, by a decision of the Government of the Republic, the Estonian Informatics Centre was given government agency status. The renamed Estonian Information System Authority (Riigi Infosüsteemi Amet – hereinafter RIA) received additional powers and resources for organising protection of the state’s information and communication technology (hereinafter ICT) infrastructure, and exercising supervision over the security of information systems. For the purposes of organising the protection of infrastructure, the Department of Critical Information Infrastructure Protection (hereinafter CIIP) was formed within the RIA. In early 2010, the RIA launched the critical information infrastructure (hereinafter CII) mapping project, which identified the dependencies of vital services on information systems. On the basis of the mapping, security requirements for vital information systems necessary for the functioning of the state were developed. In 2011, a CIIP commission was formed to promote public-private cooperation. The purpose of the commission, which brings together cyber security and IT managers from vital services agencies, is to exchange operational information, identify problems and make suggestions for improving the cyber security of the country's critical infrastructure.

In 2012, the cybercrime investigation capabilities of the Police and Border Guard Board (hereinafter PBGB) were consolidated into a single department. In addition, officials dealing with cybercrime and digital evidence management procedures from various units in the prefectures were consolidated into cybercrime and digital evidence services that were established in prefectures in 2013. The PBGB is also engaged in raising awareness regarding cyber threats, which, among other things, has resulted in the creation of the positions for web-constables. A web-constable is tasked with raising people's awareness about the security of the Internet and protecting children and young people online. The Estonian Internal Security Service strengthened its investigative capabilities in order to prevent threats to national security, including cyber attacks and espionage.

The creation of the Estonian Defence League's Cyber Unit (hereinafter EDL CU), which took place as a result of collaboration between the public, private and third-sector, has been instrumental in ensuring national defence. The expertise of EDL CU volunteers is applied to improve the security of Estonian state agencies' and companies' information systems through coordinated exercises, testing of solutions, training, etc.. The EDL CU can also be engaged to support civilian institutions and protect critical infrastructure in a crisis situation. Domestic and international cyber security training exercises have also played an important role in the development and assessment of cyber security capabilities. The Government of the Republic's cyber defence headquarters exercise "Cyber Fever" and NATO Crisis Management Exercise CMX 2012 took place in 2012. Each year, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) exercise Locked Shields takes place in Estonia. Since 2013, the NATO cyber defence exercise Cyber Coalition has also been hosted in Estonia. The Defence Forces has also created a Cyber Range to support cyber defence related training. The Range is used to carry out the aforementioned cyber exercises, organise domestic exercises and in the instruction provided by universities.

In the field of cyber security, the main provider of training and awareness-raising is the Information Technology Foundation for Education (hereinafter HITSA), formerly known as the Tiger Leap Foundation. HITSA training is offered to pre-schoolers well as older children, while also involving parents and teachers in the process. A state-private partnership project was launched in 2013 to raise the skills and security awareness of smart device users, developers and vendors. In cooperation between Tallinn University of Technology (TUT) and the University of Tartu, the international Master's programme in Cyber Security was opened in 2009, with 50 students accepted into the programme each year. In 2014, TUT, in cooperation with the Estonian Centre 2CENTRE, opened a Master's programme in Digital Forensics. Estonia's 2CENTRE Cybercrime Centre of Excellence is part of the European Union's network of 2CENTRE competency centres, where professionals are trained in the fight against cybercrime, and continuation training is arranged for them.

Estonia has successfully cooperated with other ICT-advanced countries and international organizations in the field of cyber security. An active role in shaping cyber security policy led to the establishment of the NATO Cooperative Cyber Defence Centre of Excellence in Estonia. Estonia has contributed to cyber security becoming part of NATO and European Union policy, and other countries' interest towards Estonia's experience in cyber security has grown significantly. Cyber security related cooperation has been successful on the regional level between the Nordic countries and the Baltic States, as well as with other strategic partners and like-minded countries. Estonia is also participating in newer forms of cooperation - the Freedom Online Coalition, the United Nations Group of Governmental Experts, the OSCE informal working group on developing confidence building measures in cyberspace, Friends of the Presidency of the European Union, and others.

1.2. Trends

The continued rapid development of information and communication technologies, globalization, the drastic increase in data volumes and the growing number of different types of equipment connected to data networks have an impact on daily life, the economy and the functioning of the state. On the one hand, this level of ICT development will contribute to the improved availability and usability of services, enhance transparency and citizen participation in governance, and cut public as well as private sector costs. On the other hand, the increasing importance of technology is accompanied by an increase in the state's growing dependence on already entrenched e-solutions, and cements the expectation of technology operating seamlessly. In addition, the Internet is becoming increasingly accessible, the number of users continues to grow, and with new technological solutions and services - such as the "Internet of things", and cloud computing - the number of potential vectors for attacks, along with the complexity of attacks, is growing.

Social processes are also becoming increasingly dependent on a growing number of information technology resources, and in the future attention must be drawn to the fact that society at large, and each individual in particular, will be able to maintain control over the corresponding processes. Otherwise, there is potential for information technologies to reduce the role of humans in the decision-making process, and processes may become self-regulatory (technological singularity).
The main threat is cybercrime and its growth is reflected by the significant development of cyber criminals' skills and their increased ability to carry out organized attacks. An integral part of the processing of crimes is the collection and handling of digital evidence, which poses new challenges to the procedural and digital forensics capabilities of the police.

National cyber security is affected by the actors operating in cyberspace with their various skills, targets and motivations. It is often difficult to distinguish between the actors or determine their relationship to national or international organizations. The number of state actors in cyberspace that are involved in cyber espionage targeted at computers connected to the Internet as well as closed networks continues to grow, with their aim being to collect information on both national security as well as economic interests. The amount and activeness of states capable of cyber-attacks are increasing.

In addition to the activation of state actors, the ability of politically motivated individuals and groups with limited means to organize their activities using social networks and carry out denial of service and other types of attacks is growing as well.

Meaningful and effective cooperation between the public and private sector in the development of cyber security organisation as well as in preventing and resolving cyber incidents is becoming increasingly unavoidable. National defence and internal security are dependent on the private sector's infrastructure and resources, while at the same time the state can assist vital service providers and guarantors of national critical information infrastructure as a coordinator and balancer of various interests.

1.3. Challenges

The main cyber security risks arise from the extensive and growing dependence on ICT infrastructure and e-services by the Estonian state, the economy and the population. Therefore, the key fields on which the Cyber Security Strategy focuses are ensuring vital services, combating cybercrime more effectively and advancing national defence capabilities. Additional supporting activities will include: shaping the legal framework, promoting international cooperation and communication, raising awareness, and ensuring specialist education as well as the development of technical solutions..

In the case of **vital services**, cross-border information technology interdependencies have emerged and securing them is no longer dependent solely on parties based in Estonia. The Estonian state has no option for effectively supervising services or parts of services which are provided outside of the Republic of Estonia . All vital services and their dependencies must be mapped, alternatives must be developed and operational readiness to implement them must be achieved. The preservation of data and information systems that are essential to the functioning of society must be ensured in both the public and private sectors. The timely detection of and response to cyber threats threatening the state, society and the individual must be ensured.

Cybercrime undermines the functioning of the economic space, reduces trust in digital services, and, in a worst-case scenario, could lead to incidents causing loss of life. Competent personnel and modern technical tools are needed in order to ensure prevention, detection and prosecuting of cybercrime. Operational information exchange between countries is becoming increasingly important in the fight against cybercrime.

To ensure the ability to provide **national defence** in cyberspace, the state's civilian and military resources must be able to be integrated into a functioning whole under the direction of civilian authorities as well as being interoperable with the capabilities of international partners. In addition to conventional military environments, National defence planning must increasingly take cyberspace into account.

In order to prevent and deter **future security** threats, it is necessary to constantly develop cyber security related know-how and to invest in technology. Implementing forward-looking procurement procedures is necessary to ensure production of reliable and competitive technical solutions and will support their export as well, whereas the knowledge and resources obtained in that process must be re-invested into innovative solutions.

As a **supporting activity**, a modern legal framework must be ensured to provide complete solutions to the above-listed challenges. At the international level, the preservation of a free and secure cyberspace as well as Estonia's central role in guiding and developing international cyber security policy in international organizations as well as like-minded communities must be ensured.

2. PRINCIPLES OF ENSURING CYBER SECURITY

1. Cyber security is an integral part of national security, it supports the functioning of the state and society, the competitiveness of the economy and innovation.
2. Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information, and identity.
3. Cyber security is ensured on the basis of the principle of proportionality while taking into account existing and potential risks and resources.
4. Cyber security is ensured in a coordinated manner through cooperation between the public-, private- and third sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services in cyberspace.
5. Cyber security starts with individual responsibility for safe use of ICT tools.
6. A top priority in ensuring cyber security is anticipating as well as preventing potential threats and responding effectively to threats that materialize.
7. Cyber security is supported by intensive and internationally competitive research and development.
8. Cyber security is ensured via international cooperation with allies and partners. Through cooperation, Estonia promotes global cybersecurity and enhances its own competence.

3. GENERAL OBJECTIVE OF THE STRATEGY FOR 2017

Vision:

Estonia is able to ensure national security and support the functioning of an open, inclusive and safe society.

General objective:

The four-year goal of the cybersecurity strategy is to increase cybersecurity capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace.

4. SUBGOALS

Subgoal 1: Ensuring the protection of information systems underlying important services

The functioning of the Estonian state and society, the economic and social well-being of every person, their life and health, increasingly depend on the security of the systems and services. One of the main aims of the strategy is to describe methods for ensuring the uninterrupted operation and resilience of vital services, and the protection of critical information infrastructures against cyber threats.

1.1. Ensuring alternative solutions for important services

National dependencies on ICT infrastructure and e-services are constantly updated, mapped and managed. This includes a system of alternate solutions that are to be used in cases where the normal functioning of ICT infrastructure and e-services is disrupted.

1.2. Managing cross-dependency between important services

The mapping of significant cross-dependencies between services is kept up to date, the assessment of the extent of the impact of cross-dependencies on the functioning of services is conducted in a timely manner, and related risks are systematically grounded. Information relating to dependencies on critical services provided from outside the Republic of Estonia is kept up to date, the extent of their impact on the functioning of services is promptly evaluated, and associated risks are systematically reduced.

1.3. Ensuring the security of ICT infrastructure and services

Information and communication technology infrastructure is protected from modern threats. Critical data is kept and processed in highly secure data centres, and, among other things, data may also be stored securely abroad. Information systems necessary for the operation of state and vital services will be developed and managed in a manner that accounts for security risks and provides the means and measures to manage risks.

1.4. Managing cyber threats to the public and private sector

Information technology risks will be assessed and measured, with the requisite qualified staff available, along with methodologies, training opportunities and other resources. Areas which have not yet been sufficiently addressed are mapped and corresponding awareness programs are created.

1.5. Introduction of a national monitoring system for cyber security

In order to identify and react in a timely manner to cyber threats endangering the state, society and the individual, a national comprehensive monitoring, analysis and reporting system is adopted.

1.6. Ensuring digital continuity of the state

E-services, processes, and information systems (including digital registers of evidential value) that are essential for the digital continuity of the state are constantly updated and mapped, and they have mirror and backup alternatives. Virtual embassies will ensure the functioning of the state, regardless of Estonia's territorial integrity.

1.7. Promotion of international cooperation in the protection of the infrastructure of critical information

Protection of critical information infrastructure is enhanced through the participation in the work of international organizations, being represented in the interest groups of partners and allies, and through contributing to the professional development of experts.

Subgoal 2: Enhancing of the fight against cybercrime

The economic damage deriving from cybercrime reduces trust in digital services, and, in a worst-case scenario, could lead to loss of life. Greater awareness among the general public about cyber security risks helps to prevent cybercrimes. Greater awareness is achieved by addressing cyber-related topics at all levels of education and informing people based on research and analysis of secure behaviours.

2.1. Enhancing detection of cybercrime

In order to improve the efficiency of cybercrime detection and prosecution, the current structure of law enforcement and its organisation of work will be further clarified, the number of personnel dealing with cybercrime will be increased and the capabilities of bodies conducting proceedings to process digital data carriers will be raised. In order to develop capabilities, cooperation takes place with universities and international centres of excellence.

2.2. Raising public awareness of cyber risks

In order to raise the level of awareness of actors operating in cyberspace, attention is paid to introducing actions preventing cyber threats, providing the knowledge needed to identify as well as wisely respond to incidents. Users of e-services are directed to use the most secure solutions and are informed about new technologies and how to securely use these solutions.

2.3. Promoting international cooperation against cybercrime

In order to achieve more effective and timely prosecution of cybercrimes with an international dimension, information exchange between countries is improved. Active participation in various initiatives and projects that are part of the international fight against cybercrime.

Subgoal 3: Development of national cyber defence capabilities

Civil, military, and international cooperation based on the resources at the disposal of the state must also function adequately in cyberspace – with regards to warning, deterrence and active defence.

3.1. Synchronising military planning and preparation for civil emergencies

Broad-based national defence requires that the continuous operation plans of vital service providers are coordinated with national defence threat scenarios.

3.2. Developing collective cyber defence and international collaboration

To ensure collective defence in an international environment, information exchange and cooperation are enhanced with NATO, European Union cyber instances and other partners. Efforts are made concerning the creation and development of NATO joint cyber security capabilities, standards, training and training opportunities.

3.3. Developing military cyber defence capabilities

The development of military cyber defence capabilities will result in cyber defence being a part of broad-based collective defence. The latter will be ensured by involving specialists from the Defence Forces and the Estonian Defence League, as well as other public and private sector professionals.

3.4. Ensuring a high level of awareness concerning the role of cyber security in national defence

In order to raise the level of awareness concerning cyber security risks in the field of national defence and to link it with other military domains, additional training is organised for personnel in the field.

Subgoal 4: Estonia manages evolving cyber security threats

To maintain and improve its cyber security capability, Estonia will adopt independent cyber security solutions, which are backed by cyber security training and training opportunities, research and development and entrepreneurship. In order to ensure the sustainability of solutions, the state acts as a smart contractor, and supports the export of cyber security solutions.

4.1. Ensuring the next generation cyber security professionals

To ensure the next generation of cyber security professionals, opportunities for additional education will be established, both in the form of higher education as well as forms of in-service training. Support will be given to raise the number of students having completed a Master's Degree in cyber security and increase the number of doctoral theses on cyber security. Instruction will involve more foreign lecturers and professionals.

4.2. Developing smart contracting for cyber security solutions

In order to create secure solutions, the state will contribute to cyber security-related research and development. A supervisory board shall be set up to coordinate the corresponding activities and to consolidate the domains of national defence, security, economic development and academia.

4.3. Supporting development of enterprises providing cyber security and national cyber security solutions

To support the sustainability of secure solutions, the state will contribute to the export of cyber security solutions, and to increasing their use at the international level.

4.4. Preventing security risks in new solutions

In order to avoid large-scale cyber incidents, the technological risks pertaining to the development and introduction of new technologies are investigated and assessed in depth. A high level of knowledge and risk-awareness facilitate achieving advantages in developing the state, society and economy.

Subgoal 5: Estonia develops cross-sectoral activities

To improve the capabilities necessary for combating cyber threats, a number of overarching objectives are addressed. Adjusting the legal framework and developing cyber foreign policy are vital for protecting critical services, the fight against cybercrime, as well as for designing national defence in cyberspace.

5.1. Development of a legal framework to support cyber security

In order to implement cyber security measures ensuring a more secure cyberspace, the legal framework related to cyber security will be updated.

5.2. Promoting international cyber security policy

In international organisations, an emphasis is placed on introducing and protecting Estonia's foreign cyber security policy positions and vision, along with developing a common understanding on the application of international legal norms and confidence building measures in cyber space. Special attention is paid to the protection of fundamental rights and freedoms and the topic of Internet governance. In addition, development assistance and secure e-solutions support the emergence of free and secure cyberspace in countries where the non-governmental sector lacks the freedom to act and the necessary technical base.

5.3. Closer cooperation with allies and partners

With a view to enhancing relations with allies and partners, cooperation is intensified with close neighbours and cooperation formats are expanded with like-minded countries. A significant effort is made to share cyber security related know-how and experience.

5.4. Enhancing the capability of the European Union

With the goal of promoting the European Union's common cyber security and its policies, joint efforts will be made to raise the cyber capability of Member States and to improve their readiness and ability to deal with new threats.

5. PARTIES RELATED TO THE STRATEGY

The Ministry of Economic Affairs and Communications directs cyber security policy and coordinates the implementation of the strategy. The strategy will be implemented by involving all ministries and government agencies, especially the Ministry of Defence, the Information System Authority, the Ministry of Justice, Police and Border Guard Board, the Government Office, the Ministry of Foreign Affairs, the Ministry of the Interior and the Ministry of Education and Research. NGOs, business organizations, governments, and educational institutions will cooperate in the implementation and assessment of the strategy.

At the request of the Ministry of Economic Affairs and Communications, agencies involved in executing the strategy will submit a written overview of the implementation of the measures and activities each year by 31 January, at the latest. Based on the reviews, the Ministry of Economic Affairs and Communication will evaluate the effectiveness of the measures and activities and will compile a report on the implementation of the strategy annually by 31 May, at the latest. A brief report on the execution of the strategy, consisting of an overview of the activities, difficulties with and the cost of the application, will be presented annually to the Government of the Republic by 30 June, at the latest. The final report on the execution of the strategy shall be presented by the Ministry of Economic Affairs and Communication to the Government of the Republic by 31 May 2018, at the latest.

The action plan will lay out the activities and budget of the strategy as well as the individuals responsible for each part. The four-year cost of the strategy will be nearly EUR 16 million. The report of the action plan that will be submitted to the Government of the Republic will also include propositions on improving the action plan. The activities of the action plan will be reflected in the work plans of the various ministries and other government institutions.

The strategy will not redefine the competencies of the different offices responsible for cyber security.

The list of the persons who participated in compiling this strategy or provided their advice is available in Annex 1 to the strategy, “The list of the participants in the compilation of the Cyber Security Strategy for 2014-2017.” [1]

Annexes:
Annex 1. Parties involved in the preparation of the Cyber Security Strategy for 2014–2017
Annex 2. Sectoral methodology

The strategy was compiled by Sander Retel, national cyber security coordinator of the Ministry of Economic Affairs and Communication