17.09.2019

Informative Statement

Cybersecurity Strategy of Latvia 2019–2022

Riga, 2019

Table of contents

Annex:

Priorities in each of axis (information for official use only)

Summary

Informative Statement *Cybersecurity Strategy of Latvia 2019-2022* (the Strategy) has been drafted in accordance with the Article 11.2 of the Law on the Security of Information Technologies. Strategy provides a description of national cybersecurity context, identifies future challenges and defines national cybersecurity policy courses of action for the period up to 2022.

Cybersecurity is a part of comprehensive national defence framework. In a comprehensive national defence framework, where each member of the society is organised to protect the country against all kinds of attacks, both military and non-military, cybersecurity is of increasing importance, given the impact of a cyber-attack (information technology (IT) security incident) against the country and society.

Cybersecurity policy aims to create a safe, open, free and reliable cyberspace. An environment where public and private sector can receive and provide vital services without safety, reliability or disruption concerns. A system that respects individual human rights in physical and virtual world.

Key objectives of Cybersecurity Policy 2019-2022 include strengthening and development of cyber defence capabilities, enhanced resilience against cyber-attacks and better public awareness on threats associated with cyberspace. Priorities for implementation of Cybersecurity Policy 2019-2022 are defence, deterrence and development.

Considering European Union priorities and targets defined in national-level policy planning framework and other relevant documents, Strategy 2022 is focused on five courses of action:

- promoting cybersecurity, reducing digital security risks
- strengthening the resilience of information and communication technologies, the provision of information and communication technology solutions and services critical to the society
- public awareness, education and research
- international cooperation
- rule of law in cyberspace, combating of cybercrime

More elaborate information about these courses of action can be found in Chapter 4 of the Strategy. According to vision and objectives of the Strategy, each axis consists of specific activities, delivery deadlines, managing and responsible authorities, financial sources and performance indicators, which will facilitate attainment of set strategic goals and vision. Priorities/actions in each axis, which contain information for official use only, are described in the Annex to the Strategy (information for official use only).

Managing and responsible authorities continue to deliver regular activities started under the previous period’s strategy. Moreover, activities identified in the Strategy do not preclude stakeholders from engaging in other activities not covered by the Strategy.

Responsible authorities are expected to implement 2019 activities of the Strategy based on the approved budget allocation. Any additional allocations for 2020-2022 are discussed when deciding on annual budget for the year and medium-term budgetary framework based on priority initiative funding requests submitted by all line ministries and other central government bodies.

Abbreviations

CDU	National Armed Force Cyber Defence Unit
CERT.LV	Information Technology Security Incident Response Institution
CI	Critical infrastructure
CPB	Constitution Protection Bureau
CSB	Central Statistical Bureau of Latvia
CSDP	Common Security and Defence Policy
DSI	Data State Inspectorate
ENISA	European Union Agency for Cybersecurity
EU	European Union
FCMC	Financial and Capital Markets Commission
FL	Finance Latvia
IC	Ministry of Interior Information Centre
ICT	Information and communication technologies
IoT	Internet of things
IP	Internet protocol
IT	Information technologies
LALRG	Latvian Association of Local and Regional Governments
LB	Bank of Latvia
LIA	Latvian Internet Association
LIDA	Latvian Investment and Development Agency
LIKTA	Latvian Information and Communications Technology Association
LNRTC	Latvian National Radio and Television Council
MIDD	Defence Intelligence and Security Service
MilCERT	Military Information Technology Security Incident Response Team
MoC	Ministry of Culture
MoD	Ministry of Defence
MoE	Ministry of Economics
MoES	Ministry of Education and Science
MoF	Ministry of Finance
MoFA	Ministry of Foreign Affairs
MoI	Ministry of Interior
MoJ	Ministry of Justice
MoT	Ministry of Transport
MoW	Ministry of Welfare
NAF	National Armed Forces
NATO	North Atlantic Treaty Organisation
NetSafe	Internet Safety Centre NetSafe Latvia
NGO	Non-governmental organisation
NITSC	National Information Technology Security Council
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation for Security and Co-operation in Europe
PUC	Public Utilities Commission
SBF	State Border Guard
SC	State Chancellery
SCDS	Supervisory Committee of Digital Security
SIS	State information systems
SP	State Police
Strategy	Informative Statemente Cybersecurity Strategy of Latvia 2019-2022
UN	United Nations
VARAM	Ministry of Environmental Protection and Regional Development
VDD	State Security Service
VID	State Revenue Service
VRAA	State Regional Development Agency
VSAA	State Social Insurance Agency

Introduction

Strategy describes national cybersecurity[1] context in Latvia, identifies future challenges and defines national cybersecurity policy course of action for the period up to 2022, providing continuity for key cybersecurity development initiatives implemented under Cybersecurity Strategy of Latvia 2014-2018[2].

Cybersecurity is a part of comprehensive national defence framework. Given the impact of a cyber-attack on a state or society, cybersecurity has come to the fore of comprehensive national defence framework, which seeks to mobilise every citizen in defending the state against all types of threats, both military and non-military.

Change of Information and communication technologies (ICT) is accelerating at an unprecedented speed and exponential penetration rates both in Latvia and the world. Recent generation ICT tools provide convenient and instant real-time access to all kinds of information about events and trends in Latvia and elsewhere, facilitating communication and exchange of data, wire transactions and online banking, digital services, drafting, signing and sending of electronic documents and storing of information on digital platforms operated by smart devices and cloud computing technologies that have made everyday life a lot easier.

Latvia and the world are entering the age of digital society. New paradigms and approach to everyday functioning and interactions between society, businesses and public administration is replacing the existing structures. However, the enormous variety of opportunities accompanying the dawn of digital society are tainted by various risks, such as cyber attacks on users and hardware of ICT systems run by private and non-governmental actors, as well as government bodies. One of the preconditions of successful digital society is trust of people, businesses and government sector in ability of ICTs and digital solutions to ensure uninterrupted delivery of services and security of collected, processed or shared information.

Strategy has been drafted in accordance with the mandate described under the Article 11.2 of the Law on the Security of Information Technologies and measures envisaged by the National Sustainable Development Strategy, National Security Concept, National Defence Concept, European Union (EU) and North Atlantic Treaty Organisation (NATO) cybersecurity plans and guidelines of international organisations.

[1] ‘Cybersecurity 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. Organization 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

[2] Approved by Cabinet of Ministers Decision 40 of 21 January 2014

1. Vision, objectives, priorities and fundamental principles

Cybersecurity policy aims to create a safe, open, free and reliable cyberspace. An environment where public and private sector can receive and provide vital services without safety, reliability or disruption concerns. A system that respects individual human rights in physical and virtual world.

Using opportunities offered by the digital world, Latvia can achieve economic growth and social prosperity while also reducing the general level of cybersecurity risks without placing unnecessary restrictions on use of technologies, exchange and flow of data. Access to and delivery of vital services must be ensured, critical infrastructure must be protected against disruptions and every person must be safeguarded against cybersecurity threats at all times, giving them as much concern as national security, human rights and fundamental values.

Key objectives of Cybersecurity Policy 2019-2022 include strengthening and development of cyber defence capabilities, enhanced resilience against cyber attacks and better public awareness on threats associated with cyberspace.

Specific targets of Cybersecurity Policy are designed around:

- more manageable cybersecurity risks
- development of national cyber defence capabilities
- security of ICT infrastructure, information systems and services
- better public awareness about cyber risks
- fight against cybercrime

Priorities for implementation of Cybersecurity Policy are defence, deterrence and development.

Defence requires development and boosting of capabilities, such as dedicated resources, perception and knowledge, required to protect the country against emerging cyber threats, efficiently respond to ICT security incidents and support ICT integrity and processes. Society, private and public sector actors need to keep enhancing their knowledge about cybersecurity and defence systems.

Deterrence requires detection, investigation and prosecution of digital offences, naming and penalising of offenders to prevent others from committing similar offences.

Development requires planned and regular upgrading and improvement of skills among various ICT user groups and greater focus on ICT security as a distinct security paradigm.

Key principles of cybersecurity:

- cybersecurity is not a separate concern, it is an integral part of national security – fundamental for the success of the modern state, society and economy
- promotion of cybersecurity through international cooperation with allies and partner countries is crucial for reaching the national cybersecurity objectives
- civic society, private, public and academic institutions must all be involved in coordination of cybersecurity
- cybersecurity measures must respect human rights
- early warning systems for preventing, investigating and stopping cyber attacks
- cybersecurity starts with individual responsibility for safe us of ICT

2. Management of cybersecurity

2.1 Risk management

Modern states and societies rely heavily on ICT. However, these systems are not entirely protected against possible attacks. ICT threats cannot be eliminated completely, but it is possible to reduce the risk of potential attack, and thus protect socio-economic and societal development, avoid economic losses and maximise the benefits of the use of ICT in public and private sectors.

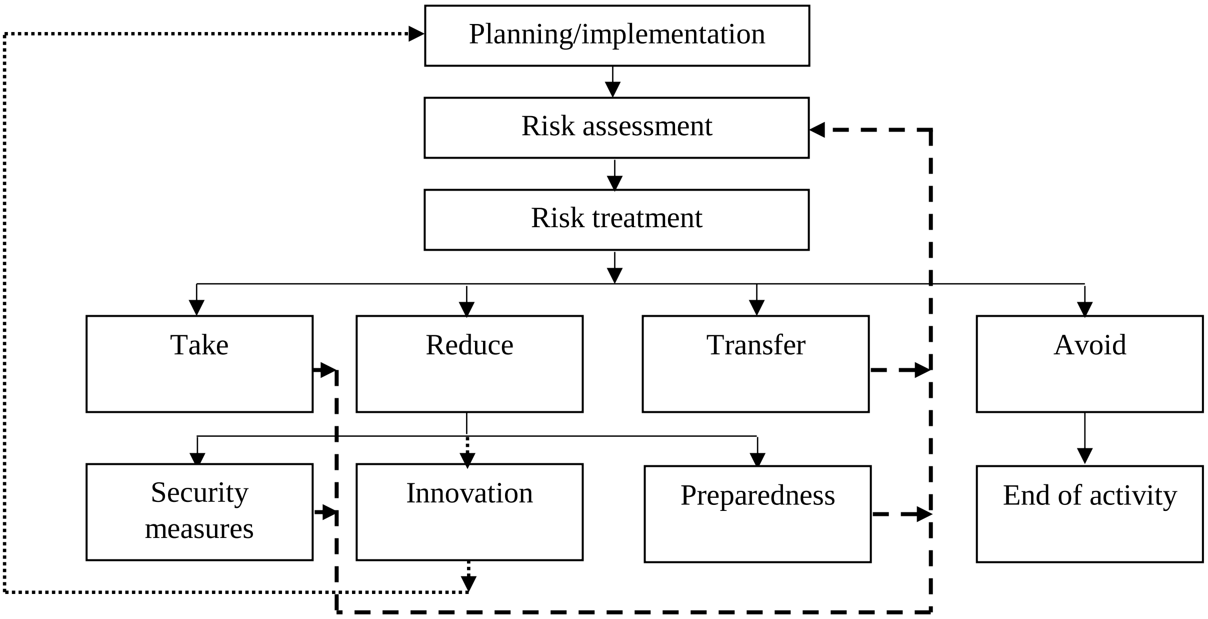
According to recommendations of the Organisation for Economic Cooperation and Development (OECD)[3], all stakeholders responsible for managing cybersecurity risks must follow these four general principles:

- all stakeholders should understand digital security risk and how to manage it
- all stakeholders should take responsibility for the management of digital security risk
- all stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values
- all stakeholders should cooperate, including across borders

Cybersecurity risk management is an integral part of the decision making process related to the planning and implementation of activities throughout their lifecycle. Cybersecurity risk management encompasses risk assessment and treatment, that is deciding which part of the risk should be taken, reduced, transferred or avoided (Figure 1). Stakeholders responsible for managing digital security risks may use the cybersecurity risk management framework described in the Strategy as a reference, fine tuning it to fit their in-house risk management system. Stakeholders may reduce risks by implementing security measures adequate and proportionate to the level of risk or consider innovations in the way these security measures are arranged, or activities are structured. They may also identify and develop necessary preparedness to achieve flexibility in terms of response to incidents and ensuring the uninterrupted flow of processes.

Figure 1

Digital security risk management cycle



Source: OECD recommendations ‘Digital Security Risk Management for Economic and Social Prosperity’, 2015

Strategy, which defines the key courses of action of cybersecurity policy and related activities, on the one hand, reinforces the four general principles of digital security risk management through the following courses of action: a) public awareness, education and

[3] OECD recommendations ‘Digital Security Risk Management for Economic and Social Prosperity’, 2015

research, b) international cooperation, while also reducing these risks through two other fundamental cybersecurity policy courses of action: a) promoting cybersecurity and reducing digital security risks, b) - strengthening the resilience of information and communication technologies, the provision of information and communication technology solutions and services critical to the society.

2.2 Governance model, roles and responsibilities of stakeholders

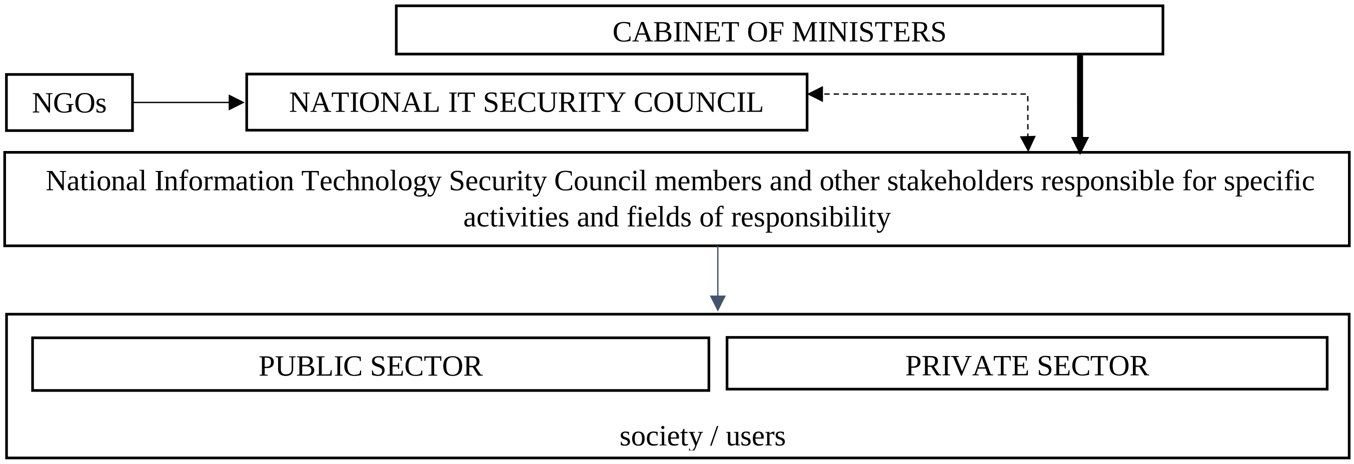
Latvia's cybersecurity governance model is semi-centralised. Managing authorities are responsible for planning of Cybersecurity Strategy and coordination of its activities, while practical introduction and implementation of various activities is delegated to individual bodies whose scope of competence covers these areas. National cybersecurity governance model builds upon horizontal cooperation, i.e., each public body responsible for specific activity, including cyber-related tasks, must directly cooperate with other government units and private sector players or cooperate with other partners in the National Information Technology Security Council[4] (NITSC) (see Figure 2).

NITSC has been created to implement the Law on the Security of Information Technologies, which identifies national digital security policy objectives and mandates NITSC to coordinate the development of cybersecurity policy, as well as plan and implement its activities. NITSC is the national body for government-private sector dialogue and cooperation on digital security. Council and its secretariat are maintained by Ministry of Defence (MoD).

Digital Security Supervisory Committee (DCSC) is a collegial body chaired by defence minister. Its responsibilities include oversight and adding of qualified and qualified high-level security trust service providers and their activities in the Register of Qualified Trust Service Providers. DCSC is a supervisory body, which acts and operates according to provisions of the Law on Electronic Identification of Natural Persons, notifies European Commission about electronic identity schemes, prepares legislative initiatives for additional supervision over qualified and qualified high-level security trust service providers and their services. It also lends its specific expertise to public and local government bodies.

Figure 2

Digital security governance model


CABINET OF MINISTERS
NGOs
NATIONAL IT SECURITY COUNCIL
National Information Technology Security Council members and other stakeholders responsible for specific activities and fields of responsibility
PUBLIC SECTOR
PRIVATE SECTOR
society / users

Here are the specific activities and fields of responsibility of government units and other stakeholders involved in governance of cybersecurity system:

[4] CoM Regulation 695 *By-laws of the Supervisory Committee of Digital Security* of 1 November 2016

- Ministry of Defence (MoD) oversees the adoption and delivery of information technology security and defence policy and contributes to international cooperation. National Cybersecurity Policy Coordination Section of the MoD Crisis Management Department is directly responsible for drafting and supporting implementation of the national cybersecurity policy.
- Ministry of Foreign Affairs (MoFA) coordinates international cooperation and Latvia's contribution to various international digital security initiatives.
- Data State Inspectorate (DSI) is responsible for data processing according to Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and Personal Data Processing Law.
- Ministry of Economics (MoE) defines economic policy and enhances competitiveness and innovations.
- Financial and Capital Markets Commission (FCMC) regulates and supervises digital activities of financial and capital market players, Bank of Latvia (LB) facilitates the security and functioning of payment systems at all times, financial institutions ensure the security and integrity of their digital services throughout the sector.
- Ministry of Interior (MoI) and State Police (SP) are responsible for policies on how to fight crime, ensure public order and safety, protects the rights and legitimate interests of individuals. Information Centre of the Ministry of Interior (IC) maintains the ICT infrastructure for law enforcement information systems.
- Information Technology Security Incident Response Institution CERT.LV monitors and analyses the cyberspace, responds to incidents and coordinates prevention, conducts research, education and training activities, checks compliance with provisions of the Law on the Security of Information Technologies. CERT.LV provides its expertise to national and international public bodies and local authorities, undertakings and natural persons.
- Ministry of Education and Science (MoES) enhances public knowledge and awareness about scientific, technological, engineering and mathematical developments that form the knowledge base on cyberspace at all levels of education. It also contributes to higher research capacity of universities through national and EU Structural Fund (European Regional Development Fund, European Social Fund) investments into development and boosting of research infrastructure, including human capital.
- Ministry of Welfare (MoW) develops and implements labour, social protection, family and children, equal opportunities for persons with disabilities and gender equality policy.
- Internet Safety Centre NetSafe Latvia operates under Latvian Internet Association (supported by MoD) educating the society about online risks and threats and promoting safer use of internet and safe online content.
- Military Information Technology Security Incident Response Team (MilCERT) monitors information and communication technologies operated by MoD and its units, including National Armed Forces (NAF). MilCERT detects, analyses and coordinates response to actual and potential IT security incidents in the sector. MilCERT conducts stress testing of military information systems and electronic communication networks. MilCERT supports and consults defence sector staff on cybersecurity of their institutions.
- NAF and National Guard Cyber Defence Unit (CDU) supports response to IT security incidents and their impact on cyberspace in case of crisis or threats.

- Non-governmental organisations support, consult and cooperate with NITSC on the content and implementation of cybersecurity policy.
- Ministry of Transport (MoT) develops the policy in the field of electronic communication networks and infrastructure.
- Constitution Protection Bureau (CPB) protects critical IT infrastructure.
- Ministry of Justice (MoJ) develops, manages and coordinates personal data protection policy.
- Latvian State Radio and Television Centre (LVRTC) is a provider of reliable certification services, i.e., it offers infrastructure for delivery of trust and authentication services.
- State Security Service (VDD) ensures internal security of Latvia and its population.
- Ministry of Environmental Protection and Regional Development (VARAM) governs national ICT systems and coordinates delivery of e-governance services, whereas State Regional Development Agency (VRAA) maintains and develops integrated national ICT resources.

All government and local institutions, owners or legal operators of critical IT infrastructure are required to comply with provisions of the Cabinet of Ministers Regulation 442 *Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements*of 28 July 2015.

3. Analysis

3.1 Description of situation

By integrating measures for strengthening the national cybersecurity implemented by line ministries and their units, Latvia must continue to deliver consolidated cybersecurity policy where specific courses of action are designed around medium-term actions, tasks and objectives that allow reducing the likelihood of cyber threats causing interruptions in operation of information systems, risk of penetration or possible consequences of cyber attacks. Better cybersecurity at the national level is a strategic priority also due to international commitments. Considering EU Digital Single Market Strategy 2020, our geographic location and commitments to NATO, Latvia is also responsible for creating fair, safe and reliable solutions that citizen of the EU can use to fully benefit from the opportunities provided by the single digital market, as well as implementation of the EU Network and Information Security Directive[5], which aims to harmonise and reinforce cyber capabilities of EU member states.

Europol's European Cybercrime Centre has estimated that availability of ICT solutions and digital technologies has resulted in an unprecedented spike in cybercrime, with losses to EU and the rest of the world peaking at around 265 billion euro and 900 billion euro a year respectively. Study 'The cost of incidents affecting critical information infrastructures', conducted by the European Union Agency for Cybersecurity (ENISA) in 2016, shows that finance, ICT and energy sectors appear to have the highest incident costs, whereas the 2018 Annual Cybersecurity Report: Impacts on Government identifies a dangerous global trend: surge in cybercrime involving uploading of phishing software, ransomware and malware to devices of government units to extract data and compromise the integrity of these systems.

Many countries are concerned about the impact of foreign electoral interventions that use various social media tools on national security. Election security coordination task force is

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

a way to coordinate community response to potential attacks on information space during the elections.

Cyberspace of Latvia continues to be the subject of various kinds of intense attacks: phishing, ransomware and malware campaigns, attempts to break into systems, networks and webpages, DoS attacks on critical information systems, e-mail scams and social engineering campaigns. The aim of these attacks is to collect personal or individual authentication data, discredit a company or organisation and commit crimes against them. Although Latvia has built a well-balanced and structured cybersecurity framework, which is based on the Cybersecurity Strategy of Latvia 2014-2018[6], a previous edition of this strategy, Law on the Security of Information Technologies and IT security incident response institutions (CERT.LV and MilCERT), national IT security needs constant upgrades to ensure that Latvia is able to predict and prevent cyber attacks even when key features of these cyber attacks are unknown, as well as mitigating the consequences of such incursions.

ICT and digital products are significant for Latvia’s society, economy and government. According to 2017 data of the Central Statistical Bureau of Latvia, almost 84% of Latvians had access to internet and 78.5% of population aged 16–74 used internet on regular basis (at least once a week). In 2018, Digital Economy and Society Index (DESI) showed that 75.3% of Latvia’s residents regularly use internet banking (have logged into their internet banking accounts at least six times in the past six months) and 99% of all bank transactions in Latvia are done using wire transfer. 70.2% of internet users use mobile devices to view online content when not at home or in the office. 55% of residents use online platforms to buy necessary products or services and the number of small and medium enterprises trading online is steadily growing, so as the turnover of e-commerce. 77% of population prefer to use e-governance platforms for formal communication with public bodies, while undertakings have access to wide range of business-related e-governance services. Public services and governance processes are actively digitised on all levels. For example, E-health is the new healthcare information platform. Official e-mail addresses for government employees became mandatory as of 1 June 2018.

This confirms the emergence of digital society in Latvia, a community where ICT solutions and digital technologies are being used to multiply well-being, economic activities and growth. Although digital transformation boosts the connectivity and access to services and products on a community level, it also creates ‘fertile ground’ for attacks on ICT and digital systems.

A wide spectrum of cyber attacks is being directed at Latvia. Considering the geopolitical changes that emerged in 2014, and their global implications, government ICT systems need to be protected against increasing threats. IT incident response institution CERT.LV has been recording an increasing intensity of attacks deploying encryption ransomware against government systems or critical information infrastructure since 2017. The whole world watched and gasped at the *WannaCry* and *NotPetya* cyber attacks in May and June of 2017. It must, however, be noted that number of those affected by attack in Latvia was rather small, none of them were either in public sector or critical infrastructure.

Monitoring of cyberspace has revealed regular attempts to hack information systems and webpages, e-mail scamming to extract personal and authentication data and attempts to plant malware in information systems. Often, data leaks and system break-ins occur due to poorly configured user data system safety and lack of understanding about which ICT systems and digital technologies are safe to use. The total of 203,455 IP addresses had security problems

[6] On 29 march 2016, CoM discussed the Information Note ‘Progress with delivery of *National Cybersecurity Strategy 2014-2018* Action Plan’ (Minutes 15, Paragraph 34). According to *National Cybersecurity Strategy of Latvia 2014-2018* , MoD, together with all responsible line ministries and NITSC, must prepare an information note on the final evaluation of the Strategy Action Plan delivery by 1 June 2019

identified in the fourth quarter of 2018. Of these, 131,394 had configuration weaknesses which could potentially be used by hackers to break in. Malicious code and attempts to hack information systems by exploiting vulnerabilities of user data systems to hijack and abuse them using botnets were the most common types of attacks.

3.2 Challenges

Digital environment keeps offering new, broader and much more integrated business and social networking opportunities, making it an attractive target for cyber criminals, foreign spies and agents of influence. On 4 October 2018, Dutch government announced that it had successfully prevented a cyber attack on Organisation for the Prevention of Chemical Weapons (OPCW) in April of 2018. This only shows that anyone, regardless of their field of activity or place of business, can become a target of state-sponsored cyber attack. This means that cybersecurity must be closely integrated into comprehensive national defence where state and local authorities, public sector and each individual have specific responsibilities that are crucial for achieving common security objectives.

Number and prevalence of cybercrime will continue to grow as digital environment keeps expanding. There are two major types of cybercrime: offences committed using or against ICT devices and use of ICT to commit a bigger offence. Considering that terrorist organisations now have wider access to diverse range of tools, it is highly possible that cyberspace and connected devices will become more popular among offenders. Dark Net, Internet's virtual underbelly offering full anonymity, will continue to be the main platform for illegal activity, including acquisition of malware and other cyber weapons. Such ‘demand’ will increase the ‘supply’ from the hackers.

Internet of Things[7] (IoT) is also one of the key future challenges. Growing data transmission capacity will generate technologies that allow integrating home electronics easier. IoT will become more widespread. Number of sensors and appliances linked through IoT will become a big security challenge. According to forecasts, real-time/online remotely-operated appliances will soon become a staple in most homes and businesses. Large amounts of *big data* will be generated and collected from these IoT devices.

After a leap several years ago, cloud computing and applications will definitely continue to advance and become more popular. Development of cloud computing technologies requires adoption of adequate security policies (Course of Action 1, Activity 1), which has always been the weak point of cloud computing.

Mobile phones are no longer just communication devices. If a phone is hacked, other connected devices come under risk – collective security is as strong as its weakest link, or device. Better cybersecurity at the institutional level should consider vulnerability of mobile phones and smart devices when used inside government institutions. This should protect in-house ICT systems from potential viruses (Course of Action 1, Activity 2).

As national economy continues to grow, Latvia is facing an ever increasing need for qualified professionals in various fields, especially the ICT. This is not a unique challenge faced only by Latvia. It is a common problem around the world. Shortage of skilled labour leads to unhealthy human resource rivalry between ICT companies. Compared to public sector, ICT employees are paid disproportionately more. This leads to inability of public bodies to find good ICT specialists and diminishes public sector’s capacity to maintain and develop its ICT resources in sufficient fashion (Course of Action 1, Activity 4).

[7] Internet of Things in the context of the Strategy means network of physical objects that are embedded with sensors and software for the purpose of connecting with other devices over the Internet.

Wider use of ICT creates more threats, which need to be managed. In doing so, balancing between efficient governance and privacy will be required to avoid creating obstacles to innovation, development and streamlining.

4. National Cybersecurity Policy courses of action

National Cybersecurity Policy 2022 courses of action need to be coherent with national policies and other planning documents relevant to the long-term cybersecurity policy objectives. Coherence is important for consistent cybersecurity policy development. However, to simplify the monitoring of decisions, the Strategy does not include targets defined in other documents approved by the Cabinet of Ministers.

Here are the national-level documents relevant to the long-term cybersecurity policy objectives:

- National Sustainable Development Strategy *Latvia 2030*
- National Security Concept
- National Defence Concept
- Information Society Development Guidelines 2014–2020
- Electronic Communications Sector Policy Plan 2018–2020
- National Armed Force Cyber Defence Unit Concept (2013)
- Informative Statement *Development of comprehensive national defence system in Latvia* (2018)

Moreover, Article 7 of the EU Network and Information Security Directive defines seven issues that member states need to address in their national strategies on the security of network and information systems. Various chapters of Latvia’s strategy for 2022 address the issues listed in the Directive, and thus Latvia complies with the requirements of the Directive.

In 2013, EU adopted *EU Cybersecurity Strategy*, which is built around 5 priorities:

- increasing cyber resilience
- drastically reducing cybercrime
- developing EU cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- developing the industrial and technological resources for cybersecurity
- establishing a coherent international cyberspace policy for the EU and promote core EU values

Considering EU-level priorities and objectives identified in national policies and other planning documents, Strategy for 2022 focuses on the following five key courses of action:

1) promoting cybersecurity, reduction digital security risks
2) ICT resilience[8], stronger ICT solutions and services critical to the society
3) public awareness, education and research
4) international cooperation
5) cyberspace and law, combating cybercrime

More detailed description of above axis is provided in the subsections of this Chapter. Information on each course of action contains activities, deadlines, managing[9] and responsible authorities, estimated costs and expected outcomes, which contribute to the vision and objectives of the Strategy. Considering that cyber offences are a complex and fickle type of crime, expected outcomes serve as a broader frame of reference and a more generalised metric.

[8] ICT resilience in the context of the Strategy means the capacity of ICT systems to absorb, recover from and adjust to various external shocks, for example, cyber attacks or natural disasters.

[9] When table indicates that there are several ‘managing authorities’, tasks and responsibilities of each institution are decided by involved institutions themselves, including the securing of required funding.

Priorities of each courses of action, which contain information for official use only, are described in the Annex of the Strategy (information for official use only).

Managing and responsible authorities continue to deliver regular activities started under the previous period's strategy. Moreover, activities identified in the Strategy do not preclude stakeholders from engaging in other activities not covered by the Strategy.

4.1 Course of Action 1: Promoting cybersecurity, reducing digital security risks

Latvia aims to create a comprehensive national defence system delivered in close cooperation between the public sector, private sector and the whole society. These actors jointly strengthen the security and defence of cyberspace. This also includes protection of critical IT infrastructure. Greater cyber resilience of Latvia means that public administration and private sector must both develop capabilities for detecting illicit activities and responding to them in an efficient manner based on shared public and private sector understanding of threats and risks in cyberspace. State must provide sufficient technical and human resources for preventing or minimising impact of any hostile acts. Shared understanding and coordinated response to crisis can be developed through joint crisis management training for national security agencies, government bodies and private sector (Activity 1.5).

Adoption of EU Network and Information Security Directive in July of 2016 was a major step towards better cybersecurity across the Union. It is the first piece of EU-wide legislation on cybersecurity. It aims to boost the cyber defence capabilities and cooperation between the member states. Companies working in strategic sectors are required to put adequate security measures in place and report major cybersecurity incidents to national IT security incident response institution. Moreover, in July 2016, NATO recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. At the Brussels Summit in 2018, Allies agreed to set up a new Cyberspace Operations Centre as part of NATO's strengthened Command Structure. As a member of NATO and the EU, Latvia is an active participant of joint cyber defence capability development and training efforts.

Governments continue to develop cyber defence and also cyber attack capabilities within the permitted international framework. Latvia will focus its current Strategy activities on development of defence capabilities, which may also require development or upgrading of cyber attack capabilities through national and multinational programmes.

Strategy activities implemented by state and local government institutions will continue to improve access to public services provided on electronic platforms, or e-services, which will significantly boost the efficiency of cooperation between state and local authorities, community and private sector. In addition to these initiatives, Latvia will also have to develop common criteria for authentication systems controlling access to specific e-services (Activity 1.3).

Table 1

Course of Action 1: Promoting cybersecurity, reducing digital security risks

No.	Activity	Time	Responsible authority[10]	Co-responsible authority	Costs (indicative), funding sources	Expected outcomes and indicators (if applicable)
1.1	Define security requirements and guidance on use of cloud computing services by state and local authorities	Q4 2020	VARAM, MoD, national security agencies	CERT.LV, LALRG	From annual appropriations determined by National Budget Law	Formal requirements for use of cloud servers
1.2	Analyse and apply necessary restrictions on use of mobile and smart devices or network access inside government buildings and when using information systems maintained by an institution	Q4 2020	All government institutions		From annual appropriations determined by National Budget Law. If possible, municipalities and their units shall earmark activity funding during the municipal and agency budget planning process.	Analysis and formal restrictions
1.3	Develop recommendations and criteria for authentication systems (eID, I-banking account) controlling access to institution's information resources	Q4 2019	MoD, VARAM		From annual appropriations determined by National Budget Law. If possible, municipalities and their units shall earmark activity funding during the municipal and agency budget planning process, as stipulated by Cabinet of Ministers Regulation 442 of 28 July 2015 'Procedures for the Ensuring Conformity of Information and	Formal recommendations and approved criteria

[10] When table indicates that there are several 'responsible authorities', tasks and responsibilities of each institution are decided by involved institutions themselves, including the securing of required funding. This means that amounts earmarked for activities of each institution are indicative.

No.	Activity	Time	Responsible authority[10]	Co-responsible authority	Costs (indicative), funding sources	Expected outcomes and indicators (if applicable)
					Communication Technologies Systems to Minimum Security Requirements '.	
1.4	Analyse and develop recommendations on how to attract more IT specialists to public and local authorities	Q4 2019	SC, VARAM		From annual appropriations determined by National Budget Law	Analysis on how to attract more IT specialists to public sector jobs
1.5	Hold biannual cybersecurity-themed crisis management training (tabletop) to enhance coordination and shared understanding on crisis response.	Regularly	MoD, CERT.LV	Public and local authorities and corporate stakeholders mentioned in scenario	From annual appropriations determined by National Budget Law	Better shared understanding and coordination in response to a crisis

4.2 Course of Action 2: - strengthening the resilience of information and communication technologies, the provision of information and communication technology solutions and services critical to the society

Government’s reliance on ICT and e-services requires constant attention. All systems must have backup for cases when ICT infrastructure is experiencing problems and e-services are either down or disrupted.

ICT infrastructure must be protected against threats. Critical data should be stored and processed by secure data centres. Some copies of critical data may also be stored outside Latvia if necessary. Information systems supporting state, local and critical services should be designed and operated on the basis of security risk assessments, budget allocation and risk control measures (Activity 2.3). Government must similarly provide crisis and conflict protection of information and cyber systems by implementing active and proactive security measures that safeguard population against external influence and protect stability of government (Activity 2.2).

Law on the Security of Information Technologies and relevant Cabinet of Ministers regulations establish minimum security standards that all government institutions, local authorities, providers of public electronic communications services and critical ICT infrastructure operators must meet. This would be the first step towards a safer and more reliable cyber domain where state and private actors can continuously provide and receive vital services in a safe, reliable and sustainable fashion.

By involving bigger part of society in boosting security of digital systems and services, Latvia can significantly enhance the resilience of government information resources. Following the principles described in National Defence Concept, it is necessary to develop regulations on responsible security vulnerability disclosure, which are important for ICT security, addressing of gaps and vulnerabilities and encouraging system designers and operators be more responsible (Activity 2.1).

Table 2

Course of Action 2: strengthening the resilience of information and communication technologies, the provision of information and communication technology solutions and services critical to the society

No.	Activity	Time	Responsible authority[11]	Co-responsible authority	Costs (indicative), funding sources	Expected outcomes and indicators (if applicable)
2.1	Develop regulatory framework for responsible security vulnerability disclosure	Q4 2021	MoD	CERT.LV, MilCERT, MoI (SP), VDD, MoJ (DSI), MoT, VARAM, MIDD, CPB	From annual appropriations determined by National Budget Law	Effective regulatory framework
2.2	Further strengthening of ICT resilience at diplomatic missions of Latvia abroad	Regularly	MoFA		From annual appropriations determined by National Budget Law	Stronger ICT resilience at diplomatic missions of Latvia abroad
2.3	CERT.LV penetration testing for government ICT solutions and infrastructure	Regularly	CERT.LV	NAF, CDU	From annual appropriations determined by National Budget Law	Regular ICT solution and infrastructure penetration tests

4.3 Course of Action 3: Public awareness, education and research

Human knowledge and behaviour are fundamental for any cybersecurity software. That is why it is paramount to ensure that everyone, from system and software developers to end users, who may be exposed to phishing e-mail scams or social engineering attempts, understands the features of cybersecurity. All stakeholders are equally important for securing networks and information systems, and that means everyone should be equally aware of risks they are exposed to when online and actions that may prevent such exposure. Assurance of cybersecurity is rooted in burden sharing. Knowledge, awareness and vigilance of each individual is crucial for assuring cybersecurity.

Latvian education system helps deliver the digital society. Digital society is a society where everyone has the skills, resources and access to ICT necessary for absorbing new knowledge or integrating such knowledge into existing knowledge systems and using it to multiply their prosperity. Focus must be on raising the overall awareness of the society, while also supporting training and development of young IT experts, which heavily relies on

[11] When table indicates that there are several ‘responsible authorities’, tasks and responsibilities of each institution are decided by involved institutions themselves, including the securing of required funding. This means that amounts earmarked for activities of each institution are indicative.

availability of informal education and cybersecurity awareness games/competitions (Activity 3.5).

According to European Commission's Digital Economy and Society Index 2018 Report, ICT specialists comprised only 2.2% of total employment in Latvia, which is well below the EU average of 3.7%. Moreover, half of Latvian population has either no or poor digital skills. In addition, according to European Commission's Joint Research Centre 2017 report, Latvia's ICT sector has relatively low R&D intensity.

It is imperative to ensure that society acquires skills for using various devices and software. It is also important to master basic online security, which is key to learning more complex cybersecurity concepts (Activity 3.2., 3.3 and 3.4). Current situation requires more attention on education and integration of computer science in school curriculum. Vocational and higher ICT education is also important in training new ICT specialists. Latvia must promote participation of children and youth in informal education and games/competitions to raise their interest in studying IT (Activity 3.5). Support to R&D initiatives would allow to pilot various solutions and receive regular government orders. More intense R&D activities in the field of modern cybersecurity should be supported by all available means, including research project grants, procurements, participation in international collaborative initiatives, i.e., European Defence Fund programmes, or cybersecurity component of national defence research programme if in-depth analysis indicates the need for such projects (Activity 3.1).

EU's Multiannual Financial Framework 2021-2027 puts great emphasis on development of digital technologies, including cybersecurity technologies. The aim is to promote EU's global digital competitiveness. This will give Latvia an opportunity to compete for funding available through several EU programmes for cybersecurity projects.

To promote awareness of defence staff about modern threats and ensure capability to respond to such threats, Latvia has created special units and cybersecurity training modules that are delivered to National Guard and Cadet Force according to National Defence Concept.

Table 3

Course of Action 3: Public awareness, education and research

No.	**Activity**	**Time**	**Responsible authority** [12]	**Co-responsible authority**	**Costs (indicative), funding sources**	**Expected outcomes and indicators (if applicable)**
3.1	Facilitate cybersecurity R&D projects focusing on current challenges through all available support programmes	Regularly	MoD	MoES	From annual appropriations determined by National Budget Law	Support to research projects in scope of existing support programmes and increasing number of research projects

[12] When table indicates that there are several 'responsible authorities', tasks and responsibilities of each institution are decided by involved institutions themselves, including the securing of required funding. This means that amounts earmarked for activities of each institution are indicative.

No.	Activity	Time	Responsible authority [12]	Co-responsible authority	Costs (indicative), funding sources	Expected outcomes and indicators (if applicable)
						focusing on current cybersecurity challenges. In-depth analysis on content of cybersecurity component of national defence research programme prepared by MoES together with relevant research institutions.
3.2	Raise awareness of students and teachers about information security, protection of privacy and reliable online services	Regularly	State and local educational establishments (except pre-school institutions), municipalities	MoES LIA	From annual appropriations determined by National Budget Law. If possible, municipalities and their units shall earmark activity funding during the municipal and agency budget planning process	Better cybersecurity awareness among pupils, students and educators
3.3	Improve public awareness about online safety (age-group-specific information and instructional materials with guidelines on online safety, social media campaign security) and deliver advanced cybersecurity training for specific target groups. Develop and implement annual multi-agency action and campaign	Regularly	MoI (SP), MoES, MoD, CERT.LV	MoC, LIKTA, LIA, FL	From annual appropriations determined by National Budget Law	Better public awareness about online safety

No.	Activity	Time	Responsible authority [12]	Co-responsible authority	Costs (indicative), funding sources	Expected outcomes and indicators (if applicable)
	plan with cybersecurity information events and awareness raising campaigns					
3.4	Promote awareness of public and municipal authority staff on ICT safety	Regularly	All public and municipal authorities		From annual appropriations determined by National Budget Law. If possible, municipalities and their units shall earmark activity funding during the municipal and agency budget planning process	Better awareness of public and local authority staff on ICT safety
3.5	Increase support for participation of Latvian children and youth in informal education and games/competitions raising awareness about cybersecurity	Regularly	MoES	VARAM, municipalities	From annual appropriations determined by National Budget Law	Latvian children and youth take part in at least one informal education activity and/or competitive cybersecurity event/games

4.4 Course of Action 4: International cooperation

Cyberspace, with all its possibilities and security risks, operates across national borders, which means that countries need to work together to successfully overcome these new security challenges.

Due to growing role of cyberspace in our everyday life, cybersecurity has become one of the key areas of international cooperation and is high on the agenda of international organisations. Bilateral and multilateral formats, which often rely on private sector representatives, are being used to address a wide range of issues, including human rights in the digital domain, cybercrime, security of critical infrastructure, prosecution of those who commit cyber attacks and prevention of national security threats. This inevitably leads to clashes between countries with varying interests, and so far, international community has failed to make any significant progress towards building a common understanding and approach. Together with likeminded countries, Latvia should try to promote shared and common global understanding of cyberspace and how international treaties apply to it.

Cybersecurity has become a vital element of national defence, while NATO allies and EU partners can reinforce national defence capabilities in case of crisis. To enhance their cybersecurity in line with NATO and EU cybersecurity guidelines, members of the Euro-Atlantic international organisations need to strengthen their individual and collective cybersecurity capabilities to be able to receive and provide efficient support when necessary. NATO and EU are faced with the same challenges. Hence, it is important to build joint cyber defence frameworks, especially in the field of information exchange, training and R&D. As a member of both organisations, Latvia is fully engaged in ongoing cybersecurity coordination and training. Strategy activities contributing to Latvia's international efforts:

- deepen cooperation with like-minded partner countries to achieve common understanding of cyberspace (Activity 4.1)
- actively engage in NATO, EU, OSCE, UN and OECD efforts to promote secure cyberspace and develop cybersecurity policy that protects freedoms and helps make ICT more secure and accessible (Activity 4.1 and 4.5)
- utilise full potential of existing international facilities and tools to prevent malicious cyber activities (Activity 4.3)
- continue supporting international efforts to promote mutual trust and cooperation on all levels, including private sector, and advocate for application of existing international rules to both physical and virtual domain (Activity 4.1 and 4.4)
- continue to host regular international cybersecurity events in Latvia in scope of national pledge to become a responsible country, which cares about national and global ICT security
- continue to develop and test national procedures for rapid, efficient and coordinated collective response to cyber threats based on Latvia-NATO Memorandum of Understanding, NATO Cyber Defence concept and Action Plan (Activity 4.2)
- continue to boost cyber defence capabilities by taking part in all kinds of international military drills, training activities and table-top exercise organised by NATO, EU, and other multinational formats, thus giving local specialists and CDU an opportunity to update their knowledge and skills in using most recent information security tools (Activity 4.2).

One of significant drivers of international cybersecurity cooperation is 'Horizon 2020'. The new 'Horizon' framework research programme will begin in 2021. Cybersecurity is one of the key components of its Pillar II, in particular the 'Civil security for society' cluster where cybersecurity is one of primary goals.

Table 4

Course of Action 4: International cooperation

No.	Activity	Time	Responsible authority[13]	Co-responsible authority	Costs (indicative), funding sources	Expected outcomes and indicators (if applicable)
4.1	Formulate and present Latvia's national position, take part in international cooperation programmes and platforms, deepen Nordic-Baltic cooperation, actively engage in NATO and EU initiatives and, inter alia, help partner countries boost cyber defence capabilities. Actively support formal and informal cooperation networks and programmes of international organisations (UN, OSCE)	Regularly	MoFA, MoD	All government institutions	From annual appropriations determined by National Budget Law	Latvia is regularly and efficiently contributing to international processes. Expert consultations on cybersecurity at least once a year. Latvia is regularly represented in international networks and platforms
4.2	Take part in international cyber defence exercise, expert and policy-maker consultations, NATO and EU security, defence and military cooperation initiatives and platforms	Regularly	MoD	MoFA, MoT, MoI, CERT.LV, NAF, MilCERT	From annual appropriations determined by National Budget Law	Latvian experts take part in international cybersecurity training events at least twice a year
4.3	Continue on-going and launch new international cybercrime reduction cooperation programmes. Cooperate with various international organisations and agencies fighting cybercrime	Regularly	MoI (SP)	MoFA	From annual appropriations determined by National Budget Law	Active cooperation with various cybercrime units and institutions on reducing cybercrime rate
4.4	Help Latvian cybersecurity service providers find cooperation partners	Regularly	LIDA		From annual appropriations determined by National Budget Law	Companies receiving help in finding cooperation partners
4.5	Formulate and present national position at OSCE Committee on Digital Economy Policy and coordinate the implementation of OSCE digital policy recommendations	Regularly	VARAM	MoD, CERT.LV, MoJ, DSI, MoW, MoT, PUC, CSB	From annual appropriations determined by National Budget Law	Regular representation of Latvia in the Committee. Recommendations integrated in digital policies

[13] When table indicates that there are several 'responsible authorities', tasks and responsibilities of each institution are decided by involved institutions themselves, including the securing of required funding. This means that amounts earmarked for activities of each institution are indicative.

No.	Activity	Time	Responsible authority[13]	Co-responsible authority	Costs (indicative), funding sources	Expected outcomes and indicators (if applicable)
						and other relevant planning documents

4.5 Course of Action 5: Rule of law in cyberspace, combating cybercrime

Cybercrime leads to all kinds of abuse, which erodes trust in digital services. Cybercrime can be reduced in two ways: prevention, which helps reduce the risk of cybercrime, and efficient prosecution (Activity 5.1 and 5.2). It is also important to engage public, because broader awareness about cyber risks will prevent cybercrime from occurring. Public participation would range from cybercrime discussions on various levels (at educational establishments, research institutes, conferences and other events) to information campaigns designed on behaviour studies and analysis.

More efficient fight against cybercrime requires better law enforcement capacity to technically identify IP addresses from which users access e-services or information systems. Due to the shortage of IPv4 addresses, providers of electronic communications services are forced to resort to network address translation. In Latvia, one and the same IPv4 address can be used by up to 100 users, which causes all kinds of problems, including security problems, because law enforcement agencies are struggling to use stored data to identify end users who have broken the law. A way to eliminate this problem would be the introduction of IPv6 in public sector. This would encourage private sector to also switch to IPv6 technology (Activity 5.3).

Table 5

Course of Action 5: Rule of law in cyberspace, combating cybercrime

No.	Activity	Time	Responsible authority[14]	Co-responsible authority	Costs (indicative), funding sources	Expected outcomes and indicators (if applicable)
5.1	Boost the capacity of State Police and national security services to investigate cybersecurity incidents, strengthen the institutional capacity of State Police and national security agencies	Regularly	MoI (SP), MoJ, MoD		From annual appropriations determined by National Budget Law.	Increased State Police and national security service capacity, and expertise, to investigate crimes against ICT infrastructure, control internal security of

[14] When table indicates that there are several ‘responsible authorities’, tasks and responsibilities of each institution are decided by involved institutions themselves, including the securing of required funding. This means that amounts earmarked for activities of each institution are indicative.

No.	Activity	Time	Responsible authority[14]	Co-responsible authority	Costs (indicative), funding sources	Expected outcomes and indicators (if applicable)
						Latvia and monitor critical infrastructure
5.2	Training of State Police, judges and prosecutors as a follow up to interdisciplinary cooperation training conducted by Court Administration and European Social Fund in scope of the project 'Justice for growth'[15]	Regularly	MoJ, MoI (SP)		From annual appropriations determined by National Budget Law.	Delivery of planned training to State police, judges and prosecutors
5.3	Enhance user identification by supporting switching to IPv6 in public sector, and thus encourage private sector to follow	Q4 2020	MoT	VARAM	From annual appropriations determined by National Budget Law. If possible, municipalities and their units shall earmark activity funding during the municipal and agency budget planning process, as stipulated by Cabinet of Ministers Regulation 442 of 28 July 2015 'Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements '.	Law enforcement agencies can easier identify users of e-services or information resources

[15] This training would be a follow up to the training provided in scope of the project 3.4.1.0/16/I/001 'Justice for Growth' supported under SO 3.4.1 'Improve the competence of the staff of courts and law enforcement authorities to promote improvement of the business environment' of the Operational Programme 'Growth and Employment' for EU Structural and Cohesion Funds in the period 2014-2020.

5. Fiscal impact analysis

Funding for the implementation of activities envisaged by the Strategy will be allocated from national and local budgets. Activities listed under priority axis can partly be funded from EU Structural Funds (European Regional Development Fund, European Social Fund, Cohesion Fund). It is also possible to attract private funding for implementation of Strategy activities by means of facilitating public and private s and other arrangements favourable for private capital participation. Detailed information about costs of strategic activities and potential funding sources is provided in Section 4 of the Strategy and its Annex (information for official use only).

If Table 1, 2, 3, 4, 5 of the Section 4 of the Strategy and Column 1 and 2 of the table provided in the Annex (information for official use only) indicate that there are several 'managing authorities', tasks and responsibilities of each institution are decided by involved institutions themselves, including the securing of required funding. This means that amounts earmarked for activities of each institution are indicative.

Implementation of Strategy activities in 2019 will be funded from annual appropriations of authorities responsible for specific activities, whereas further funding needs for 2020–2022 will be addressed during the planning of annual budget and medium-term budgetary framework and drafting of respective laws when other funding requests for priorities submitted by other ministries and government departments are considered.

Table 6

Strategy Courses of Action cost breakdown by years, projected overall funding (EUR)

Courses of Action	2019	2020	2021	2022	Aggregate
Course of Action 1: - Promoting cybersecurity, reducing digital security risks	0	0	0	0	**0**
Course of Action 2: - Strengthening the resilience of information and communication technologies resilience, the provision of information and communication technology solutions and services critical to the society	0	13,061,560	9,332,985	7,382,169	**29,776,714**
Course of Action 3: Public awareness, education and research	0	0	0	0	**0**
Course of Action 4: International cooperation	0	0	0	0	**0**
Course of Action 5: Rule of law in cyberspace, combating cybercrime	0	0	0	0	**0**
Total	**0**	**13,061,560**	**9,332,985**	**7,382,169**	**29,776,714**

Table 7

National and local budget impact of policy planning document

	3-year period (EUR)		
	2019	2020	2021
Total impact on revenues, including:	0	0	0
Impact on national budget revenue	0	0	0
Impact on local budget revenues	0	0	0
Total impact on expenditure, including:	0	-13,061,560	-9,332,985
Impact on national budget expenditure	0	-13,061,560	-9,332,985
Impact on local budget expenditure	0	*	*
Overall fiscal impact:	0	-13,061,560	-9,332,985
Financial impact on national budget	0	-13,061,560	-9,332,985
Financial impact on local budgets	0	*	*
Detailed revenue and expenditure projections (detailed revenue and expenditure projection is annexed to policy planning documents, if necessary. Impact on national and local budgets is indicated separately for national and local budget)	Implementation of Strategy activities in 2019 will be funded from annual appropriations of authorities responsible for specific activities. Further funding needs for 2020–2022 will be addressed during the planning of annual budget and medium-term budgetary framework and drafting of respective laws when other funding requests for priorities submitted by other ministries and government departments are considered. Detailed projections of future budget funding needs are provided in the Annex (information for official use only) of the Strategy.		
Budget expenditure adjustment, 2022	2022 -7,382,169	-	-

* Activities envisaged in the Strategy will have impact on local budgets. Local budget expenditure adjustments and financial impact on local budgets are currently unclear due to changing cybersecurity landscape and number of affected municipalities. Financial impact also depends on the activity delivery methodology chosen by the responsible authorities. Responsible authorities will perform the impact assessment and prepare local fiscal impact projections when planning and delivering the specific Strategy activities.

6. Reporting procedures

Ministry of Defence, together with all managing and responsible authorities and NITSC, shall prepare and submit the Information Note on the progress in delivery of activities envisaged by Strategy to the Cabinet of Ministers by 1 May 2022. Progress Report shall also contain medium-term cybersecurity policy recommendations.

7. Concluding remarks

Due to the constant cybersecurity developments and rapid evolution, ex-ante evaluation of the impact of proposed measures cannot be performed. However, priority courses of action of the Strategy are built on and provide continuity to the current priorities of National Security Concept.

None of the existing policy planning documents are repealed herewith.