Cybersecurity strategy

2025 – 2028

Содржина

[Summary 5](#_Toc190335068)

[1. Introduction 7](#_Toc190335069)

[1.1. Basis for the preparation and proposal of the Cybersecurity Strategy 7](#_Toc190335070)

[1.2 Connection with other strategies in the field and related areas 7](#_Toc190335071)

[1.2.1 National Development Strategy (2024–2044) 7](#_Toc190335072)

[1.2.2. Програма за Националната развојна стратегија (НРС) 2024-2028 8](#_Toc190335073)

[1.2.3. Decision for Strategic Priorities of the Government (2024-2028) 9](#_Toc190335074)

[1.2.5. Smart Specialization Strategy of the Republic of North Macedonia (2024-2027) 10](#_Toc190335075)

[2. Methodology of the Cybersecurity strategy 10](#_Toc190335076)

[2.1. Description of the process for inclusion of stakeholders in the Strategy preparation process 11](#_Toc190335077)

[3. Analysis of the State of the Cybersecurity Sector 11](#_Toc190335078)

[3.1. Current state of the Cybersecurity in the Republic of North Macedonia 11](#_Toc190335079)

[3.1.1. Cybersecurity Governance 12](#_Toc190335080)

[3.1.2. Incident Response 12](#_Toc190335081)

[3.2. Strategic Deficiencies and Opportunities 13](#_Toc190335082)

[3.3. Recommendations 13](#_Toc190335083)

[4. Strategic Framework 14](#_Toc190335084)

[*4.2.* Priority Areas, General and Specific Objectives within Each Priority Area 14](#_Toc190335085)

[4.3. Summary of Policies and Key Actions for Achieving the General and Specific Goals 15](#_Toc190335086)

[5. Priority area 1: Strong National Capacities for Cybersecurity 16](#_Toc190335087)

[**5.1.** Specific Objective 1. Clear and Robust Cybersecurity Governance Structure 16](#_Toc190335088)

[5.1.1. National Security Council 16](#_Toc190335089)

[5.1.2. National Council for Digital Transformation of Society 17](#_Toc190335090)

[5.1.3. National Single Point of Contact 17](#_Toc190335091)

[5.1.4. Essential and Important Entities 17](#_Toc190335092)

[5.1.5. Computer Security Incidents Response Teams 18](#_Toc190335093)

[5.1.6. Competent Authorities 19](#_Toc190335094)

[5.1.7. Management of Large-Scale Incidents and Crises 19](#_Toc190335095)

[5.1.8. Building Professional Capacities for Cybersecurity 19](#_Toc190335096)

[5.1.9. Key Measures 20](#_Toc190335097)

[5.2. Specific Objective 2: Establishment of Cybersecurity Sector within the Ministry of Digital Transformation 20](#_Toc190335098)

[5.2.1. Key Measures 21](#_Toc190335099)

[5.3. Specific objective 3. Enhanced Capacities for Defensive Cyber Operations 22](#_Toc190335100)

[5.3.1. Key Measures 22](#_Toc190335101)

[6. Priority Area 2: Security and Resilience of Essential and Important Entities, Networks, and Information and Communication Systems 22](#_Toc190335102)

[6.1. Specific Objective 1. Risk and Threat Management and Monitoring 23](#_Toc190335103)

[6.1.1. Key Measures 24](#_Toc190335104)

[**6.2.** Specific Objective 2: Secure and Resilient Essential and Important Entities 24](#_Toc190335105)

[6.2.1. Key Measures: 25](#_Toc190335106)

[6.3. Specific Objective 3. Improved Security of National Networks and Information Systems 25](#_Toc190335107)

[6.3.1. Key Measures 25](#_Toc190335108)

[6.4. Specific Objective 4. Recommendations for the Use of Security Technology in Society 25](#_Toc190335109)

[6.4.1. Key Measures 26](#_Toc190335110)

[6.5. Specific Objective 5. Partnership and Cooperation between State and Private Capacities 26](#_Toc190335111)

[6.5.1. Key Measures 26](#_Toc190335112)

[7. Priority Area 3: Society Resilient to Cyber Threats 27](#_Toc190335113)

[7.1. Specific Objective 1. Increasing Awareness of Cybersecurity and Misinformation in Cyberspace 27](#_Toc190335114)

[7.1.1. Key Measures 27](#_Toc190335115)

[7.2. Specific Objective 2. Protection of Children and Youth on the Internet 28](#_Toc190335116)

[7.2.1. Key Measures: 29](#_Toc190335117)

[8. Priority Area 4: Minimizing the Impact of incidents in Cyberspace 29](#_Toc190335118)

[8.1. Specific Objective 1. Timely identification, reporting, and appropriate response to cyberattacks and significant incidents in cyberspace. 29](#_Toc190335119)

[8.1.1. Incident Identification 29](#_Toc190335120)

[8.1.2. Reporting Cyber Incidents and Cybercrime 29](#_Toc190335121)

[8.1.3. Response to Significant Incidents 30](#_Toc190335122)

[8.1.4. Key Measures 31](#_Toc190335123)

[8.2. Specific Objective 2. Timely and Appropriate Handling of Large-Scale Incidents and Crises 31](#_Toc190335124)

[8.2.1. Key Measures 32](#_Toc190335125)

[8.3. Specific Objective 3. Timely and Appropriate Handling of 32](#_Toc190335126)

[8.3.1. Key Measures 32](#_Toc190335127)

[9. Priority Area 5: National and International Cooperation 33](#_Toc190335128)

[9.1. Specific Objective 1. Cooperation in the Field od Cybersecurity at National, Regional and International levels 33](#_Toc190335129)

[9.1.1. Key Measures 34](#_Toc190335130)

[9.2. Specific Objective 2. Responsible behavior of the state and measures to build trust in cyberspace 34](#_Toc190335131)

[9.2.1. Key Measures 34](#_Toc190335132)

[10. Framework for monitoring, Evaluation and Reporting 34](#_Toc190335133)

[10.1. Performance Indicators for Monitoring Goal Achievement 34](#_Toc190335134)

[10.2. Implementation of the Cybersecurity Strategy 34](#_Toc190335135)

[10.3. Stakeholders 35](#_Toc190335136)

[11. Risk Management 36](#_Toc190335137)

[12. Action Plan 38](#_Toc190335138)

[13. Indicative Financial Plan 38](#_Toc190335139)

[Conclusion 38](#_Toc190335140)

[Annex 1 – List of High-Criticality Sectors 40](#_Toc190335141)

[Annex 2 – List of Other Critical Sectors 41](#_Toc190335142)

[Annex 3 – Definitions 42](#_Toc190335143)

[Annex 4 – Acronyms 46](#_Toc190335144)

[Annex 6 – List of Used Information and References 48](#_Toc190335145)

Summary

As part of the state's digital transformation process, the security of information systems (cybersecurity) is a key national priority for protecting the digital infrastructure and services utilized by citizens, government and public institutions, and the economy.

The rapid advancement of information and communication technologies, coupled with the uneven digitization of processes across various societal dimensions, significantly reshapes the cybersecurity landscape and increases the risk of cyberattacks and cyber incidents. A secure, resilient, and trustworthy digital transformation—both of processes and society as a whole—can only be achieved if it is built on solid foundations within a robust and resilient cyber ecosystem.

The **Cybersecurity Strategy 2025–2028** of the Republic of North Macedonia is a strategic document aimed at ensuring a secure, resilient, and reliable digital environment through a range of activities and measures. This strategy positions North Macedonia as a safe space for online activities and business operations, strengthened by advanced human and technical capacities. The core premise of the Cybersecurity Strategy is to establish conditions for a **coordinated national response** to cybersecurity challenges, as well as **the prevention of cyber incidents and attacks** through the development of a resilient digital infrastructure and human resources.

By achieving the strategic goals set forth in the Cybersecurity Strategy, North Macedonia seeks to safeguard and promote its national interests **within and through cyberspace**, foster greater economic growth, and enhance the prosperity of its citizens. In an era of **hybrid warfare**, a secure and resilient cyber environment plays a crucial role in **reinforcing national security capacities** and strengthening the overall national security framework.

The Cybersecurity Strategy 2025–2028 is based on the following fundamental principles:

• Cybersecurity is a shared responsibility;  
• Coordination, cooperation, and support at the national and international levels;  
• Cybersecurity by design;  
• Risk-based cybersecurity approach;  
• A holistic approach to cybersecurity as a driver of societal development.

The development methodology of the Cybersecurity Strategy is based on the ITU Guide for Developing a National Cybersecurity Strategy and the guidelines and tools provided by ENISA. The strategy builds upon the 2018–2022 national strategic document, aligning it with the evolving cybersecurity landscape and the challenges posed by increased digitization in the Republic of North Macedonia.

The Cybersecurity Strategy 2025–2028 will be implemented over four years, from 2025 to 2028, in accordance with the measures and tasks defined in the Action Plan, which is an integral component of the Cybersecurity Strategy 2025–2028. The Cybersecurity Strategy and the Action Plan define the roles of various cybersecurity stakeholders, enhanced cooperation between the public and private sectors, and the quality management of cybersecurity professionals at the national level.

As part of the Action Plan, an indicative budget is allocated for each activity within the framework of the Cybersecurity Strategy 2025–2028. Funding for the implementation and monitoring of the Cybersecurity Strategy 2025–2028 will be provided within the budget of the institution responsible for the activity, but where permitted, donor funds may also be utilized for support.

In the Action Plan, each activity specifies the responsible institution, involved stakeholders, implementation timeline, budget, as well as key performance and objective indicators. A list of involved stakeholders is provided in Section 9.3 of this document.

The implementation, monitoring, and evaluation of the Cybersecurity Strategy 2025–2028 fall under the jurisdiction of MDT. The implementation process will involve multiple stakeholders from the public and private sectors, academia and research communities, non-governmental organizations, and other actors who, through their activities, are directly or indirectly engaged in the cyber ecosystem.

The **Cybersecurity Strategy 2025–2028** of the Republic of North Macedonia is a strategic document aimed at ensuring a secure, resilient, and reliable digital environment through a range of activities and measures. This strategy positions North Macedonia as a safe space for online activities and business operations, strengthened by advanced human and technical capacities. The core premise of the Cybersecurity Strategy is to establish conditions for a **coordinated national response** to cybersecurity challenges, as well as **the prevention of cyber incidents and attacks** through the development of a resilient digital infrastructure and human resources.

By achieving the strategic goals set forth in the Cybersecurity Strategy, North Macedonia seeks to safeguard and promote its national interests **within and through cyberspace**, foster greater economic growth, and enhance the prosperity of its citizens. In an era of **hybrid warfare**, a secure and resilient cyber environment plays a crucial role in **reinforcing national security capacities** and strengthening the overall national security framework.

1. Introduction

In the digital age, cybersecurity is a fundamental pillar of national security, economic growth, and societal resilience. The Cybersecurity Strategy 2025–2028 reflects the commitment of the Government of the Republic of North Macedonia to build a secure and resilient digital environment as an integral part of the process of full digital transformation of society.

The Cybersecurity Strategy 2025–2028 is crucial for the digital transformation of the country. It ensures the security of networks and information systems, fostering trust in digital technologies and promoting innovation in the field of cybersecurity. The Cybersecurity Strategy 2025–2028 aims to protect critical ICT services, systems, and products, network and information infrastructure, ensuring continuity of essential services. It also protects the digital rights of citizens, contributing to a free and open digital society. The Cybersecurity Strategy 2025–2028 seeks to promote equality by including all user groups, especially vulnerable and at-risk groups, such as children, women, and other groups.

The Cybersecurity Strategy 2025–2028 not only contributes to the defense against cyber threats but also, through proactive preventive protection, works towards enabling a safe, resilient, and prosperous digital state, ready to embrace the opportunities and challenges that the digital age brings.

* 1. Basis for the preparation and proposal of the Cybersecurity Strategy

The basis for the adoption of the Cybersecurity Strategy 2025–2028 is not established in a separate act or document. The proposer of the draft planning document prepared a report presenting the need for the development and adoption of the strategy. This need arises from the National Cybersecurity Strategy 2018–2022, which was adopted by the Government of the Republic of North Macedonia at its 107th session held on 11.12.2018. The Cybersecurity Strategy 2025–2028 is proposed as a continuation of the Government of the Republic of North Macedonia’s commitment to cybersecurity. According to the Law on Amendments and Additions to the Law on the Organization and Operation of State Administration Bodies, Article 26-a, (Official Gazette of the Republic of North Macedonia, No. 121/24), the Ministry of Digital Transformation has responsibilities in the area of network and information systems security.

* 1. Connection with other strategies in the field and related areas

In the specific area of cybersecurity, no existing strategic planning documents have been identified, except for the National Cybersecurity Strategy 2018–2022.

* + 1. National Development Strategy (2024–2044)

The Cybersecurity Strategy 2025–2028 and the National Development Strategy (NDS) for 2024–2044 are closely linked through complementary goals for sustainable, secure, and resilient development of the Republic of North Macedonia. Both strategies share common principles of inclusiveness, sustainability, digital transformation, and resilience to modern threats. The alignment is expressed in several key aspects:

**•** **Security and resilience of society:** One of the key strategic areas in the NDS is “A Secure, Safe, and Resilient Society,” which includes the security of information systems and the protection of critical infrastructure, covered in the Cybersecurity Strategy 2025–2028. Both strategies emphasize risk management, improving system resilience, and strengthening national capacities to protect against cyber and hybrid threats.

• **Digital transformation and human capital**: The NDS defines digital transformation as a central component of development, while the Cybersecurity Strategy 2025–2028 lays the foundations for a secure digital environment that supports economic, educational, and administrative transformations. Staff training, the development of digital skills, and raising awareness of cybersecurity are common priorities in both strategies.

• **Rule of law and good governance**: The strategic area of the NDS “Rule of Law and Good Governance” expresses the need for effective cybersecurity management, which is a key element of the Cybersecurity Strategy 2025–2028 through the establishment of clear governance structures, such as the National Council for Digital Transformation of Society.

• **Social inclusion and protection**: The NDS emphasizes the importance of social inclusion, which is reflected in the Cybersecurity Strategy 2025–2028 through the protection of vulnerable groups, such as children and youth, through cybersecurity education and internet safety programs.

• **International cooperation and integration**: Both strategies highlight international cooperation as a critical factor. The NDS underscores the ambition for European integration and alignment with EU policies, while the Cybersecurity Strategy 2025–2028 stresses partnerships with the EU and NATO to address cyber threats.

The Cybersecurity Strategy 2025–2028 and the National Development Strategy are complementary documents that complement and synchronize to enable the transformation of the Republic of North Macedonia into a sustainable, digital, and secure state. The connection is reflected through the shared areas of action, such as resilience, digitalization, rule of law, and social inclusion, ensuring a coordinated approach to achieving the development and security goals of the state.

* + 1. Programme for National Development Strategy (NDS) 2024-2028

The Cybersecurity Strategy 2025–2028 is aligned with the Program for the National Development Strategy (NDS) 2024–2028 through shared goals for sustainable development, digital transformation, and strengthening national capacities. These two strategies share complementary goals in several key areas:

• Knowledge-based economy, innovation, and digitalization: The NDS, in Strategic Goal 1.1, defines economic growth based on digitalization and innovation, which is supported by the Cybersecurity Strategy 2025–2028 through the creation of a secure and safe digital infrastructure. Both strategies emphasize the development of startup ecosystems and entrepreneurship, which are essential for economic prosperity and security.

• Resilient critical infrastructure: The NDS Program highlights the importance of resilient capital infrastructure for a better quality of life. The Cybersecurity Strategy 2025–2028 supports this goal through measures to protect critical infrastructure from cyberattacks.

• Integration of digital technologies: The NDS lists digitalization as a central driver for effective governance and reducing inequalities. The Cybersecurity Strategy 2025–2028 supports this through initiatives to strengthen cybersecurity capacities and promote digital trust in both the public and private sectors.

• Improvement of human capital: The NDS emphasizes the development of a qualified workforce for the future labor market. The Cybersecurity Strategy 2025–2028 complements these goals through cybersecurity skills training, which is crucial for building a skilled workforce and improving employability.

• International cooperation and integration: Both strategies emphasize the importance of international cooperation to promote economic and security development. The NDS highlights integration into global economic chains, while the Cybersecurity Strategy 2025–2028 promotes partnerships with the EU and NATO to address cyber threats and incidents.

* + 1. Decision for Strategic Priorities of the Government (2024-2028)

The Cybersecurity Strategy 2025–2028 is aligned with the strategic priorities of the Government of the Republic of North Macedonia (2024-2028), in accordance with the Decision, with a particular focus on digitalization, innovation, security, and the rule of law. Through shared goals and activities, an integrated approach is ensured to strengthen digital and institutional resilience.

• Professional and efficient public administration, development of the digital economy, ICT sector, artificial intelligence, innovations, and startup ecosystem:

The connection through the goal "establishing a strategic, institutional, and legal framework to ensure a cybersecurity-safe society" serves as the foundation for the realization of the strategic priority for professional and efficient public administration, digital economy, and the ICT sector. The Cybersecurity Strategy 2025–2028 supports this goal by developing a clear institutional framework, including the formation of a Cybersecurity Sector within the Ministry of Digital Transformation, encouraging innovations and the use of artificial intelligence for managing cyber risks and data protection, and ensuring a secure foundation for the development of startup ecosystems through improving public-private partnerships for cybersecurity protection.

• Renewing trust in institutions, enhancing security, effective fight against corruption and crime, judicial independence, and ensuring the rule of law:

Connection: The Government of the Republic of North Macedonia’s strategic priority includes "strengthening cybersecurity and institutional resilience," with the goal of protecting critical infrastructure and boosting trust in public services. The Cybersecurity Strategy 2025–2028 addresses these aspects by enhancing the legal framework for cybersecurity to improve transparency and integrity, implementing risk management measures, and protecting critical sectors such as energy and healthcare, as well as fostering international cooperation to combat cybercrime and transnational threats.

* + 1. Cyber Hybrid Threats Resilience Strategy (2021–2025) (2021 – 2025)

The Hybrid Threats Resilience and Response Strategy (2021-2025) addresses modern threats that combine both military and non-military methods to achieve strategic goals by state and non-state actors. These threats include disinformation, cyberattacks, economic pressures, misuse of ideologies and culture, and manipulations through informational operations. The strategy focuses on six operational areas: politics, economy, defense and security sector, civil sector, information sector, and critical infrastructure. Each area identifies specific objectives, such as continuity of government services, energy and economic independence, and increased media literacy. To counter these threats, the strategy is based on an integrated approach combining national capacities, inter-sectoral coordination, and international cooperation, with a special emphasis on NATO and EU initiatives.  
Prevention of hybrid threats, as emphasized in the strategy, is based on three main pillars: early detection, reducing vulnerabilities, and building response and recovery capacities. Through disinformation detection systems, enhanced cybersecurity, and risk management, the state aims to reduce the potential impacts of hybrid threats on critical infrastructures and institutions. Additionally, the strategy encourages public education and media literacy to mitigate the effects of disinformation, as well as the development of legislative frameworks for protecting critical sectors. This prevention is supported by international partnerships with NATO and the EU, which provide resources for training, strategic communications, and information exchange.  
The Cybersecurity Strategy 2025-2028 and the Hybrid Threats Strategy (2021-2025) are complementary, as both recognize cyberattacks as a key tool of hybrid threats. Hybrid threats often target critical infrastructure through cyberspace, including highly critical sectors. The Cybersecurity Strategy 2025-2028 focuses on building a strong national cyber ecosystem by strengthening institutional capacities, improving incident response, and promoting public-private collaboration. On the other hand, the Hybrid Threats Strategy includes cyberspace as a key component in protecting critical national sectors, emphasizing the need for international cooperation with NATO and the EU to jointly tackle cyber and hybrid challenges.

* + 1. Smart Specialization Strategy of the Republic of North Macedonia (2024-2027)

The Cybersecurity Strategy 2025-2028 is complementary and aligned with the Smart Specialization Strategy (S3-MK) through shared priorities for digital transformation, innovation, and sustainable economic growth. These strategies share a vision for integrating cybersecurity as a foundation for the development of the innovation ecosystem, which is essential for supporting the critical priority domains defined in S3-MK.

• Digital Transformation and ICT Sector Development: S3-MK identifies digital transformation as crucial for the competitiveness of the economy and the development of the Information and Communication Technology (ICT) sector. The Cybersecurity Strategy 2025-2028 supports this vision by ensuring secure infrastructure for digital platforms and networks, which is necessary for the implementation of digitalization.

• Innovation and Research Capacities: S3-MK emphasizes the need to strengthen research and innovation capacities as a foundation for a knowledge-based economy. The Cybersecurity Strategy 2025-2028 supports this by developing innovative solutions for cyber risk protection and incorporating advanced technologies like artificial intelligence into the research ecosystem.

• Promoting Green and Digital Transition: S3-MK promotes the integration of green and digital transformation for sustainable development, including smart buildings, sustainable materials, and smart agriculture. The Cybersecurity Strategy 2025-2028 provides a security framework for digital technologies that form the basis for implementing green initiatives and the circular economy.

• Support for the Innovation Ecosystem and Startups: S3-MK highlights the need to create a startup ecosystem as a catalyst for economic growth. The Cybersecurity Strategy 2025-2028 supports startup development by promoting secure digital innovations and protecting intellectual property.

These strategies provide a foundation for the development of a knowledge-based economy, innovations, and secure digital systems, which are key to the sustainable growth and integration of the Republic of North Macedonia into the European and global market.

1. Methodology of the Cybersecurity strategy

The Cybersecurity Strategy 2025–2028 has been developed in accordance with the methodology outlined in the Guide to Developing a National Cybersecurity Strategy – developed by ITU[[1]](#endnote-1), while also taking into account the existing guidelines and tools for the development of national cybersecurity strategies provided by ENISA[[2]](#endnote-2).

The Cybersecurity Strategy 2025–2028 builds upon the experiences gained from the National Cybersecurity Strategy 2018–2022, including the Action Plan, proposed activities, and guidelines. It has been developed by an intersectoral working group under the leadership of the Ministry of Digital Transformation. The working group was established by Decision No. 08-503/1, dated 30.08.2024, and includes members from the following institutions: MDT, MIA, MFANT, MES, ARM, UGD Military Academy – Skopje, Agency for Electronic Communications, Agency for National Security, Agency for the Protection of Personal Data, Intelligence Agency, Directorate for Security of Classified Information, Operational-Technical Agency, State Audit Office, and UGD Štip. Through regular working meetings, the members of the working group actively contributed to the preparation of this document.

During the development of the Cybersecurity Strategy 2025–2028, consideration was also given to the Information on Standardizing the Sectoral Strategy Development Process, including the methodology for preparing, implementing, monitoring, reporting, and evaluating sectoral strategies[[3]](#endnote-3), developed by the Government of the Republic of North Macedonia, as well as the Roadmap for the Digital Transformation of Society[[4]](#endnote-4).

Additionally, the Cybersecurity Strategy 2025–2028 aims to align cybersecurity-related activities with European directives 2022/2555[[5]](#endnote-5) and 2022/2557[[6]](#endnote-6), as well as with EU Regulation 881/2019 – Cybersecurity Act[[7]](#endnote-7).

* 1. Description of the process for inclusion of stakeholders in the Strategy preparation process

The draft text of the planning document, along with the corresponding Action Plan, was published on the Electronic National Register of Regulations of the Republic of North Macedonia (ENER) on 15.10.2024. This was done to inform all relevant stakeholders and to allow for the submission of comments and opinions.

Additionally, after the 20-day period for submitting comments and opinions via ENER had elapsed, a public debate on the draft text of the planning document and the Action Plan was held in the Government of the Republic of North Macedonia on 01.11.2024. During this debate, participants had the opportunity to express their views and proposals.

1. Analysis of the State of the Cybersecurity Sector

The purpose of this analysis is to assess the current state of cybersecurity capacities in the country and to propose strategic solutions that align with EU standards and global best practices. The objective is to emphasize the importance of international cooperation, the legal framework, and capacity building as fundamental pillars for the development of a resilient cybersecurity ecosystem.

* 1. Current state of the Cybersecurity in the Republic of North Macedonia

The Republic of North Macedonia is facing a growing number of cyberattacks targeting critical sectors such as energy, finance, water supply, and healthcare. High-profile incidents, including the attack on the Ministry of Agriculture, Forestry, and Water Economy in 2022[[8]](#endnote-8), the Health Insurance Fund attack in 2023[[9]](#endnote-9), and the MEPSO attack this year[[10]](#endnote-10), have caused significant disruptions to public services, exposing vulnerabilities within these sectors.

Findings from the State Audit Office of the Republic of North Macedonia, published in the 2024 report on "Effectiveness of Measures Taken by Competent Authorities for the Protection of Critical Information Systems,"[[11]](#endnote-11) reveal significant deficiencies in cybersecurity measures for critical information systems. The audit determined that institutions lack an adequate legal framework to ensure full cybersecurity, as national legislation has not yet been aligned with the **EU NIS Directive** (2016) and NIS2 Directive (2023), which establish minimum cybersecurity standards.

Although a National Cybersecurity Strategy was in place until 2022, its implementation has not been fully realized. The report also highlights the limited activity of the National Cybersecurity Council, established in 2019. The audit found that since its creation, the Council had met only once by the time of the audit report. Additionally, the audit revealed that institutions lack sufficient technical and administrative capacities to protect against cyber incidents. A shortage of trained personnel and incident response teams, along with the absence of risk assessments, further increases the vulnerabilities of critical systems.

Despite a 41.68% increase in cybersecurity funding in 2023, institutions still struggle to implement the necessary protective measures, and the number of reported incidents remains low. The audit provides recommendations for urgent reforms, including:

* Aligning national legislation with EU directives
* Enhancing coordination among institutions and strengthening cybersecurity teams
* Continuous investment in training and capacity development

These measures are essential to mitigate potential cyber risks that could disrupt the functioning of key sectors such as energy, healthcare, and transportation.

* + 1. Cybersecurity Governance

Between 2019 and 2023, several initiatives were undertaken to introduce cybersecurity legislation, with the most recent attempt in 2023, when a draft Law on Network and Information Systems Security and Digital Transformation was published in September 2023. This document remains publicly available on the Electronic National Register of Regulations (ENER) [[12]](#endnote-12).

At the sectoral level, only the energy, banking, and public electronic communications networks and services sectors have a legal framework that defines measures and controls related to information or cybersecurity, along with supervisory mechanisms for ensuring compliance by operators in these sectors.

In December 2018, the Government of the Republic of North Macedonia adopted the first National Cybersecurity Strategy[[13]](#endnote-13), which covered the period 2018–2022. The country is now in its second year without a strategic document providing guidelines for improving resilience against cyberattacks and incidents.

The Ministry of Digital Transformation (hereinafter referred to as: MDT), as the successor to the former Ministry of Information Society and Administration (hereinafter referred to as: MISA), was established following amendments to the Law on the Organization and Operation of State Administrative Bodies[[14]](#endnote-14) (hereinafter referred to as: ZORODU), enacted on June 10, 2024, and published in the Official Gazette of the Republic of North Macedonia No. 121/24. According to these amendments, MISA was split into two ministries: Ministry of Digital Transformation (MDT) and Ministry of Public Administration (MPA).

Compared to the digitalization-related competencies previously held by MISA, the following new competencies have been introduced under MDT, which are either directly or indirectly related to both digitalization and cybersecurity:

* Technological development and technological culture
* Preparation of strategic documents in the field of digitalization
* Organization and implementation of digital skills training
* Network and information systems security
* Digitalization of public services
* Administration of the integrated population database and relevant civil registry records

Among these responsibilities, Security of network and information systems is an entirely new competency, whereas the others were either directly or indirectly part of MISA’s portfolio.

* + 1. Incident Response

The National Computer Incident Response Team (MKD-CIRT[[15]](#endnote-15)) is responsible for addressing incidents at the national level but faces resource limitations and needs strengthening to respond effectively to the growing range of threats. Despite several announcements regarding the establishment of additional CSIRT teams, there is currently no publicly available information on other operational teams at the sectoral or organizational level within the country.

National cybersecurity exercises, such as the National Cybersecurity Coordination Exercise 2023, revealed significant deficiencies in the capabilities for detecting and responding to cyber incidents. Coordination between sectors remains a critical aspect for improvement, along with the lack of resources and teams capable of providing fast, professional, and high-quality responses to cyber incidents or cyberattacks.

Although the national and sectoral cybersecurity legal frameworks are being developed in alignment with EU directives, their implementation and updating, particularly in relation to protecting critical infrastructure, digital services, and cybersecurity in the public sector, are still lacking.

* 1. Strategic Deficiencies and Opportunities

Key Deficiencies:

* Shortage of Skilled Workforce: The Republic of North Macedonia lacks enough trained cybersecurity professionals. Additionally, there is a shortage of formal and professional educational programs to develop this workforce.
* Coordination Issues at National Level and in Critical Sectors: Poor coordination between the public and private sectors, as well as with international organizations, presents a critical challenge.
* Insufficient Legal Provisions: The existing legal framework needs to be enhanced and updated to address contemporary cybersecurity challenges and ensure effective implementation.

Opportunities:

* Capacity Building: Through a coordinated internal approach and collaboration with international partners such as NATO and the EU, programs can be established to train and develop a qualified workforce.
* Public-Private Partnerships: Strengthening collaboration between the public and private sectors can significantly enhance and improve national cybersecurity.
* Improvement of the Legal Framework: With a modern legal framework based primarily on EU directives, including NIS2, and a strong commitment to its implementation, the country can build and continuously improve its cybersecurity and critical infrastructure protection.
  1. Recommendations

The following recommendations from this analysis are included in the goals, measures, and activities of the Cybersecurity Strategy 2025 - 2028:

* Analysis and Development of a National Plan and Program for a systemic approach to education, employment, retention, and development of cybersecurity personnel, with the aim of establishing a comprehensive educational framework. This framework will include cybersecurity curricula for primary, secondary, and higher education, incorporating international experiences from other countries. Additionally, an analysis of the need for skilled personnel and a plan for employment and development is required.
* Improvement of Incident Response Mechanisms. The goal is to build a network of incident response teams, which will be well-equipped and capable of responding to incidents and threats in a coordinated and efficient manner.
* Public Awareness Campaigns to improve cybersecurity hygiene in the country and educate the public on good cybersecurity practices.
* Strengthening the Legal Framework. The adoption of a legal solution dedicated to cybersecurity will define obligations for implementing and overseeing measures and controls for the protection of critical sectors and government services and systems. This legal solution will enable clear definition of roles and functions within the national cybersecurity framework.
* Encouraging International Cooperation to enable timely exchange of useful information regarding threats, risks, and incidents, as well as a coordinated international approach in responding to and handling cross-border incidents and attacks.

1. Strategic Framework

The strategic framework provides a structured approach to achieving the goals of the Cybersecurity Strategy 2025 - 2028, with a specific focus on certain goals or a set of goals. The strategic framework represents a comprehensive plan that outlines the vision, principles, strategic priorities, and objectives, as well as the activities that are part of the Cybersecurity Strategy 2025 - 2028. It identifies and describes the activities of all stakeholders, including organizations from both the public and private sectors, as well as operators (key and important entities) from high-criticality sectors and other critical sectors in the country, in their efforts to improve cybersecurity.

* 1. Vision

***„WE ARE CREATING A SECURE DIGITAL FUTURE THROUGH CYBERSECURITY THAT DRIVES THE PROCESS OF DIGITAL TRANSFORMATION IN THE REPUBLIC OF NORTH MACEDONIA!“***

* 1. Priority Areas, General and Specific Objectives within Each Priority Area

The key principles underlying the Cybersecurity Strategy 2025-2028 are:

1. **Cybersecurity is the responsibility of all**: Promote collective and individual responsibility for creating and maintaining a mature cybersecurity culture. Integration and coordination of cybersecurity efforts across the public and private sectors, with a comprehensive and coordinated approach to building cyber resilience. Establish, maintain, and upgrade ICT infrastructure resilient to cyber threats according to established standards.
2. **Collaboration and support at national and international levels**: Building and engaging in mutually beneficial activities between the public and private sectors, such as sharing information and lessons learned regarding cybersecurity, and improving protection against common threats. Promoting a cybersecurity culture among citizens, public and private sectors, focusing on understanding risks, cybersecurity hygiene, prevention, and response to threats. International cooperation and cybersecurity diplomacy, including exchanging best practices.
3. **Cybersecurity by design**: Provide guidance, management, and oversight to ensure that cybersecurity requirements are met in the planning, design, development, implementation, and management of information systems. Building and enhancing the necessary capacities for protection.
4. **Cybersecurity based on risk assessment**: Focus on identifying, prioritizing, and addressing the most critical threats based on their potential impact. Strengthening the country’s resources and capabilities for continuous risk assessment will ensure focused and efficient resource allocation for protection against cyberattacks and threats. Clear identification and definition of sources of threats to national interests in cybersecurity, prevention, and development of a clear response to cybercrime.
5. **Holistic approach to cybersecurity**: Apply an integrative and comprehensive method to protect information systems, networks, and data. This approach involves technologies, processes, and people to ensure full protection and maintenance of cybersecurity.

The five priority areas, general and specific objectives, whose fulfillment leads to the realization of the vision of the Cybersecurity Strategy 2025-2028, are as follows:

* **Priority Area 1: Strong National Cybersecurity Capabilities**
  + **General Objective**: Ensure a resilient and secure national cyberspace.
    - **Specific Objective 1**: Clear and robust cybersecurity governance structure
    - **Specific Objective 2**: Establishment of a Cybersecurity Sector in the MDT
    - **Specific Objective 3**: Enhanced defense capabilities in cyberspace
* **Priority Area 2: Security and Resilience of Critical and Essential Entities, Networks, and Information and Communication Systems**
  + **General Objective**: Ensure the security, confidentiality, and resilience of critical networks, information systems, and essential entities.
    - **Specific Objective 1**: Risk and threat management and monitoring
    - **Specific Objective 2**: Secure and resilient essential and critical entities
    - **Specific Objective 3**: Improved security of national networks and information systems
    - **Specific Objective 4**: Recommendations for the use of security technology in society
    - **Specific Objective 5**: Public-private sector partnership and collaboration
* **Priority Area 3: Cyber-Resilient Society**
  + **General Objective**: Create a cybersecurity-aware and resilient society.
    - **Specific Objective 1**: Raise awareness on cybersecurity and disinformation in cyberspace
    - **Specific Objective 2**: Protection of children and youth online
* **Priority Area 4: Minimizing the Impact of Cyber Incidents**
  + **General Objective**: Ensure timely and coordinated response to cyber incidents and crises.
    - **Specific Objective 1**: Timely identification, reporting, and appropriate response to cyberattacks and significant incidents
    - **Specific Objective 2**: Timely and appropriate handling of large-scale incidents and crises
    - **Specific Objective 3**: Timely and appropriate handling of cybercrime
* **Priority Area 5: National and International Cooperation**
  + **General Objective**: Strengthen national capacities and build trust in cyberspace.
    - **Specific Objective 1**: Cooperation in cybersecurity at national, regional, and international levels
    - **Specific Objective 2**: Responsible state behavior and measures to build trust in cyberspace
  1. Summary of Policies and Key Actions for Achieving the General and Specific Goals

The **Cybersecurity Strategy 2025-2028** of the Republic of North Macedonia sets five priority areas for building a resilient and secure cyberspace. The main political directions include strengthening national capacities through the formation of governance structures such as the Cybersecurity Sector and Incident Response Teams (CSIRTs); ensuring the security and resilience of critical infrastructure through risk management and public-private collaboration; improving awareness and education on cyber threats; minimizing the impact of cyber incidents through timely identification, coordinated response, and crisis management; and strengthening national and international cooperation with NATO, the EU, and other partners to promote confidentiality and protection in the digital space. These directions are implemented through measures such as developing a risk management framework, introducing early warning mechanisms, strengthening the legislative framework, and promoting a security culture in society.

1. Priority area 1: Strong National Capacities for Cybersecurity

**General Objective: Ensuring Resilient and Secure National Cyberspace**

In the process of dynamic digital transformation, of which the Macedonian digital ecosystem is a part, the existence of a comprehensive national framework that guarantees resilience against cyber threats is of paramount importance. This framework represents a set of interconnected rules, standards, institutions, functions, processes, and individuals organized to protect us from cyber threats, attacks, and incidents.

These structures and functions will operate in close cooperation with other entities in the country, including the government, public, private, and civil sectors, as well as the academic and research community. This united effort is crucial for the protection of sensitive data and the establishment of a secure digital environment.

The Government of the Republic of North Macedonia will develop a clear cybersecurity governance structure to enhance capabilities for prevention, detection, response, and recovery from cyber threats and incidents. The ultimate goal is to ensure that the country is equipped with the right policies and capabilities to improve cybersecurity at all government levels.

* 1. Specific Objective 1. Clear and Robust Cybersecurity Governance Structure

The Republic of North Macedonia is committed to establishing a robust national cybersecurity system through the development of the National Cybersecurity Governance Framework (NCGF). The Government of the Republic of North Macedonia plays a leading role in managing the country's cybersecurity, serving as the key driver in implementing cybersecurity measures and controls, as well as ensuring cooperation among stakeholders in the prevention, detection, response, and recovery from cyber incidents and attacks. To counter the growing cybersecurity threats, through the Cybersecurity Strategy 2025–2028 and its accompanying Action Plan, the Government of the Republic of North Macedonia pledges to invest in enhancing cyber resilience and fostering the growth of a secure digital environment.

The Cybersecurity Strategy 2025–2028 outlines the identification of operational organizational structures and functions, high-criticality sectors, and other key industries while also defining essential and important entities. Annex 6 provides a diagram of the organizational structure of entities and functions within the National Cybersecurity Governance Framework.

* + 1. National Security Council

The National Security Council of the Republic of North Macedonia plays a crucial role in overseeing the country's security, including cybersecurity. Security agencies provide the Council with critical intelligence, ensuring a well-informed decision-making process. Regarding cybersecurity, these agencies work closely together to identify threats, mitigate risks, and formulate strategic responses to cyber incidents.

Within the National Cybersecurity Governance Framework, the involvement of security agencies is essential for protecting critical infrastructure and ensuring a strategically coordinated approach to national resilience against emerging threats and cyberattacks. These agencies will actively participate in information sharing and incident response coordination for significant cyber incidents and crises, working in collaboration with relevant stakeholders, including the MDT and MKD-CIRT.

* + 1. National Council for Digital Transformation of Society

The Cybersecurity Strategy 2025–2028 proposes that the Government of the Republic of North Macedonia integrate the National Cybersecurity Council into the National Council for the Digital Transformation of Society (NCDTS). This integration aims to enhance coordination between the Government's activities related to cybersecurity and the digital transformation of society.

The NCDTS will collaborate with the MDT in defining new strategic directions and recommendations concerning cybersecurity, monitoring the implementation of the Cybersecurity Strategy 2025–2028, and providing expert opinions on programs and action plans for large-scale incident response and cyber crisis management.

* + 1. National Single Point of Contact

The National Single Point of Contact (SPOC) is a dedicated function responsible for coordinating cybersecurity matters and cross-border cooperation. The SPOC ensures effective international collaboration with relevant authorities in other countries, EU member states, the European Commission (EC), ENISA, and NATO. It also facilitates the exchange of notifications on significant and large-scale incidents with cross-border implications, ensuring seamless intersectoral cooperation with other competent authorities and stakeholders within the country[[16]](#endnote-16). MDT will assume the role of the National Single Point of Contact, ensuring timely access to critical information and notifications regarding reported incidents, threats, cyberattacks, and other cybersecurity-related events.

* + 1. Essential and Important Entities

For the definition of essential and important entities, the criteria set out in Article 2 of Directive (EU) 2022/2555[[17]](#endnote-17) are applied.

*Essential Entities*

Essential entities are those that fall within the categories listed in Annex I of the NIS2 Directive and exceed the upper limits for medium-sized enterprises, in accordance with Article 2 of Recommendation 2003/361/EC, and are identified as medium-sized entities under Article 470 of the Law on Trade Companies[[18]](#endnote-18). This category also includes Qualified trust service providers, Top-level domain name registries, DNS service providers, Operators of public electronic communications networks or publicly available electronic communication services that qualify as medium-sized enterprises, Public administration entities, any other entities identified as essential entities

Entities classified as critical under Directive (EU) 2022/2557 are also considered essential entities[[19]](#endnote-19).

*Important Entities*

Important entities are those that are not identified as essential entities but are listed in Annex I or II of the NIS2 Directive[[20]](#endnote-20)

*Obligations of Essential and Important Entities*

* Ensure the security of networks, information systems, and data used in their operations[[21]](#endnote-21).
* Adopt a broad range of fundamental cybersecurity measures and controls, including zero-trust principles, software updates, device configuration, network segmentation, data management and secure storage, identity and access management, and user awareness.
* Organize training for their personnel and raise awareness of cyber threats, phishing, and social engineering techniques[[22]](#endnote-22).
* Assess their own cybersecurity capabilities and, where appropriate, integrate cybersecurity-enhancing technologies, such as artificial intelligence (AI) or machine learning systems[[23]](#endnote-23).
* Evaluate and consider the overall quality and resilience of products and services, the built-in cybersecurity risk management measures, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures[[24]](#endnote-24).
* Be subject to administrative penalties in case of non-compliance or failure to implement the prescribed obligations[[25]](#endnote-25).
  + 1. Computer Security Incidents Response Teams

The state will ensure that CSIRT (Computer Security Incident Response Team) teams for responding to computer security incidents have the infrastructure for sharing and processing information, as well as a well-trained and trusted professional staff[[26]](#endnote-26).

CSIRT teams are responsible for monitoring and analyzing cyber threats, providing early warnings and sharing information, incident response, forensic analysis, risk assessment, and collaborating with other CSIRT teams at the national and international levels[[27]](#endnote-27).

The Government CSIRT will have activities related to the oversight and protection of the systems and services of the Government of the Republic of North Macedonia, as well as the response and coordination of dealing with incidents in these systems and networks and for public sector entities. The role of the Government CSIRT will be performed by the MDT.

The National CSIRT coordinates the work of sectoral CSIRTs. Since 2016, the role of the National CSIRT has been performed by the National Computer Incident Response Center MKD-CIRT, which operates as a separate organizational unit within the Agency for Electronic Communications.

Cooperation between the National CSIRT and sectoral, organizational, military, and other CSIRTs includes the exchange of information on cyber incidents and threats, national coordination, coordination of responses to international incidents, and establishing secure and efficient protocols for information exchange with CSIRTs both domestically and internationally[[28]](#endnote-28)

The National CSIRT will have activities related to the oversight and protection of systems and services for essential and important entities from high-criticality sectors where no sectoral authorities are assigned. These activities include incident reporting, response and coordination in dealing with incidents in these systems and networks, and the exchange of information and coordination with the Government CSIRT and relevant authorities from other high-criticality sectors.

The competencies and cooperation between the National CSIRT and Government CSIRT will be regulated by new cybersecurity legislation and by amendments and harmonization with existing EU and NATO legislation and best practices.

* + 1. Competent Authorities

Competent authorities are entities that have the powers for cybersecurity, including setting standards, measures, and controls, supervising compliance, and responding to incidents. They oversee critical and essential entities, conduct inspections and audits, issue guidelines, and cooperate to enhance cybersecurity resilience and coordinate incident responses. International cooperation is also important, especially when critical and essential entities provide services in other countries, as well as cooperation with data protection authorities[[29]](#endnote-29)

The national competent authority for cybersecurity in the country is the MDT. The establishment and operation of the National Competent Authority and sectoral competent authorities will be regulated by a new legal framework for cybersecurity and alignment with existing sectoral legal provisions, transposing the obligations and powers for competent authorities from Directive (EU) 2022/2555. When drafting the new legal framework for cybersecurity and determining the sectoral competent authorities, the maturity of critical sectors according to existing legal frameworks, established obligations, measures, and controls, as well as financial implications, will be considered to ensure continuity and progress of existing functions and cooperation. Identified sectoral competent authorities include the National Bank of the Republic of North Macedonia for the "Banking" sector, the Energy Regulatory Commission for the "Energy" sector, and the Agency for Electronic Communications for the sub-sectors "Providers of Public Electronic Communications Networks" and "Providers of Publicly Available Electronic Communications Services" within the "Digital Infrastructure" sector.

Sectoral competent authorities cooperate, exchange information, and coordinate their activities with the National Competent Authority (MDT) and forward reported incidents to MKD-CIRT.

* + 1. Management of Large-Scale Incidents and Crises

Coordination and handling of cyber crises and large-scale cybersecurity incidents are carried out by MDT and the Government CSIRT, through incident response in cooperation with the National CSIRT, the Crisis Management Center, the National Council for Digital Transformation of Society, the Ministry of Foreign Affairs, the Ministry of Defense, security structures, critical and essential entities, and other involved parties.

The competences of MDT will include adopting a framework policy for coordination and sharing information on risks and incidents, implementing and testing a Plan for Coordinated Response to Large-Scale Cross-Border Crises, and identifying and updating resources needed for a rapid and efficient crisis response. The management of large-scale incidents and crises will be regulated by the new legal framework for cybersecurity and through alignment with the existing legislation on crisis management.

* + 1. Building Professional Capacities for Cybersecurity

Building a skilled workforce for cybersecurity in the public sector is essential for protecting national infrastructure from growing cyber threats. The rapid digitization of critical services and the continuous evolution of cyberattacks require the state to undertake activities aimed at strengthening cybersecurity capacities. It is necessary to introduce or improve existing commitments for the continuous professional development of professionals, support for specialized training programs, and encourage collaboration with academic institutions.

* + 1. Key Measures

The key measures for achieving this goal will be:

* Creating a clear organizational structure for the cybersecurity framework of the Government of the Republic of North Macedonia.
* Establishing clear government policies for communication and cooperation, with defined roles and responsibilities related to cybersecurity.
* A new legal framework for cybersecurity that will define the National Cybersecurity Framework.
* Integration of the National Cybersecurity Council into the National Council for Digital Transformation.
* Formalizing existing working groups and establishing new ones related to cybersecurity protection, network and information system protection, and cybersecurity as the foundation for successful digital transformation.
* Developing specialized cybersecurity training and education programs for public sector employees.
* Strengthening public-private partnerships, cooperation with chambers of commerce, the public, civil, and private sectors, the academic and research communities, and knowledge sharing in cybersecurity.
* Practical workshops for public sector employees, focused on incident response and infrastructure protection.
* Specific career paths and career development programs for cybersecurity jobs in the public sector.
* Developing incentives for employees who retrain for cybersecurity jobs in the public sector.
* International cooperation for the development of cybersecurity talent.
* Framework policy for coordination and sharing information on risks and incidents.
* A plan for coordinated response to large-scale incidents and crises.
* Identifying and updating resources needed for a rapid and efficient crisis response.
  1. Specific Objective 2: Establishment of Cybersecurity Sector within the Ministry of Digital Transformation

To keep pace with current and future cyber threats, the Government of the Republic of North Macedonia will continuously enhance its technical and operational capabilities for detecting and responding to cybersecurity incidents. Operational units will be established within the Ministry of Digital Transformation (MDT), equipped with the necessary human, technical, and financial resources. These units will collaborate effectively with national bodies, the private sector, research communities, and international organizations[[30]](#endnote-30).

For this purpose, a **Cybersecurity Sector (CSS)** will be established within MDT, consisting of operational units at the departmental level. This sector will be responsible for security oversight of government networks, systems, and services, as well as the implementation of preventive and reactive measures in response to security incidents affecting them. The sector will provide on-site support for serious cybersecurity incidents in public sector institutions, detect and assess incidents affecting government networks, systems, and services, and strengthen the state’s strategic commitment to a secure cyber environment[[31]](#endnote-31).

The Cybersecurity Sector (CSS) at MDT will consolidate the following operational functions:

* National authority responsible for cybersecurity
* National Single Point of Contact (SPOC) for cybersecurity
* Government Computer Security Incident Response Team (Government CSIRT)
* National authority for coordination and management of large-scale cybersecurity incidents and crises
* Preparation of strategic documents and policies
* Monitoring the implementation of the Cybersecurity Strategy and Action Plan, as well as other strategic documents
* Analysis for strategic planning needs in the field of national cybersecurity
* Setting cybersecurity standards, measures, and controls for government networks, systems, services, and the public sector
* Supervision of security for government networks, systems, and services
* Compliance oversight of public sector institutions with prescribed cybersecurity standards, measures, and controls
* Collaboration with the National CSIRT and other government institutions and organizations in the country
* International cooperation and building strategic partnerships
* Cooperation with EU organizations and networks responsible for managing large-scale incidents and crises (EU-CyCLONe)

For the effective operation of the Cybersecurity Sector (CSS) at MDT, it is essential to ensure adequate human, technical, and financial resources. This will enable CSS to address the increasing demand for professional on-site support for government critical ICT systems and services, as well as public sector institutions[[32]](#endnote-32).

Through CSS, the strategic cybersecurity capacity of the Republic of North Macedonia will be strengthened, ensuring a positive impact on progress toward a secure cyber environment. This will enhance the state's ability to detect, respond to, and defend against malicious cyberattacks.[[33]](#endnote-33)

* + 1. Key Measures
* Establishing the Cybersecurity Sector (CSS) within MDT as the National Authority for Cybersecurity and Single Point of Contact (SPOC) for Cybersecurity.
* Setting up a Government Security Operations Center (SOC) to provide proactive monitoring and cybersecurity management for the networks, systems, and services of MDT and the Government of the Republic of North Macedonia.
* Enhancing international cooperation and building strategic partnerships to strengthen national cybersecurity capabilities.

Establishing a National Authority for Coordination and Management of Large-Scale Cybersecurity Incidents and Crises.

* Developing strategic documents and policies, as well as monitoring the implementation of the Cybersecurity Strategy, Action Plan, and other strategic frameworks.
* Defining cybersecurity standards, measures, and controls for government networks, systems, services, and the public sector.
* Supervising compliance of public sector institutions with prescribed cybersecurity standards, measures, and controls.
  1. Specific objective 3. Enhanced Capacities for Defensive Cyber Operations

To effectively address cyber risks, the Republic of North Macedonia will develop cyber defense capabilities in accordance with the highest standards, as an integral part of the National Cybersecurity Framework.

The development of cyber defense capacities within the Armed Forces is of strategic importance for the country’s overall national defense. The Armed Forces will establish a Military Computer Security Incident Response Team (Mil-CSIRT) and develop capabilities for deploying cyber operations to enhance national resilience and defense in cyberspace.

* + 1. Key Measures
* Enhancing military cyber operations capabilities through the development of a comprehensive strategy to improve the Armed Forces' cyber operations capacity.
* Establishing a military team for responding to computer security incidents.
* Developing cyber defense capabilities for national and military needs by creating a solid framework for deploying cyber defense capabilities to protect national security and military operations.

1. Priority Area 2: Security and Resilience of Essential and Important Entities, Networks, and Information and Communication Systems

**General Objective: Ensuring the Security, Confidentiality, and Resilience of Critical Networks, Information Systems, and Essential and Important Entities**

The availability, confidentiality, and integrity of data and services provided by essential and important entities contribute to the smooth functioning of society and the state. The public and private sectors, through the joint use of human, technical, and organizational resources, will work together to achieve the security and resilience of critical information infrastructure.

Protecting the networks and information systems of essential and important entities (critical infrastructure operators) and securing industrial control systems is of great importance, as these entities predominantly own the network and information infrastructure crucial to the state. Additionally, safeguarding ICT services and systems used by the Government of the Republic of North Macedonia, as well as the public and private sectors, is a key priority.

To achieve a secure and resilient network and information infrastructure and ensure data protection, it is necessary to implement regular security measures, focusing on prevention, detection, and incident response. This includes developing new security solutions, strengthening coordination, and appropriately adapting legal requirements.

* 1. Specific Objective 1. Risk and Threat Management and Monitoring

The identification and management of national cyber risks aim to prioritize and develop appropriate procedures for addressing them, with a particular focus on risks related to ICT equipment and service providers, as well as supply chain vulnerabilities.

Collaboration between the public and private sectors and highly critical sectors will lead to a better understanding, prioritization, and management of cyber risks and threats affecting one or more critical sectors.

A continuous risk assessment and mitigation approach will be introduced for the public sector and essential and important entities in the country, utilizing trained professionals and international cybersecurity risk management standards.

Support for the private sector in assessing and managing cyber risks will be provided through guidance based on international standards and educational training for legal entities.

A National Cybersecurity Risk Assessment Framework will be adopted and implemented across government institutions, the public sector, and essential and important entities.

A Register of Identified Critical Information Assets will be established, continuously updated, and assessed for vulnerabilities, threats, and risks related to ICT systems and networks in the public sector and among essential and important entities. These registries must be periodically updated in line with emerging vulnerabilities and threats.

Information sharing on vulnerabilities, threats, incidents, and risks will be enhanced through the National CSIRT Information Sharing Network and the National Cybersecurity Authority. To support this, a Vulnerability Management Policy will be implemented to promote and facilitate coordinated vulnerability disclosure [1].

Essential and important entities must adopt appropriate and proportionate technical, operational, and organizational measures to manage security risks associated with the networks and information systems they use for their operations or services. These measures should prevent or minimize the impact of incidents on service users and interconnected services. The security level of networks and information systems must be proportionate to the identified risks. The proportionality of these measures will be assessed based on an entity's exposure to risk, size, and the likelihood and severity of incidents, including their social and economic impact.

A Critical Supply Chain Security Risk Assessment Policy will be introduced to evaluate the security risks of specific critical ICT services, systems, or supply chains, considering both technical and non-technical risk factors. This assessment will align with evaluations conducted at the European Union level and by EU Member States.

The National Competent Authority, in collaboration with other relevant bodies, will define and regularly update operational and organizational risk management measures for essential and important entities. These entities will be required to implement the prescribed security measures for the networks and information systems they rely on.

Regulatory oversight will ensure compliance, with the National Competent Authority, in coordination with other relevant agencies, monitoring the implementation of risk assessment measures and controls.

Legislation will mandate that essential and important entities implement appropriate and proportionate cybersecurity measures to manage network and information system security risks effectively.

* + 1. Key Measures
* National Cybersecurity Risk Assessment Framework
* Operational and Organizational Measures for Managing Security Risks in Networks and Information Systems for Essential and Important Entities
* Supervision of Essential and Important Entities regarding the implementation of prescribed security measures, controls, and risk assessments
* Vulnerability Management, including the promotion and facilitation of coordinated vulnerability disclosure
  1. Specific Objective 2: Secure and Resilient Essential and Important Entities

The responsibility for ensuring the security of data, networks, and information systems, including IT (Information Technologies) and OT (Operational Technologies) systems, as well as control systems, largely falls on essential and important entities. The Cybersecurity Strategy 2025–2028 promotes a risk management culture, which includes risk assessments and the implementation of cybersecurity risk management measures that align with the threats we face. Establishing robust cybersecurity measures based on risk assessment in identified critical sectors is imperative. Furthermore, their implementation is recommended for public, private, and civil sectors[[34]](#endnote-34).

Collaboration between the public and private sectors, essential and important entities in early threat detection and information sharing is crucial for protecting critical infrastructure and ensuring a rapid response to cyber threats and incidents[[35]](#endnote-35). This cooperation and information exchange contribute to early detection of malicious activities, enabling a proactive approach and faster response to potential cyber threats[[36]](#endnote-36).

The establishment and development of Computer Security Incident Response Teams (CSIRTs) with national, governmental, and sectoral responsibilities within competent authorities, as well as the creation of Security Operations Centers (SOCs) within essential and important entities, is vital for building a comprehensive approach to resilience against threats and vulnerabilities[[37]](#endnote-37).

Operators categorized as essential and important entities in high-criticality sectors will receive support in protecting their infrastructure, contributing to the development of security measures to counter cyber threats and achieve resilience against attacks on information and communication systems[[38]](#endnote-38).

Essential and important entities will implement cybersecurity risk management policies and measures[[39]](#endnote-39), as part of the National Cybersecurity Risk Management Framework, following a Risk Assessment Methodology.

The identification of essential and important entities will be regulated by a new cybersecurity law and by aligning existing sectoral regulations, incorporating the obligations and responsibilities of competent authorities from Directive (EU) 2022/2555.

* + 1. Key Measures:
* Development and adoption of a National Cybersecurity Risk Management Framework with a Risk Assessment Methodology
* Enhancement of the resilience of essential and important entities
* Support for entities in handling cyber attacks and incidents
  1. Specific Objective 3. Improved Security of National Networks and Information Systems

Networks and information systems that are of national importance are those that provide services essential for maintaining critical societal and economic activities. A disruption to these systems would have a significant impact on public safety, public health, or the economy, and include sectors of high criticality.

It is necessary to establish an effective system for the protection and certification of national networks and information systems through which classified information is processed, for the continuous improvement of protection against cyber attacks and cyber espionage.  
At the national level, binding Minimum Technical and Organizational Cybersecurity Measures will be established for operators in high-criticality sectors. These will align with existing ISO and NIST standards, as well as the National Risk Management Framework for Cybersecurity, which will include national networks and information systems.

These measures will continuously be adapted in accordance with the current level of cyber threats and the rapid development of technology. A mandatory compliance check will be introduced for essential and important entities (operators) with the established Minimum Technical and Organizational Cybersecurity Measures.

* + 1. Key Measures
* Defining a minimum set of technological and organizational cybersecurity measures
* Support for implementation and oversight of compliance with the minimum set of technological and organizational cybersecurity measures
* Continuous improvement of the security accreditation for communication and information systems through which classified information is processed, in order to ensure the highest level of protection against cyber attacks and espionage.
  1. Specific Objective 4. Recommendations for the Use of Security Technology in Society

The Government of the Republic of North Macedonia is committed to creating a secure digital environment through strategic support and promotion of the use of digital security technologies, artificial intelligence, quantum technologies, and electronic communications. These technologies, when effectively implemented and managed, can provide significant protection from current and future cyber threats.

To achieve this, the Cybersecurity Strategy 2025-2028 envisions monitoring and supporting new security technologies, cooperation between the academic sector, the public sector, and CSIRT teams for effective security assessments. The Strategy introduces the promotion of certified technologies, particularly among essential and important entities using ICT products, services, and processes certified under European cybersecurity certification schemes, in accordance with Regulation (EU) 2019/881. Additionally, cybersecurity requirements will be included in public procurement, and registers of secure and high-risk technologies will be established.

* + 1. Key Measures
* Policy for the inclusion and specification of cybersecurity-related requirements for ICT solutions and ICT services in public procurement, including those related to cybersecurity certification, encryption, and the use of open-source cybersecurity products;
* Register of secure new technologies;
* Register of technologies that represent a high security risk;
* Permanent interdepartmental working group at the NSSD responsible for monitoring new technologies, assessing their security, and issuing recommendations for their use.
  1. Specific Objective 5. Partnership and Cooperation between State and Private Capacities

The Cybersecurity Strategy 2025-2028 emphasizes that public-private partnerships (PPPs), collaboration with business chambers, and outsourcing are key models for strengthening cybersecurity and building a resilient society. These forms of cooperation allow for the combination of resources, expertise, and innovations from various sectors, leading to a more efficient and rapid response to cyber threats.

PPPs play an important role by uniting the capacities of the Government of the Republic of North Macedonia and the private sector for the development of joint infrastructures and protection systems. On the other hand, outsourcing enables the use of external expertise and technical solutions, which can improve defense capabilities against cyberattacks. Cooperation with business chambers provides support to micro, small, and medium-sized enterprises, which are vital to the Macedonian economy, in developing cybersecurity strategies.

All of these forms of cooperation are essential for building a trustworthy and secure digital infrastructure that will protect society from growing cyber threats.

* + 1. Key Measures
* Multisectoral Working Group: Establishing a permanent working group led by the Ministry of Digital Transformation (MDT), which will unite the public and private sectors, business chambers, and outsourcing providers for the exchange of information and joint initiatives in cybersecurity.

1. Priority Area 3: Society Resilient to Cyber Threats

**General Objective: Creating an aware and resilient society.**

Digital transformation brings benefits but also security challenges that must be addressed with preparedness. The increased use of technology, along with the lack of awareness of risks in cyberspace, highlights the need for appropriate measures and procedures to ensure that society remains resilient to cyber risks. It is of utmost importance to foster a civic culture of resilience against cyber threats.  
This priority area includes the implementation of programs and activities in the education system to increase awareness and provide basic knowledge about cybersecurity. It is particularly important to implement appropriate programs and activities to raise cybersecurity awareness among employees in both the public and private sectors, as well as among the general population. The development and implementation of programs in higher education to educate and train cybersecurity professionals who will be capable of handling sophisticated and complex cyberattacks is of great importance for achieving this objective.

* 1. Specific Objective 1. Increasing Awareness of Cybersecurity and Misinformation in Cyberspace

Awareness of the risks in cyberspace for citizens, as well as for employees in the public and private sectors, is a fundamental prerequisite for more effective protection against cyberattacks and misinformation in cyberspace. The majority of users are either unaware of or do not properly practice basic security rules. By implementing the Plan to improve the overall level of cybersecurity awareness among citizens, a systemic approach to enhancing citizen protection will be ensured.  
Critical and important entities should adopt a broad range of basic cybersecurity hygiene practices, such as zero trust principles, timely software updates, device configuration, network segmentation, and identity and user access management. Entities should organize training for employees and raise awareness about cyber threats, phishing, and other social engineering techniques. Critical and important entities should continuously assess their own cybersecurity capabilities. Where appropriate, entities should continue integrating technologies to enhance cybersecurity, such as artificial intelligence or machine learning systems.  
Curricula in primary, secondary, and higher education should be upgraded and updated to raise awareness and provide education on cybersecurity, critical thinking, and protection against misinformation in cyberspace. Existing curricula should be improved and new programs developed across all study cycles at universities in the Republic of North Macedonia to fully meet the state's needs for educating and training cybersecurity professionals, as well as for participation in research projects and supporting research capacities and business innovations in this field.  
The establishment of a national institute and other institutes/centers for education and research in cybersecurity and digital forensics, aimed at educating, further educating, and training cybersecurity professionals at the government level, public administration, and other stakeholders requiring such education and training, is also crucial to fulfilling this objective.

* + 1. Key Measures
* Plan to improve the overall level of cybersecurity awareness, including at least the necessary measures;
* Plan to improve education in primary and secondary schools on critical thinking and protection against misinformation in cyberspace;
* Raising awareness and providing education on cybersecurity in primary and secondary education;
* Raising awareness and providing education on cybersecurity in higher education;
* Raising awareness and providing education on cybersecurity for employees in the public and private sectors;
* Mandatory cybersecurity training for all employees in the public sector;
* Continuously improving existing study programs at all levels of higher education related to cybersecurity, creating new programs and related activities for students in the field of cybersecurity;
* Raising awareness and providing education on cybersecurity for citizens;
* Coordination of activities for the development and implementation of programs for the education and training of cybersecurity professionals;
* Development and enhancement of the Institute for Cybersecurity and Digital Forensics;
* Development and enhancement of existing institutes/centers/laboratories for cybersecurity and digital forensics at relevant Macedonian universities;
* Continuous improvement of existing study programs at all levels of higher education related to cybersecurity, creating new programs and accompanying activities related to cybersecurity and students.
  1. Specific Objective 2. Protection of Children and Youth on the Internet

The Cybersecurity Strategy 2025 - 2028 includes a special focus on the protection of children and youth on the internet.

The Ministry of Digital Transformation (MDT), in collaboration with the Ministry of Social Policy, Demography and Youth (MSPDY), Ministry of Education and Science (MoES), Ministry of Internal Affairs (MoI), Ministry of Foreign Affairs and Foreign Trade (MFAFT), MKD CIRTs, and other stakeholders, will initiate the development of a Plan for the Protection of Children and Youth on the Internet.

The Republic of North Macedonia will exchange information and good practices with other countries through international initiatives and promote the implementation of international standards and frameworks for the protection of children on the internet in the country.

There will be improvements to the existing cybersecurity laws to include specific provisions for the protection of children from online abuse, harassment, and exploitation.

Partnerships will be established with technology companies and internet service providers to create tools that protect children from harmful content, cyberbullying, and sexual exploitation.

A center dedicated to the protection of children on the internet will be formed, bringing together experts from the public and private sectors, academia, and non-governmental organizations. This center will be responsible for monitoring online threats and providing advice and support to children and parents. The project for establishing the National Center for a Safer Internet, MKSafeNet, responds to the call “Accelerating the best use of technology (DIGITAL-2023-DEPLOY-04)” with support from national Safer Internet Centers in EU member states and associated members. The Republic of North Macedonia does not yet have a National Safer Internet Center (SIC). Through this project, basic infrastructure will be created to introduce a comprehensive SIC, enhancing existing initiatives from the public and private sectors. The goal is to improve services, ease access to appropriate content, and increase awareness of online risks and reporting opportunities. MKSafeNet focuses on strengthening national capacities to support children, youth, parents, and educators for a safer digital experience and providing support for victims of cyberbullying and vulnerable groups.

* + 1. Key Measures:
* Plan for the protection of children on the internet.
* Creation of clear legal mechanisms for reporting and monitoring online crimes against children.
* MDT initiative with internet service providers to promote filters for blocking harmful content for children.
* Promotion and introduction of parental control tools and safe internet browsing for younger users.
* National Safer Internet Center, MKSafeNet.

1. Priority Area 4: Minimizing the Impact of incidents in Cyberspace

**General Objective:** **Ensuring a timely and coordinated response to cyber incidents and crises.**

Cyberattacks and incidents occur daily with increasing intensity. To minimize the damage and provide support to the victims, measures for prevention, deterrence, identification, and mitigation of incidents must be taken. It is important to implement technical and organizational measures for risk management, as well as mandatory reporting of significant incidents. Improving coordination for incident management and providing support for the victims will enable effective handling of threats.

* 1. Specific Objective 1. Timely identification, reporting, and appropriate response to cyberattacks and significant incidents in cyberspace.
     1. Incident Identification

Incident identification related to cyberspace is critical for the protection of networks and information systems of national significance, especially those belonging to essential and important entities. These networks and systems are vital for maintaining national security and economic stability, making their protection from cyberattacks a priority.

Implementing continuous monitoring and surveillance of these systems is key for early detection of cyber incidents, such as malicious intrusions, DDoS attacks, or data breaches. Network sensors and Intrusion Detection Systems (IDS) play an important role in identifying suspicious activities, while cooperation with the national and government Computer Security Incident Response Teams (CSIRTs) will ensure a rapid response and coordination.

* + 1. Reporting Cyber Incidents and Cybercrime

Simplified reporting of cyber incidents and cybercrime, along with the expertise and capability of state bodies responsible for handling cyberattacks and incidents, will enable appropriate and timely support. This will help increase the number of reported incidents and improve visibility of ongoing cyber events facing the state. The reported information will be used for analyzing incidents, generating guidance for preventing future incidents, supporting computer crime investigations, and providing strategic information for the country.

An incident will be considered significant if:  
(a) it has caused or is capable of causing a serious operational disruption to services or financial losses for the affected legal entity; and  
(b) it has affected or is capable of affecting other individuals or legal entities, resulting in significant material or immaterial damage.

Identified essential and important entities (hereafter "entities") will be required to report significant incidents to the National CSIRT (MKD-CIRT), as well as to the sectoral and National competent authority if mandated by legal provisions.  
Public sector entities will report significant incidents to the Cybersecurity Sector at MDT (Government CSIRT). The Government CSIRT will promptly forward these reports to the National CSIRT. The Cybersecurity Sector at MDT will build response and assistance capabilities to handle these incidents.

Establishing a single point of contact for reporting cyber incidents and computer crime will enable even better cooperation between the National CSIRT, Government CSIRT, and the Ministry of Internal Affairs. The single point will be part of a system for collaboration, information exchange, support during response, and coordination in managing incidents. Cyber incidents often transition into cybercrime, and enhanced cooperation will allow the exchange of useful information between organizations for the effective and timely resolution of incidents and criminal cases.

The legal provision for cybersecurity, which will introduce and regulate mandatory reporting of incidents and attacks by essential and important entities, as well as attacks on critical ICT services, systems, and solutions, in the government and public sectors, will positively impact the cyberspace. This will lead to broader awareness and understanding of current attacks and risks.

National categorization and classification of cyber incidents and prioritization in their resolution, with specific roles and responsibilities for participants, will assist in timely and quality responses and coordination, ensuring the successful and efficient handling of cyber incidents and attacks.

* + 1. Response to Significant Incidents

In order to ensure timely identification and response to significant incidents, well-established, adequately equipped, staffed, and operational CSIRT teams and rapid response teams will contribute to a faster and more effective exchange of incident information and a prompt, quality response following an incident. These CSIRT teams will be responsible for the security of critical infrastructure in their respective sector, with a defined mandate, authorities, and collaboration with operators in the affected sector, as well as coordination with the National CSIRT and Government CSIRT.

A system for collaboration and information exchange, support during response, and coordination in managing incidents will be developed between the Government CSIRT, the National CSIRT team, sectoral and other CSIRT teams, competent authorities, and other relevant organizations within the country. This will ensure improved visibility of adverse events in cyberspace, coordination in handling incidents spanning multiple sectors, significant incidents, and cyberattacks of national importance. The system will be established by the National CSIRT in cooperation with the Government CSIRT and other relevant parties.

The implementation of mechanisms for detection and response to cyber incidents among entities will provide detailed and timely insight into the national situation and reduce the response time, action, and resolution of incidents.

Establishing a National Rapid Response Team for cyber incidents is of great importance for the country. In collaboration between MDT, sectoral competent authorities, the National CSIRT, Government CSIRT, and other CSIRT teams, a register of experts with specific high-specialized knowledge and skills will be created. These experts will be called upon and coordinated by MDT in cases of response to cyberattacks and incidents of major importance for the country. The register will also include hardware and software tools that are critical for a timely response to cyberattacks and incidents, facilitating the quick organization and effective coordination of responses to attacks and incidents.

* + 1. Key Measures
* Oversight of networks and information systems of essential and important entities by MKD-CIRT and Government CSIRT for government networks and systems.
* System for cooperation and information exchange, support in response, and coordination in handling incidents.
* Establishment of a single point of contact for reporting cyber incidents and cybercrime in cyberspace, and further cooperation between the National CSIRT, Government CSIRT, and the Cybercrime Sector of the Ministry of Internal Affairs, integrating into the system for cooperation and information exchange.
* National categorization and classification of cyber incidents and attacks, with prioritization in their resolution.
* Support for establishing well-equipped, staffed, and operational CSIRT teams at sectoral competent authorities, especially in high-criticality sectors and other critical sectors.
* Standardized operational procedures, rules, and obligations for cooperation and information exchange, support in response, and coordination in handling incidents among the National CSIRT team, Government CSIRT, other CSIRT teams, and other relevant parties.
* Detection and response mechanisms for cyberattacks and incidents in organizations – essential and important entities.
* Rapid response teams for cyberattacks and incidents of national significance.
* National Cyber Resource Register. 
  1. Specific Objective 2. Timely and Appropriate Handling of Large-Scale Incidents and Crises

The Cybersecurity Strategy 2025 - 2028 foresees the establishment of a National Framework for Cyber Crisis Management, through the identification of authorities responsible for coordination, response, and handling of cybersecurity crises. The framework includes the definition of necessary tools and resources for effective crisis management, as well as the measures to be implemented by the entities involved.

Regular review and practical testing of responses to large-scale incidents at both national and international levels, including political responses where needed and involving private sector entities[[40]](#endnote-40).

Effective response to large-scale cybersecurity incidents and crises at the international level requires swift and efficient cooperation among all relevant stakeholders. This relies on the preparedness and capabilities of individual countries, as well as coordinated joint actions[[41]](#endnote-41).

Timely and effective response to incidents depends on previously established and well-exercised procedures and cooperation mechanisms, which clearly define the roles and responsibilities of key actors at both national and international levels[[42]](#endnote-42).

The coordinated response plan applies to cybersecurity incidents that cause significant disruption to the point where the country cannot handle them alone or that affect two or more countries or international organizations. These incidents have significant technical or political impacts and demand timely coordination and response[[43]](#endnote-43).

The plan takes into account a set of guiding principles (proportionality, subsidiarity, complementarity, and confidentiality of information), presents the main goals of cooperation (effective response, shared situational awareness, public messaging) at three levels (strategic/political, operational, and technical), the mechanisms, the involved actors, and the activities to achieve the stated primary objectives[[44]](#endnote-44).

* + 1. Key Measures
* MDT as the Authority for Coordinating and Managing Large-Scale Incidents and Crises;
* A Coordinated Response Plan for Large-Scale Incidents and Crises, which will include procedures for crisis management.
  1. Specific Objective 3. Timely and Appropriate Handling of

Cybersecurity incidents often escalate into cybercrime, which has a significant impact on both the public and private sectors. In this context, the Ministry of Internal Affairs and the Sector for Computer Crime play a key role in managing and resolving these challenges. To effectively address these threats, the Cybersecurity Strategy 2025-2028 outlines enhanced collaboration with high-criticality sectors and relevant authorities, focusing on coordination and rapid response to cybercrime.

The establishment of a Permanent Working Group for Cooperation between the Ministry of Internal Affairs, the National CSIRT, and the Government CSIRT at the Ministry of Digital Transformation will accelerate the exchange of information and coordinated responses to cyber incidents and cybercrime. Moreover, creating a single point of contact for reporting cyber incidents and computer crime will facilitate effective communication and response with other stakeholders.

Collaboration with international organizations in the field of computer crime and security, such as Interpol and Europol, will provide important information and guidance on handling cybercrime. Additionally, public awareness campaigns on cybersecurity related to cybercrime will be conducted.

The development of a new Strategy for Cybercrime, with an emphasis on cooperation and coordination with various institutions and involvement in interinstitutional partnerships, is a key step in addressing these challenges. The goal of this strategy will be not only to detect and prevent serious forms of cybercrime but also to contribute to the protection of critical ICT infrastructure and systems in the country.  
The strategy also includes the establishment of international partnerships for monitoring and prosecuting online crimes against children.

* + 1. Key Measures
* Enhancing capabilities for handling cybercrime;
* Harmonizing national policies with international ones related to cybercrime;
* Establishing effective procedures for reporting and investigating cybercrime;
* Providing expert-specialist education and training for individuals working in the field of cybercrime identification and investigation;
* Implementing cybersecurity campaigns related to computer crime;
* Ongoing assessment of the relevance and effectiveness of national cybercrime regulations;
* Continuous education of judicial authorities in the areas of cybersecurity, cybercrime, and electronic evidence;
* New Strategy for Cybercrime;
* Conducting cybersecurity campaigns related to computer crime;
* International partnerships for monitoring and prosecuting online crimes against children.

1. Priority Area 5: National and International Cooperation

**General Objective: Strengthening national capacities and building trust in cyberspace.**

The state, through partnerships with the private sector and international allies, will enhance its resilience to cyberattacks and incidents. Inter-institutional cooperation and collaboration between the public and private sectors are fundamental prerequisites for building a society that will successfully address the challenges brought by digitalization.

International cooperation is one of the key segments in efforts to increase capacities for handling threats in cyberspace, especially in the areas of information exchange, experience, and best practices.

In the international dialogue, the Republic of North Macedonia advocates for the consistent implementation of open information exchange and freedom of expression, emphasizing non-discrimination. Agreements and standards related to international law are also applicable to the cyber domain.

Foreign policy instruments, such as diplomatic communication, warnings, and sanctions, can significantly contribute to limiting and mitigating the damage caused by cyberattacks and to their prevention and deterrence.

* 1. Specific Objective 1. Cooperation in the Field od Cybersecurity at National, Regional and International levels

The National Council for Digital Transformation of Society, through its working group for cybersecurity, as well as other working groups for cyber and information security, and the Critical Information Infrastructure Security Working Group (CICWG) led by MDT, are key to coordinating collaboration between the public and private sectors. The single point of contact will be responsible for communication and information exchange within the country, as well as for international cooperation in the field of cybersecurity.

The Republic of North Macedonia will continue to build bilateral and multilateral partnerships and be part of joint platforms at the regional and international levels to address cyber threats.

* + 1. Key Measures
* Cooperation within the frames of NATO and EU, the countries from the region, other countries and relevant international organizations;
  1. Specific Objective 2. Responsible behavior of the state and measures to build trust in cyberspace

Through a resolution, the United Nations General Assembly formed an open-ended working group (OEWG), in which all UN member states, including the Republic of North Macedonia, on December 31, 2020, adopted resolution 75/240 to establish an open working group on the security and use of information and communication technologies with a mandate of five years (2021-2025). In line with the EU and its member states, the Republic of North Macedonia aligned with the comments and proposals shared by member countries and gave its consent for the adoption of the final version of the General Assembly resolution on the annual progress report.

The Republic of North Macedonia will strive to fulfill the main points adopted in this assembly. In this context, the Republic of North Macedonia also remains committed to implementing the 16 Confidence-Building Measures of the OSCE, aimed at reducing the risk of conflict arising from the use of information and communication technologies.

* + 1. Key Measures
* Promoting norms, rules, and principles of responsible state behavior, in accordance with internationally established principles.
* Protecting national interests through participation in the definition of international legal acts related to behavior in cyberspace, freedom of expression, personal data protection, privacy rights, and fundamental human rights and freedoms.

1. Framework for monitoring, Evaluation and Reporting
   1. Performance Indicators for Monitoring Goal Achievement

The framework for monitoring the achievement of the objectives of the Cybersecurity Strategy 2025–2028 is based on Key Performance Indicators (KPIs) and Key Goal Indicators (KGIs) defined at the level of objectives, measures, and tasks outlined in the Cybersecurity Strategy 2025–2028 and the Action Plan.

* 1. Implementation of the Cybersecurity Strategy

The Cybersecurity Strategy 2025–2028 will be implemented over four years, from 2025 to 2028, in accordance with the objectives, measures, and activities detailed in the Action Plan.

The Ministry of Digital Transformation (MDT) is responsible for monitoring and reporting on the implementation process of the Cybersecurity Strategy 2025–2028. MDT will oversee the overall execution of the Strategy.

The monitoring process will involve collecting data on the progress of activity implementation and identifying potential risks arising from uncompleted activities or unachieved results. All stakeholders participating in the activities outlined in the Strategy will contribute to this process.

MDT will submit semi-annual and annual reports to the Government of the Republic of North Macedonia, detailing the implementation progress of the Action Plan of the Cybersecurity Strategy 2025–2028. These reports will be published on the MDT website.

MDT, through a working group composed of representatives from relevant stakeholders, will conduct an annual review of the Cybersecurity Strategy 2025–2028 and its Action Plan. This review will assess the implementation status of planned activities and update the Strategy, Action Plan, and accompanying documents in accordance with the Methodology for Reporting and Evaluating Sectoral Strategies and the Guidelines for Structuring, Content, and Preparation, Implementation, Monitoring, Reporting, and Evaluation of Sectoral and Multisectoral Strategies. Additionally, the Action Plan will be updated following Article 43 of these Guidelines. The review process will align with obligations derived from current cybersecurity developments and proposals from working group members.

This approach will provide a clear overview of the implementation progress concerning the 2025 - 2028 Cybersecurity Strategy’s objectives and ensure the validation of plans and activities for its continued execution.

* 1. Stakeholders

As the lead implementing body of the Cybersecurity Strategy 2025–2028, the Ministry of Digital Transformation (MDT) will collaborate with the Government of the Republic of North Macedonia, the Council for Digital Transformation of Society, and all relevant stakeholders involved in the Strategy’s implementation. This collaboration aims to ensure the efficient and timely execution of the activities outlined in the Action Plan of the Cybersecurity Strategy 2025–2028.

Since cybersecurity is a shared responsibility, the engagement of MDT, the Government of the Republic of North Macedonia, and state institutions will be complemented by significant contributions from the private sector, donors, academia, research organizations, the non-governmental sector, and other stakeholders. Their involvement will be crucial in achieving the objectives of the Cybersecurity Strategy 2025–2028.

Below is a list of authorities and stakeholders participating in the implementation of the Cybersecurity Strategy 2025–2028:

* National Security Council
* Government of the Republic of North Macedonia
* National Council for Digital Transformation of Society
* National ICT Council
* Ministry of Digital Transformation
* Ministry of Internal Affairs
* Ministry of Defense
* Ministry of Justice
* Ministry of Foreign Affairs and Foreign Trade
* Ministry of Education and Science

Ministry of Energy, Mineral Resources, and Mining

* Ministry of Finance
* Ministry of Transport
* Ministry of Public Administration
* Ministry of Labor and Social Policy
* Army of the Republic of North Macedonia
* Bureau for Educational Development
* Universities:
* Ss. Cyril and Methodius University – Skopje
* St. Clement of Ohrid University – Bitola
* Goce Delchev University – Shtip
* State University of Tetovo
* University for Information Science and Technology "St. Paul the Apostle" – Ohrid
* Mother Teresa University – Skopje
* South East European University – Tetovo
* Agency for Electronic Communications, National Computer Incident Response Center, MKD-CIRT
* Crisis Management Center
* Personal Data Protection Agency
* National Security Agency
* Directorate for Security of Classified Information
* Intelligence Agency
* Academy for Judges and Public Prosecutors
* Ministry of Local Self-Government

1. Risk Management

This chapter identifies the key risks at the highest level. It is recommended that, during the implementation of each specific activity under the Cybersecurity Strategy 2025–2028, the responsible entity maintains a dedicated risk register. This will enable the anticipation of steps to mitigate individual risks and based on the probability of occurrence and the impact on the implementation of the respective activity, appropriate actions and financial resources will be planned to minimize the effect of those risks.

**Risk 1: Lack of Support for the Implementation of the Cybersecurity Strategy 2025–2028**

The absence of political support from all stakeholders and relevant actors in the process of fully establishing cybersecurity management structures in the country, as envisaged in the Cybersecurity Strategy 2025–2028, is a critical risk to fulfilling the commitments of the Strategy.  
To mitigate this risk, full political support and strong coordination among all actors in the process of creating and establishing cybersecurity management structures are necessary. These structures are the foundation for achieving the strategic objectives, particularly in establishing a robust and secure cyber environment that is resilient to cyber risks and capable of effectively responding to potential cyberattacks.

**Risk 2: Lack of Financial Resources**

Given the current state of the country and the budgets available to state institutions, there is a real risk of insufficient budgetary resources for implementing the Cybersecurity Strategy 2025–2028.  
To address this risk, regular prioritization of activities will be conducted, and, if necessary, reallocation of planned budgetary funds will be made to implement the highest-priority measures and tasks. Additionally, where applicable, efforts will be made to seek additional donor support for the realization of these tasks.

**Risk 3: Shortage of Human Resources and Cybersecurity Experts**

The shortage of qualified and professional ICT personnel, particularly cybersecurity professionals, is increasingly pronounced not only in the country but also across the region and beyond. This presents a significant risk to achieving certain objectives of the Cybersecurity Strategy 2025–2028.  
To mitigate this risk, the Government of the Republic of North Macedonia will work on finding modalities to attract and retain cybersecurity professionals while simultaneously fostering an increased level of innovation activities among businesses. Additionally, as an important objective of the Cybersecurity Strategy 2025–2028, the Government and state institutions will focus on training, specialization, and retraining of existing human resources to enhance their professional capabilities for working in the field of cybersecurity.

**Risk 4: Global Crises and Natural Disasters**

Global economic, security, and health crises, as well as natural disasters (earthquakes, floods, wildfires), pose a risk that, if they occur, could have a significant impact and a negative effect on achieving the objectives of the Cybersecurity Strategy 2025–2028.  
Since global crises and natural disasters are difficult to predict and even harder to control, it is essential for the Government of the Republic of North Macedonia to implement preventive measures that will facilitate crisis management should such incidents occur. This includes well-defined operational procedures for handling large-scale crises and incidents, ensuring business continuity, and training personnel to operate effectively in crisis situations.

**Template No. 4, RISK IDENTIFICATION**

|  |  |  |  |
| --- | --- | --- | --- |
| **RISK** | **PROBABILITY OF RISK OCCURRENCE** | **IMPACT OF THE RISK ON ACHIEVING THE OBJECTIVES** | **MEASURES TO HANDLE THE RISK** |
| Lack of support for the implementation of the Cybersecurity Strategy 2025 - 2028 | Middle | Large | -Ensuring full political support from all relevant stakeholders.  -Good coordination of institutions.  -Strengthening the cybersecurity management structures. |
| Lack of financial resources | Large | Large | -Motivating and retaining cybersecurity professionals.  -Training, specialization, and reskilling of personnel.  -Promoting innovation in the business sector. |
| Shortage of Human Resources and Cybersecurity Experts | large | Large | -Motivating and retaining cybersecurity professionals.  -Training, specialization, and reskilling of personnel.  -Encouraging innovation in the business sector. |
| Global Crises and Natural Disasters | Middle | Middle | -Developing procedures for crisis management.  -Ensuring continuity of operations.  -Training personnel to work in crisis situations. |

1. Action Plan

The Action Plan is provided in the Appendix - Form No. 3 Action Plan for the Implementation of the Cybersecurity Strategy 2025 - 2028.

1. Indicative Financial Plan

The financial resources for the implementation of all activities included in the Action Plan of the Cybersecurity Strategy 2025 - 2028 will be planned accordingly with indicative budgets and will be provided from the budget of the activity holder specified in the Action Plan.

Potential future crisis measures and risks of budget cuts for certain activities included in the Action Plan, the nature of which allows for this, may require donor support to supplement government funds.

Conclusion

Before you is the strategic document, the Cybersecurity Strategy 2025 - 2028, developed with great dedication by the working group, formed by experts from all relevant parties, led by the Ministry of Digital Transformation (MDT).

The successful implementation of the Cybersecurity Strategy 2025 - 2028 and the Action Plan will have a positive impact on increased cybersecurity, thus further contributing to the overall security of the country.

By adopting the Cybersecurity Strategy 2025 - 2028, the Government of the Republic of North Macedonia and the relevant stakeholders commit to ensuring financial resources and necessary support for achieving the objectives, measures, and tasks outlined in the Strategy, thereby contributing to improving resilience in the cyber domain in the Republic of North Macedonia, with the ultimate goal of making the Republic of North Macedonia a secure and trusted digital environment for online activities and operations.

Annex 1 – List of High-Criticality Sectors

At the time of adoption of this document, the Republic of North Macedonia does not have a valid law identifying critical sectors in the country. For this reason, the List of Other Critical Sectors is in accordance with Annex 2 of the European Directive (EU) 2022/2555.

|  |  |
| --- | --- |
| Sector | Subsector |
| Energy | (a) Electricity |
|  | (b) District Heating and Cooling |
|  | (c) Oil |
|  | (d) Gas |
|  | (e) Hydrogen |
| Transport | (a) Air |
|  | (b) Railway |
|  | (c) Water |
|  | (d) Road |
| Banking |  |
| Financial Market Infrastructures |  |
| Health |  |
| Drinking Water |  |
| Wastewater |  |
| Digital Infrastructure |  |
| ICT Services Management |  |
| Public Sector (Public Administration) | Central government institutions |
|  | Local government institutions |
| Space |  |

Annex 2 – List of Other Critical Sectors

The Republic of North Macedonia does not have a valid law that identifies critical sectors in the country. For this reason, the List of Other Critical Sectors is in accordance with Annex 2 of the European Directive (EU) 2022/2555.

|  |  |
| --- | --- |
| Sector | Subsector |
| Postal and courier services |  |
| Waste management |  |
| Manufacturing, production, and distribution of chemicals |  |
| Production, processing, and distribution of food |  |
| Manufacturing | (a) Production of medical devices and in vitro diagnostic medical devices |
|  | (b) Production of computer, electronic, and optical products |
|  | (c) Production of electrical equipment |
|  | (d) Production of machinery and equipment |
|  | (e) Production of motor vehicles, trailers, and semi-trailers |
|  | (f) Production of other transportation equipment |
| Providers of digital services |  |
| Research |  |

Annex 3 – Definitions

**Academy** refers to an educational or research institution, university, or other professional entity playing a key role in the education, training, and development of human resources in the field of cybersecurity. The academy acts as a partner in developing expert personnel, conducting scientific research, and promoting awareness and knowledge of cybersecurity within society.

**Outsourcing** is the practice of transferring certain functions or services to external organizations to increase efficiency, reduce costs, and improve service quality, allowing the organization to focus on its core activities.

**Civil sector** refers to the part of society comprised of organizations and initiatives not part of governmental institutions or the private sector. This sector includes non-governmental organizations (NGOs), civil society associations, foundations, activist groups, and other collectives working to address social issues, promote human rights, protect the environment, engage in cultural activities, and pursue similar goals.

**Digitalization** is the process of converting physical information, documents, or processes into digital format. This transformation enables data to be easily accessible, transferable, and processable through computer systems.

**Digital infrastructure** refers to the essential technological components and resources required to support and operate digital systems and services. This includes network infrastructure (such as the internet and local area networks), servers, cloud services, software applications, databases, and hardware devices.

**Digital environment** refers to the virtual space created by computer systems, the internet, and digital technologies, where communication occurs, information is exchanged, and various activities are performed. This environment includes websites, social networks, online platforms, applications, and digital devices.

**Digital transformation** is the process of integrating digital technologies into all areas of business operations through a digital business model.

**Digital rights** are rights and freedoms related to the use of digital technologies and the internet, including the right to privacy, freedom of expression, access to information, and security, in order to protect individual interests and freedoms in the digital environment.

**Malware (malicious software)** refers to software specifically designed to disrupt, damage, or gain unauthorized access to information systems.

**Industrial control systems** are information systems in SCADA (Supervisory Control and Data Acquisition) and distributed control systems, used for industrial operations such as manufacturing, production control, and distribution management through programmable logic controllers, which differ from conventional information technologies.

**Incident** refers to an event that occurs, often unpleasant or unexpected, which may lead to problems or disrupt the normal course of activities.

**Internet** is a global computer network that provides connectivity for information and communication devices and systems through standardized communication protocols.

**Internet Service Providers (ISPs)** are companies or organizations that offer internet access services, enabling users to connect to the global network. They may provide various types of services, including broadband internet, mobile internet, Virtual Private Networks (VPNs), and hosting services.

**Information Security** refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.

**Information and Communication Technologies (ICT)** are technologies that enable the collection, processing, storage, and transmission of information, including computers, the internet, software, and communication tools, playing a key role in modern society for supporting communication and data management.

**Classified Information** refers to information within the scope of the work of a state or local government authority, established according to the Constitution of the Republic of North Macedonia and by law, a legal entity established by the Republic or municipalities, the city of Skopje, and municipalities in the city of Skopje, or other legal entities related to public safety, defense, foreign affairs, or security or intelligence activities of the state, which, according to the law, must be protected from unauthorized access and is marked with an appropriate classification level according to the Law on Classified Information ("Official Gazette of RSM", No. 275/19).

**Critical Information Infrastructure (CII)** refers to any information and communication systems whose maintenance, security, and protection are critical to national security, the economy, public safety, and health. The national critical information infrastructure is part of critical infrastructure (CI).

**Personal Data** refers to any information that relates to an identified or identifiable natural person (data subject), while an identifiable natural person is one whose identity can be determined, directly or indirectly.

**National Security** is a system for the modern organization and functioning of society for implementing specific activities and preventive and repressive measures to protect fundamental societal values from all types and forms of security challenges, threats, and risks at all levels.

**National Networks and Information Systems** are structures and platforms that facilitate the exchange of information and communication between various government institutions and agencies, as well as between state authorities and citizens. These networks and systems include infrastructure for computer networks, software solutions for data management, and systems for securing information. Their main objective is to improve the efficiency of public administration, increase transparency and accountability, and facilitate citizens' access to public services.

**Competent Authorities** are government bodies, other state bodies, agencies within ministries, administrative organizations, and independent bodies, judicial authorities and courts, municipal authorities, the City of Skopje, and municipalities within the city of Skopje, as well as legal and other entities entrusted by law with exercising public powers. In this context, the term "other entities" refers to legal persons that provide and ensure public interest services, including entities in the fields of education, healthcare, finance, banking, insurance, energy, water supply, electronic communications, postal services, and public utilities.

**Competent Authorities (in the context of the Cybersecurity Strategy 2025-2028 and in accordance with NIS2)** are institutions designated by the EU Member States to implement network and information systems security measures in line with the Directive on Network and Information Systems Security (NIS2). They are tasked with ensuring compliance with legislation, monitoring and assessing security risks, conducting inspections, and coordinating responses to cybersecurity incidents in order to protect infrastructure and data from threats and attacks.

**Government Authorities** are institutions established by law to perform functions of executive power, administrative and professional work. These may include ministries or other bodies divided into independent (directorates, archives, agencies, commissions) and bodies within ministries (offices, bureaus, services, inspectorates, captaincies).

**Private Sector** refers to the part of the economy consisting of organizations and companies that are owned by individuals or legal entities, not the state. This sector focuses on generating profit through manufacturing and service activities, and includes small, medium, and large businesses.

**Robustness** refers to the property of a system, organization, or process to be resistant to disruptions, to function stably under changing conditions, and to recover from unforeseen situations. Robust systems are capable of maintaining their efficiency and functionality even when faced with challenges or risks.

**Awareness** refers to security awareness among all individuals responsible for information security.

**Cybersecurity** is the practice of protecting networks, devices, and data from unauthorized access or criminal use, ensuring the confidentiality, integrity, and availability of information. The term "cybersecurity" is sometimes also referred to as "cyber security."

**Cyberbullying** is a form of harassment that takes place via digital platforms such as social media, text messages, emails, and other online channels. This type of bullying can involve sending threatening or offensive messages, spreading false information, posting embarrassing photos, or creating fake profiles.

**Cyber Ecosystem** is a complex system that includes various elements such as technology, infrastructure, users, regulatory bodies, and services, all of which operate together in the digital environment. The goal of the cyber ecosystem is to provide a secure, efficient, and inclusive digital environment where individuals and organizations can communicate and exchange information safely and confidentially.

**Cyber Threat** is the potential cause of an incident in cyberspace that could cause harm to an institution or system.

**Cyber Incident** is an event that threatens the availability, integrity, or confidentiality of information or information and communication technology (ICT) systems.

**Large-Scale Cyber Incident** is a cyber incident that causes a level of disruption exceeding a country's capacity to respond or that has significant impact in at least one other country.

**Cyber Crisis** refers to an event or series of events in cyberspace that could cause or have already caused significant disruption to the social, political, and economic life of the Republic of North Macedonia. Such a situation may affect citizens' security, the democratic system, political stability, the economy, the environment, and other national values, including national security and defense.

**Cybercrime** includes various criminal activities where information systems are involved either as the primary tool or as the primary target of the attack.

**Cyberattack** refers to operations deliberately carried out by individuals and/or information systems anywhere in cyberspace to compromise the confidentiality, integrity, or availability of information systems within the national cyber space.

**Cyber Defense** is a proactive measure to detect or obtain information related to a cyber intrusion, cyber attack, or cyber operation, or to determine the origin of an operation that involves preventive or cyber counter operations against the source.

**Cyber Resilience** refers to the ability to prepare for, adapt to, withstand, and quickly recover from disruptions caused by deliberate attacks, accidents, or natural threats or incidents in cyberspace.

**Cyber Professionals** are experts who specialize in the security of computer systems, networks, and data. Their work includes protection from cyberattacks, identifying security threats, developing security policies and procedures, and responding to incidents.

**Cyber Risk** refers to the potential risk of causing damage by exploiting vulnerabilities in one or more information entities.

**Cyber Espionage** is a cyberattack targeting the confidentiality of ICT systems.

**Chambers of Commerce** are independent, non-profit, and voluntary organizations that unite business entities to represent their interests, promote the economy, and support economic development. They provide a platform for cooperation, services for members, and promote dialogue between the private and public sectors. In the Republic of North Macedonia, there are several important chambers, such as the Chamber of Commerce of North Macedonia, the Chamber of Northwest Macedonia, the Union of Chambers of Commerce of Macedonia, MASIT – Chamber of Commerce for ICT, and MACAM-TRANS – Chamber of Commerce for Transport, which play a crucial role in supporting the business community and the economy.

**Hybrid Warfare** is a strategy that combines traditional military operations with unconventional tactics and tools, such as cyberattacks, disinformation, economic pressures, and support for informal armed groups.

**Hybrid Threats** refer to situations or activities that combine traditional and unconventional methods to create instability or risks, such as military invasions, cyberattacks, disinformation, economic sanctions, and support for paramilitary groups. These threats are complex and difficult to predict, making them particularly dangerous for national security and stability.

**CSIRT (Computer Security Incident Response Team)** is a specialized group or team that manages and responds to cybersecurity incidents to minimize their impact and improve security in the future.

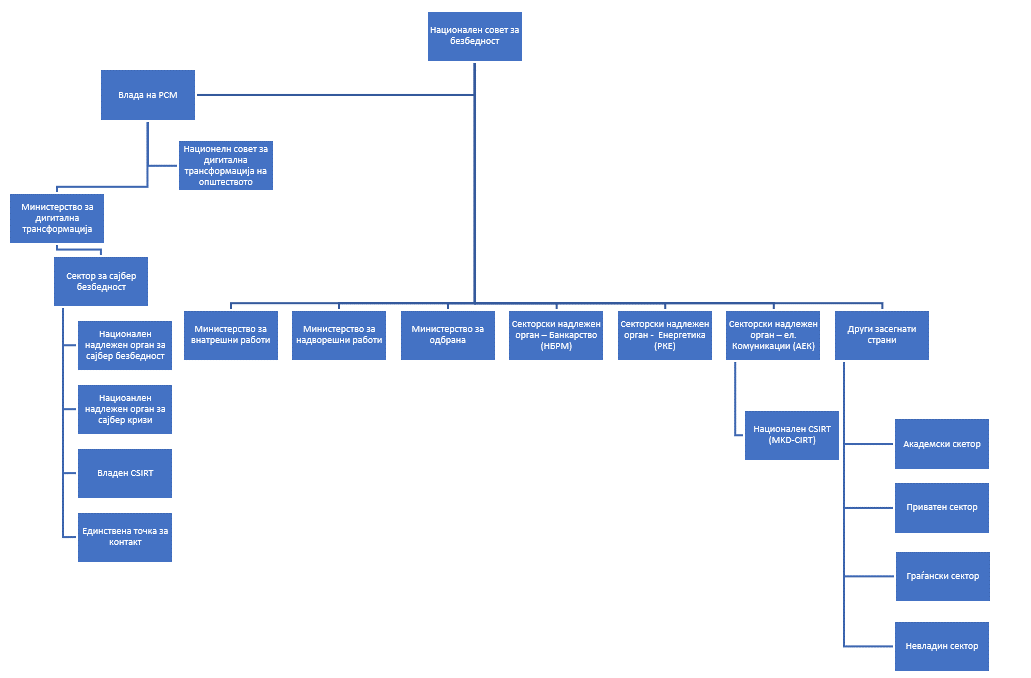
**SOC (Security Operation Center)** refers to the structure or function of an essential or important entity or organization responsible for activities related to cybersecurity and information security within the organization. It operates both proactively and reactively. A CSIRT may be a part of an SOC.

**Public Sector** consists of government bodies and other authorities and organizations established by law, municipal authorities, the city of Skopje, and municipalities within the city of Skopje, public institutions and services, public enterprises, legal and natural persons performing public duties as defined by law.

Annex 4 – Acronyms

**ARM** – Army of the Republic of North Macedonia  
**IT** – Information Technology  
**ICT** – Information and Communication Technology  
**CII** – Critical Information Infrastructure  
**NDTSC** – National Council for the Digital Transformation of Society  
**NRUCS** – National Framework for Cybersecurity Management  
**MDT** – Ministry of Digital Transformation  
**MFAE** – Ministry of Foreign Affairs and Foreign Trade  
**MSPYD** – Ministry of Social Policy, Demography, and Youth  
**MES** – Ministry of Education and Science  
**MoI** – Ministry of Internal Affairs  
**CVET** – Center for Vocational Education and Training   
**OT** – Operational Technologies  
**RSM** – Republic of North Macedonia  
**CCS** – Cybersecurity Sector within MDT  
**CERT** – (Computer Emergency Response Team)  
**CIRT** – (Computer Incident Response Team)  
**CSIRT** – (Computer Security Incident Response Team)  
**SCADA** – (Supervisory Control and Data Acquisition) is a system used to control industrial processes remotely by collecting and analyzing real-time data.  
**EU** – European Union  
**NATO** – North Atlantic Treaty Organization  
**MKD-CIRT** – National Computer Incident Response Team  
**USAID** – (United States Agency for International Development)  
**DCAF** – (Geneva Centre for Security Sector Governance)  
**SOC** – (Security Operations Center)  
**ISO** – (International Organization for Standardization)  
**NIST** – (National Institute for Standards and Technology)  
**PPP** – Public-Private Partnerships  
**ITU** – (International Telecommunications Union)  
**ENISA** – (European Cybersecurity Agency)   
SPOC – (Single Point of Contact) – National Single Point of Contact **NIS 2** – (Network and Information Systems Directive 2)

Annex 5 –Proposal for Placement of Entities and Functions in the National Cybersecurity Management Framework



Annex 6 – List of Used Information and References

1. ITU, https://www.itu.int/pub/D-STR-CYB\_GUIDE.01, Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity. [↑](#endnote-ref-1)
2. <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools> [↑](#endnote-ref-2)
3. <https://vlada.mk/sites/default/files/dokumenti/informacija_i_metodologija.pdf> [↑](#endnote-ref-3)
4. <https://vlada.mk/konceptDT> [↑](#endnote-ref-4)
5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), https://eur-lex.europa.eu/eli/dir/2022/2555/oj [↑](#endnote-ref-5)
6. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, https://eur-lex.europa.eu/eli/dir/2022/2557/oj [↑](#endnote-ref-6)
7. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), https://eur-lex.europa.eu/eli/reg/2019/881/oj [↑](#endnote-ref-7)
8. https://zelenaberza.com.mk/mvr-postapuva-po-hakerskiot-napad-vo-ministerstvoto-za-zemjodelstvo-koj-bara-otkup/ [↑](#endnote-ref-8)
9. https://telma.com.mk/2023/02/16/it-sistemot-na-fondot-za-zdravstvo-e-osvoen-od-hakeri-koi-baraat-otkup-potvrdi-i-kovachevski/ [↑](#endnote-ref-9)
10. https://www.slobodnaevropa.mk/a/32852038.html [↑](#endnote-ref-10)
11. https://dzr.mk/mk/240624-it-revizija-2023-efektivnost-na-prezemenite-merki-na-nadlezhnite-organi-za-zashtita-na [↑](#endnote-ref-11)
12. https://ener.gov.mk/default.aspx?item=pub\_regulation&subitem=view\_reg\_detail&itemid=80751 [↑](#endnote-ref-12)
13. https://mvr.gov.mk/Upload/Editor\_Upload/AP%20v1\_13MK.pdf [↑](#endnote-ref-13)
14. https://www.mchamber.mk/mk/home/propisi\_info/962 [↑](#endnote-ref-14)
15. https://mkd-cirt.mk/ [↑](#endnote-ref-15)
16. Стр. 8, Directive (EU) 2022/2555(https ://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555). [↑](#endnote-ref-16)
17. Directive (EU) 2022/2555(https ://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555) [↑](#endnote-ref-17)
18. Закон за трговските друштва – консолидиран текст, https://www.economy.gov.mk/Upload/Documents/ZTD%20konsolidiiran.pdf [↑](#endnote-ref-18)
19. Directive (EU) 2022/2555, стр. 30 [↑](#endnote-ref-19)
20. Directive (EU) 2022/2555, стр. 30 [↑](#endnote-ref-20)
21. Directive (EU) 2022/2555, стр. 16 [↑](#endnote-ref-21)
22. Directive (EU) 2022/2555, стр. 16 [↑](#endnote-ref-22)
23. Directive (EU) 2022/2555, стр. 16 [↑](#endnote-ref-23)
24. Directive (EU) 2022/2555, стр. 16 [↑](#endnote-ref-24)
25. Directive (EU) 2022/2555, стр. 16 [↑](#endnote-ref-25)
26. Directive (EU) 2022/2555, стр. 8. [↑](#endnote-ref-26)
27. Directive (EU) 2022/2555, стр. 39. [↑](#endnote-ref-27)
28. (Directive (EU) 2022/2555 Directive, Article 10, Стр. 38). [↑](#endnote-ref-28)
29. Page. 55, Directive (EU) 2022/2555(https://eur-lex.europa.eu/legal-content /EN/TXT/?uri=CELEX%3A32022L2555). [↑](#endnote-ref-29)
30. (Directive (EU) 2022/2555, стр. 28, член 1) [↑](#endnote-ref-30)
31. (Directive (EU) 2022/2555, Стр 36, член 8) [↑](#endnote-ref-31)
32. (Directive (EU) 2022/2555, Стр 36, член 8) [↑](#endnote-ref-32)
33. (Directive (EU) 2022/2555, стр. 36, член 8). [↑](#endnote-ref-33)
34. Directive (ЕУ) 2022/2555, член 1. [↑](#endnote-ref-34)
35. Directive (ЕУ) 2022/2555, член 1. [↑](#endnote-ref-35)
36. Directive (ЕУ) 2022/2555, член 1. [↑](#endnote-ref-36)
37. Directive (ЕУ) 2022/2555, член 1. [↑](#endnote-ref-37)
38. Directive (ЕУ) 2022/2555, член 3. [↑](#endnote-ref-38)
39. Directive (EU) 2022/2555, член 21. [↑](#endnote-ref-39)
40. Recommendation by the Commission (ЕУ) 2017 г. /1584, стр. 4. [↑](#endnote-ref-40)
41. Recommendation by the Commission (ЕУ) 2017/1584, стр. 1. [↑](#endnote-ref-41)
42. Препорака на Комисијата (ЕУ) 2017/1584, стр. 1. [↑](#endnote-ref-42)
43. Препорака на Комисијата (ЕУ) 2017/1584, стр. 5. [↑](#endnote-ref-43)
44. Препорака на Комисијата (ЕУ) 2017/1584, стр. 5. [↑](#endnote-ref-44)