Cyber Security Strategy of Latvia

2014–2018

Cyber Security Strategy of Latvia

2014–2018

CONTENTS

1. Introduction

Latvian state administration, society and economy depend on the opportunities and services ensured by information and communication technology (hereinafter – ICT), and ICT determines the existence of information society in Latvia. The Sustainable Development Strategy of Latvia defines the promotion of the further development of a modern and innovative society, open for new ideas and the use of high technology as an asset for the economic development and global competitiveness of Latvia.[1]

Due to the increasing use of ICT in society, state administration, and the economy, its illegal use, damage, paralysis or destruction may cause threats to state and public security, public order and economic activity, as well as the hindrance of the further development of the national economy. It is possible to intentionally and unintentionally disturb or suspend the operation of the network of state information systems and electronic communications, as well as to encumber the functions of the political, economic and military decision-making mechanisms of the state, cause material damages, misinformation of society, and trigger technogenic failures. Insecurity in cyber space may impact the reliability of the use of ICT and thus prevent the development of a modern and innovative society. During politically, socially, or economically sensitive developments, major cyber attacks may be directed against Latvia. A secure and reliable information society and e-government is not possible in a state without a national competence in cyber security and cryptography.

With the increasing trend of society's range and use of services in cyber space, the number of cyber attacks and methods in which attacks are carried out is increasing respectively.[2]

To reduce and prevent the risks and threats in cyber space, a unified and coordinated cyber security policy involving both the public and private sector is required. The Cyber Security Strategy of Latvia lays down strategic priorities in developing cyber security policy and an accompanying action plan will be introduced in the first half of 2014. The Strategy has been developed in line with documents of international organisations, especially the EU and NATO as well as according to the measures specified in the National Security Concept and the State Defence Concept.

[1] Sustainable Development Strategy of Latvia until 2030.

[2] *Symantec* Internet Security Threat Report 2013 about the increase of attacks and vulnerability in the world.

2. Aims and Basic Principles of the Policy

The aim of the cyber security policy is a secure and reliable cyber space, which ensures a safe, reliable, and continuous supply of services essential for the state and society.

In implementing the cyber security policy, the following principles are being used — development, cooperation, responsibility, and openness.

Development – it is possible to protect against rapidly growing threats in cyber space only by constantly and systematically developing and improving skills in the ICT sector and its security specialisation.

Cooperation – the effective protection against threats in cyber space unrestricted by geographical boundaries of countries or administrative boundaries of institutions is only possible through cooperation at both the national and international level.

Responsibility – it is possible to effectively reduce risks in cyber space only if all parties involved in cyber space, including individuals, state institutions, and private businesses are informed about and aware of the effects of their activity or inactivity on their own security and the security of others.

Openness – the cyber security policy is to be implemented by facilitating the accessibility of information and communication technology while respecting the rights and fundamental freedoms of an individual, searching for a balance between freedom, privacy, and security, as well as promoting good practices, ethics, and standards in cyber space.

3. Overview of Cyber Security in Latvia

Modern society uses ICT more extensively by both directly acquiring information and processing it and creating new and widely accessible tools for self-expression. Convenient and diverse mutual communication tools and platforms are being used to receive services. A total of 75.8 % of the inhabitants of Latvia have used the Internet, while 70.3 % use the Internet at least once a week[1]. The number of electronic transactions in the biggest banks in Latvia exceeds 90 % of the total number of transactions,[2] and more than 25 % of state institution services are available electronically[3].

Extensive use of ICT has changed the daily routine of society, and a virtual environment where physical and digital actions merge has been created. The idea that ICT is a matter of interest of just a small group of professionals has been gradually substituted by the understanding that the entire society is, to a greater or lesser extent, linked with ICT, and the range of services provided and supported by ICT will increase in the following years. Since ICT is widely used, all members of society — from ICT users to managers, decision makers and legislators — should have an understanding about the basic principles of the processes and security of cyber space.

ICT solutions and services have a complicated structure, but they are widely accessible. It is easy to use cyber space to cause damage to an individual, a societal group, or a country as a whole. Furthermore, the use of ICT tools can restrict the rights and fundamental freedoms of an individual or violate the right to privacy and personal data protection.

The situation in Latvian cyber space is characterised by a considerable number of ICT security incidents, from several incidents of high significance to hundreds of incidents of low significance affecting state and municipal institutions, private businesses and individuals. According to an overview by CERT.LV, 4964 high priority incidents and over 200 thousand low priority incidents have been registered in 2013.[4] The trend of politically, socially or economically sensitive developments being accompanied by intentionally organised cyber attacks in is increasing. Latvia may be subject to an increased risk during its 2015 Presidency of the Council of the EU.

In order to reduce the number of cases when with the help of ICT damage to society is caused, it is important to develop a set of comprehensive measures that would protect cyber space and its services. The strategy sets five priority areas of action:

1. Governance and Resources of Cyber Security.
2. Rule of Law in cyber space and reduction of Cyber Crime.
3. Crisis management.
4. Awareness raising, education and research.
5. International cooperation.

[1] Central Statistical Bureau. Inhabitants using computer/Internet at the beginning of the year. 2012.

[2] Latvian Internet Association. Study of Internet Banking in Latvia. 2011.

[3] Ministry of Environmental Protection and Regional Development. Results of Assessment and Qualification of all Public Services Provided by the State. Summary of all Department Services. Version 1.0.2012.

[4] CERT.LV Overview 2013.

4. Key Areas of Action

4.1. Governance and Resources of Cyber Security

ICT solutions and services are developed, improved and maintained in both the public and the private sector. For the solutions and services to be reliable, safe and continuous, it is necessary to apply information security requirements, standards, and good practices throughout their entire life cycle by including risk analysis based security planning, and assessing political, economic, social, legal, and personal data protection aspects. Cyber security policy implementation in Latvia involves a broad, comprehensive range of interested parties; therefore it is necessary to create an effective cyber security governance model.

National Cyber Security

National cyber security should be viewed in three dimensions — infrastructure, services, and processes — where the provision of information safety is required. At the moment, cyber security governance is organised in a partially centralised model, where the leading institutions (according to the respective authority) perform the function of handling the strategy, methodology and coordination of cyber security, whereas supervisors of specific ICT solutions and services constantly ensure practical implementation and execution of the established requirements. National cyber security is based on mutual cooperation, where each state authority performs its functions, including in cyber space, and cooperates with other involved parties directly or through the National Information Technology Security Council (hereinafter — Council). The Council has been established by the Law on the Security of Information Technology, which determines the development of cyber security policy at a national level. According to the Law the Council coordinates the development of cyber security policy and planning and implementation of objectives and measures. The Council is the central national authority for the exchange of information and cooperation between the public and private sector, and its operation is ensured by the National Cyber Security Policy Coordination Section of the Ministry of Defence.

National cyber security policy is developed by (Visualisation in Appendix No. 1):

1. **Ministry of Defence (MOD)** – coordinates development and implementation of information technology security and protection policy, as well as cooperates in the provision of international cooperation. The National Cyber Security Policy Coordination Section of the MOD organises and provides support for the implementation of cyber security policy.
2. **Ministry of Foreign Affairs (MFA)** – coordinates international cooperation and Latvia's participation in various international initiatives related to the cyber security.
3. **Financial and Capital Market Commission (FCMC)** – regulates and supervises activities in cyber space of members of the financial and capital market cyber space; **the Bank of Latvia (BoL)** promotes secure and smooth operation of payment systems, while credit institutions are responsible for secure availability of electronic services in their sector.
4. **Ministry of Economics (MoE)** – develops economic policy and promotes the development of competitiveness and innovation.
5. **Ministry of the Interior (MoI), State Police (SP)** and **Security Police (SeP)** – implement the policies for combating crime, public order, security protection, and the

protection of rights and legal interests of individuals, as well as coordinates the settlement of crisis situations.

6. **Information Technology Security Incident Response Institution CERT.LV** – monitors and analyses developments in cyber space, reacts to incidents and coordinates their prevention, carries out research, organises educational events and training, as well as supervises the implementation of obligations specified in the Law on the Security of Information Technology. CERT.LV provides support for Latvian and foreign state and municipal institutions, entrepreneurs, and individuals.
7. **Ministry of Education and Science (MoES)** – promotes knowledge and understanding of cyber space and its secure use.
8. **Ministry of Welfare (MoW)** – implements the social policy and the policy for the protection of children's rights.
9. Operation of the **Safer Internet Centre of Latvia *NetSafe* Latvia** is ensured by the Latvian Internet Association, educates society about possible risks and threats online, and promotes the use of secure internet content.
10. **National Armed Forces (NAF) and Cyber Defence Unit (CDU)** – provide support in crisis situations.
11. **Non-governmental organisations in the IT sector** – provide support, consult and cooperate with the Council in developing and implementing the cyber security policy[1].
12. **Ministry of Transport (MoT)** – organises the implementation of communication policy.
13. **Constitution Protection Bureau (CPB)** – oversees the critical infrastructure.
14. **Ministry of Justice (MoJ) and Data State Inspectorate (DSI)** – develop, organise and coordinate the policy on rights in the field of personal data protection, freedom of information and supervision of electronic documents.
15. **State Joint Stock Company "Latvian State Radio and Television Centre" (LSRTC)** – the only provider of reliable certification services, which ensures the infrastructure of electronic identity cards and electronic signatures.
16. **Ministry of Environmental Protection and Regional Development (MEPRD)** – organises the governance of state ICT and coordinates the electrisation of public services, whereas **State Regional Development Agency (SRDA)** ensures the operation and development of solutions for shared use of state ICT.

The Law on the Security of Information Technology and related Cabinet regulations determine basic security requirements for state and municipal institutions and providers of public electronic communications services, as well as supervisors of the critical infrastructure of ICT. In cases of incidents, a set of definite procedures for state and municipal institutions and owners and legal managers of the critical infrastructure are established.

In the private sector, the governance of information security is based on the sustainability of business and secure and reliable provision of services. In some sectors, there are laws and regulations which, for example, apply to credit institutions, providers of electronic services, or personal data protection; but good practices and standards for the security of ICT solutions are not widely used. The market of electronic communication operators is scattered, and a part of service

[1] Existing partners of the Council: association "ISACA Latvia Chapter", Latvian Open Technology Association, Latvian Information and Communication Technology Association, Latvian Internet Association, Association of Commercial Banks of Latvia, Latvian Chamber of Commerce and Industry.

providers do not fulfil the requirements specified in the legislation, thus causing security risks to both clients and other users of ICT infrastructure in Latvia and abroad.

According to the Law on the Security of Information Technology, a national Information Technology Security Incident Response Institution CERT.LV has been created. CERT.LV maintains common monitoring of cyber space, provides support for Latvian and foreign state and municipal institutions, entrepreneurs and individuals in preventing IT security incidents as well as coordinates the prevention of security incidents. As activity in cyber space increases, CERT.LV together with institutions from the public and private sectors must develop resources which would allow the summarization of technical information about incidents in cyber space and storage of this information for analysis and evaluation.

Required actions:

1. Improve coordinated development, implementation and evaluation of the national cyber security policy within the framework of the National IT Security Council through cooperation of representatives of public, non-governmental and private sectors. Strengthen the leading position of the Ministry of Defence in a coordinated development and implementation of the cyber security policy.
2. Create an information exchange medium (platform) by promoting the exchange of information among entrepreneurs about topical cyber security threats, problems, solutions, good practices, and their application.
3. Implement the assessment of risks to national cyber security.
4. Promote the standards and practices of good security management in the public and private sector by creating understanding about ICT security in the business environment and organising regular training for leading employers.
5. Improve the mechanism of implementation and monitoring of security requirements for electronic communication operators.
6. Improve the ability of CERT.LV to observe, analyse and prevent IT security incidents and cooperate with NATO and EU partners on information exchange.
7. Develop CERT.LV resources and competences to perform centralised security tests.

State owned ICT

Cyber security at a national level is closely connected to the state ICT governance system, which is now partially regulated by the Law on State Information Systems. Its further development has been outlined in the concept of the organisational model of state ICT management. The concept sets many tasks for the optimisation of state ICT and the improvement of management processes of state ICT. Fulfilment of necessary tasks would allow reaching a homogenous, more shared and professionally and rationally maintained state ICT infrastructure, which would attract better motivated human resources with a higher degree of specialisation and higher professional competences, thus increasing the overall level of state ICT security. The optimisation of state ICT would, inter alia, allow focusing of resources for the improvement of the technological security of state ICT solutions, for example, by creating shared solutions for the continuity of operations, etc. With respect to the management of state ICT, the concept provides for the development and implementation of standards and guidelines for the continuity, reliability and security of electronic state administrative processes.

Currently used state ICT solutions and especially state information systems (SIS) contain information, illegal exposure

or acquisition, distortion or deletion of which can cause significant damage to a specific person, society, or state. Denying access to SIS or interrupting the operation of support systems can completely or partially paralyse the work of the public administration. Therefore it is important that the development, introduction and operation of state ICT solutions, including security management, is carried out in a rational, effective, transparent and mutually harmonised manner by using best practices of the sector and guidelines to minimise to the occurrence of ICT security threats due to mistakes as well as deliberate actions.

The Law on State Information Systems provides for a single level of technical and organisational requirements for all registered systems irrespective of their functionality, value of the collected information, and influence on the execution of functions of the public administration, both within the institution and outside of it. The lack of differentiation of requirements causes inadequate pressure on systems of varying significance and capacity, as well as the willingness to avoid system registration. Differentiation of the requirements and categorisation of the systems would allow the application of more precise and - appropriate legal measures in case of a criminal offence.

The case study by MoEPRD suggests that one half of the holders of state information systems do not ensure measures for security management, as they are not motivated or competent. The state ICT security monitoring and control system is insufficient.

Required actions:

1. Continue the implementation of improved management measures specified in the conceptual organisational model of state ICT management, which provides for the development of a unified ICT architecture and development or improvement of management processes, standards and guidelines.
2. Develop a legal order for a unified management of the provision of state ICT that provides for a categorisation of systems based on a risk analysis and appropriately differentiated requirement framework for security management.
3. Improve the understanding and knowledge of the holders of ICT solutions and infrastructure by organising training programmes for the managing staff of the state administration and the staff involved in ICT security management.
4. Evaluate the efficiency of the supervision of ICT security management, the responsibility and penalties for not implementing the security management measures, as well as to establish minimum requirements for the work of security managers.
5. Organise extraordinary audits and security tests of state ICT solutions and infrastructure performed by independent organisations.
6. Develop the procedure according to which the institutions report to a common competent authority about the implementation of information security measures.
7. Improve the cooperation between the Latvian Association of Local and Regional Governments, Municipalities and Institutions in order to improve the security management of municipal ICT resources.

Critical Infrastructure

Critical infrastructure of information technology has been established for the performance of basic functions essential for state and society to ensure the integrity, accessibility and confidentiality of the critical infrastructure. Once a year the Cabinet of Ministers establishes and reviews the information technology infrastructure whose termination

can substantially threaten the existence of the state.[1] The critical infrastructure of information technology has been included in the critical infrastructure of the state, and its owners and legal managers, in cooperation with security institutions and CERT.LV, consistently improve security measures. Planning and implementation of security measures for critical infrastructure is regulated by the Cabinet of Ministers.[2] For the purposes of exchange of knowledge and experience, as well as for the improvement of procedures, representatives of critical infrastructures are regularly involved in training organised by CERT.LV.

Required actions:

1. Improve the processing of information and experience exchange about incidents, protection of the critical infrastructure and prevention of risks among the holders of critical infrastructures, CERT.LV and state security institutions.
2. Organise crisis training and security breach tests at a national, regional and international level and in cooperation with the Cyber Defence Unit of the National Armed Forces (NAF).
3. Strengthen the security of state ICT resources by developing technical tools for the automatic provision and control of security, as well as to improve the capacity, knowledge and mutual cooperation of the security staff.

[1] Cabinet Regulation No. 496 of 1 April 2010 "Planning and Implementation Procedure of Identification and Security Measures for the Critical Infrastructure, including the Critical Infrastructure of Europe."

[2] Cabinet Regulation No. 100 of 1 February 2011 "Planning and Implementation Procedure of the Security Measures for the Critical Infrastructure of Information Technology"

Human Resources

The situation in state and municipal institutions is characterised by significant differences in human and material resources, from institutions with well-paid and highly qualified employees and modern technical resources to — in most cases —institutions with employees with inadequate qualification and low quality information technology. This creates an unequal level of fulfilment of obligations laid down by the legislation in the area of information security management in the state administration. Furthermore, the restricted availability of highly qualified experts in the labour market does not meet the demand of the private sector and companies are using outsourcing services to carry out their functions.

The number of ICT security management experts and security technology experts in the Latvian labour market is small. The professional standard for ICT security managers and a certification procedure for this speciality have not been established, and study programmes in computing, computer science and information technology do not purposefully train experts for this specialisation. There are minimum competency requirements established for the ICT security managers in state administration institutions. IT specialists from state and municipal institutions participate in "Be secure" training seminars and annual briefings in the institutions; however, the acquired amount of knowledge is restricted and its use in practical situations is not being practised and tested.

Required actions:

1. Assess and raise existing professional standards related to the ICT by including the requirements for the knowledge about and skills for cyber security.
2. Define, increase and assess the professional competencies of experts responsible for cyber security and promote

the use of expert certifications acquired abroad for the confirmation of such competencies.
3. Promote the contribution of higher education institutions by including cyber security specialisation in study programmes.
4. Perform a labour market analysis about the demand, supply, remuneration of cyber security experts and the employment level of experts prepared by educational institutions.
5. Improve the competencies of the teaching staff in the area of cyber security and to support the preparation of methodological materials.

4.2. Rule of Law in Cyber Space and Reduction of Cyber Crime

Rule of Law in cyber space is based on the principle of equivalency, which provides for the observation of laws and regulations both in the physical and the virtual environment. The state is obliged to ensure the basic rights and freedoms of any person laid down by the Constitution and the observation of principles of universal rights irrespective of their field of application. The provided technological opportunities have favoured the increase of criminal offences in cyber space. To commit such offences, criminals use automatic data processing systems as a tool for committing crimes that direct them towards another protected or publicly inaccessible automatic data processing system or its resources. An automatic data processing system can also be used as a medium for the circulation of illegal or offensive and defamatory (incitement to racial hatred, distribution of child pornography, etc.) information.

The reduction of cybercrime requires action in two basic directions — preventive work for the reduction of criminal offences and effective combating of crime.

The complicated structure and operation of cyber space outline two problematic areas in the implementation of effective combating of cybercrime. Firstly, the understanding of the concept "significant damage" and its application is an important precondition for establishing constituent elements of a criminal offence and appropriate qualification and punishment of a criminal offence. Secondly, investigation and collection of evidence in cyber space requires specific knowledge.

Implementation of preventive actions requires organised ICT and a legislative base regulating its security, as well as effective use thereof. The existing capacity in combating cybercrime should be developed by strengthening electronic evidence. Investigation, as well as collection and assessment of evidence requires special knowledge and a sufficient level of competence is crucial in law enforcement agencies, prosecutor's offices and courts to ensure the rule of law in cyber space.

Required actions:
1. Assess the laws and regulations in the ICT sector as a foundation for applying the Latvian Administrative Violations Code and Criminal Law and to improve this foundation to ensure effective protection of individuals' interests through and in relation to criminal law.
2. Assess the present situation and the necessary amendments in legislation that provide for punishment for causing damage to the security or operation of information systems directed towards automatic data processing systems.
3. Develop the terminology related to the information security and cyber security in the Latvian language and harmonise its use in the legislative enactments.

4. Assess and improve the supervision of obligations in the area of cyber security laid down by the legislative enactments and to promote support for the fulfilment thereof.
5. Facilitate discussions and exchange of opinions about the identification of new ICT crimes and improvement of the legal basis for the restriction thereof in line with the international trends.
6. Combat and investigate cybercrimes by assessing and improving the existing resources, procedures, cooperation mechanisms, and their efficiency.
7. Assess and develop the existing capacity of acquiring and analysing evidence in the process of investigation of cybercrimes by developing the competence of SP and improving the cooperation with CERT.LV.
8. Develop methodical materials for studies about the ICT sector for the purposes of increasing the knowledge of police officers, persons directing the proceedings and judges about the ICT sector and to implement an in-depth training programme about the issues of combating cybercrime.
9. Develop a unified mechanism for listing the criminal offences in cyber space (statistics) in the system of police, prosecution and court.

4.3. Preparedness and Capacity to Act in Crisis Situations

Institutions which ensure national cyber security capabilities have been set up in Latvia. Plans for action in the case of increased threat have been developed and are being regularly updated. Cooperation with the Ministry of the Interior for solving different crisis situations has been established. The involvement of experts is available in collaboration with the private sector. However, the present resources and measures are not sufficient and organised enough to ensure efficient and prompt action in the case of serious and extensive ICT security incidents or cyber attacks.

The present situation in Latvia and threats in cyber space, as well as resources for the prevention of risks and management of a crisis that are at the disposal of the state have been assessed in the cyber crisis exercise by the Cabinet of Ministers on 7 December 2012. Reduction of incidents and the prevention of a crisis require individual understanding about cyber security and the responsibility of each organisation, where CERT.LV can give advice on daily work or provide support in cases of serious and unexpected incidents.

Considering the limited resources of the state administration and the conclusions of the cyber crisis exercise, the NAF are developing a Cyber Defence Unit to provide support for CERT.LV and NAF units in preventing ICT security incidents and management of consequences in crisis situations in cyber space or in war time. The Unit would be used should CERT.LV resources be insufficient and involvement of the Unit would faster expedite the implementation of emergency measures or if the Unit had at its disposal special resources for performing such activities.[1] The Unit is being created as a back-up team of experts consisting of volunteers from the public and private sector according to the legal basis of the service of the National Guard.

To ensure the functioning and strengthening of the infrastructure of electronic communication the existing infrastructural capabilities should be developed (especially with respect to resistance to the influence of external conditions),

[1] Concept of the National Armed Forces Cyber Defence Unit of the Ministry of Defence, Rīga, 2013.

as well as a new infrastructure for securing the basic functions of a state, especially when the daily use of electronic communication networks can be restricted.

Required actions:

1. Evaluate the definition of a crisis, its procedures, legislation and the use thereof in the case of a possible cyber crisis.
2. Develop the capabilities of the NAF and the Cyber Defence Unit to react in a crisis situation and in managing the consequences of major incidents by providing and ensuring operational capability of the Unit.
3. Develop information technology and communication systems for the NAF to ensure the support of NAF management capabilities in crisis situations.
4. Organise regular theoretical and practical training at a national level with the involvement of high officials and merchants in order to develop mutual understanding and coordinate the management of crisis situations.
5. Improve the competence and resources of state institutions when preparing and ensuring the presidency of the Council of the European Union in 2015 when global cyber attacks may be directed against Latvia.
6. Develop regional and international cooperation, to ensure regular training for providing and receiving support in a crisis situation.
7. Establish an electronic communication network for emergency situations.
8. Develop a technological and organisational solution that provides state institutions with infrastructure and ensures high confidentiality and integrity of and accessibility to state information systems.
9. Strengthen the outer scope of the national external communication network: establish, categorise, coordinate, evaluate risks, and make necessary improvements to ensure a reliable and secure flow of data between Latvia and other countries, but, when necessary, to use the network for changes in data flows or the restriction thereof between countries.

4.4. Awareness Raising, Education and Research

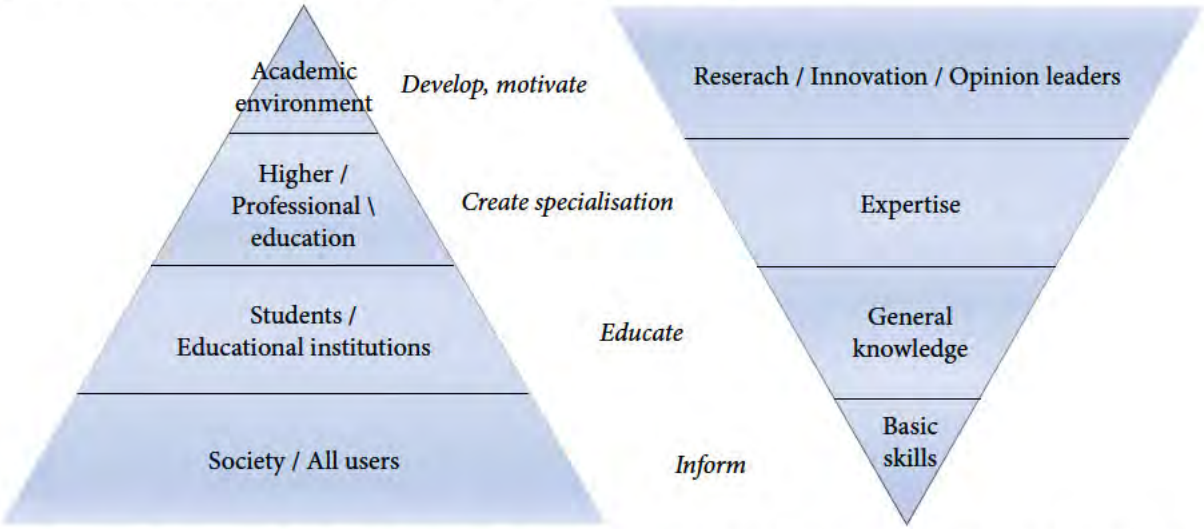
An informed society is a crucial part of a secure and reliable cyber space. Awareness is ensured by purposeful and regular explanatory work, including the policy and communication implemented by the leading officials of a country, raising the issues in educational institutions and organising regular discussions of experts in the media.

The level of awareness of a society about the threats to ICT, tools available for their prevention, personal rights in the electronic medium and their infringement, as well as about action in the case of a threat is low. According to the statistics of CERT.LV, in almost all cases when the devices of users have been infected and have become a part of botnets (approximately 15–20 thousand a month), the users have not deliberately caused damage and the cause of the infection is software that has not been updated or the lack of antivirus solutions when malicious e-mail attachments are opened. Along with raising awareness of society, it is important to increase understanding about ethical norms and moral responsibilities in the electronic environment.

To improve the knowledge of ICT users, it is necessary to implement a set of complex measures, starting from primary and secondary education. It is necessary to organise regular information campaigns in cooperation with non-governmental and private institutions, as well as constantly reflect the information in mass media. At the moment, cyber security issues are only tested in a uniform model in general education in an informatics examination (knowl-

edge test part) at the secondary education level. Although the average level of answered questions is comparatively high (2013 — 0.79%), it is impossible to assess the actual actions of students in daily life. The type of communication (channel), content and methodology is to be applied according to the chosen target audience (see Figure 1).

Figure 1. The level of cyber space security knowledge according to the target audience.



At the moment, there are no academic study programmes and scientific activity in the area of cyber security and people studying the respective subjects abroad are not motivated to return to Latvia due to low salaries, lack of opportunities for professional development. According to a study by the World Economic Forum, Latvia ranks 110th with regard to the availability of scientists and engineers.[1]

To develop new study programmes and educate experts and professionals from other sectors (e.g., experts in law) about ICT issues, a teaching staff with an appropriate competency is required. Competency should be increased by creating and supporting security research groups at universities and scientific institutes. These would, firstly, attract Latvian specialists who are currently working abroad, serve as a basis for the creation of a national cyber security (including cryptography) school, provide the opportunity in the future to successfully participate in scientific EU projects and, finally, to create commercial products with a high added value.

Required actions:

1. Increase the competency of educational institutions and teaching staff and their contribution to educating children and youth about the issues of ICT security by integrating these issues into the educational system and

[1] World Economic Forum "The Global Competitiveness Report 2012–2013", p. 227.

organising learning activities that create understanding about information security, privacy protection and the use of reliable e-services. Additionally, opportunities must be ensured for children and youths to report violations on the Internet and to receive support from a psychologist. Further education of the teaching staff about the issues of cyber security must be organized.

2. Develop educational and informative materials about cyber security for use in educational institutions and interest groups that are easily accessible and differentiated according to various age groups.
3. Develop academic studies and research in cyber security to train experts, promote innovation, establish public-private partnerships for the support of science and research, and to attract European funds, grants and financial instruments.
4. Create an ICT security laboratory and to organise scientific conferences about topical issues concerning cyber security and cybercrime in cooperation with universities and scientific institutes.
5. Implement educational and informative campaigns and other measures for the overall enhancement of the understanding of society about the cyber security, cybercrime and important threats, to expand the accessibility of various ICT security software.
6. Develop the exchange of information and opinions among public administration, associations of the sector, experts, business leaders, as well as creators of public opinion — non-governmental organisations and the academic environment.
7. Participate in international informative initiatives and platforms, use the European Cyber Security Month and the e-Skills Week to raise issues about the cyber security.
8. Promote innovation in the cyber security sector and develop a unified academic resource of high-capacity computing (supercomputer).

4.5. International Cooperation

The opportunities and security threats provided by cyber space do not recognize national borders and therefore no state can effectively face new security challenges on its own.

Due to the awareness of the increasing role of cyber space in every society, cyber security as an important issue has been included on the agenda of cross border cooperation and by international organisations. In bilateral and multilateral cooperation, a wide range of issues are usually considered — from observation of human rights in the virtual environment to combating of crime, often also involving the private sector. Under these conditions, different national interests inevitably collide, and thus far the international community has not reached significant progress in creating a common understanding and approach. At the same time, many non-harmonised processes still take place. It is important for Latvia to have knowledge of the work of international and regional organisations and to participate in this work while at the same time expressing support for ensuring the basic principles of a democratic society in the virtual environment. It should be not only be safe, but also free and accessible.

Latvia is taking part in international processes, including the work of NATO, the EU, OSCE and UN, to promote the improvement of a secure, free and accessible cyber space. Latvia supports the first comprehensive resolution of the United Nations Human Rights Council on human rights in the virtual space and will continue to participate and strengthen such initiatives as the Freedom Online Coalition, which focuses on observing human rights and basic freedoms in cyber space, especially the freedom of speech.

Latvia has joined the Council of Europe Convention on Cyber Crime and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. According to the Convention, all involved countries harmonise their legal regulations to cooperate in the investigation of crimes and to ensure that the people responsible for committing cybercrimes are held liable.

Cyber security is an important part of national defence, and nationally developed defence capabilities can be strengthened by cooperating with NATO and EU member states in a crisis situation. To receive effective support when necessary and to strengthen cyber security measures in the Euro-Atlantic space, the development of both collective and individual cyber protection capabilities of each member state should be facilitated in accordance with the approved NATO and EU cyber security planning documents. NATO has approved the Cyber Defence Concept and Action Plan and corresponding planning documents, which provide for the necessity to promote the development of cyber security capabilities of both NATO as a whole and each individual member state.

Required actions:

1. Strengthen cooperation with countries from the Baltic and Northern European countries and improve the cooperation with NATO, the EU, OSCE and UN to improve the security, accessibility and freedom of ICT.
2. Support international efforts in enhancing mutual trust and cooperation, emphasising the equal applicability of international legal norms to both the physical and the virtual environment.
3. Create a common Baltic university study programme to combine regional educational resources to preparing strong and qualified experts.
4. Organise international cyber security events in Latvia on a regular basis, highlighting Latvia as a country that takes care of the security of ICT at a national and international level.
5. Develop and test national procedures to receive prompt and effective help in case of a cyber threat according to the Memorandum of Understanding between Latvia and NATO and pursuant to the NATO Cyber Defence Concept and Action Plan.
6. Strengthen cyber protection capabilities by participating in various international training courses, exercises and cyber attack simulations within NATO, the EU, and other international organizations and forums, giving local experts and the Cyber Defence Unit the opportunity to improve their knowledge about the latest solutions in information systems security.

5. Link to Other Development Planning Documents

National documents:

- National Security Concept
- State Defence Concept
- Law on the Security of Information Technology
- Law on State Information Systems (authored by MoEPRD)
- Sustainable Development Strategy of Latvia until 2030
- Guidelines for the Development of Information Society in 2014–2020
- Concept of the Organisational Model of the State Information and Communication Technology Management.
- Guidelines for the Electronic Communication Policy in 2011–2016
- Authentication Law (authored by MoEPRD)
- Concept of the National Armed Forces Cyber Defence Unit of the Ministry of Defence, 2013.

International documents:

- UN Human Rights Council resolution: The promotion, protection and enjoyment of human rights on the Internet
- NATO Strategic Concept
- NATO Concept on Cyber Defence
- NATO Cyber Defence Policy Action Plan
- EU Cyber Security Strategy
- Convention on Cybercrime (Budapest Convention)
- Europe 2020 A Strategy for Smart, Sustainable and Inclusive Growth
- Digital Agenda of the EU
- Directive of the European Parliament and of the Council on attacks against information systems

6. Conclusions

An ex-ante evaluation of the proposed solution has not been carried out, since cyber security is constantly and rapidly developing, but the fields of action established in the guidelines are a continuation of priorities specified in the National Security Concept and actions initiated so far. The evaluation of the cyber security provided for in the guidelines will create a basis for assessing and improving further policy and the action plan.

Based on the guidelines, an action plan will be developed, which will include detailed results of the actions and calculations on the influence on state and municipal budgets in 2014 and in the following years. Every two years, the Ministry of Defence performs an evaluation of the guidelines and implementation of the action plan within the Council and submits an informative report and, if necessary, proposals for raising the issues of the guidelines to the Cabinet of Ministers.

There are no policy planning documents that are be deemed as having lost their validity. At the same time, implementation of priorities laid down by the National Security Concept shall continue.

7. Acronyms and Definitions of Terms

Acronyms

BoL	Bank of Latvia
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence in Tallinn
CDU	Cyber Defence Unit of the National Armed Forces
CERT.LV	Information Technology Security Incident Response Institution
CPB	Constitution Protection Bureau
DISS	Defence Intelligence and Security Service
DSI	Data State Inspectorate
ENISA	European Union Agency for Network and Information Security
EU	European Union
FCMC	Financial and Capital Market Commission
ICT	Information and communication technology
IT	Information technology
LSRTC	Latvian State Radio and Television Centre
MoE	Ministry of Economics
MoEPRD	Ministry of Environmental Protection and Regional Development
MoES	Ministry of Education and Science
MoFA	Ministry of Foreign Affairs
MoI	Ministry of the Interior
MoJ	Ministry of Justice
MoT	Ministry of Transport
MoW	Ministry of Welfare
NAF	National Armed Forces
NATO	North Atlantic Treaty Organization
NetSafe	Safer Internet Centre of Latvia Net-Safe Latvia
OSCE	Organization for Security and Co-operation in Europe
SeP	Security Police
SIS	State information systems
SP	State Police
SRDA	State Regional Development Agency
UN	United Nations

Electronic communication operator
A merchant or affiliation of a foreign merchant who has the right to perform commercial activities, provide a public electronic communication network or electronic communication services pursuant to the procedure laid down by the Law on Electronic Communications.

Electronic communication network
Transmission systems, commutation and routing devices (including elements of the network that are not used) and other resources that allow to transmit signals in the network with the help of cables, radio waves, optical or other electromagnetic means irrespective of the information transmitted.

E-government
Effective management of the state and municipal administration with the use of information and communication technology.

Information society
A society whose members are able and have the opportunity to acquire information with the help of information and communication technology, link it with the existing knowledge and use the newly acquired knowledge for increasing their welfare.

Information technology
Technology that uses electronic processing of data, including creation, deletion, saving, reflection and transmitting, for the purposes of performing the required tasks.

Information technology security incident
A harmful event or offence, as a result of which the integrity, availability or confidentiality of information technology is endangered.

Information and communication technology
A set of knowledge, methods and technical equipment that ensures acquisition, storage and distribution of any information with the help of computers and communication tools.

Cyber security
Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.[1]

Cyber space
Cyber space is an interactive environment that includes users, networks, computing technology, software, processes, information in transit or storage, applications,

[1] Definition by the International Telecommunication Union in the English language: *"Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment."* ITU-T X.1205.

services, and systems that can be connected directly or indirectly to the Internet, telecommunications and computer networks. Cyber space has no physical boarders.[1]

Critical infrastructure

Critical infrastructure is the objects, systems, or their parts in Latvia, which are important in providing the performance of functions essential to society, as well as for ensuring the protection of human health, security, economic or social welfare, whose destruction or malfunctioning may significantly influence the performance of state functions. The critical infrastructure of information technology is protected in order to ensure the performance of basic functions essential to the state and society.

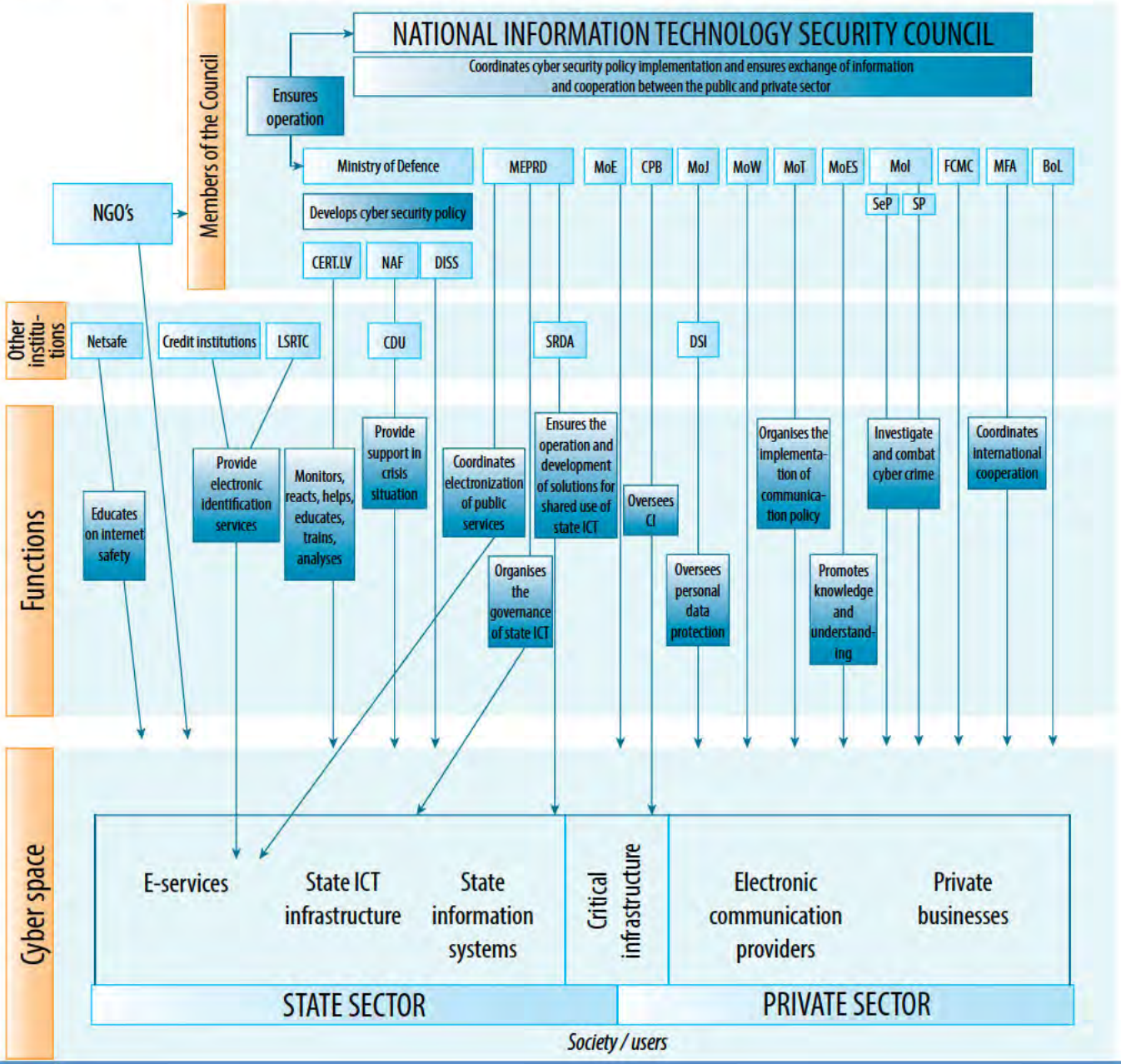
State information and communication technology

According to the scope and objective of the Concept of the Organisational Model of the State Information and Communication Management, state information and communication technology in this document refers to information and communication technology solutions and services used, introduced, maintained, and operated by direct administration institutions and institutions under direct subordination or supervision thereof.

With respect to municipalities and legal entities or natural persons of private law delegated to perform the duties of the state, the concept of state information and communication technology is applicable to the information and communication technology solutions and services that are used in order to perform such delegated duties of the state.

[1] Definition of the "cyber space" from the International Telecommunication Union National Cyber Security Strategy Guide in the English language. *"We use the term cyberspace to describe systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks"* and the description of cyber space in the ITU recommendation *"[This] includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks."* ITU-T X.1205. Available at: http://ej.uz/OverviewOfCybersecurity

Appendix No. 1 — Visualisation of National Cyber Security Policy Coordination



National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu