



THE CYBERSECURITY STRATEGY OF LATVIA


2023-2026





THE CYBERSECURITY STRATEGY OF LATVIA

2023-2026





CONTENT

Executive Summary	5
Abbreviations	6
Introduction	7
Vision, Priorities, and Key Principles	7
Analysis of Cybersecurity Situation	8
Situation Description	8
Current Affairs and Future Challenges	10
Cybersecurity Governance.....	13
Risk Management	13
Governance model and functions and responsibilities of involved participants	13
Directions of National Cybersecurity Policy Actions.....	17
Direction 1 “Enhancement of Cybersecurity Governance”	17
Direction 2 “Promotion of Cybersecurity and Strengthening Resilience”	21
Direction 3 “Public Awareness, Education and Research”	25
Direction 4 “International Cooperation and Rule of Law in Cyberspace”	27
Direction 5 “Prevention and Combating of Cybercrime”	29
Financial Impact Assessment.....	31



Evaluation of Strategy Implementation	32
Evaluation Methodology	32
Procedure for Submission of Reports	32
Closing remark	33



EXECUTIVE SUMMARY

“The Cybersecurity Strategy of Latvia 2023-2026” (hereinafter referred to as the Strategy) has been developed based on Section 11, Paragraph 2 of the Law on the Security of Information Technologies. It describes the cybersecurity situation in Latvia, identifies future challenges, and defines the key directions of the national cybersecurity policy for the period up to 2026 (inclusive).

The vision of the cybersecurity policy is to create a secure, open, free, and trustworthy cyberspace in Latvia, where the secure, reliable, and uninterrupted provision and receipt of essential services to the state and society are guaranteed, and individual human rights are respected both in the physical and virtual environment.

The goal of the cybersecurity policy for the period from 2023 to 2026 is to strengthen the security of Latvia’s cyberspace through the development of cyber defence capabilities, bolstering resilience against cyber attacks, and fostering public awareness of cyber threats. The policy is guided by the following priorities: protection, deterrence, and development.

Taking into account the priorities set by the European Union and the goals outlined in national policy planning and other documents, the Strategy identifies five directions for action:

- Enhancing Cybersecurity Management,
- Promoting Cybersecurity and Strengthening Resilience
- Public Understanding, Education, and Research
- International Cooperation and Rule of Law in Cyberspace,
- Prevention and Combating Cybercrime.

All the aforementioned action directions have been detailed in separate sections, and the tasks derived from the Strategy for the reporting period will be summarized in the National Cybersecurity Strategy Task Plan. During the period covered by the Strategy, the responsible and involved institutions will continue to implement the ongoing tasks initiated in the previous Strategy.

The tasks outlined in the Strategy will be carried out in 2023 within the framework of the allocated state budget funds. The question of additional allocation of state budget funds for the years 2024-2026 will be considered in the process of preparing the annual state budget draft law and the medium-term budget framework draft law, together with the priority measures proposed by all ministries and other central government institutions.

ABBREVIATIONS

CDU	National Armed Forces National Guard Cyber Defence Unit	NCC-LV	European Cybersecurity Competence Centre National Coordination Centre in Latvia
CERT.LV	Information Technology Security Incident Response Institution)	NetSafe	Net-Safe Latvia Safer Internet Centre
CI	Critical Infrastructure	NGO	Non-Governmental Organizations
CSB	Central Statistical Bureau	NITSC ¹	National Information Technology Security Council
DSI	Data State Inspectorate	NCSC	National Cybersecurity Centre
EEAS	European External Action Service	OECD	Organization for Economic Cooperation and Development
ENISA	European Union Agency for Cybersecurity	OSCE	Organization for Security and Co-operation in Europe
EU	European Union	PUC	Public Utilities Commission
ICT	Information and Communication Technologies	SAB	Constitution Protection Bureau
IP	Internet Protocol	SC	State Chancellery
IT	Information Technology	SCDS	Supervisory Committee of Digital Security
LB	The Bank of Latvia	SIS	State Information Systems
LLA	Finance Latvia Association	SP	State Police
LVRTC -	Latvian State Radio and Television Centre	SRS	State Revenue Service
MIDD -	Defence Intelligence and Security Service	Strategy	The Cybersecurity Strategy of Latvia 2023-2026
MilCERT	Military Information Technology Security Incident Response Institution	UN	United Nations
MoD	Ministry of Defence	VDD	State Security Service
MoE	Ministry of Economy		
MoEPRD	Ministry of Environmental Protection and Regional Development		
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 Organization		

¹ In the draft law National Cybersecurity Law², it is proposed to re-name the National Information Technology Security Council as the National Cybersecurity Council. Since the draft law has not been adopted yet, the previous name of the Council is still used in this document.

INTRODUCTION

The National Cybersecurity Strategy **defines the key directions of national cybersecurity policy** for the period until 2026, ensuring the continuity of the action directions set in the “Cybersecurity Strategy of Latvia 2019-2022”² for strengthening Latvia’s cybersecurity. It characterizes Latvia’s cybersecurity situation, as well as identifies future challenges. The involvement of various stakeholders plays a crucial role in the development of the strategy and the execution of tasks, aiming to create a secure, open, free, and trustworthy Latvian cyberspace.

In the comprehensive national defence system, each entity - both state and non-state organizations, as well as the private sector and individuals - has a clearly defined role in crisis situations. Cybersecurity is increasingly being given a significant role as an element of the comprehensive national defence system, focusing not only on improving cybersecurity management and promoting international cooperation but also raising public awareness. The main priorities of cybersecurity policy for this planning period are defence, deterrence, and development.

The strategy was developed in connection with the revised Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of network and information system security across the Union³ (hereinafter referred to as the NIS2 Directive), as well as the EU’s Cybersecurity Strategy for

the Digital Decade⁴. In developing the strategy, national digital policy planning documents were also taken into account to ensure coherent digital and cybersecurity development in Latvia. One of the key policy planning documents in this area, which was considered in the development of the strategy, is the “Digital Transformation Guidelines 2021-2027”⁵, approved by Cabinet of Ministers Order No. 490 of July 7, 2021.

In the first quarter of 2023, a specific action plan to achieve the goals set in the Strategy will be submitted to the Cabinet of Ministers. This plan will identify the tasks, responsible institutions, deadlines for task completion, as well as the expected results to be achieved.

VISION, PRIORITIES, AND KEY PRINCIPLES


The vision of the cybersecurity policy is to create a secure, open, free, and trustworthy Latvian cyberspace where secure, reliable, and uninterrupted provision and receipt of services that are important to the state and society are guaranteed, and individual human rights are respected in both the physical and virtual environments. In implementing the cybersecurity policy, the following priorities have been defined: defence, deterrence, and development.

² Approved by Cabinet of Ministers Order No. 40 of September 17, 2019.

³ NIS Directive, available at: <https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32016L1148>.

⁴ EU’s Cybersecurity Strategy for the Digital Decade, available at: <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>

⁵ Cabinet of Ministers Order No. 490 of July 7, 2021, “On Guidelines for Digital Transformation 2021-2027. <https://likumi.lv/ta/id/324715>



Defence - Develop and enhance capabilities to defend against growing and evolving cyber threats, strategically plan ICT security, effectively respond to ICT vulnerability reports and security incidents, and ensure ICT security and functionality. This includes providing the necessary technological resources, as well as raising awareness and knowledge in the private and public sectors, as well as in the society as a whole, about the opportunities to protect themselves. At the same time, it is important to ensure appropriate decision-making and response speed and the effectiveness of the chosen measures.

Deterrence - Detect, investigate, and stop malicious activities in cyberspace by identifying offenders and holding them accountable, thereby deterring others from engaging in such actions. It also involves developing active cyber defence capabilities.

Development - Develop and enhance the protection of ICT and critical ICT infrastructure in the public sector, essential service providers, and important service providers. This includes establishing a systematic approach to monitoring and controlling ICT security requirements while promoting understanding and competence in the private sector regarding the need for regular cybersecurity training (cyber hygiene) and compliance with ICT security requirements.

Taking into account the priorities set by the EU, the goals defined in national policy planning documents, as well as evaluating the achievements during the previous reporting period, the Strategy sets out five action directions for the period until 2026:


- Enhancement of Cybersecurity Governance,
- Promotion of Cybersecurity and Strengthening Resilience
- Public Awareness, Education, and Research
- International Cooperation and Rule of Law in Cyberspace,
- Prevention and Combating of Cybercrime.

ANALYSIS OF CYBERSECURITY SITUATION

Situation Description

In the National Cybersecurity Strategy for 2019-2022, increased attention was given to cybersecurity resilience, investments in ICT security, and personnel training. During the reporting period, several significant steps were taken to promote cybersecurity, mitigate digital security risks, enhance ICT resilience, strengthen the provision of critical ICT and services to society, promote public awareness, education and research growth, enhance international cooperation, ensure rule of law in cyberspace, and reduce cybercrime. Out of the 21 tasks set during the reporting period, 19 tasks, or 90%, have been completed.

With the Russian invasion of Ukraine, there has been a rapid deterioration of the regional security situation, which has further highlighted the need to strengthen cybersecurity in Latvia. There has been an observed increase in attacker activity, including active scanning, vulnerability searching in critical systems, information gathering attempts, phishing campaigns, including fraudulent emails and social engineering campaigns. There has been a significant number of targeted Distributed Denial of Service



(DDoS) attacks not only against public sector systems but also against service providers that are important to society, particularly intensifying during politically or socially significant events. Latvia's active role in the international arena and its strong stance against Russian aggression in Ukraine make it a popular target for organized cyber attacks. The significant increase in malicious activities in cyberspace in 2022 indicates the need to ensure appropriate personnel resources to respond to cybersecurity incidents and the necessity to strengthen national-level capabilities by developing and improving monitoring and control mechanisms to ensure the continuity of critical ICT resources for the functioning of the state.

ICT development, both in Latvia and abroad, has reached unprecedented speed and scale. The latest generation of ICT solutions provides opportunities to quickly and conveniently access a wide range of information about events and processes in Latvia or abroad, communicate and exchange information, conduct online transactions and payments, receive electronic services, create, sign, and send electronic documents, and store information in electronic form, utilizing the benefits offered by smart devices and cloud computing service providers.

Many of these technologies are utilized in state governance and are vital for the independent and efficient functioning of public and government institutions. Therefore, it is crucial for these technologies to be secure. Cybersecurity is increasingly being prioritized, considering the consequences that a cyber attack directed against the state and society can have. It is undeniable that the intensity and complexity of cyber attacks are on the rise, impacting daily life and posing threats to both civilian and military


infrastructure. Additionally, both non-state and state actors contribute to cyber threats. With the onset of the Russian war in Ukraine, there has been a trend of increased activity from state actors and supporting entities with the aim of influencing the political, economic, or security situation in the country, illicitly obtaining data, or making changes to it.

In the international system as a whole, increased attention is being given to various cyber threats and, consequently, to cybersecurity. Among NATO allies, there is a strengthening of the political stance that cyber attacks, particularly their consequences, can be equated to conventional attacks in certain circumstances. Accordingly, malicious activities in cyberspace that result in significant consequences can serve as a basis for invoking Article 5 of NATO. Latvia's national cyber defence policy is determined by state-level planning documents such as the State Defence Concept of Latvia⁶ and specific sectoral planning documents.

Similarly, among EU member states, there is an overall increase in the relevance and importance of cybersecurity issues. It is projected that this trend will only intensify, with an estimated 22.3 billion devices worldwide being connected to the Internet of Things⁷ by 2024. Responding to the trends in the field of cybersecurity, the European Commission and the European External Action Service (EEAS) introduced the new EU's Cybersecurity Strategy

6 The announcement by the Saeima "On the Approval of the State Defence Concept" of September 24, 2020. <https://likumi.lv/ta/id/317591>.

7 EU cybersecurity policy, available at: <https://www.consilium.europa.eu/lv/policies/cybersecurity/>.



for the Digital Decade⁸ in December 2020. Its aim is to strengthen Europe's overall resilience to cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy services and digital tools they can rely on. To achieve this, the EU's Cybersecurity Strategy plans to review existing legal acts and introduce new ones, imposing several new obligations on member states in the field of cybersecurity. Moreover, cybersecurity was further prioritized by the EU in response to the Covid-19 pandemic and its challenges and implications for the ICT sector.

Since 2016, an important role has been assigned to one of the EU initiatives - the European Parliament and Council Directive No. 2016/1148 of July 6, 2016, on measures for a high common level of network and information system security across the Union⁹ (hereinafter referred to as the NIS Directive). The revised NIS Directive, also known as the NIS2 Directive, has entered into force. Unlike the original NIS Directive, which established security requirements for basic service providers and digital service providers in member states, the proposed revision of the NIS Directive includes additional sectors. It will apply to specific public or private "essential entities" in the fields of energy, transportation, banking services, financial market infrastructures, healthcare, drinking water, wastewater, digital infrastructure, public administration, and space. Additionally, it will cover "important entities" in the areas of postal and courier services, waste management, manufacturing and distribution of chemicals, food production, processing and distribution, as well as manufacturing and

⁸ EU's Cybersecurity Strategy, available at: <https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX:52020JC0018>.

⁹ NIS Directive, available: <https://eur-lex.europa.eu/legal-content/LV/TEXT/?uri=CELEX:32016L1148>.

provision of digital services. As the competent authority, MoD is responsible for identifying the entities operating in the sectors specified in the NIS2 Directive and ensuring that these entities implement appropriate and proportionate technical and organizational measures for managing cybersecurity risks. MoD, in collaboration with CERT.LV, will also monitor compliance with the prescribed security and incident reporting requirements by these entities. Additionally, in accordance with the provisions of the NIS2 Directive, AM will determine the actions to be taken in case of non-compliance with these requirements.


Current Affairs and Future Challenges

Workforce

In the joint statement to the European Parliament and Council titled "Resilience, Deterrence, and Defence: Building Strong Cybersecurity in the EU" (JOIN (2017) 450 final)¹⁰, it was emphasized that by 2022, there will be a shortage of 350,000 professionals with cybersecurity skills in the private sector in Europe, and this trend is likely to continue. The challenge arises not only from the direct shortage of cybersecurity specialists but also from the overall demographic development, which, in the medium and long term, will lead to a situation where fewer and fewer people will enter the labor market, unable to meet the demand for professionals in certain fields.

Such a shortage creates significant competition in the European and global labour market, where the public sector also has to compete. Latvia is no exception to this trend,

¹⁰ Resilience, Deterrence, and Defence: Building Cybersecurity in the EU, available: <https://eur-lex.europa.eu/legal-content/lv/TX-T/?uri=CELEX:52017JC0450>.



which is why the training and attraction of qualified specialists in both the public and private sectors are and will be essential challenges in the coming years. The lack of competent personnel has a negative impact on daily work and the ability to respond promptly to cyber threats and crises. Particularly negative effects are observed in areas that involve specific cybersecurity issues and functions that can only be performed by specially trained personnel. The problem is particularly relevant in the case of technical personnel, where the average salary for equally qualified and experienced specialists in the private sector is approximately twice as high as the maximum salary set by the remuneration system for state and municipal institution officials and employees. According to the amendments approved on November 16, 2021, in the Law on Remuneration of Officials and Employees of State and Local Government Authorities, there are possibilities to bring the remuneration level of qualified experts closer to that of the private sector. However, this alone cannot fully address the shortage of cybersecurity specialists. So far, there has been no systematic approach to the training of cybersecurity specialists, and, considering the undeniable future potential and the need for this profession at the national level, it will be necessary to find a solution in the near future.

New EU-level initiatives

One of the most important binding EU documents is the aforementioned NIS2 Directive, which will serve as the basis for many tasks of the newly established National Cybersecurity Centre (NCSC). Additionally, the Cyber

Resilience Act¹¹ will introduce changes aimed at protecting customers and businesses from products with insecure elements by implementing unified cybersecurity standards. With the Cyber Resilience Act, regulations will be introduced to safeguard digital products that were not previously covered by existing regulations. The Cyber Resilience Act will be the world's first legislative act regulating the Internet of Things (IoT). While these EU-level initiatives are significant and supportable, they will impose an additional bureaucratic burden on both supervisory state institutions and other stakeholders. Cybersecurity is a sector that is not yet fully regulated, and it continues to evolve. It should be noted that the workload associated with the implementation of various EU and, consequently, national-level cybersecurity requirements will only increase in the medium and long term.

The availability of information systems and the receipt of e-services

According to the 2022 State Audit Office's audit report "Can We Rely on the Availability of Information Systems and the Receipt of e-Services," deficiencies have been identified in the assessment of information system availability and overall management of information systems. It is necessary not only to establish an adequate internal control environment and implement information system security and ICT governance but also to measure the achieved results.

Insufficient level of cybersecurity in state administration institutions

¹¹ Information on the Cyber Resilience Act is available here: <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>



In the current situation, it is often observed that cybersecurity aspects are considered in state ICT projects only after receiving a report from CERT.LV about identified problems or past incidents. However, these are only isolated projects that come under the attention of CERT.LV. The problem was partially highlighted in the KPMG study conducted in 2019, “How cyber secure are Latvian municipalities?”¹² Within the scope of the study, high-risk vulnerabilities were discovered in 10 out of 15 evaluated municipal websites, while medium-risk and low-risk vulnerabilities were found in all the municipalities examined. It should be noted that since 2019, both the number of municipalities and the geopolitical situation have changed, and comprehensive studies on the situation in municipalities in 2022 are not available. Nevertheless, it is necessary to continue actively improving the level of cybersecurity in the public sector as a whole. In order for the state to keep pace with the rapid development of ICT, achieve the objectives and goals set out in the Digital Transformation Guidelines for 2021-2027, and effectively counter cyber threats, well-organized and managed ICT infrastructure must be ensured in state and municipal institutions. They should ensure the development, maintenance, and management of ICT solutions and information systems in accordance with best practices. As the creator and implementer of state ICT security and defence policies in this field, the Ministry of Defence (MoD) has identified problems at various stages, namely, during the planning and development of ICT solutions and information systems, as well as during the implementation and maintenance stages. In the long term, it is necessary to promote the allocation of adequate resources for cy-

bersecurity measures in the state and municipal sectors, ensuring funding from existing institutional budgets and exploring possibilities for additional state budget funding and utilizing opportunities provided by EU funds. For example, work is currently being done on regulations for the Cyber Emergency Fund, which could be one of the potential tools for strengthening cybersecurity in both the public and private sectors.

Secure implementation of new technologies and digital solutions

In addition to the development of existing technologies, new digital opportunities are being offered, and the implementation of existing ones continues. These include artificial intelligence, big data, quantum technologies, 5G, and now even 6G. This poses new requirements for the protection of valuable information and digital infrastructure, which are critical for ensuring vital societal functions. It also places additional demands on the private sector, which is part of the supply chains for delivering essential services to the public. Both the public and private sectors need to keep pace with these advancements, and preparatory work must be done in a timely manner, including ensuring the availability of specialized professionals in the field.

¹² How cyber secure are Latvian municipalities (study), available at: <https://assets.kpmg/content/dam/kpmg/lv/pdf/2019/05/cik-kiberdro%C5%A1sas-ir-latvijas-pasvaldibas.pdf>.

CYBERSECURITY GOVERNANCE

Risk Management

Adhering to the recommendations of the Organization for Economic Cooperation and Development (OECD)¹³, the following four general principles of cybersecurity risk management should be observed by all participants involved in cybersecurity governance:

- understanding of cybersecurity risks and their management;
- assuming responsibility for cybersecurity risk management;
- addressing cybersecurity risks in a transparent manner and in accordance with human rights and fundamental values;
- collaboration, including at the international level.

In addition to the general principles mentioned above, four operational principles are identified:¹⁵:

- risk assessment and treatment cycle;
- security measures;
- innovations;
- preparedness and continuity.

13 OECD recommendations “Recommendation of the Council on Digital Security of Critical Activities” (2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456>

14 OECD recommendations “Digital Security Risk Management for Economic and Social Prosperity” (2015) <https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf>, 10 – 11.


15 OECD recommendations “Digital Security Risk Management for Economic and Social Prosperity” (2015) <https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf>, 10 – 11.

The principles were taken into account when developing the Strategy, focusing on both individual and organizational responsibility, as well as national and international processes.

GOVERNANCE MODEL AND FUNCTIONS AND RESPONSIBILITIES OF INVOLVED PARTICIPANTS

On June 7, 2022, the Cabinet of Ministers approved the informative report “On the Improvement of National Cybersecurity Governance,” developed by the Ministry of Defence, and the implementation of cybersecurity governance reforms began on January 1, 2023. As a result of the reforms, cybersecurity governance in Latvia will be implemented through a partially centralized governance model. The newly established National Cybersecurity Centre, operated by the Ministry of Defence and CERT. LV, will serve as the main competent authority in the field of cybersecurity. It will oversee NIS2 and national regulatory entities in the cybersecurity domain, except for critical ICT infrastructure, which will continue to be monitored by the Constitution Protection Bureau (SAB), as before.

The governance of national cybersecurity is based on mutual cooperation, where each state institution fulfils its functions, including in cyberspace, by directly collaborating with other institutions and the private sector, or in a unified cooperation format within the framework of the National Information Technology Security Council. As a result of the reform implementation, the functions and responsibilities of the participants in the new cybersecurity governance model are as follows:



The National Cybersecurity Centre (NCSC) formulates national cybersecurity policy and oversees its implementation. It ensures the implementation of the NIS2 Directive and structured monitoring of requirements. NCSC supports the operation of the European Cybersecurity Competence Centre (ECCC) National Coordination Centre NCC-LV in Latvia and is responsible for preventing cyber incidents and raising public awareness. Within its competence, NCSC also establishes and implements international cooperation.

The Ministry of Foreign Affairs (MoFA), within its competence, supports international cooperation and Latvia's participation in various international initiatives related to cybersecurity.

The Data State Inspectorate (DSI) performs the tasks assigned to it in the field of personal data processing, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation), the Law on the Processing of Personal Data of Natural Persons, and the Law "On the Processing of Personal Data in Criminal Proceedings and Administrative Offense Proceedings."

Ministry of Economy (MoE) develops economic policies and promotes the development of competitiveness and innovation.

Ministry of Interior (MoI), State Police (SP) implement policies for crime prevention, protection of public order


and security, and protection of personal rights and legitimate interests. **The Information Centre of the Ministry of the Interior (IC)** ensures the operation of information systems' ICT infrastructure for law enforcement agencies.

Ministry of Education and Science (MoES) promotes public awareness and understanding of building a knowledge base in the field of cyberspace, science, technology, engineering, and mathematics at all levels of education. It also strengthens the research capacity of higher education institutions by providing funding from the state budget and EU structural funds (European Regional Development Fund, European Social Fund) for research infrastructure, including the development and strengthening of human capital.

Ministry of Culture (MoC) is responsible for strengthening media literacy among people in formal and non-formal education, promoting the recognition of fake news and disinformation in society, as well as fostering critical thinking.

Ministry of Welfare (MoW) shapes and implements the policy in the fields of labour, social protection, children and family rights, as well as equal opportunities for people with disabilities and gender equality.

The Bank of Latvia (LB) regulates and supervises the activities of financial market participants in cyberspace and promotes secure and uninterrupted operation of payment systems. Meanwhile, credit institutions are responsible for the security and availability of their sector's electronic services.



The operations of the Latvia's Safer Internet Centre "Net-Safe Latvia" are ensured by **the Latvian Internet Association (with support from the MoD)**, which educates the public about potential risks and threats in the online environment, promotes safe internet usage, and safe internet content.

The Military Intelligence and Security Service unit (MilCERT) ensures ICT monitoring for the MoD and its subordinate institutions, including the National Armed Forces (NAF). Within the sector, it detects and processes information technology security incidents, coordinates their mitigation, and conducts security audits of the ministry's information systems and electronic communication networks. MilCERT provides support and consultations to personnel responsible for cyber security in defence sector institutions.

NAF and National Guard Cyber Defence Unit (CDU) provides support in crisis or threat situations in preventing IT security incidents and overcoming the resulting consequences in the cyber environment.

Non-governmental organizations in the sector provide support, consultation, and collaborate with the NITSC in shaping and implementing cybersecurity policy.

Ministry of Transport (MoT) organizes policy in the field of electronic communications and network operations

Constitution Protection Bureau (SAB) oversee critical ICT infrastructure.

Ministry of Justice (MoJ) develop, organize, and coordinate policy in the field of personal data protection.

The State Joint-Stock Company "Latvia State Radio and Television Centre" (LVRTC) is a trusted certification service provider that ensures the infrastructure necessary for the operation of electronic identification means, authentication tools, qualified electronic signatures, and a logically unified data centre. It also ensures the operation and protection of the state unified Internet Exchange Point (GLV-IX) against denial of service attacks.

The State Security Service (VDD) is an anti-espionage and internal security service.

The Ministry of Environmental Protection and Regional Development (MoEPRD) develops and coordinates the implementation of the policy for the governance of the information society, management of public administration services, and management of digital technologies in public administration. The State Regional Development Agency (SRDA) ensures the operation and development of shared IT solutions in the public sector.

To ensure the transition to a partially centralized cybersecurity governance model and implement reforms, the MoD in collaboration with CERT.LV has identified specific steps to improve the national cybersecurity governance:

- 1) establishment and development of the National Cybersecurity Centre (NCSC),
- 2) involvement of the MoD in evaluating security requirements for state and municipal information systems,



- 3) creation of competency centres and development of a framework for grading data centre security requirements,
- 4) establishment of Security Operations Centres (SOC) for hosting information systems of state institutions in data centres,
- 5) national implementation of the NIS2 Directive, including the development and amendment of national legislative acts in the cybersecurity field, such as the “Cabinet of Ministers Regulation No. 442 of July 28, 2015, on the Procedure for Ensuring Compliance of Information and Communication Technology Systems with Minimum Security Requirements”,
- 6) oversight of entities subject to the NIS2 Directive and national cybersecurity legislation, in accordance with the division of responsibilities between the NCSC and Constitution Protection Bureau (SAB).

DIRECTIONS OF NATIONAL CYBERSECURITY POLICY ACTIONS

The strategy has been developed in line with the NIS2 Directive and the requirements therein, the EU's Cybersecurity Strategy for the Digital Decade, Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Industrial, Technological and Research Competence Centre for Cybersecurity and the Network of National Coordination Centres, and the cybersecurity strengthening measures included in the Work Programme of the Digital Europe Programme¹⁶, which outline the planned European-level actions in the field of cybersecurity. In developing the Strategy, national digital policy planning documents have also been taken into account to ensure coherent development of digital and cybersecurity in Latvia. One of the key policy planning documents in the field of digital development that has been considered in the development of the Strategy is the "Guidelines for Digital Transformation for 2021-2027" approved by Cabinet of Ministers Order No. 490 of 7 July 2021.¹⁷

DIRECTION 1 "ENHANCEMENT OF CYBERSECURITY GOVERNANCE"

Objective of the direction: a comprehensive, effective, and systematic cybersecurity governance model that ensures the supervision of NIS2 entities with NCSC as the leading institution.

¹⁶ Information about the Digital Europe Work Programme: <https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital>

¹⁷ Cabinet of Ministers Order No. 490 of 7 July 2021 "On Guidelines for Digital Transformation for 2021-2027". <https://likumi.lv/ta/id/324715>

Tasks:

- *Reflect a clear distribution of functions and responsibilities in the regulatory framework.*
- *Establish a system for providing ICT sharing services.*
- *Actively participate in the improvement and development of binding EU legislation.*
- *Integrate binding requirements of EU legislation into national regulatory acts and processes.*
- *Strengthen collaboration between the public and private sectors.*

According to the National Security Concept, control and reduction of cyber threats is only possible in connection with effectively implemented national cybersecurity policy that ensures long-term and systematic crisis management capabilities, develops legal regulation in the field of information and technology, educates society, and works purposefully on the development of responsible institutions and human resources in the sector.¹⁸ **The main goal during the reporting period in the direction of improving cybersecurity governance is to create a comprehensive, effective, and systematic cybersecurity governance model that ensures the NIS2 subject monitoring system with the NCSC and SAB as leading institutions.**

With the increasing importance of cybersecurity, the scope and complexity of tasks related to cybersecurity for MoD and CERT.LV have grown, including tasks arising from EU legislation. Simultaneously, as the need to strengthen the security of the national cyberspace incre-

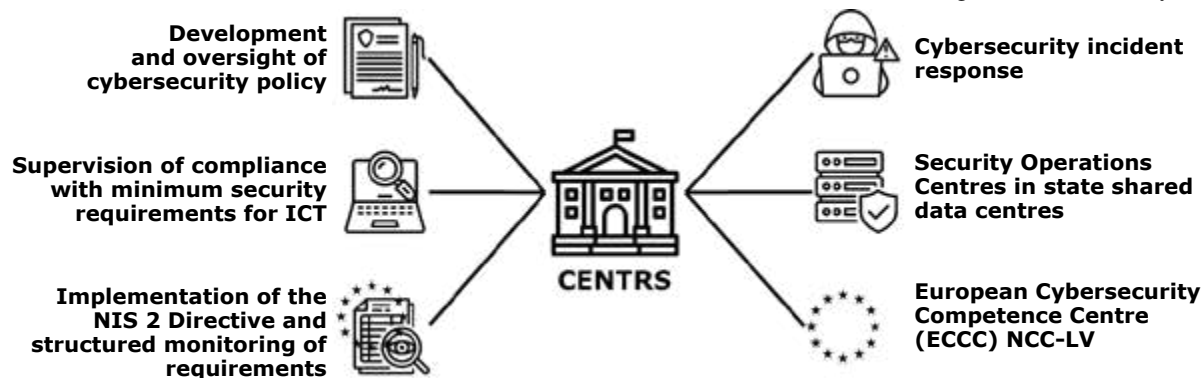
¹⁸ The announcement of the Saeima on September 26, 2019, "On the Approval of the National Security Concept." <https://likumi.lv/ta/id/309647>

ases within the framework of comprehensive national defence implementation, a national competent authority in the field of cybersecurity, the NCSC, will be established, with MoD and CERT.LV ensuring its operations. The NCSC, together with SAB, will form the core of the national cybersecurity management system.

To establish such a governance model, specific working directions have been identified. One of the key steps is the administrative implementation of the new cybersecurity

management model. In 2023, the new NCSC, operating as the main competent authority in the field of cybersecurity, will begin its operations. MoD will develop national cybersecurity policy and oversee its implementation, while CERT.LV will be responsible for incident response, prevention, public awareness, and supervision of the Security Operations Centre (SOC) (see Diagram 1). The new management model will involve close collaboration between the NCSC and SAB, which oversees critical ICT infrastructure.

Diagram 1. Functions of NCSC.



NCSC will perform the following functions:

- development of cybersecurity policy (both nationally and through participating in the analysis and expression of opinions on EU and NATO initiatives), and oversight of its implementation;
- international cooperation in the field of cybersecurity (including representing Latvia’s interests in EU and NATO working groups on cybersecurity, in ENISA, CyCLONE, NIS Cooperation Group, in European

- Cybersecurity Industrial, Technology and Research Competence Centre, and in National Coordination Centre Network, NATO CCDCOE);
- implementation of the functions of the National Coordination Centre, including the establishment, implementation, monitoring, and coordination of the EU financial instrument management system indirectly managed by ECCC;

- coordination of the establishment of information systems for state governance institutions and their continuous evaluation in terms of cybersecurity, as well as providing recommendations on cybersecurity issues and overseeing the implementation of cybersecurity requirements and NCSC recommendations;
- supervision of essential service providers and digital service providers (as defined by the NIS2 directive, after the NIS2 Directive comes into effect) with the exception of those subject to oversight as owners and operators of critical information infrastructure, whose oversight will continue to be carried out by SAB;
- imposition of sanctions for non-compliance with NCSC and SAB recommendations;
- oversight of cybersecurity certification, electronic identification, and trust service providers;
- provision of secretarial functions for NITSC and the Digital Security Monitoring Committee;
- prevention of cybersecurity incidents;
- raising public awareness and engagement;
- determination of security requirements gradation for state shared data centres that facilitate cloud-based data processing (referred to as shared data centres) and other data centres that maintain state ICT resources, as well as ensuring compliance with requirements of Competence Centres.

According to the new governance model, it is necessary to clarify the regulatory framework by establishing a clear distribution of functions and responsibilities. Ensuring ICT shared services is also crucial - it involves defining the gradations for shared data centres based on their provided level of security and establishing operational mo-


dels for security operations centres within the shared data centres.

In order for the state to keep up with the rapid development of ICT, achieve the objectives and tasks set forth in the Digital Transformation Guidelines for 2021-2027¹⁹, and effectively address cybersecurity threats, it is crucial for government and municipal institutions to ensure well-organized and managed ICT infrastructure. Government and municipal institutions should ensure the development, maintenance, and management of ICT solutions and information systems in accordance with best practices. The Ministry of Defence, as the creator and implementer of the state's ICT security and defence policy, has identified challenges in various stages, including the planning and development stages of ICT solutions and information systems, as well as their implementation and maintenance.

One of the identified problems is the inadequacies observed during the planning and development stages of ICT systems. ICT projects are implemented without sufficient assessment of security-related risks, without ensuring compliance with the required security level, and without planning sufficient security testing before putting the systems into operation. During the planning and development stages, institutions tend to focus on basic functional requirements and usability, paying insufficient attention to system deployment, integration, and security requirements.

According to the procedure established by Cabinet of

¹⁹ Digital Transformation Guidelines for 2021-2027, available at: <https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam>.



Ministers²⁰, all information system development projects must be coordinated with the relevant institutions, including the MoD. To ensure proper involvement of the MoD in assessing the security requirements of state and municipal information systems, it is necessary to strengthen the procedure where the supervising ministry, together with the institution, discusses the planned development activities, identifies system security risks and other security criteria, and agrees on the system's security class in accordance with the methodology determined by the Cabinet of Ministers. Additionally, the adequacy of the prepared description should be evaluated. To implement the aforementioned monitoring mechanism from the MoD's side, changes to binding regulations need to be made during the review period.

The planned procedure will include the evaluation of the compliance of state information systems with the defined security level during the planning and development phase. The Ministry of Defence will ensure that the requirements corresponding to the specified security level are included in the information systems. By implementing this step, the oversight of state information system security would be partially centralized, promoting cybersecurity in the country and achieving the objective set out in the National Development Plan of Latvia for 2021-2027²¹, which states that a cybersecurity risk assessment will be conducted for every electronic service and solution before

their implementation, ensuring cybersecurity throughout their lifecycle. This approach will ensure continuity, integrity, and data protection of the services and solutions.


At the same time, as an EU member state, Latvia is required to ensure the integration of binding documents and regulations at the Union level into national legislative acts and practices. During the review period, significant attention should be given to the incorporation of the NIS2 Directive requirements in legislative acts, ensuring the establishment of a supervision model for NIS2 entities. Starting from 2023, this role will be fulfilled by the NCSC. Considering that NIS2 Directive entities can also be owners of ICT critical infrastructure and competent authorities whose supervision is carried out by SAB, clear provisions will be defined in legislative acts regarding the division of supervisory functions, rights, and tasks between the NCSC and SAB, creating a unified supervisory process applicable to both NIS2 Directive entities and national legislative entities in the field of cybersecurity. The unified supervisory process will be organized at three levels²²:

- 1) mandatory annual cybersecurity assessment for all NIS2 Directive subjects, and ICT critical infrastructure owners and legal administrators;
- 2) extraordinary risk-based inspections of thematic ICT systems and resources;
- 3) voluntary implementation of coordinated vulnerability disclosure processes within institutions.

²⁰ At present, the procedure is determined by the Cabinet of Ministers Regulation No. 597 of August 31, 2021, "Procedures for Monitoring State Information System Development Projects." However, new regulations will be developed in 2023.

²¹ The announcement of the Saeima of July 2, 2020, "On the National Development Plan for Latvia 2021-2027 (NAP2027)". <https://likumi.lv/ta/id/315879>

²² It is planned that SAB will be responsible for implementing the measures mentioned in Points 1 and 2 regarding ICT critical infrastructure..



SAB is responsible for monitoring ICT critical infrastructure, and in the new cybersecurity governance model, SAB will have the authority to provide necessary information to NCSC (for example, in case of non-compliance with recommendations or regulatory requirements). NCSC will have the authority to issue binding administrative acts (e.g., requiring the remediation of identified non-compliance) to ICT critical infrastructure owners and legal administrators.

Effective cybersecurity management is not possible without the involvement of the private sector, which is why promoting collaboration between the public and private sectors is crucial during the review period. It is necessary to establish the principles of this collaboration and start implementing them in practice. The task is to develop a collaboration model that is flexible, involving the private sector in both long-term projects and initiatives, as well as providing operational consultations when needed. The collaboration model should be based on two-way communication and mutual benefit, without creating unnecessary formal processes and additional administrative burden.


Building relationships based on mutual trust is essential, ensuring the flow of relevant information where government institutions proactively inform about potential threats, while the private sector openly reports incidents or other problem situations. It is important to maintain a system where government collaboration with the private sector occurs in an open, fair, and non-discriminatory manner, ensuring transparency in decision-making processes as much as possible.

DIRECTION 2 “PROMOTION OF CYBERSECURITY AND STRENGTHENING RESILIENCE”

Objective of the direction: Government institutions and private sector businesses with secure, monitored, and renewable ICT resources and employees who are aware of cybersecurity risks and able to respond appropriately to threats and incidents.

Tasks:

- *Promote the development and testing of functioning business continuity plans.*
- *Reduce vulnerabilities by focusing on cyber hygiene and implementing security standards.*
- *Foster understanding of the need for cybersecurity standards within the private sector, evaluating the possibilities of implementing standards within the cybersecurity community.*
- *Establish clear security requirements for NIS2 entities and implement a national certification model.*
- *Develop a cyber crisis management plan.*
- *Ensure secure information exchange within the government administration and develop state-managed strategically important digital infrastructure services to strengthen national strategic autonomy.*
- *Provide the public with a secure, state-managed toolkit for electronic communication, promoting its use among the population.*
- *Ensure that long-term maintenance costs, including the allocation of appropriate personnel and auditing, are included in new state IT projects and development plans for existing projects.*
- *Develop and maintain the ICT systems for European Parliament, Parliamentary, and municipal elections.*

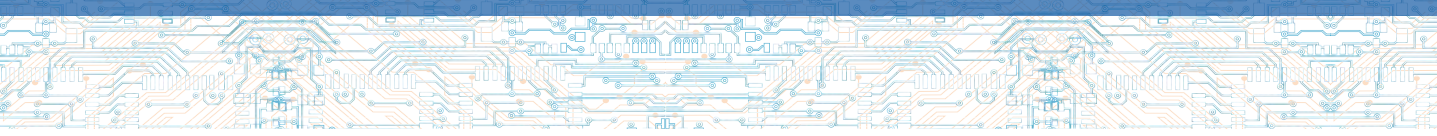


According to the National Defence Concept, cybersecurity and the resilience of information technology systems are an integral part of a comprehensive national defence system, where both the public and private sectors play a crucial role. To ensure effective functioning of the system, it is necessary to continue to make improvements not only within the government but also in the private sector, including promoting closer collaboration between both sectors. **The main goal during the reporting period is to ensure a situation where the ICT resources of government institutions and private sector businesses are secure, monitored, and renewable, and where their employees are aware of cybersecurity risks and able to respond appropriately to threats and incidents.**

To reduce the vulnerability of state institutions, society, and businesses in the field of cybersecurity and ensure uninterrupted system operation, it is necessary to focus on several essential aspects. These include resource inventory policies, creation of information, information system and backup policies, cybersecurity training (cyber hygiene), as well as the development and testing of business continuity plans. One of the steps in the cybersecurity management reform towards a partially centralized ICT governance model is the provision of ICT shared services through the use of state data processing clouds. It is planned that four shared data centres (LVRTC, National Library of Latvia, the Information Centre of the Ministry of the Interior, and Agricultural Data Centre) will ensure the development and operation of the state data processing cloud. State and municipal institutions will be able to utilize standardized cloud services for data processing, including various levels of virtualization and data storage services. From electronic service catalogues, institutions

will be able to select resources that will be provided in a centralized manner, as well as choose the level of decentralized duplication of resources corresponding to the risk class of the hosted information system. Institutions will also have the option to electronically enter into service contracts. Additionally, institutions will be able to deploy information systems in private data centres located within the territory of Latvia, provided that they comply with the necessary security standards. It is planned to educate personnel responsible for information system management about system risk assessments and necessary measures to mitigate their impact. An independent and centralized monitoring of critical resources in the state data processing cloud will be established, along with maintaining close intersectoral cooperation in the development, implementation, and enforcement of security standards, policies, and maintenance guidelines.

During the reporting period, relevant regulatory acts will be specified to clearly establish that state and municipal ICT resources are maintained in shared data centres that meet at least the minimum security requirements. It is also planned to establish a clear gradation of shared data centres and other data centres where state and municipal ICT resources are maintained (hereinafter all together - data centres), security levels, and corresponding security requirements, by standardizing the minimum security requirements. The ICT resources located in data centres - information systems, registries, databases - are of various types, ranging from document and resource management systems and informational websites to widely used e-services that can become a target of cyber attacks, or critical registers whose data compromise can have broad, sometimes irreversible consequences.




Along with the establishment of data centres, it is necessary to develop a comprehensive, centralized model for strengthening cybersecurity in the country, which involves integrating CERT.LV's operational cells (Security Operations Centres, hereafter referred to as SOCs) in each of the planned shared data centres by the Ministry of Environmental Protection and Regional Development (MoEPRD). This will ensure that the shared data centres have the capabilities for monitoring, responding to, investigating, and identifying threats that are in line with modern challenges. The operation of the SOCs will be provided by NCSC. NCSC will operate as an expert team that oversees the flow of data exchange between institutions, including monitoring, analyzing, and responding to security threats and attacks directed at the data centre infrastructure or specific institutions. The establishment of SOCs in each of the data centres is another necessary step towards the implementation of a partially centralized cybersecurity monitoring model for ICT systems of state administration institutions.

In each institution, there would still be a need for ICT personnel and a security manager who would be responsible for the institution's infrastructure, planning and implementing cybersecurity measures, as well as educating employees in the field of cybersecurity. ICT personnel and security managers can also be unified within a ministry or department. However, with the deployment of SOCs in data centres, the security manager within an institution would not require in-depth technical knowledge in mitigating security incidents, although an understanding of the processes themselves would be necessary. Similarly, the monitoring, analysis, and mitigation of cyber threats would primarily be carried out by the SOC team.

On the other hand, within the private sector, it is essential to promote the interest and knowledge of executives and managers of institutions and companies regarding the importance of cybersecurity, not only in crisis situations but also in the long term, under any circumstances. This also includes paying additional attention to facilitating voluntary information exchange among businesses. An ongoing task in promoting cybersecurity is to improve, assess, and monitor the implementation of minimum cybersecurity standards throughout the country, encompassing both the public and private sectors. While ensuring the fulfilment of this crucial initial step, it is also necessary to raise these security standards by promoting the understanding that compliance is required, not only because it is mandated by regulations but also because the awareness of its necessity has been solidified. The elevation of security standards also involves clearly defining the equipment and software the usage of which is not recommended or is prohibited for the respective entities. With the European Commission's plan for cybersecurity certification of ICT products, it is expected that work will commence on the development of corresponding EU legislation, which, in turn, will determine additional obligations for competent authorities of member states in the field of cybersecurity certification of ICT products. This is also identified as one of the challenges during the review period – to establish/designate a national accreditation body to fulfil this responsibility.

During times of crisis and war, the protection of information and cyberspace must be ensured through active and passive defence measures to prevent external interference and the paralysis of operational capabilities. To achieve this, it is necessary to promote cooperation among sta-



te institutions in times of crisis by establishing and testing various crisis mechanisms and procedures. Ensuring the security of supply chains also plays a significant role, minimizing the risks of disruptions during crisis situations. Additionally, the cybersecurity and resilience of state public media should be strengthened to ensure their uninterrupted operation even in crisis conditions.


To ensure effective and secure functioning of the state administration and local government, it is necessary to improve and enhance the secure exchange of restricted information among public sector institutions. Currently, the organization of such information exchange varies across different institutions, potentially posing risks to information security and hindering digital flow of restricted information within the public sector. These differences are objectively justified as the proportion of restricted information in the overall information exchange varies significantly among institutions, resulting in different practices, availability of necessary systems, and other factors. However, despite these differences, it is necessary to promote secure digital circulation of restricted information among public sector institutions during the review period.

The creation and issuance of identification documents for individuals is one of the crucial functions of the state, and managing and independently carrying out this task is a hallmark of state sovereignty. In the current context, where an increasing number of activities are performed in the digital environment, the importance of secure electronic identification of individuals is growing. By defining the concept of national electronic identification of individuals in the Law on Electronic Identification of

Natural Persons, this highly reliable means of electronic identification is effectively equated to a state-issued identification document in the digital realm. Considering the technological basis for providing electronic identification solutions, namely the dependency of the identification means on the continuous operation and accessibility of the supporting technological platform, full state control is necessary for the assured independent execution of the functions related to individuals' electronic identification. This control extends not only to the issuance of the national electronic identity means but also to the development, operation, and maintenance of the technological platform that supports its functionality. Based on these considerations, a national platform for electronic identification and trusted services is being developed and operated.

The Latvian state develops and provides its residents with digital equipment, including the national electronic identification means and the official electronic address, which enables safe communication with state institutions and facilitates the use of digital services. Equally important to the creation and maintenance of the respective technological platforms is the distribution of digital equipment to the population and the acquisition of secure and efficient skills for its use. The goal of ensuring that every resident in Latvia has access to secure digital equipment and the skills to use it effectively will be achieved gradually. This will involve strengthening the regulation of rights and obligations related to the use of digital equipment, improving the usability of digital devices, expanding the range of possible applications, and promoting targeted activities for the development of communication and digital skills.

With the deployment of fifth-generation (5G) mobile



networks, ensuring the security of these networks has become a strategic priority on the agenda of every country. It involves considering technical, technological, and political factors. It also imposes additional requirements on the private sector, which is part of the delivery chain for services that are important to society. Both the public and private sectors need to continue ensuring the secure implementation of 5G networks while also preparing for further technological advancements in advance.

Free and fair elections are one of the essential elements of a democratic state. Similarly, to other areas, information and communication technology (ICT) is also utilized in the electoral process and result aggregation. Therefore, increased attention must be paid to the security of ICT systems that are used in the elections for the European Parliament, national parliaments, and local governments to ensure the integrity of the electoral process. To ensure the security of the ICT systems used in elections, it is necessary to provide sufficient funding for their development, improvement, and maintenance on an annual basis, rather than just during election years. Such an approach would allow for consistent and well-thought-out development of electoral ICT systems and enable competent authorities to verify their security in a timely manner. As the importance and utilization of ICT in elections grow, it is essential to strengthen the ICT capacity of the Central Election Commission.

DIRECTION 3 “PUBLIC AWARENESS, EDUCATION AND RESEARCH”


Objective of the direction: aggregated information on the current training opportunities for cybersecurity specialists

and identified needs for future cybersecurity education programs, as well as developed focused cybersecurity awareness campaigns for various segments of society.

Tasks:

- *Identify the needs for upgrading the qualifications of existing specialists and establish a system for the education and recruitment of new cybersecurity professionals.*
- *Promote the involvement of industry professionals in knowledge exchange and training processes.*
- *Develop training programs for IS/ ICT security managers to improve their qualifications.*
- *Identify and implement specific initiatives (information campaigns, etc.) targeting different segments of society - children and youth, seniors, employees of government institutions - to strengthen their knowledge and understanding of cyber hygiene.*
- *Strengthen the development of cybersecurity research in Latvia, utilizing the funding opportunities provided by the Digital Europe program and establishing necessary national support mechanisms for cybersecurity research.*

The implementation of cybersecurity policy at both strategic and technical levels is only possible through the recruitment of qualified cybersecurity specialists in government institutions and private sector companies. **The main goal during the review period is to identify the current training opportunities for cybersecurity specialists and determine the necessary educational programs for future cybersecurity professionals. Additionally, it aims at developing focused cybersecurity awareness campaigns for various societal groups.**



In the Guidelines for Digital Transformation for the period 2021-2027²³, it is mentioned that nearly half of all Latvian businesses seeking to hire ICT professionals report difficulties in filling the advertised vacancies. Similar trends are observed in the annual comparative study by the State Chancellery on salary levels.²⁴ The study concludes that the group of positions where it has been most challenging to attract and retain suitable candidates is the ICT field (39% and 34% of organizations, respectively). Furthermore, according to the informational report on medium and long-term labour market forecasts by the Ministry of Economy²⁵, the shortage of ICT specialists is expected to continue to grow. The shortage of qualified and knowledgeable ICT professionals (particularly those with knowledge of current cybersecurity issues) affects both policy-making in the MoD and the technical level of CERT.LV. The lack of competent personnel has a negative impact on daily work and the ability to respond promptly to cyber threats, incidents, and crises. The negative impact is particularly noticeable in areas that involve specific cybersecurity issues and functions that can only be carried out by specially trained personnel. However, it is worth noting the positive effect of the salary reform in the public administration implemented in 2022, which allows for higher remuneration for cybersecurity specialists and potentially generates greater interest in these positions, although it addresses the existing problem only partially.


23 Guidelines for Digital Transformation 2021-2027, available at: <https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam>.

24 Comparative study on salary levels, available at: <http://petijumi.mk.gov.lv/node/3305>.

25 Information report on medium and long-term labour market forecasts, available at: <https://www.em.gov.lv/lv/darba-tirgus-zinojums>.

To develop a long-term plan for the training of cybersecurity specialists, ranging from vocational education to second-level higher education, it is necessary to first identify the current training opportunities for cybersecurity specialists both within and outside academic institutions, as well as to determine the needs for future cybersecurity specialist education programs. Understanding the current situation in relation to future needs will help identify gaps in the current offer, allowing educational institutions to develop training programs accordingly. It is also important to introduce professional standards which are in line with existing international standards. Additionally, the role of the Cyber Defence Unit (CDU) in ensuring qualified cybersecurity personnel should be emphasized, providing support not only in the training process but also in personnel recruitment, while also offering assistance to CERT.LV and milCERT when necessary.

Citizens must be able to safely navigate their digital lives, including fully utilizing secure electronic communication tools such as eID cards and/or the mobile e-Signature application. This applies to children, youth, and adults alike, in order to minimize the risk of Latvian citizens falling victim to cybercrime or digital fraud in the future. It is important to emphasize that strengthening each individual's understanding of cyber hygiene is a cornerstone of cybersecurity in digital work environments, encompassing both the general public and employees of state institutions. Citizens, businesses, and government institutions need to know how to protect themselves and be digitally secure. During the reporting period, there is a need to improve public awareness of safe behaviour in the digital space, including the secure use of the internet and digital services, as well as to provide in-depth education



on cybersecurity issues for specific segments of society. Among these, attention should also be paid to secure electronic identification and communication. To achieve this, it is necessary to support the involvement of Latvian children and youth in international cybersecurity initiatives, competitions, and contests, ensuring that a knowledge base is established among children at a school-age level. It is necessary to develop and distribute educational materials for different age groups to ensure that basic skills and knowledge about security measures in the digital space and internet usage can be acquired by and accessible to not only the most active technology users but also, for example, seniors. Simultaneously, various social campaigns will be organized on current issues, such as an informative campaign on digital fraud and the risks of phone scams. Active participation in Cybersecurity Month should be ensured, making related activities the most recognizable and engaging in the field of cybersecurity in Latvia. It is also important to promote the knowledge and competency level of government institutions, especially at the municipal level, by fostering employees' understanding of secure ICT usage and involving them in educating and enhancing understanding among the public and clients of government institutions about secure communication with institutions and the receipt of institutional services.

The development of science and research is also significant in order to timely prepare for new cyber challenges and adapt to technological advancements. Considering the establishment of the European Cybersecurity Competence Centre and the network of national coordination centres of EU member states, it is important during the operational period of the Strategy to be able to identify

the priority areas for strengthening and developing Latvia's cybersecurity competence community. It is important to ensure that the available EU support is directed towards the development of these priority areas, including the implementation of innovative cybersecurity solutions and cybersecurity research. In this process, the central role will be played by the National Coordination Centre (NCC-LV), established within the Ministry of Defence, which is responsible for establishing and coordinating the cybersecurity competence community, collaborating with other national coordination centres of EU member states, as well as implementing EU cybersecurity support programs in Latvia in collaboration with the Central Finance and Contracting Agency. It is also crucial to develop competencies to be able to conduct future technology risk and impact analysis, in order to develop appropriate planning documents and development scenarios.

DIRECTION 4 "INTERNATIONAL COOPERATION AND RULE OF LAW IN CYBERSPACE"

Objective of the direction: To continue developing international cooperation to enhance international and national cybersecurity, by promoting the application of international norms in cyberspace and by establishing a clear and reliable network of cooperation partners who are capable of providing mutual support in cyber threat assessment and crisis situations, as well as ensuring swift information exchange and sharing best practices.

Tasks:

- *Strengthen multilateral and bilateral cooperation in cyber threat assessment and prevention, cyber incident detection, including active participation in international training and simulations.*
- *Promote the development of cyberspace that ensures secure provision of services important to the state and society, while respecting human rights.*

The objective of the review period is to continue developing international cooperation to promote international and national cybersecurity, by promoting the application of international norms in cyberspace and by establishing a clear and reliable network of cooperation partners capable of providing mutual support in cyber threat assessment and crisis situations, as well as ensuring swift information exchange and sharing best practices. It is necessary to continue promoting information exchange and best practices, cooperation, and the development of joint projects in multilateral formats, in order to strengthen information exchange mechanisms and promote the principle of responsible state behaviour in cyberspace.


Cyber threats have a transnational nature and can simultaneously pose risks to Latvia's national security, NATO, EU, and Latvia's international partners, endangering international and regional peace and security. Latvia will continue to be an active participant in the international fight against cyber threats, being a reliable partner and supporting international efforts to create a secure, open, free, and trustworthy cyberspace. Latvia advocates for a cyberspace where the secure, reliable, and uninterrupted

provision of services crucial to the state and society is guaranteed, while respecting human rights.

In multilateral formats, including the UN and OSCE, efforts should continue to promote trust and security, firmly supporting the principle that ensuring human rights in the virtual environment is equal to ensuring human rights in the physical world. Participation in the UN's work on ICT security²⁶ should be sustained, together with like-minded partners, promoting the effectiveness of existing international norms in cyberspace and advocating for responsible state behaviour in it.

In the EU format, legislative and policy initiatives should be promoted to ensure the secure and predictable development of the EU cyberspace, both in the operations of state institutions and in meeting the needs of individuals and legal entities. To deter cyberattacks and cyber incidents against EU ICT systems, the implementation of the EU Cyber Diplomacy Toolbox should be supported, with a consideration for its enhancement if necessary. Active cooperation and information exchange should be established within expert working groups and high-level meetings in the context of the EU and NATO. Latvia's active participation in international exercises and cyber attack simulations, including the improvement of NATO and EU cooperation procedures, should be continued to enhance cyber defence capabilities. At the same time, the active utilization of existing multilateral and bilateral cooperation formats should be supported, carefully evaluating the need for new formats to maintain focus and more effectively utilize limited resources.

²⁶ UN Open-ended working group on security of and in the use of information and communications technologies (OEWG).



International cooperation is a prerequisite for detecting and addressing serious cyber incidents, and it should be further deepened with Baltic, Nordic, and transatlantic partners. The region already has close economic ties and regional integration in the private sector, making it important to promote further integration in cyber threat awareness, cyber incident information sharing, and other aspects. One potential collaborative project is the establishment and development of a Baltic and Nordic Regional Security Operations Centre (SOC), which would enable real-time monitoring of the cyber space in the region, including analysis of telemetry and statistical data, as well as facilitate information exchange among the cyber incident response institutions of the regional countries regarding current cyber threats and incidents.

In this review period, it is also crucial to continue information exchange in bilateral cooperation formats, which provide practical contributions to timely risk identification, rapid incident response, and the exchange of best practices that can be used to enhance Latvia's cyber security governance.

DIRECTION 5 "PREVENTION AND COMBATING OF CYBERCRIME"

Objective of the direction: strengthened capabilities of the State Police and state security institutions by implementing new tools and fully utilizing existing ones to combat cybercrime.

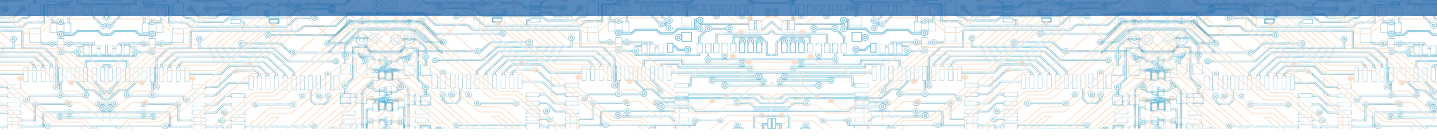
Tasks:

- *Develop the capabilities of the State Police and state security institutions to investigate cyber security incidents and enhance their operational capacities.*

- *Effectively implement existing tools for combating cybercrime in full and consolidate them.*
- *Introduce new tools for combating cybercrime, both for active engagement and preventive actions.*

The objective of the review period is to develop the capabilities of the State Police and state security institutions to investigate cybercrime incidents and strengthen their operational capabilities. According to the survey conducted by CERT.LV in 2021, more than 70% of surveyed Latvian citizens falsely believe that they are not at risk of cyber attacks. In reality, every Latvian citizen is exposed to such risks, as indicated by the statistics compiled by the State Police since 2017 on the losses suffered by individuals in various international online fraud schemes - with at least 1,500 victims defrauded of a total amount exceeding 14.5 million euros. This statistic only represents known cases, and the actual amount of incurred loss could be even higher as not all victims report to law enforcement agencies. Considering the aforementioned, it is important to promote public understanding of cyberspace and the risks of cybercrime in order to strengthen the resilience of Latvian society against cyber attacks, mitigate their impact, and promote prevention.

In the fight against cybercrime, it is necessary to strengthen and expand existing tools, as well as introduce new tools for cybercrime prevention. Attention should be paid not only to providing information that facilitates reporting of potential criminal activities, which can increase the activity of informants, but also to the prompt processing, sorting, targeted directing, and response to received information to ensure the most effective flow



of information. As the activity of informants increases, it will also be necessary to increase the resources of the State Police and security institutions. Therefore, it is crucial to attract and support qualified specialists, enhance knowledge, and promote international cooperation in cybercrime investigation and prevention, enabling the State Police to timely prevent, detect, and stop cybercrimes and hold the perpetrators accountable.

Special attention should be given to preventive methods and initiatives that allow for blocking websites used for criminal purposes or criminal activities, as well as the recognition and implementation of these initiatives, while also improving the collaboration among relevant institutions and the responsiveness of responsible authorities.

FINANCIAL IMPACT ASSESSMENT

The planned financial sources for the implementation of the strategy are the state and local government budgets. The implementation of the action plan tasks can involve financial resources from EU structural funds (European Regional Development Fund, European Social Fund, Cohesion Fund). It is also possible to attract funding for projects in the field of cybersecurity within the framework of EU financial instruments such as “Digital Europe” and “Horizon Europe” sub-programs. Private capital can also be attracted for financing the action directions specified in the Strategy, which can be achieved through the development of public-private partnerships and other solutions for attracting private capital. The implementation of the tasks outlined in the Strategy for the period 2023-2026²⁷ will be ensured within the framework of the state budget funds allocated to the responsible institutions mentioned in the strategy..

Table 1

Summary of allocated funding for the implementation of the action directions included in the Strategy within the budget framework of the Ministry of Defence (EUR) by year:*

Action direction	2023	2024	2025	2026 and beyond	Total
1 Enhancement of Cybersecurity Governance	4 031 872	5 210 269	5 611 654	5 611 654	20 465 449 ²⁸ (not exceeding)
2 Promotion of Cybersecurity and Strengthening Resilience ²⁹	0	0	0	0	0
3 Public Awareness, Education, and Research	0	0	0	0	0
4 International Cooperation and Rule of Law in Cyberspace	0	0	0	0	0
5 Prevention and Combating of Cybercrime	0	0	0	0	0
Total	4 031 872	5 210 269	5 611 654	5 611 654	20 465 449

* The amount of funding for several projects has also been identified, but the amount and distribution by years is restricted information, which is why it is not included in this report table.

²⁷ The question of providing additional state budget funding for the years 2024-2026 will be addressed within the process of preparing the draft law on the state budget for the respective year and the medium-term budget framework. This process will involve the consideration of priority measures proposed by all ministries and other central state institutions.

²⁸ The additional personnel costs related to the establishment of the National Cybersecurity Centre in accordance with the informative report of the Ministry of Defence “On Improving the National Cybersecurity Governance” (approved by the Minutes No. 30/4\$ of the Cabinet of Ministers meeting on 7 June 2022). The calculations do not include the costs associated with the setup, maintenance, and other related expenses of the workspaces of the Ministry of Defence and CERT.LV.

²⁹ The funding for the provision of personnel for the establishment of SOC in this action direction is currently included in the overall funding for the implementation of the direction “Strengthening Cybersecurity Governance.” Detailed costs for the establishment of the SOC will be calculated separately. The funding for the SOC project during the planning and initial implementation stage in the strategic action period from 2023 to 2026 will be provided within the budget allocated to the Ministry of Defence from the state budget.



EVALUATION OF STRATEGY IMPLEMENTATION

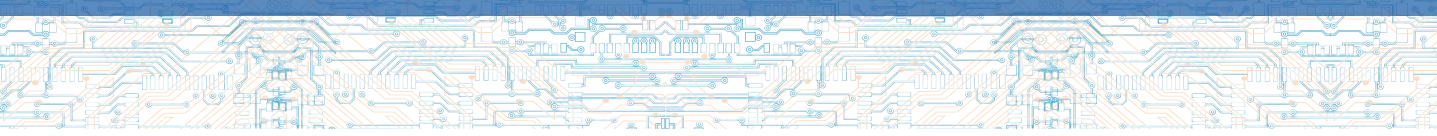
EVALUATION METHODOLOGY

In order to ensure the achievement of the goals and priorities set forth in the strategy, it is necessary to establish a regular mechanism for evaluating the implementation of the strategy. It is envisaged that twice a year, within the framework of the National IT Security Council, the current status of tasks will be reviewed, updates will be made, and solutions will be discussed if any obstacles to timely task completion are identified.

To determine the progress, the evaluation of the maturity level of cybersecurity will be taken into account, using the ENISA classification as a basis for self-assessment.

PROCEDURE FOR SUBMISSION OF REPORTS

The Ministry of Defence, in collaboration with all the relevant institutions and the National IT Security Council (NITSC), submits an informative report to the Cabinet of Ministers by May 1, 2026, on the evaluation of the implementation of the Strategy's tasks. The report includes proposals for future years in the field of cybersecurity policy.



CLOSING REMARK

The initial ex-ante impact assessment of the proposed solution has not been conducted, as cybersecurity is constantly and rapidly evolving. However, the action directions specified in the Strategy are a continuation of the priorities set forth in the National Security Concept and the actions that have been initiated thus far.

There are no policy planning documents that have been deemed obsolete.

