Ministry of Digital Affairs
Republic of Poland

Annex to Resolution No. 92 of the Council of Ministers of 10 March 2026 (M.P., item 309)

# Cybersecurity Strategy of the Republic of Poland

**TLP: CLEAR**

# Table of contents

## List of abbreviations

1) ABW – Internal Security Agency;
2) Cybersecurity Act – 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;
3) Cyber Resilience Act – Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828;
4) AW – Foreign Intelligence Agency;
5) R&D – research and development;
6) R&D&I – research, development, and innovation;
7) CBZC – Central Cybercrime Bureau;
8) CPPC – Digital Poland Projects Centre;
9) CSAM – child sexual abuse material;
10) CSIRT – computer security incident response team;
11) CTI – cyber threat intelligence;
12) DEP – Digital Europe Programme;
13) DKWOC – Cyberspace Defence Forces Component Command;
14) DLT – distributed ledger technology;
15) DSP – digital service provider;
16) Directive 2022/2556 – Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector;
17) CER Directive – 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;
18) NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union;
19) NIS 2 Directive – 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;
20) EBSI – European Blockchain Services Infrastructure;
21) ECCC – European Cybersecurity Industrial, Technology and Research Competence Centre;
22) ECSC – Cybersecurity Training Centre of Excellence;
23) ENISA – European Union Agency for Cybersecurity;
24) EUCC – European Common Criteria-based cybersecurity certification scheme;
25) ICS – industrial control systems;
26) ICT – information and communications technology;
27) CI – critical infrastructure;
28) IŁ – National Institute of Telecommunications – State Research Institute;
29) WIIP Initiative – "Common State IT Infrastructure" Initiative;
30) IoT – Internet of Things;

31) ISAC – Information Sharing and Analysis Centre;
32) IT – information technologies;
33) LGUs – local government units;
34) Network Code – Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows;
35) KNF – Polish Financial Supervision Authority;
36) KG PSP – National Headquarters of the State Fire Service;
37) KG SG – National Headquarters of the Border Guard;
38) Penal Code – the Act of 6 June 1997 – Penal Code;
39) KSC – National Cybersecurity System;
40) MAP – Ministry of State Assets, the office supporting the minister responsible for state assets;
41) MC – Ministry of Digital Affairs, the office supporting the minister responsible for computerisation;
42) MEN – Ministry of National Education, the office supporting the minister responsible for education and upbringing;
43) MF – Ministry of Finance, the office supporting the minister responsible for the budget, the minister responsible for public finance, and the minister responsible for financial institutions;
44) MI – Ministry of Infrastructure, the office supporting the minister responsible for transport, the minister responsible for maritime economy, the minister responsible for inland navigation, and the minister responsible for water management;
45) ME – Ministry of Energy, the office supporting the minister responsible for energy and the minister responsible for the management of energy raw materials;
46) MKSS – Minister Coordinator of Special Services;
47) MNiSW – Ministry of Science and Higher Education, the office supporting the minister responsible for higher education and science;
48) MON – Ministry of National Defence;
49) MRiT – Ministry of Economic Development and Technology, the office supporting the minister responsible for the economy, and the minister responsible for construction, spatial planning and zoning, and housing;
50) MS – Ministry of Justice;
51) MSWiA – Ministry of the Interior and Administration, the office supporting the minister responsible for internal affairs, the minister responsible for public administration, and the minister responsible for religious denominations as well as national and ethnic minorities;
52) MSZ – Ministry of Foreign Affairs, the office supporting the minister responsible for foreign affairs and the minister responsible for the Republic of Poland's membership of the European Union;
53) MZ – Ministry of Health, the office supporting the minister responsible for health;
54) NASK – Research and Academic Computer Network – State Research Institute;
55) NATO – North Atlantic Treaty Organisation;
56) NCBR – National Centre for Research and Development;
57) NCC-PL – National Cybersecurity Competence Centre;
58) NCH – National Cyber Hub;
59) OChK – National Cloud Operator;
60) UN – United Nations;
61) OES – operator of essential services;

62) competent authority – authority responsible for cybersecurity, referred to in Article 41 of the Act on the National Cybersecurity System;
63) OT – operational technologies;
64) QKD – quantum key distribution
65) PCOC – Joint Cybersecurity Operations Centre;
66) Plenipotentiary – Government Plenipotentiary for Cybersecurity;
67) Action Plan – Action Plan for the Implementation of the Cybersecurity Strategy of the Republic of Poland;
68) PK – National Prosecutor's Office;
69) PWCyber – Cybersecurity Cooperation Programme;
70) PZP – the Act of 11 September 2019 – the Public Procurement Law;
71) RM – Council of Ministers;
72) RCB – Government Centre for Security;
73) RP – Republic of Poland;
74) MON – Ministry of National Defence;
75) Regulation 2022/2554 – Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011;
76) SBŁP – Secure State Communication System;
77) SKW – Military Counterintelligence Service;
78) Strategy – Cybersecurity Strategy of the Republic of Poland;
79) SWW – Military Intelligence Service;
80) SZRP – Armed Forces of the Republic of Poland;
81) EU – European Union;
82) UKE – Office of Electronic Communications;
83) Act on the National Cybersecurity System – the Act of 5 July 2018 on the National Cybersecurity System;
84) Act on the National Cybersecurity Certification Scheme – the Act of 25 June 2025 on the National Cybersecurity Certification Scheme;
85) WIŁ – Military Communications Institute – State Research Institute.

# 1. Introduction: Rationale for cybersecurity enhancement measures

Since the adoption, by Resolution No. 125 of the Council of Ministers of 22 October 2019,[1)] of the Cybersecurity Strategy of the Republic of Poland (the Strategy) for 2019–2024, social and economic development consistently remains dependent on fast and unhindered access to information and its use in management, production, the service sector, and the public sector. Actions taken on the basis of the Strategy for 2019–2024 have allowed all sectors of the Polish economy to develop in the digital dimension, and society and the state to function in a manner that ensures an achievable level of cybersecurity.

However, the level of cyber threats continues to rise both globally and domestically, as new types of threats emerge and the operations of groups engaged in illegal activities in the digital world increases – ranging from hacktivists to profit-driven cybercriminal groups, to groups affiliated with other countries or even operating directly within institutions of hostile states. These threats impact the daily functioning, security, and privacy of citizens (especially children, youth, and seniors), enterprises, and public institutions.

Radical changes in the security environment have led, among other things, to ongoing hostile and malicious activities in cyberspace. Russia's full-scale aggression against Ukraine has been accompanied by high-intensity cyberattacks on its information systems and IT infrastructure. Polish cyberspace has also become the target of increasingly numerous cyberattacks, some of which form part of unprecedented hybrid warfare efforts directed against the Republic of Poland (RP) and other Member States of the European Union (EU) and the North Atlantic Treaty Organisation (NATO). The ongoing struggle for economic dominance – encompassing, among other things, products and raw materials essential for technology development (including the "chip war") – alongside digitalisation and the expansion of digital services accelerated by the COVID-19 pandemic, and the emergence of new and disruptive technologies (such as artificial intelligence and quantum technologies) affecting all areas of society, economies, and national security systems, are the primary factors driving the radical transformation of the world. They also profoundly impact the security of cyberspace.

Major crises, such as the COVID-19 pandemic and the war waged by the Russian Federation against Ukraine, have demonstrated the vital importance of ensuring supply chain security, highlighting how disruptions can trigger negative multi-sectoral and cross-border economic and social consequences. Consequently, ensuring supply chain security to maintain critical social and economic activities, the continued operations of public administration and the Armed Forces of the Republic of Poland (SZRP), as well as the services rendered to them, has become a key challenge facing the Republic of Poland.

In the face of new and escalating threats, and taking into account their cross-border nature, international cooperation is of paramount importance. This includes collaboration within international organisations such as the EU, NATO, and the United Nations (UN), as well as through bilateral and multilateral formats, particularly with closest allies and partners.

The role of the state is to undertake actions that systematically elevate the level of national cybersecurity and mitigate cyberspace-related risks. In particular, the state must ensure the resilience of key resources and essential services against threats, safeguarding social and economic activities, public administration, as well as national security and defence. The adoption of the new Strategy results from the five-year timeframe specified in the Act of 5 July 2018 on the National Cybersecurity System[2)] and is necessitated by ongoing global developments. The adoption of the new Strategy must also align with other strategic documents and Poland's internal and foreign policies across all operational domains.

[1)] M.P., item 1037.
[2)] Dz.U. /Journal of Laws/ of 2026, items 20 and 252.

## 2. Strategic context of cybersecurity in the Republic of Poland

This Strategy represents a continuation and expansion of actions undertaken by the government administration to enhance the level of cybersecurity in Poland.

Regarding legislative acts, previous actions included the entry into force of the Act on the National Cybersecurity System and its subsequent amendments. This Act transposed Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) into the Polish legal order.[3)]

Legislative work has concluded on an amendment to the Act on the National Cybersecurity System, which aims to transpose 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).[4)] As a result, the National Cybersecurity System will undergo significant modifications, notably through the expansion of the catalogue of entities covered by these regulations.

Further, the Act of 25 June 2025 on the National Cybersecurity Certification Scheme[5)] adapted the Polish legal order to the obligations arising from 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 (the Cybersecurity Act).[6)] These regulations serve as a crucial complement to the National Cybersecurity System in the field of cybersecurity certification.

In terms of strategic documents, previous government actions included the adoption of:

1) in 2013, the Cyberspace Protection Policy of the Republic of Poland, adopted by Resolution No. 111/2013 of the Council of Ministers of 25 June 2013 on the Cyberspace Protection Policy of the Republic of Poland;[7)]
2) in 2017, the National Cybersecurity Policy Framework of the Republic of Poland for 2017–2022, adopted by Resolution No. 52/2017 of the Council of Ministers of 27 April 2017 on the National Cybersecurity Policy Framework of the Republic of Poland for 2017–2022;[8)]
3) in 2019, the Cybersecurity Strategy of the Republic of Poland for 2019–2024, adopted by Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024.[9)]

The issue of cybersecurity is also addressed in the National Security Strategy of the Republic of Poland, approved in 2020 by the President of the Republic of Poland. It will also be incorporated into the upcoming National Security Strategy of the Republic of Poland, thereby ensuring strategic coherence between this Strategy and the National Security Strategy. The development of this Strategy also took into account the ongoing work on the National Development Strategy 2035 – the country's new medium-term development strategy.

This Strategy is consistent with the main goals and actions set out in The EU's Cybersecurity Strategy for the Digital Decade.[10)] Its implementation, through the strengthening of the National Cybersecurity System, will consequently elevate the EU's overall level of cyber resilience.

---

[3)] OJ EU L 194, 19.07.2016, p. 1.
[4)] OJ EU L 333, 27.12.2022, p. 80 and OJ EU L 2025/90884, 6.11.2025.
[5)] Dz.U. /Journal of Laws/ of 2025, item 1017
[6)] OJ EU L 151, 07.06.2019, p. 15 and OJ EU L 2025/37, 15.01.2025.
[7)] Resolution not published in M.P.
[8)] Resolution not published in M.P.
[9)] M.P., item 1037.
[10)] Joint Communication to the European Parliament and the Council "The EU's Cybersecurity Strategy for the Digital Decade", Brussels, 16.12.2020, JOIN(2020) 18 final.

This Strategy will replace the Cybersecurity Strategy of the Republic of Poland for 2019–2024, governing actions from 2025 for the subsequent five-year period, i.e., until 2029.

The intention of this document is to define strategic goals alongside appropriate policy and regulatory measures designed to increase cyber resilience and enhance information protection across the public, military, and private sectors. Furthermore, it aims to promote knowledge and basic computer hygiene practices, empowering citizens to better protect their personal data and information. The implementation of these strategic goals is also expected to bolster national security, improve the capacity to identify cyber threats, and secure the capability to conduct both defensive and offensive operations in cyberspace. It seeks to neutralise threats posed by state-sponsored actors, and increase the effectiveness of law enforcement agencies and judicial authorities in detecting and combating cybercrime, hybrid warfare events (including terrorist incidents), and cyberespionage. A critical addition, essential to comprehensive national security, is the capability to anticipate and forecast situational developments (foresight) and perform data-driven analysis (data science).

The Strategy aligns with ongoing efforts concerning the security of network and information systems of critical infrastructure (CI) operators, as well as the systemic changes stemming from the pending transposition into Polish law of 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 (the CER Directive).[11)] It also addresses the necessity of ensuring that the SZRP possesses the capabilities to conduct military operations within national, allied, and coalition frameworks in the event of a cyber threat requiring defensive action.

In implementing the Strategy, the government will unequivocally guarantee the right to privacy and uphold the principle that a free and open internet is a fundamental component of modern society. Concurrently, it is imperative that the right to privacy does not impede the identification and prosecution of cybercriminals, nor afford them impunity.

[11)]OJ EU L 333, 27.12.2022, p. 164.

## 3. Scope of the Cybersecurity Strategy of the Republic of Poland

The Strategy covers the following in particular:[12)]

1) cybersecurity goals and priorities;
2) entities involved in the implementation and execution of the Strategy;
3) measures serving the implementation of the Strategy's goals;
4) the definition of preparedness, response, and disaster recovery measures, including the principles of public-private partnership;
5) the approach to risk assessment;
6) actions relating to cybersecurity training, education, and awareness programmes;
7) actions relating to research programmes and development plans in the field of cybersecurity.

The Strategy also addresses the prevention and combating of cybercrime and the achievement of capabilities to conduct a full spectrum of operations in cyberspace.

Moreover, it encompasses international cooperation in the area of cybersecurity.

Adopted via a resolution of the Council of Ministers, the Strategy directly affects government administration entities. Indirectly, following the Council of Minister's initiative to enact universally applicable laws, it impacts other entities, including entrepreneurs and citizens.

Cybersecurity is indirectly linked to matters such as the security of the information space, cognitive warfare, and disinformation. Given the Strategy's scope as defined in the Act on the National Cybersecurity System, the statutory definition of cybersecurity, and the comprehensive framework of the Act on the National Cybersecurity System – which do not directly encompass these matters – the Strategy addresses them solely in the context of actions to bolster cyber resilience against hybrid threats combining disinformation campaigns with cyberattacks, and efforts to build citizens' cybersecurity awareness and societal resilience against malicious cyber activities.

[12)] Article 69(1) and (2) of the Act on the National Cybersecurity System.

# 4. Vision, main goal, specific goals

## 4.1. Vision

Ensuring the security and successful development of the RP, the growth of its prosperity, economic efficiency, and the operational efficacy of its institutions and entities – including social activity and the daily functioning of every member of society – are inextricably linked to the efficient and secure operation of information systems and electronic communication means. Therefore, through the actions outlined in the Strategy, the government will systematically strengthen and develop the National Cybersecurity System. These actions encompass systemic organisational, financial, operational, technological, and legal solutions, the cultivation of social awareness, the execution of research and development, and the advancement of the Polish cybersecurity industry, ensuring adherence to high cybersecurity standards across software, connected devices, and digital services. The government's actions will be executed with profound respect for citizens' rights and freedoms, fostering trust between the government administration and various market sectors. Internationally, the government's efforts will focus on mutually beneficial cooperation, championing an open, stable, and secure cyberspace founded upon human rights, fundamental freedoms, democracy, and the rule of law.

## 4.2. Main goal

Increasing the level of resilience of national entities by elevating information security, enhancing the capability to detect and respond to threats, promoting knowledge and basic computer hygiene practices, and advancing cybersecurity competencies across the public (including military) and private sectors, as well as among citizens.

## 4.3. Specific goals

**Specific goal 1.** Development of the National Cybersecurity System.

**Specific goal 2.** Preventing and combating cybercrime and achieving capabilities to conduct a full spectrum of operations in cyberspace.

**Specific goal 3.** Increasing the level of resilience of information systems in the public (including military) and private spheres.

**Specific goal 4.** Increasing the potential of the national technological and industrial base and strengthening the technological sovereignty of the Republic of Poland in the area of cybersecurity.

**Specific goal 5.** Building the awareness, knowledge, and competencies of the staff of the National Cybersecurity System entities, as well as of citizens and entrepreneurs.

**Specific goal 6.** Strengthening the Republic of Poland's solid international standing in the field of cybersecurity.

## Table 1. Structure of goals and directions of intervention

| **Main Goal** | Increasing the level of resilience of national entities by improving information security, enhancing the capability to detect and respond to threats, promoting knowledge and basic computer hygiene practices, and advancing cybersecurity competencies across the public (including military) and private sectors, as well as among citizens | | | | | |
|---|---|---|---|---|---|---|
| **Specific goals** | 1. Development of the National Cybersecurity System | 2. Preventing and combating cybercrime and achieving capabilities to conduct a full spectrum of operations in cyberspace | 3. Increasing the level of resilience of information systems in the public (including military) and private spheres | 4. Increasing the potential of the national technological and industrial base and strengthening the technological sovereignty of the Republic of Poland in the area of cybersecurity | 5. Building the awareness, knowledge, and competencies of the staff of the National Cybersecurity System entities, as well as of citizens and entrepreneurs | 6. Strengthening the Republic of Poland's solid international standing in the field of cybersecurity |
| **Directions of intervention** | 1.1 Improvement of the National Cybersecurity System | 2.1 Introduction of regulations to more effectively combat cybercrime | 3.1 Increasing the level of resilience of information systems | 4.1 Strengthening supply chain security at the national and international levels | 5.1 Increasing awareness and knowledge, and strengthening the competencies of the staff of the National Cybersecurity System entities | 6.1 Active international cooperation at the strategic, political, and legal levels |
| | 1.2 Increasing the efficiency of the National Cybersecurity System | 2.2 Strengthening specialised cybercrime combating structures | 3.2 Development of national cryptology, including the migration to post-quantum cryptography and the development of quantum technologies | 4.2 Stimulating research, development, and innovation in the area of cybersecurity | 5.2 Developing the cybersecurity awareness and knowledge of citizens and entrepreneurs | 6.2 Active international cooperation at the operational and technical levels |
| | 1.3 Development of an integrated information sharing system to ensure the continuity of government administration, national security, and civil protection | 2.3 Enhancing the analytical capabilities of law enforcement agencies, special services, and judicial authorities using new technologies | 3.3 Cloud computing services for strengthening the resilience of information systems | | | 6.3 Coordination of international activities related to civil-military cooperation in the field of cybersecurity |
| | 1.4 Increasing the cybersecurity of entities supervised by authorities responsible for cybersecurity | 2.4 Increasing the effectiveness of law enforcement agencies through the exchange of knowledge and experience regarding cybersecurity and methods used by cybercrime perpetrators | 3.4 Development of capabilities for the effective prevention of and response to cybersecurity incidents | | | |
| | 1.5 Development and implementation of a risk assessment methodology at the national level | 2.5 Combating cyberterrorism and cyberespionage | 3.5 Development of standardisation in cybersecurity | | | |
| | | 2.6 Achieving capabilities to conduct a full spectrum of operations in cyberspace | 3.6 Public-private partnership in the area of cybersecurity | | | |

# 5. Specific goal 1. Development of the National Cybersecurity System

## 5.1. Improvement of the National Cybersecurity System

The National Cybersecurity System was formally established in 2018 through the enactment of the Act on the National Cybersecurity System. However, in practice, this system has existed for years and continues to evolve. Significant changes to the functioning of the National Cybersecurity System will occur with the amendment to the Act on the National Cybersecurity System, which will transpose the NIS 2 Directive, adopted in 2022, into the Polish legal order. However, the forthcoming legislative amendments do not solely pertain to the transposition of EU law; they also respond to identified needs for change, technological progress, new threats, and the evolution of the security environment.

The most significant changes resulting from the transposition of the NIS 2 Directive involve replacing the former division between operators of essential services (OES) and digital service providers (DSPs) with essential entities and important entities. Furthermore, the scope of sectors covered by the NIS 2 Directive will be expanded. This directive also establishes a series of obligations for essential and important entities. The fundamental obligation involves implementing appropriate and proportionate technical, operational, and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Through the amendment to the Act on the National Cybersecurity System, the provisions of the EU toolbox for 5G security (5G Toolbox) will also be implemented.

Moreover, the amendment to the Act on the National Cybersecurity System, enacted on 23 January 2026, specifically concerns:

1) expanding the catalogue of National Cybersecurity System entities to include new sectors of the economy;
2) imposing obligations regarding cybersecurity risk management measures on essential and important entities, in accordance with the NIS 2 Directive;
3) introducing mandatory incident reporting by essential and important entities to the relevant sectoral CSIRTs and national-level CSIRTs via the IT system of the minister responsible for computerisation;
4) creating sectoral CSIRTs that will support essential and important entities in cybersecurity incident handling;
5) strengthening the supervisory competencies of authorities responsible for cybersecurity (competent authorities);
6) introducing new administrative fines for the failure to comply with statutory obligations by essential and important entities;
7) introducing the national cyber crisis management framework for large-scale cybersecurity incidents;
8) expanding the competencies of the minister responsible for computerisation (this authority will be empowered to legally designate a high-risk supplier by administrative decision, and issue a safeguarding order specifying measures to mitigate the effects of an ongoing critical incident);
9) expanding the competencies of the minister responsible for computerisation and the Minister of National Defence regarding the handling of large-scale cybersecurity incidents and cybersecurity crisis management;
10) expanding the scope of tasks of the national-level CSIRTs (CSIRT MON, CSIRT NASK, and CSIRT GOV), which will be authorised, among other things, to: conduct security assessments of information systems used by National Cybersecurity System entities and carry out activities related to identifying vulnerabilities in systems accessible on public electronic communications networks;

11) introducing the liability of the management body of an essential or important entity for the execution of cybersecurity tasks.

An evaluation of the National Cybersecurity System highlights the need for better coordination and institutionalised management of cybersecurity at the national level. Therefore, in the amendment to the Act on the National Cybersecurity System, the role of the Government Plenipotentiary for Cybersecurity (the Plenipotentiary) will be strengthened, granting greater powers to better manage and coordinate the National Cybersecurity System. The function of the Plenipotentiary will be permanently integrated with the office supporting the minister responsible for computerisation. The Plenipotentiary will also chair the Critical Incidents Team, and the support for this Team will be transferred to the office assisting the Plenipotentiary. The role of the Plenipotentiary will be further reinforced. The Plenipotentiary will coordinate, in consultation with the Minister of National Defence, activities related to civil-military cooperation in the area of cybersecurity during peacetime. This will enhance operational efficiency, properly synchronise cybersecurity activities undertaken in both the military and civilian spheres, and thereby achieve strategic goals more effectively.

The enacted amendment to the Act on the National Cybersecurity System will formalise the functioning of the Joint Cybersecurity Operations Centre (PCOC), which has been operating since 2022. The format of coordination meetings within the PCOC, attended by representatives of institutions crucial to national cybersecurity, constitutes a significant added value for the National Cybersecurity System by enabling rapid information sharing and efficient responses to emerging cybersecurity incidents.

As a next step, the PCOC will be expanded by establishing an organisational unit under this name within the office supporting the minister responsible for computerisation. This unit will provide organisational and substantive support to the Plenipotentiary and PCOC meetings, coordinate – on behalf of the Plenipotentiary – the activities of institutions ensuring cybersecurity at the national level, and perform some of the tasks of the minister responsible for computerisation as provided for in the Act on the National Cybersecurity System.

Ultimately, the PCOC will be transformed into a central institution responsible for cybersecurity at the national level, with the appropriate institutional status, authority, personnel, budget, and infrastructure. The new institution will act as a coordinating body within the National Cybersecurity System, serve as a single point of contact for National Cybersecurity System entities and citizens regarding incident reporting, and be responsible for supporting the Plenipotentiary's activities. This will further enhance the system's efficiency and ensure a swifter response to cyber threats. Domestic experiences and lessons learned from other countries demonstrate the necessity of establishing a new central institution responsible for cybersecurity across the entire state, allowing for the centralised management of cybersecurity in Poland. Due to the expanding and increasingly complex cybersecurity regulations at the EU level, the PCOC will support efforts aimed at simplifying and harmonising the application of cybersecurity regulations. This includes identifying overlapping regulatory areas, synchronising activities, and streamlining procedures for entities required to comply with cybersecurity regulations.

Concurrently, an important complement to the National Cybersecurity System is the Act on the National Cybersecurity Certification Scheme, which established a cybersecurity certification system in Poland and set forth the procedures necessary to ensure the integrity of the certification processes.

In light of the growing number of EU and national legislative acts concerning cybersecurity, efforts will be made to ensure their proper harmonisation and coordinated implementation. Sector-specific Union legal acts will also be transposed into the national legal order or otherwise their application will be ensured. This includes Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Regulation 2022/2554)[13)] and Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU,

[13)]OJ EU L 333, 27.12.2022, p. 1 and OJ EU L 2024/90177, 12.03.2024.

2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector.[14)]

## 5.2. Increasing the efficiency of the National Cybersecurity System

The escalating scale of threats and the concomitant expansion of activities within the National Cybersecurity System necessitate continuous monitoring and improvement of the overall system's efficiency to properly ensure the security of Polish cyberspace and coordinate related actions.

Improving the National Cybersecurity System's operational efficiency is carried out through such means as the S46 system, launched on 1 January 2021 by the minister responsible for computerisation, which supports:

1) cooperation between National Cybersecurity System entities;
2) generating and issuing recommendations on actions improving cybersecurity;
3) cybersecurity incident reporting and handling;
4) risk assessment at the national level;
5) early warning about cyber threats;
6) supervisory activities of competent authorities;
7) reporting personal data breaches.

The S46 system will be further developed, which includes increasing its efficiency and introducing new functionalities, such as gathering information on essential and important entities (upon the entry into force of the planned amendment to the Act on the National Cybersecurity System), which are crucial from a National Cybersecurity System management perspective. Moreover, additional National Cybersecurity System entities will be connected to the S46 system, including all essential and important entities. The S46 system will form the basis for information sharing among essential entities, important entities, and state institutions. Information from this system will also be transferred to authorities responsible for crisis management. The upgraded S46 system will also be utilised by the PCOC to automate information sharing within the National Cybersecurity System.

The cyber.gov.pl portal has also been launched – a modern, governmental platform created with the digital security of citizens, businesses, and public institutions in mind. All key services and tools are located in one place, from incident reporting and threat monitoring to access to solutions such as the Artemis system, S46, or the moje.cert.pl application. The platform also offers access to a knowledge base, cybersecurity training, warnings, and practical information regarding obligations arising from the Act on the National Cybersecurity System and the NIS 2 Directive. Thanks to integration with the national electronic identification node, referred to in Article 21a of the Act of 5 September 2016 on trust services and electronic identification,[15)] logging in and using the portal will be straightforward and secure.

An initiative aimed at building national and European cybersecurity will involve the creation of a national platform based on the S46 system and the n6 security incident information sharing service. This platform will assist in detecting and building situational awareness of cybersecurity threats and incidents for the public and private sectors, constituting the National Cyber Hub (NCH). Ultimately, this platform will become an element of the European Cyber Shield.

The role of competent authorities will be strengthened by expanding their powers related to the supervision of a given sector; moreover, the competent authority will establish a sectoral CSIRT. In addition to the ability to conduct on-site inspections, competent authorities will gain the power to, among other things, issue binding instructions requiring an entity to undergo a security audit, as well as the authority to order entities to take specific actions concerning incident handling. Under statutorily defined

[14)] OJ EU L 333, 27.12.2022, p. 153.
[15)] Dz.U. /Journal of Laws/ of 2024, item 1725, and of 2026, item 252.

circumstances, a competent authority will have the power to enter a given entity into the national registry of essential and important entities on an ex officio basis. Competent authorities will also play a significant role in supply chain security assessments. The competent authorities will also strengthen cooperation among themselves to properly coordinate actions taken in individual sectors, provide mutual assistance, and, where appropriate, conduct joint supervisory activities.

The efficiency of cybersecurity teams of National Cybersecurity System entities will be enhanced, in particular those whose ICT systems or networks are included in the uniform list of objects, systems, devices, and services comprising the critical infrastructure (CI). Specialised cybersecurity exercises and workshops – including in international formats – utilising modern CyberRange platforms and advanced scenarios addressing contemporary cybersecurity challenges and threats, will provide an opportunity to build
cohesive cybersecurity teams and verify their skills in direct operations.

The NASK Cybersecurity Centre (CCN) will be established within the structures of the Research and Academic Computer Network – State Research Institute, which houses one of the national-level CSIRTs (CSIRT NASK). It will consist of qualitatively new, specialised thematic centres, facilities, and laboratories crucial for strengthening the National Cybersecurity System. Executing this measure will raise the level of information security by bolstering resilience and the capacity to effectively prevent and respond to incidents in the information systems of the state and entities of critical importance to the economy.

Necessary structural changes will also be implemented within the Internal Security Agency (ABW), involving the establishment of a new organisational unit with competencies in identifying, preventing, and combating cyberterrorism and cyberespionage.

Local government units (LGUs) are a key component of the National Cybersecurity System. Voivodeship teams of cybersecurity specialists will be created, operating locally to support public administration entities in incident handling, disaster recovery, and conducting cybersecurity awareness-raising activities. The "Cybersecure Local Government" programme, encompassing training and the procurement of necessary hardware and software, will be continued. The government will support LGUs in building and expanding their local cybersecurity structures, which is particularly vital given the limited resources of individual LGUs. To mitigate the shortage of cybersecurity specialists within LGUs, a project to build Local Cybersecurity Centres will be launched. Operating as Shared IT Service Centres, they will ensure a high level of cybersecurity for multiple institutions at the local and regional levels. Actions will also be undertaken to support local governments in implementing cybersecurity initiatives within regional programmes.

Providing access to expert knowledge regarding cyber threats is of key importance for elevating the level of cybersecurity. One method of securing such access is establishing Information Sharing and Analysis Centres (ISACs) and competence centres. An ISAC gathers information on vulnerabilities and cyber threats, and subsequently disseminates this information along with best practice guidelines to entities participating in the information sharing network. The operation of ISACs in sectors covered by the Act on the National Cybersecurity System and its amendments, which are of key significance to the Polish economy, will contribute to strengthening cooperation and trust among entities within the same sector. The creation of ISACs will continue to be supported under general principles – for instance, in the form of associations, foundations, public-private partnerships, or other organisational units, without regulating this matter in the Act on the National Cybersecurity System.

Cybersecurity actions within the crisis management framework and cybersecurity crisis management within the National Cybersecurity System will be continued. A new element will be the preparation of the National Large-Scale Cybersecurity Incident and Crisis Response Plan and monitoring its execution. This will align National Cybersecurity System and crisis management regulations, ensuring the flow of necessary information and synergy of actions. These actions will also encompass enhancing the cybersecurity of CI. In accordance with Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity

flows[16] (the Network Code), the National Plan will also incorporate crisis management and response issues pertaining to cross-border electricity flows (Article 41(2) and (3) of the Network Code).

Data-driven analytical capabilities will be developed to chart the future course of the National Cybersecurity System and to anticipate and forecast situational developments in the cybersecurity environment (cyber foresight). Information and communications technology (ICT) solutions supporting analytical activities will be shared by National Cybersecurity System entities, and the analytical products generated using these solutions will be exchanged.

## 5.3. Development of an integrated information sharing system to ensure the continuity of government administration, national security, and civil protection

Secure information sharing systems for national security command and control are essential not only for domestic cybersecurity but also for the comprehensive national security framework.

A Secure State Communication System (SBŁP) will be established to facilitate information exchange between authorities responsible for executing tasks related to crisis management, national security, public order protection, rescue operations, civil protection, and civil defence. The subsystems constituting the SBŁP will encompass classified and unclassified fixed communication lines, video conferencing infrastructure, secure mobile communications (including classified cellular networks), trunked radio systems, radio communications, and secure satellite communications. The resilience of, and capability to effectively prevent and respond to incidents within, information flow systems will be enhanced. Efficient, secure, and available electronic communications services will be provided, ensuring the delivery of communication services even when command and control posts are relocated, thereby enhancing civil protection, citizen security, and the effectiveness of crisis response. Cryptographic solutions, including encryption mechanisms and secure data transmission protocols, will be developed. A hybrid infrastructure will be established to enable switching between terrestrial networks and satellite systems in the event of disruptions. A mechanism for communication between the system and military solutions will be developed for peacetime, crises, and conflicts.

Direct users of the system will include public administration entities, their supporting offices, and subordinate or supervised organisational units executing tasks related to national security, public order protection, rescue operations, civil protection, civil defence, crisis management, and public warning and alarm systems.

The secure mobile communication solutions that have already been developed and implemented will continue to be used: a mobile communication system capable of handling classified information up to the "Restricted" level based on the CATEL (SKR-Z), complying with the guidelines regarding the construction and operating principles of the CATEL system, as well as "Komunikator", designed to ensure secure (unclassified) government and National Cybersecurity System communications on official devices. Emphasis will be placed on maintaining high availability of these systems, ensuring their digital accessibility, successively increasing the user base, and enriching system functionalities. An electronic classified document management platform secured by domestic cryptographic solutions will also be developed, accompanied by necessary legal amendments to enable its operation in compliance with classified information protection requirements. A national communicator for public administration will also be created. Efforts will be made to replace commercial communication solutions currently in use with those provided by state institutions.

[16] OJ EU L 2024/1366, 24.05.2024, OJ EU L 2024/90558, 16.09.2024 and OJ EU L 2025/1759, 25.08.2025.

## 5.4. Increasing the cybersecurity of entities supervised by authorities responsible for cybersecurity

The enacted amendment to the Act on the National Cybersecurity System, associated with the transposition of the NIS 2 Directive, will result in operators of essential services (OES) and digital service providers (DSPs) being replaced by essential entities and important entities. The previous division into OES and DSPs proved outdated, as it did not reflect the significance of specific sectors and services for the social and economic activities of EU Member States. Therefore, the scope of the NIS 2 Directive, and thus the draft act transposing it, was expanded to include new economic sectors crucial to Poland's social and economic activities.

In addition to expanding the scope of entities covered, the NIS 2 Directive also introduced, among other things, a significantly expanded list of obligations applicable to critical and important entities. The obligation for essential and important entities to implement cybersecurity risk management measures will substantially elevate their cybersecurity posture, and consequently national security, by achieving an appropriate level of security for network and information systems used to provide services and ensuring proper incident handling.

The rise in cyberattacks necessitates concrete strategic actions that bolster the cybersecurity of essential entities and important entities. CSIRTs will provide appropriate support (including proactive measures) concerning the cybersecurity and security of essential and important entities. Particular attention will be paid to entities functionally or technologically linked to CI, public administration, and national security and defence institutions, as they are potential targets for attacks. Cybersecurity training for National Cybersecurity System entities will also encompass the legal safeguarding of entity interests in the event of a significant incident.

The cybersecurity of essential and important entities will also be enhanced through effective supervision exercised by competent authorities for cybersecurity, either ex ante or ex post, depending on the type of entity. Equipping competent authorities for cybersecurity with broader supervisory and enforcement measures will ensure a consistently high level of cybersecurity, particularly by enabling them to issue binding instructions regarding incident handling, mandate the implementation of security audit recommendations, or order compliance with cybersecurity risk management measures. Ex ante supervision will play a critical role in ensuring the cybersecurity of essential and important entities by verifying their capacity to prevent cyber threats and avoid breaches of the Act on the National Cybersecurity System that could lead to incidents. Moreover, these entities will be granted access to the S46 system, enabling them to manage cybersecurity more effectively and collaborate and share information with other National Cybersecurity System entities, among other things. The provisions of the Network Code will be implemented, facilitated by the prepared amendment to the Act on the National Cybersecurity System. The Network Code introduces an additional catalogue of cybersecurity-enhancing obligations for entities affecting cross-border electricity flows, as well as a catalogue of supervisory powers and domestic and international cooperation duties for the designated competent authority. These measures will strengthen collaboration between individual entities and relevant authorities in the electricity and cybersecurity domains, and help prevent electricity crises potentially rooted in cybersecurity incidents.

Essential and important entities will also participate in recurring, large-scale cybersecurity exercises.

Support will be provided to 500 National Cybersecurity System entities for the modernisation and expansion of cybersecurity infrastructure within IT networks, including support for entities utilising information technologies (IT) and industrial operational technologies (OT) applied in industrial control systems (ICS).

## 5.5. Development and implementation of a risk assessment methodology at the national level

A methodology for static and dynamic risk assessment for ICT systems was developed and subsequently implemented in the S46 system to serve national-level cybersecurity management. Practical application demonstrated that this methodology is difficult to implement within National Cybersecurity System entities and fails to yield expected results.

A new risk assessment approach will be developed and implemented in the S46 system, linked to achieving the desired cybersecurity, both at the level of individual National Cybersecurity System entities and as an aggregated national risk profile. This will utilise information reported by essential and important entities, as well as cyber threat intelligence regarding threats, vulnerabilities, and incidents acquired from other sources, notably CSIRTs. The new risk assessment solution will be more effectively utilised and easier to implement across entities of varying sizes.

# 6. Specific goal 2. Preventing and combating cybercrime and achieving capabilities to conduct a full spectrum of operations in cyberspace

## 6.1. Introduction of regulations to more effectively combat cybercrime

A comprehensive ecosystem of regulations pertaining to combating cybercrime, securing digital evidence, and preventing identity theft will be ensured. The evolution of modern information and communications technology, the availability of remote communication means, and the associated growth of digital services have altered the methods used by perpetrators of crimes against various legally protected interests.

To expedite the identification of perpetrators online, draft legislative amendments will be prepared to grant law enforcement agencies faster access to information covered by banking secrecy. Proposed legal changes will also make it possible to request data covered by banking secrecy solely based on a prosecutor's order, without the involvement of a locally competent regional court. Such a change will significantly enhance the effectiveness of ongoing proceedings and the concentration of evidence, particularly in the initial phases of an investigation or inquiry.

Amendments will be proposed regarding the obligations of banks and other financial institutions to retain and transmit information and data concerning bank accounts, services, and products provided via the internet. A solution will be proposed mandating financial institutions (including banks) and entities providing services via electronic means[17)] to collect information regarding ports assigned to a specific IP address by unequivocally indicating source ports as data identifying the telecommunications network termination point. This will vastly improve the ability to identify perpetrators during preparatory proceedings. Legislative work will be undertaken to enable prosecutors conducting criminal proceedings (including those concerning fraud on the over-the-counter forex market) to block websites used to carry out criminal activities.

Legal frameworks will also be proposed regarding data retention and the transfer of information and data by entities providing crypto-asset services. Ultimately, over a longer timeframe, legal mechanisms enabling the "freezing" of these assets will be proposed.

Concurrently, the enactment of legislation ensuring the proper application of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)[18)] will introduce mechanisms to enforce the financial liability of online platforms through which illegal advertisements are disseminated (specifically, fraudulent ads encouraging investment in non-existent products), including the possibility of imposing adequate financial penalties on platforms that repeatedly publish fraudulent and misleading content.

Legislative, organisational, and technical solutions will be prepared to enhance the protection of internet users against harmful and dangerous content, with a particular focus on protecting children and youth (combating child sexual abuse material (CSAM), live-streamed abuse, grooming,[19)] etc.). This will encompass the creation and deployment of a hash value sharing system (HASH database) and a national database of child sexual abuse material (CSAM image repository), as referred to in sections 2.1.12 and 2.4.2 of the National Plan to Counter Crimes against Sexual Freedom and Decency Affecting Minors for 2023–2026.[20)]

Regulations combatting identity theft – specifically concerning remote customer identity verification using electronic identification means during transactions, the use of new financial products, and the

[17)] Operating pursuant to the Act of 18 July 2002, on the Provision of Electronic Services (Dz.U. /Journal of Laws/ of 2024, item 1513), in particular within the scope specified in Article 18(5)(2) of that Act.

[18)] OJ EU L 277, 27.10.2022, p. 1 and OJ EU L 163, 29.06.2023, p. 107.

[19)] Actions taken to befriend a child and form an emotional bond with them, in order to lower their resistance and later sexually abuse them.

[20)] Introduced by Resolution No. 204 of the Council of Ministers of 17 October 2023 on the adoption of the National Plan to Counter Crimes against Sexual Freedom and Decency Affecting Minors for 2023–2026 (M.P. item 1235).

registration of prepaid SIM cards – will be adapted to the challenges posed by technological progress. Legal solutions will be proposed to curtail the mass activation of SIM cards and their illicit use, including artificially boosting entity credibility or supporting the operations of organised crime syndicates and hybrid warfare operations.

A review of the provisions concerning criminal liability for specific cybercrimes will be conducted, with proposals to update them to reflect current realities.

Tools introduced by the Act of 28 July 2023 on combating abuse in electronic communications,[21] designed to counter spoofing-based[22] fraud and fraudulent text messages, will be further developed. This type of crime is particularly burdensome for citizens and undermines trust in both public institutions – which criminals frequently impersonate – and legally operating enterprises. The minister responsible for computerisation will be reviewing the mechanisms contained in the aforementioned Act and will, if necessary, propose amendments to ensure the effective application of measures combating electronic communication abuse. An evaluation of the implemented solutions will take place in 2026, with subsequent evaluations occurring biennially. This will permit dynamic regulatory adaptation to changes in this field, particularly accommodating new methods employed by cybercriminals.

Solutions will be proposed to monitor and restrict the use of artificial intelligence (AI) for criminal activities in cyberspace, i.e. terrorist offences, the automation of phishing attacks, the generation of false content, and the evasion of threat detection systems.

Regarding the fight against cybercrime, amendments will be proposed to the governing acts of individual special services, as well as to the Act of 6 June 1997 – the Penal Code[23] (Penal Code), which will ultimately permit the execution of a full spectrum of operations, including defensive and offensive operations, in response to cyberterrorism and cyberespionage threats.

Legislative amendments will be prepared to introduce statutory exemptions from criminal liability for operational and analytical activities undertaken in cyberspace by officers of special services and law enforcement agencies. Such exemptions will apply when an officer's actions fall within their statutory mandate, serve the public interest, adhere to specific conditions of legality and oversight, comply with the principle of proportionality, and are subject to judicial or prosecutorial supervision. This will enable the effective prosecution of the most severe forms of cybercrime while affording adequate legal protection to personnel executing official duties using appropriate tools and methods, simultaneously guarding against abuse.

The Police, the prosecutor's office, and other relevant institutions will employ centralised IT tools ensuring that actions against a single criminal group are conducted in a unified manner. This cooperation will be executed using the latest ICT tools. The cybercrime reporting process will be reorganised to ensure more victims contact law enforcement agencies.

## 6.2. Strengthening specialised cybercrime combating structures

The establishment of the Central Cybercrime Bureau (CBZC) in 2021 was an important step towards specialising police structures to combat cybercrime. The CBZC integrates technical, operational, and analytical competencies; however, its effectiveness depends on cooperation with prosecutors specialised in cybercrime and the understanding of technology by courts (e.g., when adjudicating cases involving digital evidence, blockchain, or electronic security measures). Therefore, in addition to further strengthening the capabilities of the CBZC, the expansion of specialised units in other state structures, including the prosecutor's office and courts, will continue to ensure the coherence and effectiveness of the entire system.

[21] Dz.U. /Journal of Laws/ of 2024, item 1803, and of 2026, item 252.

[22] A cyberattack in which the attacker impersonates a trusted person, device, or institution in order to deceive the victim and gain access to confidential data or money.

[23] Dz.U. /Journal of Laws/ of 2025, items 383, 1818 and 1872.

A specialised human resource pool dedicated to combating cybercrime will be created and developed, and cybercrime combating divisions will be equipped with the necessary tools to collect and analyse evidence, including digital evidence, during criminal proceedings.

Actions will be undertaken to integrate technical and legal knowledge among the staff of law enforcement agencies and judicial authorities. Combating cybercrime combines aspects of criminal law, computer forensics, evidence law (e.g., the admissibility and integrity of digital material), and international investigative cooperation. Without specialised staff – from police officers and prosecutors to judges – proceedings become excessively prolonged, evidence is ineffectively secured, and there is a risk of acquittals due to procedural reasons.

Given the development of modern technologies and the associated emergence of new vulnerabilities, attack vectors, electronic services used in criminal activities, and new methods employed by perpetrators, continuous education will be provided for the staff of judicial authorities, the Police, and special services. Further, specialised cybercrime organisational units will be established within the prosecutor's office and the Police.

Further specialisation in cybercrime prosecution will be pursued. At the level of prosecutor's office organisational units, this should manifest in the training of selected prosecutors in combating this type of crime at the district prosecutor's office level, and the creation of cybercrime divisions or departments within district and regional prosecutor's offices, staffed by prosecutors specialising in combating this type of crime.

## 6.3. Enhancing the analytical capabilities of law enforcement agencies, special services, and judicial authorities using new technologies

Enhancing the analytical capabilities of law enforcement agencies, special services, and judicial authorities is a key element of an effective strategy to combat cybercrime. Law enforcement agencies will be equipped with the capabilities to quickly and accurately analyse large volumes of data from various sources, such as server logs, network traffic records, and data from mobile devices. Advanced data analysis will permit the identification of criminal activity patterns, potentially leading to the detection of both individual perpetrators and entire criminal groups. Additionally, the use of predictive analytics will enable the forecasting of future attacks and the detection of potential vulnerabilities in security systems. The enhancement of analytical capabilities will be achieved through the implementation of modern data analysis systems (including those based on artificial intelligence (AI), which can automate information analysis and processing). Advanced technologies will be utilised for this purpose, such as quantum computers for decoding encrypted data, tracking cryptocurrency transactions, and analysing the Darknet.

Regular training sessions will be organised for law enforcement officers and representatives of judicial authorities regarding new technologies, cybersecurity, and data analysis methods, including legal aspects. Cooperation with universities and technology companies will be pursued to improve the qualifications of personnel involved in the fight against cybercrime.

Concurrently, organisational, legislative, and procedural changes will be introduced within law enforcement structures to maximise the potential of new technologies.

## 6.4. Increasing the effectiveness of law enforcement agencies through the exchange of knowledge and experience regarding cybersecurity and methods used by cybercrime perpetrators

Educational initiatives will be undertaken to provide representatives of judicial authorities and law enforcement agencies with detailed theoretical and practical knowledge regarding the fight against

cybercrime. The acquired skills will streamline criminal proceedings, including through the use of new technologies, and improve the quality of cooperation between specialised services.

Cooperation with Interpol and Europol in combating cybercrime will be developed. Due to ongoing globalisation, training activities will involve cooperation with foreign entities providing internet services as well as those established to combat cybercrime.

Training concerning the acquisition of data from foreign entities – which frequently constitutes a major obstacle in the evidentiary process – will also be expanded. The victims of cybercrime include economic entities, public utility institutions, and individuals. In parallel with educational activities targeting law enforcement agencies and judicial authorities, educational campaigns will be conducted among the public to inform them about the methods used by cybercriminals.

## 6.5. Combating cyberterrorism and cyberespionage

To achieve the capability to combat cyberterrorism and cyberespionage, actions will be undertaken – led by the Internal Security Agency (ABW) and the Military Counterintelligence Service (SKW) – consisting of the detection, analysis, and prevention of threats targeting the cybersecurity of Poland and allied states. Special services will be continuously supported in identifying cyber threats by national-level CSIRTs and other competent state institutions.

Amendments will be proposed to the acts regulating the functioning of special services to enable the effective conduct of operational activities in cyberspace. This will be achieved by granting appropriate and unambiguous powers to special services to conduct activities regarding the identification, prevention, and combating of threats of a terrorist nature as well as the activities of foreign special services in cyberspace. To this end, the provisions of the Penal Code will also be appropriately amended.

The potential of special services to execute cybersecurity tasks, including combating cyberterrorism and cyberespionage, will be expanded through the development of organisational structures, and the necessary financial support will be allocated for the execution of new tasks.

A system will be developed to enable the effective preservation of content generated by individuals involved in terrorist activities who use internet messengers and other means of interpersonal communication. For this purpose, necessary legal amendments will be proposed, and cooperation with other states will be undertaken. This will constitute significant support for law enforcement agencies and services responsible for national security, enabling them to more effectively detect, monitor, and prevent terrorist threats in cyberspace.

Solutions will be developed to limit irregularities associated with the registration of SIM cards using incorrect or fictitious personal data. This will be achieved by increasing the effectiveness of identification data verification during the SIM card registration process, including the regulation of the resale market – such as on internet portals – and the secondary use of such SIM cards, along with the possibility of their blockage by the operator. The above measures will also contribute to more effectively combating other types of serious cybercrimes beyond cyberterrorism and cyberespionage.

Through various projects, the Polish scientific community will be engaged in the development and implementation of modern technological solutions for combating terrorism, as well as in the development of IT solutions supporting the detection of cyberespionage tools used by foreign special services – e.g. in end-user devices – which are intended to acquire information from Polish citizens, particularly those holding public office.

Concurrently, the growing importance of technology for Poland's strategic position makes scientific and research units and the high-tech industry particularly vulnerable to hybrid threats, including cyberespionage operations. Therefore, actions will be taken to raise the level of cybersecurity in the scientific and industrial sectors. In the digital dimension, the state will enhance the protection of intellectual property and protection against industrial and technological espionage, particularly

concerning new and disruptive technologies as well as technologies applied in the field of national security and defence.

Special services will continue activities aimed at acquiring information impacting security in its political, defence, and economic aspects. Actions will be conducted in cyberspace to acquire information about adversaries' network infrastructure in order to counter and minimise the effects of hostile activities in cyberspace directed against Polish institutions and private entities. An important aspect will also be the coordination of actions and information sharing with competent domestic and foreign partners.

In connection with cybersecurity threats, tasks related to analysing, identifying, and limiting the dissemination of propaganda and disinformation content targeting the Polish information space will be continued, and actions to prevent the dissemination of terrorist content on the internet will be carried out. Disinformation campaigns and information operations pose a threat to Polish society, the interests of Poland, and its position in the international arena. As needs in this area are identified, appropriate amendments to the law will be introduced. The execution of tasks in this area will be supported by other relevant branches of government administration to ensure appropriate practical knowledge, skills, and resources for executing new tasks. Furthermore, capabilities to detect the use of artificial intelligence mechanisms for creating text- and audiovisual-based disinformation messages will be increased.

## 6.6. Achieving capabilities to conduct a full spectrum of operations in cyberspace

Cyberspace is recognised as another domain, equal to the maritime, land, air, and space domains, in which operational activities can be conducted. This was reflected in the commitments undertaken by NATO member states in 2016 at the NATO summit in Warsaw, referred to as the Cyber Defence Pledge.[24)] Their main goal is to strengthen cyber resilience at the national level, which aligns with the direction of changes in the cybersecurity area of EU Member States. These commitments will continue to be implemented, taking into account recommendations resulting from the current assessment of the state of cybersecurity at the national level.

Poland's cyberspace is subjected to numerous adversary activities involving reconnaissance and attempts to breach security, leading up to the compromise of network and information systems of entities essential to national security and defence. Consequently, the SZRP and special services will continue to develop their capabilities regarding the proactive protection and active defence of cyberspace elements and resources, which is crucial for ensuring cybersecurity at the national level. Such an approach to pre-emptive defence will enable actions in cyberspace that prevent cyberattacks before they are even launched by disrupting hostile activities.

At the same time, the rules for using offensive cyber tools against today's communication tools, including interpersonal communication, will be precisely regulated, and the technical potential in this area will be developed.

New technologies (including artificial intelligence and quantum technologies) and the possibilities of using dual-use tools will be developed and implemented to expand the potential of the SZRP and special services in cyberspace. Priority will be given to technologies, solutions, and concepts aimed at

[24)] 1) Taking decisive action to strengthen the protection of the national ICT infrastructure;
2) Allocating the necessary funds for the organisation of cyber defence;
3) Strengthening cooperation between key national stakeholders in order to foster collaboration and the exchange of best practices;
4) Making efforts to improve understanding of the nature of cyber threats, including the exchange of experiences and information and the assessment of the situation;
5) Taking steps to raise awareness among the countries' key decision-makers responsible for national security regarding the fundamental principles that must be observed in cyberspace;
6) Placing greater emphasis on cybersecurity education;
7) Accelerating the implementation of national commitments to strengthen these cyber defence capabilities, on which the security of the entire Alliance depends.

identifying the techniques, tactics, and procedures employed by current and future adversaries, in order to counter their actions, limit their impact, and thereby neutralise their ability to achieve specific objectives in or through cyberspace. Systems enabling the execution of tasks related to monitoring and detecting cyber threats, as well as incident handling in systems used by the SZRP, special services, and cooperating entities, will be expanded. This will ensure both protection and timely disaster recovery, thereby providing adequate stability to the utilised digital space and increasing resilience against new threats.

Due to the changing security conditions in cyberspace, including the growing threat in the information and psychological domain – particularly the intensity of information operations targeting state defence – actions will be taken to enhance the capabilities of the SZRP and special services to identify, counter, and respond to such threats.

Actions aimed at developing the detection system and building a cyber threat intelligence sharing network will be continued, which will consequently significantly increase situational awareness in cyberspace.

The human resources potential of the SZRP and special services in the areas of IT, cybersecurity, and cryptology will be developed, particularly by adapting existing structures, creating new ones that respond to changing conditions in cyberspace, and conducting specialised training. Ultimately, actions will aim to build the MON's own capabilities to conduct a full spectrum of training in the aforementioned areas.

A comprehensive approach to the competence management process will be implemented, including defining competencies for professional roles and training, building strictly tailored training paths, and systematising the training process. As a complement to the competence management system, a competence validation and certification project will be developed. The verification of acquired knowledge and skills, as well as the teambuilding for cybersecurity personnel, will be conducted through specialised cybersecurity exercises at both the national and international levels. This will translate into the effective development of the competencies of military personnel, special services officers, and civilian employees of the MON, enabling them to achieve the capability to conduct comprehensive actions and operations in cyberspace.

# 7. Specific goal 3. Increasing the level of resilience of information systems in the public (including military) and private spheres

## 7.1. Increasing the level of resilience of information systems

Public procurement will incorporate cybersecurity requirements regarding ICT products, ICT services, and ICT processes, as well as the specifications of these requirements for the purposes of such procurement, including in terms of cybersecurity certification, the obligation to apply cryptographic mechanisms using generally recognised standards, and the use of cybersecurity products based on open-source software.

Solutions will be proposed to enable the rapid acquisition of cybersecurity-related services and products in urgent cases related to national security, while maintaining the transparency of the procurement process and defining a specific procedure for applying this type of process. This is particularly justified by the lengthy duration of procurement procedures compared to the need for rapid incident response. This will also encompass the possibility of urgently purchasing services and products related to combating cybercrime when there is a justified need for the rapid prevention, detection, or prosecution of the perpetrators of such a crime, and when the existing services or IT tools are insufficient.

Vulnerability management solutions will be introduced, including promoting and facilitating coordinated vulnerability disclosure.

Actions will be taken to enhance the cybersecurity of state systems and registries as well as digital public services, to ensure that citizens, entrepreneurs, and public administration have access to secure systems, registries, and services. The entities maintaining such systems, registries, and services will ensure 24/7 security monitoring by cybersecurity teams, continuously improve incident response capabilities, implement new technical, procedural, and systemic solutions, conduct periodic business continuity tests, and integrate cybersecurity aspects at the earliest possible stage of development and maintenance.

New legal provisions regulating various areas of social and economic life will incorporate Security by Design and Privacy by Design standards (including the use of biometrics and artificial intelligence systems), along with a corresponding impact assessment.

Protection against DDoS (Distributed Denial of Service) attacks – which involve overloading a server, network, or internet service by flooding it with an enormous number of requests – will be continued and expanded for entities performing public tasks and entities essential to national security.

The Plenipotentiary will actively issue recommendations and communications containing guidelines for National Cybersecurity System entities regarding detected vulnerabilities, cyberattacks, and campaigns in cyberspace, which will help minimise their impact.

Actions will be taken to support the private sector, including SMEs, in increasing digital resilience, particularly regarding supply chain security. Tools strengthening the basic level of cyber resilience and basic computer hygiene among SMEs will be developed through the cybersecurity certification of ICT processes at these enterprises. Support mechanisms will be created for projects aimed at implementing and applying standards and management systems that directly affect business continuity management, information security, and cybersecurity management standards.

Greater emphasis will be placed on the development of mechanisms and tools that primarily focus on incident prevention, rather than solely on detection and impact mitigation.

Actions will be implemented to maintain the general availability, integrity, and confidentiality of the public core of the open internet, including, where applicable, the cybersecurity of submarine communication cables. Cooperation will be developed within working groups at the NATO and EU forums, and in collaboration with NATO and EU institutions, to conduct, among other things, a consolidated assessment of risks, vulnerabilities, and dependencies, encompassing both the cybersecurity and physical security of the submarine cable infrastructure and its supply chains.

Efforts to raise the level of cybersecurity will also address the sensitive issues of industrial automation systems and Internet of Things (IoT) devices.

To ensure the cyber resilience of information systems, actions counteracting interference and spoofing in the electromagnetic spectrum will be implemented with regard to the cybersecurity of public administration entities, critical infrastructure, and other entities crucial to national security.

## 7.2. Development of national cryptology, including the migration to post-quantum cryptography and the development of quantum technologies

To increase the resilience of information systems, national cryptographic potential will be developed, addressing the challenges of post-quantum cryptography. This includes the capability to design and manufacture solutions based on cryptographic techniques, the capacity for risk assessment and operation in crisis situations, and a scientific and research base prepared to develop and validate cryptographic technologies independently of foreign organisations and institutions.

It is necessary to select and implement fundamental cryptographic components in areas such as electronic identification (eID) for natural and legal persons based on multi-factor identity sources and Self-Sovereign Identity (SSI) technologies, tools for pseudonymous authentication and identification, time-stamping tools not reliant on trust in the issuer, tools for end-to-end encryption, and tools for protecting data turnover by creating mechanisms to confirm the integrity and origin of documents – both digital and traditional – and their secure replication and distribution. These mechanisms should be accessible and easy to use for individuals with limited digital skills.

The trust system being built requires the identification and gradual elimination of single points of failure. Data distribution and replication are essential. This requires, among other things, the creation of secure cloud computing mechanisms, including the migration of key data to cloud resources under the effective control of domestic entities. It is necessary to create a distributed trust ecosystem that can easily incorporate data held by multiple independent entities.

Mechanisms increasing the accountability of operations performed on data will be built. This applies in particular to the development of available mechanisms such as distributed ledger technology (DLT), as well as the development and widespread application of techniques such as electronic signatures, electronic seals, and electronic registered delivery services.

In the face of advancing cryptanalytic techniques, particularly quantum cryptanalysis, the development of hostile cryptography capabilities, and the possibility of embedding hostile components in hardware and software products, techniques will be developed to limit the effectiveness of attacks through alternative safeguards that at least allow for the detection of data resulting from an attack. New cryptographic standards and algorithms adopted by foreign bodies will be evaluated regarding the method of their implementation in Poland.

To develop national technological and industrial competencies, research and development projects and programmes in the field of cryptographic technologies will be established, encompassing new technologies like post-quantum cryptography and new communication techniques (including quantum key distribution (QKD) solutions), but also focusing on technologies useful in emergencies, such as natural disasters, terrorist attacks, or economic blockades. Poland's cybersecurity will be strengthened by utilising the potential of domestic entities, including special services. Mechanisms for civil-military cooperation and the involvement of Polish industry and academia in the development of cryptography and cryptanalysis will be expanded. To this end, Poland will also actively engage in the international arena, including at the EU and NATO forums, and bilaterally with key partners, while retaining full control and sovereignty over cryptography used for national security purposes.

## 7.3. Cloud computing services for strengthening the resilience of information systems

To increase the resilience of information systems and the digital development of government administration, actions will be taken regarding the development of cloud computing services. The currently applicable Resolution No. 97 of the Council of Ministers of 11 September 2019 on the

"Common State IT Infrastructure"[25] Initiative (WIIP Initiative), which regulates the use of cloud computing services by government administration entities, has been amended[26] so that as many entities as possible can use services in the Public Computing Cloud. This is immensely important from the perspective of national security, data security, and building a state based on the *Cloud First* approach. In connection with the amendment to the WIIP Initiative, an update will be prepared for the Cloud Computing Cybersecurity Standards, determined by the minister responsible for computerisation in agreement with the minister responsible for internal affairs, the Minister of National Defence, and the Minister Coordinator of Special Services (MKSS).

Ultimately, it is planned that the Council of Ministers resolution concerning the WIIP Initiative will be replaced by an act that comprehensively regulates the use of cloud computing services by public administration. Ensuring effective regulations that permit data processing in cloud computing is a priority for a modern digital state, drawing on international experiences based on the geopolitical situation and taking into account the direction chosen in this regard by other EU Member States and beyond.

Introducing uniform, high standards for the protection of ICT systems and supporting public administration entities in maintaining these systems and acquiring the services necessary for their construction, development, and maintenance will contribute to ensuring a high level of services provided to society by public administration. The WIIP Initiative assumes the optimisation of existing ICT resources and applications in public administration by delivering modern and cost-effective IT technologies. The adopted cloud computing model can significantly assist offices struggling with the need to rapidly deliver highly reliable, innovative services using existing resources and cooperating with the private sector. Necessary changes will be made to the WIIP Initiative to increase the level of cybersecurity and adapt to new technological solutions, including broader possibilities for using cloud solutions.

A separate cloud for processing classified information (classified cloud), protected by domestic cryptographic solutions, will also be established to streamline access to data and software for entities executing tasks in the area of national security and defence. This will increase the resilience of information systems used by these entities and streamline the exchange of classified information between them. For this purpose, appropriate legislative changes will be introduced, encompassing rules, regulations, and restrictions that will ensure adequate security of processed information and mandate their strict application by all entities and authorities executing tasks related to the protection of classified information. All actions related to the creation of the classified cloud will stem from decisions made by the national security authority and will account for the needs of all units covered by this service. For national security reasons, all data repositories (including infrastructure) stored in the classified cloud will be the property of Poland. Furthermore, the classified cloud will be organised in a manner that precludes dependence on a single provider.

Based on experiences from recent armed conflicts, IT systems built by the state will be developed and modified under the premise of ensuring security and maintaining continuous access to data in the event of a significant threat to national security or war. The "Plan for the Migration of Key IT Systems of Poland in the Event of a Crisis or War" will be developed, incorporating rules for the secure and, above all, confidential processing of data in cloud solutions.

## 7.4. Development of capabilities for the effective prevention of and response to cybersecurity incidents

Mechanisms for coordinating the National Cybersecurity System and the proper management of the entire system will be developed and streamlined. In this regard, undertakings will be carried out concerning the Government Plenipotentiary for Cybersecurity, as well as within the Joint Cybersecurity

[25] M.P. of 2021, item 1006, and of 2024, item 908.

[26] Resolution No. 127 of the Council of Ministers of 23 October 2024 amending the resolution on the "Common State IT Infrastructure" Initiative (M.P., item 908).

Operations Centre (PCOC). Actions will be implemented to increase the operational capabilities of institutions responsible for ensuring cybersecurity at the national level, and initiatives raising the resilience of National Cybersecurity System entities – including their potential for preventing and responding to cybersecurity incidents – will be supported. Efforts in this area will encompass, among other things, measures for cyber threat intelligence, the development of protection against DDoS attacks, and software and hardware solutions enhancing cybersecurity. Some of these initiatives will be executed centrally by the Plenipotentiary – the office supporting the minister responsible for computerisation – for the benefit of National Cybersecurity System entities, which will allow for a more effective and cost-efficient provision of necessary resources. Common consolidated cybersecurity systems will be built for the needs of the entire public administration.

Appropriate legal regulations regarding the use of active defence in cyberspace will be proposed, and operational capabilities in this regard will be developed. Threats from adversary states and criminal groups, frequently linked to the institutions of hostile states, necessitate actions referred to as active defence. To this end, regulations will be introduced enabling selected public National Cybersecurity System entities to have the authority, as part of incident handling, to block attackers' network traffic, e.g., by temporarily restricting this traffic from IP addresses or URLs, domains, and autonomous systems identified as the cause of the incident. These actions will make it possible to reduce damage caused by cyberattacks by providing tools and services and applying appropriate tactics to hinder and prevent the execution of cyberattacks.

The operational capabilities development of National Cybersecurity System entities will be enhanced by the use of new and disruptive technologies, in particular artificial intelligence, post-quantum cryptography, blockchain technology, large database management systems, new communication networks and means, and cloud computing solutions. However, in the hardware dimension, the development of operational capabilities will be supported by the use of advanced microelectronics, in particular through investments in developing the capacity of the national technological and industrial base, including through research and development (R&D) activities, so that it can effectively meet the needs of the most important state institutions responsible for cybersecurity and the private sector. For this purpose, Poland will utilise the opportunities created by international cooperation (bilateral as well as at the EU and NATO forums).

## 7.5. Development of standardisation in cybersecurity

A national centre responsible for standardisation in cybersecurity will be established. Through it, a continuous process of monitoring and analysing the applicability of standards and normative documents (European and international) will be implemented. The current state of the National Cybersecurity Standards issued by the Ministry of Digital Affairs – which constitute a set of recommendations standardising security solutions in network and information systems used by National Cybersecurity System entities – along with framework and industry recommendations, including recommendations for National Cybersecurity System entities, will be reviewed and analysed. An initiative will be undertaken to collect, analyse, and systematise recommendations regarding the application of norms, standards, and technical regulations, as well as other documents of a normative or directive nature, such as recommendations and guidelines. Based on the analysis, a decision will be made regarding the further development of national standardisation norms. Actions will be taken to provide formal and legal bases for implementing the recommendations within National Cybersecurity System entities. Financial resources will be secured to ensure adequate resources for the implementation of the aforementioned recommendations.

To ensure secure and cost-optimal processing infrastructure for public sector ICT/OT systems that utilise new forms of information processing and storage – including through the use of cloud computing services – actions will be continued regarding the preparation of recommendations and the promotion of best practices, including the certification of sensitive systems and devices, increasing resilience to cyber threats. Recommendations related to the most important aspects of cybersecurity, presented in a brief and universally understandable format, will provide the necessary knowledge on basic computer hygiene practices and cybersecurity standards to a wide range of internet users, including

recommendations incorporating Security by Design and Privacy by Design, and cybersecurity and data protection by default.

## 7.6. Public-private partnership in the area of cybersecurity

Cooperation in the area of cybersecurity with the private sector will be continued under the Cybersecurity Cooperation Programme (PWCyber) for the benefit of the National Cybersecurity System, which has been running since 2019. The cooperation under the programme is public, transparent, and non-financial. The partnership programme is open to all organisations, including NGOs, that wish to contribute to the development of Poland's cybersecurity system. A key area of cooperation within the partnership is increasing the competencies of National Cybersecurity System entities in terms of awareness of threats, attack methods in cyberspace, and the legal, organisational, and technical skills to counter threats in ICT systems and networks, as well as the sharing of cyber threat intelligence.

# 8. Specific goal 4. Increasing the potential of the national technological and industrial base and strengthening the technological sovereignty of the Republic of Poland in the area of cybersecurity

## 8.1. Strengthening supply chain security at the national and international levels

The COVID-19 pandemic, trade and technological wars between superpowers, and the repercussions of the Russian Federation's armed aggression against Ukraine have demonstrated the importance of economic resilience to global turmoil and the necessity of possessing technological independence in critical areas and the ability to ensure secure supply chains. The instability of the global political and economic system is linked, among other things, to the aggressive policy of the Russian Federation and the risk of conflict in Southeast Asia, which is of critical importance to the global economy, particularly regarding semiconductors and electronic components.

Actions will be taken to increase the security of supply chains at the national and international levels, including through the use of cybersecurity certification. This will encompass both hardware and software dimensions. Organisational and formal initiatives will be implemented to create a favourable environment for this type of business activity in Poland, and expenditures on research and development and the construction of industrial production potential will be significantly increased.

Large-scale investments from allied and partner states will be supported. This is of fundamental importance in the economic dimension and for strengthening relations with allies, although it is of limited significance when it comes to building domestic technological potential and sovereignty in this regard. Consequently, investments will be made in national, sovereign technological and industrial capabilities concerning, among other things, semiconductors and modern hardware and software, IT, and cryptographic technologies, with particular emphasis on the needs of national security and defence. This will also contribute to increasing the sovereignty of the EU. Only by fully controlling hardware and software technology can security in the infrastructural and application layers of ICT systems be ensured, which will be achieved by introducing the obligation to use certified products for this type of equipment.

To increase supply chain resilience and strengthen national technological potential, the deployment of prototype cybersecurity technologies developed by domestic producers will be supported. These actions will include, among other things, procurement facilitations in public procurement, pilot deployments in public institutions, and certification support. Implementing such mechanisms will enable the practical verification of the effectiveness of solutions, accelerate their commercialisation, and increase the share of Polish technologies in the national cybersecurity ecosystem.

Given the growing importance of open-source software in Poland's digital infrastructure, initiatives ensuring national technical support, development, and maintenance of key open-source components used in public administration systems and by National Cybersecurity System entities will be supported. Strengthening the national open-source software base will contribute to increasing Poland's technological independence and the resilience of the supply chain to external threats.

An important element in ensuring security and quality in the supply chain is the evaluation and certification of products (in particular software, devices, and services) and processes. The National Cybersecurity Certification Scheme enables the establishment of the procedures necessary to ensure the proper conduct of certification processes and the definition of the methods for supervising and monitoring compliance with the provisions of the Act.

To increase the National Cybersecurity System resilience and support the development of national technological competencies, the use of prototypes of national cybersecurity technologies by entities covered by the Act on the National Cybersecurity Certification Scheme will be promoted. Such an approach will enable the testing and improvement of solutions in a real operational environment, simultaneously supporting the development of the domestic cybersecurity market.

The cybersecurity of ICT systems as well as devices and components used in individual sectors of the National Cybersecurity System will be strengthened. Competent

authorities and sectoral CSIRTs, in cooperation with other National Cybersecurity System entities, will develop recommendations aimed at strengthening cybersecurity, including regarding cybersecurity requirements to be met by devices and software applied in modern systems used in individual sectors. In particular, this would apply to new ICT and OT devices (including new smart technologies, such as new types of energy sources and technologies utilising artificial intelligence algorithms) that are to become part of technological systems used in the sector.

Thanks to the enactment of the Act on the National Cybersecurity Certification Scheme, this scheme will support the processes of issuing cybersecurity certificates under European cybersecurity certification schemes, which will be recognised throughout the EU. Conformity assessment bodies and certified ICT products, ICT services, and ICT processes will be subject to supervision by the national cybersecurity certification authority, which will be the minister responsible for computerisation. As part of this supervision, it will be possible to conduct independent testing of products to determine whether they consistently meet the requirements contained in the certification scheme. Thanks to such certificates, essential entities and important entities will be able to ensure the selection of appropriate products and services that provide a level of cybersecurity suitable for a given application. At the same time, the Act on the National Cybersecurity Certification Scheme creates the foundations for creating national cybersecurity certification schemes, enabling the promotion of cybersecure solutions in areas not covered by European certification schemes. Moreover, these will also support the use of secure solutions in areas deemed important by the minister responsible for computerisation and other competent authorities.

To ensure the effectiveness of the cybersecurity certification scheme, capabilities for certification and conducting security assessments will be developed, respectively, in certification bodies and testing laboratories located in state research institutes. The first step in this area will be adapting current certification schemes to the EU Common Criteria-based Cybersecurity Certification Scheme (EUCC). Subsequently, the capability for certification under further European and national cybersecurity certification schemes will be developed, including EUCS (European Cybersecurity Certification Scheme for Cloud Services) and EU5G (European Cybersecurity Certification Scheme for 5G).

Certification is an essential element of ensuring a secure supply chain, including mitigating the risk of installing "backdoors", particularly with regard to equipment used for the purposes of national security and defence, critical infrastructure, as well as essential and important entities. At the same time, an instrument enabling the exclusion of ICT products, types of ICT services, or specific ICT processes originating from a high-risk supplier is also necessary, based on strictly defined criteria and when justified reasons arise. An appropriate legal mechanism allowing for the designation of a specific supplier of hardware or software to particular types of economic and social entities as a high-risk supplier will be introduced into the national legal system through an amendment to the Act on the National Cybersecurity System. This solution will make it possible to ensure national security with regard to the protection of vital state interests.

Addressing the risk arising from a given entity's supply chain and its relations with suppliers is particularly important due to the frequency of incidents in which entities fall victim to cyberattacks, and attackers are able to compromise the entity's network and information systems by exploiting vulnerabilities present in the products and services of third parties (including SMEs). All essential and important entities will have to incorporate the issue of supply chain security within their information security management systems. Therefore, tools will be developed to support essential and important entities, both public and private, in executing these obligations.

To mitigate the risk associated with the use of ICT components originating from high-risk suppliers, mechanisms for assessing the security of products and services throughout the entire supply chain will be developed. In particular, the application of national and European cybersecurity certification schemes will be supported, as well as the development of tools for analysing the origin, integrity, and vulnerabilities of hardware and software components. These actions will enable informed purchasing decisions by public and private entities and increase the transparency and security of Poland's digital infrastructure.

The Plenipotentiary's recommendation mechanism will also be more widely used, including regarding the necessity of updating or excluding software with identified vulnerabilities. Actions will be taken to ensure the proper and most effective application in the Polish legal order of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).[27] This will make it possible to establish standards regarding cybersecurity rules for internet-connected devices, particularly in the area of the Internet of Things (IoT). Manufacturers of hardware and software will be required to meet a number of key requirements, including:

1) ensuring that potential vulnerabilities to threats are effectively removed throughout the expected usage period of the product or for 5 years from its placement on the market;
2) promptly reporting (within 24 hours) identified product or service defects to the European Union Agency for Cybersecurity (ENISA);
3) incorporating cybersecurity principles at the design stage of goods and services.

The issue relating to the use of cybersecurity certificates in public procurement will be regulated. There are numerous certificates present on the market, the value of which can differ diametrically. For this reason, the Act on the National Cybersecurity Certification Scheme enables the distinction of specific certificates in this process, e.g., certificates issued under the European cybersecurity certification scheme EUCC or certificates issued under other European cybersecurity certification schemes, in particular by introducing an obligation to possess this type of certificate when executing a specific category of purchases for National Cybersecurity System entities.

One vital element of strengthening technological sovereignty will be the implementation of a conformity assessment system for radio equipment against essential cybersecurity requirements specified in Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC[28] (RED Directive), so as to ensure that domestic manufacturers can compete on the EU market.

## 8.2. Stimulating research, development, and innovation in the area of cybersecurity

The development of Polish industrial, technological, and scientific potential in the field of cybersecurity will be supported and stimulated, including with the participation of State Treasury companies. Research, development, and innovation programmes and projects in the field of cybersecurity will be executed, which will make it possible to build national technological and industrial competencies and increase the technological and digital sovereignty of the country while also contributing to increasing the sovereignty of the EU. The National Centre for Research and Development (NCBR) will serve as the main vehicle for executing R&D; however, activities in this area may also be carried out in other formats, including within individual ministries. Financing for R&D projects in the field of cybersecurity will also be increased, including for the execution of classified projects.

To ensure cyber sovereignty and stimulate the development of the cybersecurity sector, work will be conducted to create Polish cybersecurity solutions – both in terms of hardware and software. Efforts on creating a national industrial cybersecurity potential will be intensified, enabling, among other things, the creation of microprocessors and other types of integrated circuits, memory modules, microcontrollers, cryptographic chips for programmable network devices, and machine learning algorithms, which will ensure the continued maintenance and development of technologies key to cybersecurity and state sovereignty in the event of a technological blockade.

[27] OJ EU L 2024/2847, 20.11.2024, OJ EU L 2025/327, 05.03.2025, OJ EU L 2025/90555, 02.07.2025 and OJ EU L 2025/90828, 17.10.2025.

[28] OJ EU L 153, 22.05.2014, p. 62, OJ EU L 212, 22.08.2018, p. 1, OJ EU L 315, 07.12.2022, p. 30, OJ EU L 223, 11.09.2023, p. 1, OJ EU L 2024/2839, 07.11.2024 and OJ EU L 2024/2749, 08.11.2024.

For the purposes of cybersecurity, investments will be made in the further development of disruptive technologies, including artificial intelligence, quantum technologies, blockchain technology, cloud computing, large database systems, new generation networks and communication means (including 5G and 6G), and IoT.

The organisation of cooperation between institutions responsible for national security and scientific and R&D units, organisations commercialising the results of scientific research and development work, and analytical centres will focus on the direct utilisation of disruptive technologies for cybersecurity, including by National Cybersecurity System entities.

Solutions for the needs of cybersecurity will be developed within the national innovation system. Polish start-ups from the cybersecurity sector will also be supported in various forms. Technology parks, technology accelerators, Digital Innovation Hubs, and financial support mechanisms, including venture capital funds, will be utilised, which will enable support for the development of native start-ups operating in the cybersecurity area and ensure protection against their takeover by foreign capital, particularly from states that are deemed hostile. Actions supporting the stimulation of development and innovation in cybersecurity will encompass initiatives such as hackathons, technological challenges, competitions, or bug bounty initiatives. Support will encompass the research and implementation of disruptive technologies and new algorithms in the field of cybersecurity, which can build the presence of Polish entrepreneurs in global markets for new cybersecurity products. Stimulating innovation will only be effective if it is accepted that some projects will not achieve their intended objectives. Supporting actions will take into account the significant risks associated with the creation of innovative technologies.

The promotion of the cybersecurity sector will be conducted to create new development opportunities for Polish companies from this sector.

In their activities, public institutions and State Treasury companies, within legally permitted forms – including while respecting the rules of the EU internal market – will primarily use the cybersecurity solutions of Polish companies, provided they are competitive and meet the contracting authority's requirements. This will make it possible to build strong brands and a robust cybersecurity sector in Poland, support the foreign expansion of Polish cybersecurity enterprises, as well as translate into strengthening Poland's sovereignty regarding technology and strategic decision-making autonomy. Further, this will contribute to gaining independence from major foreign tech corporations. Concurrently, actions will be undertaken to attract foreign investments related to cybersecurity to Poland.

For the purposes of developing national potential in the cybersecurity area, the participation of Polish industrial and scientific-research entities in international research, development, and innovation programmes regarding cybersecurity will be supported, in particular within the EU and NATO (in the field of digitalisation, security, and defence), and actions will be undertaken to utilise the results of these initiatives for national cybersecurity.

The activities of the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) along with the network of National Coordination Centres (including the Polish National Cybersecurity Competence Centre (NCC-PL)) will carry out actions to increase the EU's technological sovereignty through joint investments in strategic cybersecurity projects, which will positively contribute to maintaining research excellence and strengthening the competitiveness of EU industry in this field.

Within the framework of the NCC-PL's activities, a Competence Community is being created – a large, open, interdisciplinary, and diverse group of European stakeholders involved in the development of cybersecurity, as referred to in Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.[29)] The Competence Community comprises stakeholders conducting scientific research, representing industry, business, academia, and the public sector, who are intended to contribute to maintaining and developing the technological and

[29)]OJ EU L 202, 08.06.2021, p. 1.

industrial capabilities in the field of cybersecurity, which are necessary to secure the EU's Digital Single Market. This will strengthen the capabilities of Poland and the EU. Moreover, this will also be a response to the challenges facing Europe in the area of cybersecurity thanks to cross-border and cross-sectoral cooperation among entities possessing specialised cybersecurity knowledge.

# 9. Specific goal 5. Building the awareness, knowledge, and competencies of the staff of the National Cybersecurity System entities, as well as of citizens and entrepreneurs

## 9.1. Increasing awareness and knowledge, and strengthening the competencies of the staff of the National Cybersecurity System entities

It is necessary to undertake and continue actions aimed at increasing the awareness and knowledge, and strengthening the competencies of the personnel of National Cybersecurity System entities. Training initiatives will be conducted for entities of the National Cybersecurity System, including within the framework of PWCyber. The training courses will ensure an increase in the digital competence in the area of cybersecurity among the personnel of National Cybersecurity System entities and will increase the awareness and culture of cybersecurity as an integral element of functioning in a digital reality. The training initiatives will raise the level of knowledge and skills of the participants in both general and specialised dimensions, which is crucial for effectively countering cyber threats. The training activities will also cover international legal implications with regard to operations in cyberspace.

Public administration, as one of the pillars of the National Cybersecurity System, requires a constant increase in the awareness of cyber threats. Therefore, digital hygiene training will be organised for public administration personnel, aimed at increasing their knowledge about threats and ways to avoid them, which is essential in the context of securing public information. Preventive and educational activities will also be implemented, directed at top state officials, including parliamentarians and persons holding senior public office, in order to ensure an appropriate level of protection at the highest levels of government.

It is equally important to raise knowledge and awareness among local administration personnel, as it is often at the local level that the first contact with cyber threats occurs. For this reason, educational projects and undertakings will be organised, aimed at increasing their competencies in the field of cybersecurity. In the case of representatives of the executive and legislative branches, as well as LGUs, it is assumed that preventive and educational activities in the field of cybersecurity will be continued, as part of the SecureV project, which concerns cybersecurity training for the most important persons in the state and building competence in the scope of creating a cybersecurity culture in LGUs. This project will be expanded to include, among other things, subsequent groups of recipients to increase the Republic of Poland's resilience to cyberspace threats.

The efforts to raise the awareness of cyber threats will concern not only educational and training activities, but will also encompass simulated social engineering tests, which may be supported by National Cybersecurity System entities for the benefit of interested public sector units and enterprises.

In parallel to training courses intended for a broad audience, including primarily National Cybersecurity System entities, a system for the certification of competence will be developed – along with training courses preparing for this certification – intended also for the management personnel of essential entities and important entities. At the same time, a certification programme will be prepared for employees of public administration and LGUs.

One of the measures contributing to these objectives will also be the establishment of a cybersecurity competence certification scheme, designed to assess the knowledge and skills of those carrying out cybersecurity tasks, particularly within public sector organisations.

To limit the outflow of cybersecurity specialists from the public sector, solutions that ensure competitive remuneration in relation to the private sector and specialised training will be maintained. As part of the implementation of this objective, the Act of 2 December 2021 on the special rules of remunerating

persons performing tasks in the field of cybersecurity was introduced into the Polish legal system.[30] Its main objective is to support actions aimed at ensuring the protection of ICT systems against cyber threats by financing ICT allowances, which are supplements to remuneration for work, and in the case of officers and professional soldiers, a monetary allowance. However, to limit the discretionary nature of the ICT allowance financed from the Cybersecurity Fund, work will be undertaken to modify the formula of this Fund.

Close cooperation will be conducted in this area with the ECCC, ENISA, and other EU institutions, bodies, and agencies in connection with the activities conducted by these entities to strengthen and develop competence among personnel handling cybersecurity tasks.

## 9.2. Developing the cybersecurity awareness and knowledge of citizens and entrepreneurs

In the face of the dynamically changing situation in cyberspace and the growing number of threats, it is vital to raise competence in the field of cybersecurity among all internet users. Activities will be implemented in the scope of education and cybersecurity training, raising skills and awareness in the field of cybersecurity – including good practices and digital hygiene – as well as issues of online privacy and personal data protection. Social campaigns aimed at increasing the awareness of cyber threats and promoting secure digital practices are essential to reach the widest possible audience. Educational activities will be tailored to various groups of internet users, taking into account their specific characteristics.

Education in this area must begin already at the early childhood education stage; therefore, educational programmes in schools will include education in the field of cybersecurity, including online privacy and personal data protection, in an appropriately adapted format. Computer science curricula in primary and secondary schools will be modified so that they incorporate the basic principles of prevention and response to various types of cyber threats.

Cybersecurity education will also be provided through the introduction of a new vocational qualification within the vocational education system, i.e. that of cybersecurity technician. A cybersecurity technician will be responsible for the protection of information systems, computer networks, as well as services and applications, against digital threats. Their task will be to ensure the confidentiality, integrity, and availability of data, as well as the business continuity of information systems in public and private organisations.

Additional educational projects will also be implemented, directed at children and youth, as well as teachers, educators, psychologists, parents, and guardians, with particular emphasis on current trends that threaten children and youth, as these projects play a crucial role in preparing children for safe participation in the digital world. Information on cybersecurity will also be provided to young people taking part in the digital skills assessment carried out by job centres.

Academic education in the field of cybersecurity will be strengthened, which will provide future specialists with solid theoretical and practical foundations. Academic and research institutions will receive support in developing, improving, and propagating the introduction of tools in the field of cybersecurity and secure network infrastructure. In academic education, National Cybersecurity System entities will use their knowledge and experience to help raise awareness of cyber resilience through lectures that highlight the real-world and practical challenges students face in this area in their personal, academic and future professional lives. The potential of research and development units will be supported so that they can more effectively develop new technologies, commercialise them, and cooperate efficiently with enterprises.

Awareness and education campaigns will also be aimed at the elderly, who need to be made more aware of issues relating to various types of online fraud, including the theft of sensitive data (known as "phishing"), impersonating trusted entities (known as "spoofing"), and which will also make senior

[30] Dz.U. /Journal of Laws/ of 2024, item 1662, of 2025, item 1017 and of 2026, item 252.

citizens more aware of the social engineering techniques and manipulations used by fraudsters. In this regard, educational campaigns taking into account the needs of persons with disabilities will also be implemented. The educational campaigns will be tailored to the specific characteristics of individual target groups (including youth, seniors, persons with disabilities, and entrepreneurs) and will take into account the requirements of communication accessibility for persons with special needs.

Activities supporting the development of personnel in Polish cybersecurity companies will be implemented as well. Campaigns will be launched to reach Polish businesses and their employees, raising awareness of cybersecurity technologies. The planned result of the campaigns will be the raising of cybersecurity competence among entrepreneurs. Activities directed at SMEs will be divided into multiple layers and will concern the problems of both microenterprises as well as small and medium-sized enterprises. Digital services will also be prepared, aiming to verify the level of digital maturity and cybersecurity for SMEs, to support producers of information technologies (IT) in implementing the requirements arising from the Cybersecurity Act, and to assess whether a company's operations are subject to NIS2 regulations, which will be implemented by the amendment to the Act on the National Cybersecurity System.

Activities strengthening cybersecurity and promoting digital hygiene among enterprises will be conducted. Existing cybersecurity certification schemes, including the "Digitally Secure Company" scheme, will be expanded. These schemes aim to enhance the level of protection within the small and medium-sized enterprise sector, improve the stability of the country's economic activity, and promote and implement a new cybersecurity standard within companies. Educational campaigns aimed at increasing the level of awareness of Polish enterprises on the subject of cybersecurity will also be conducted. Activities in this area will also be supported by the development of degree programmes at higher education institutions, forms of public-private partnership, the development of Information Sharing and Analysis Centres and cybersecurity competence centres, and cooperation with secondary schools, with a view to sparking young people's interest in the potential of the cybersecurity sector. The cybersecurity knowledge base available on the government portal – gov.pl – will be continuously expanded, offering support and information on cybersecurity, thereby enabling internet users to quickly access the educational resources they need. The implementation of these initiatives is essential in order to effectively build competence, knowledge, and awareness of threats and challenges in cyberspace, which is crucial for the security of the entire country. As part of efforts to expand the cybersecurity knowledge base on the gov.pl portal, information relating to cybersecurity will be published, including warnings about current threats, guides, recommendations, and cybersecurity standards. Furthermore, information about ongoing online training courses, together with the possibility of registering for them, will also be posted there.

# 10. Specific goal 6. Strengthening the Republic of Poland's solid international standing in the field of cybersecurity

## 10.1. Active international cooperation at the strategic, political, and legal levels

Since cyberspace is an area of strategic competition, the threat to security and defence increases during times of deepening geopolitical tensions and a growing reliance on digital technologies. The significant deterioration of the security situation, both globally and within Europe, the growing scale of cyber attacks from hostile states, state-sponsored actors (APTs) and hacktivist and international cybercriminal groups, as well as hybrid warfare and terrorist incidents in cyberspace, make international cooperation – especially among allied states and those sharing similar values – more important than ever before.

Partners sharing common values play a significant role in maintaining a global, open, stable, and secure cyberspace, and can increase the capacity of Poland, NATO, and the EU to counter, deter, prevent, and respond to malicious cyber activities. Poland remains open to extensive, ambitious, and mutually beneficial cooperation in the area of security and defence, including cyber defence. Further, Poland will participate in efforts aimed at redefining the standards of international law – both the law of war and the law of armed conflicts – for the new domain of warfare that cyberspace has become, or the creation of new conventional norms in this area. It will strive to increase the Polish presence in international structures, including international military structures.

The EU and its Member States must further strengthen their cyber resilience and enhance common cybersecurity and cyber defence against malicious cyber activities. Poland will actively participate in the EU's efforts to raise the level of cybersecurity in Europe, in particular in the legislative dimension. Within the framework of NATO, Poland will undertake activities serving to strengthen the defence capabilities, effectiveness, and cohesion of the Alliance, particularly in the areas of collective defence and cyber deterrence. Moreover, cooperation with international organisations will be intensified in order to strengthen international security and stability in cyberspace, as well as to promote compliance with international law, including the protection of human rights and fundamental freedoms in cyberspace. Poland will also engage in digital security efforts within the framework of work conducted at the United Nations (UN), the Organisation for Security and Cooperation in Europe (OSCE), the Organisation for Economic Cooperation and Development (OECD), and other international organisations and formats of international cooperation.

Further, Poland will work to promote cybersecurity through multilateral and bilateral cooperation. Particularly important partners will include the United States of America, the United Kingdom, other non-European states sharing common values regarding cybersecurity, and the EU Member States, as well as candidate countries to the EU (including Ukraine). Poland will strive to establish tailor-made partnerships in the area of cybersecurity, provided they bring mutual benefits to the partners. In order to enhance our deterrence capabilities by ensuring a strong common response of the international community to cyber attacks, Poland will actively seek opportunities – through diplomatic activities – to strengthen the international coordination of joint actions, including collective attribution and sanctions.

Poland will also cooperate to promote compliance with international law in cyberspace. In particular, it will participate in discussions relevant from the perspective of international law in the forums of the UN, OSCE, NATO, and the EU. It will also engage in the exchange of views on the relationship between international law and cyberspace by publicly presenting its position and through bilateral dialogue with other states.

Together with its partners at the international level, Poland will continue to support Ukraine, including within the framework of dialogue on cyberspace issues. Taking into account Ukraine's experience in building capacity in cyber resilience and cyber defence, exchanging best practices in the field of cyber defence, including cyber threat intelligence and situational awareness, as well as exchanging information on significant policy developments, is in the common interest of Ukraine and Poland, and therefore will be continued and expanded.

Support will be provided to strengthen the international standing of Polish companies in the cybersecurity sector. Activities will be conducted to enhance their export potential, and the cybersecurity solutions of Polish companies will be promoted internationally.

Strengthening of the international position of Poland will only be possible through close internal cooperation between the institutions and agencies responsible for ensuring cybersecurity in Poland, particularly between the minister responsible for computerisation and the minister responsible for foreign affairs, who oversees Poland's overall foreign policy.

Additionally, significant investments in increasing cyber resilience and deploying full-spectrum cyber defence capabilities – both individual and joint at the EU level – are vital. In this context, EU cooperation frameworks and financial incentives, as well as the introduction of common standards and mutual recognition of certified devices, can be of crucial importance.

National experts will continue to actively participate in discussions held in forums and within regional and global initiatives, and will also aspire to hold key roles in international organisations, thereby contributing to the effective implementation of foreign policy regarding cybersecurity.

Building cyber resilience is a global challenge. By engaging in the initiatives of international organisations and conducting bilateral activities, Poland will contribute to strengthening the capabilities of partners whom it will be cooperating with in pursuit of its foreign policy objectives.

## 10.2. Active international cooperation at the operational and technical levels

International cooperation at the operational and technical level will be implemented, including within the framework of NATO, ENISA, the CSIRT Network (Article 15 of the NIS Directive), and the INHOPE and INSAFE Association at the EU level, as well as in other information sharing and cooperation forums, such as the FIRST network or TF-CSIRT, which bring together CSIRTs, the TF-CSIRT Forum, information sharing platforms such as the MISP threat intelligence sharing platform or n6, and within the framework of bilateral and multilateral cooperation. It is essential for effective international cooperation at the operational and technical levels that all national CSIRTs actively participate in the work of the CSIRT Network. Ultimately, as part of the European Cybersecurity Alert System referred to in the Cyber Solidarity Act, the NCH will be established. The next step will be its cooperation with selected NCHs in at least 3 other Member States in the form of a Cross Border Cyber Hub.

Poland will actively participate in exercises conducted by EU, NATO, and other international entities, as well as organise specialised cybersecurity training and exercises in the international dimension. This will enable, among other things, the verification of knowledge and acquired skills, as well as the strengthening of the interoperability of cybersecurity teams and cyber forces.

Efforts to enhance international cooperation will also continue through the participation of public bodies involved in ensuring cybersecurity in official international forums for the exchange of information on threats and vulnerabilities, as well as within international standardisation bodies responsible for developing and publishing cybersecurity standards.

The enhancement of international cooperation in the field of cybersecurity will take place at the level of the relevant state authorities and through the bilateral communication channels they maintain with NATO partner services.

Poland will engage in European initiatives to increase cybersecurity by protecting the new technology industry and ensuring its sovereign competitiveness in breakthrough technologies in the regional and global dimension. These joint European initiatives already include quantum technologies with applications in cybersecurity.

International cooperation at the operational and technical level will also cover the expansion and support of international scientific and research and development cooperation in the area of cybersecurity.

## 10.3. Coordination of international activities related to civil-military cooperation in the field of cybersecurity

The Government Plenipotentiary for Cybersecurity, executing their statutory tasks of coordinating activities and implementing government policy on ensuring cybersecurity, will manage Poland's activities in the international arena regarding civil-military cooperation in the area of cybersecurity, in agreement with the minister responsible for computerisation, the minister responsible for foreign affairs, and the Minister of National Defence, as well as other government administration bodies within the scope of their competence. This will enhance the effectiveness of international relations and ensure that cybersecurity activities undertaken within both military and civilian contexts are properly coordinated, thereby enabling the more effective pursuit of national strategic objectives.

## 11. Management of the Cybersecurity Strategy of the Republic of Poland

The Strategy is adopted by the Council of Ministers by way of a resolution for 5 years.

The minister responsible for computerisation is the Coordinator of the Strategy's implementation.

Two years after its adoption and in the fourth year of its validity, the Strategy is subject to a review and an evaluation of its impact The results of the review are presented to the Council of Ministers. Following the review, the minister responsible for computerisation develops a proposal for corrective actions or a draft document for the next five-year period. In justified circumstances, the Strategy may be updated at times other than those referred to above.

The Action Plan for the implementation of the Cybersecurity Strategy of the Republic of Poland (Action Plan) constitutes an annex to the Strategy. The Action Plan sets out the tasks of the Coordinator, members of the Council of Ministers, heads of central offices, the director of the Government Centre for Security (RCB), and other cybersecurity authorities defined in the Act on the National Cybersecurity System, in accordance with their statutory competencies.

The Action Plan includes the following:

1) area of action;
2) task number;
3) task name;
4) schedule;
5) competent institution(s);
6) expected results;
7) metric.

The Action Plan covers project activities, characterised by a start and end of the implementation period and products created as a result of the implementation of a given activity.

The Coordinator will prepare an annual report on the progress made in implementing the Strategy over the previous year, based on information received from the entities involved in its implementation. The reports will be submitted to the Council of Ministers by 30 September.

## 12. Funding

The financial impact of the measures taken on the state budget will be covered within the expenditure limits set for the relevant financial year in the appropriate parts of the state budget. Implementing the measures described in the Strategy, which have financial implications, will require either the use of currently available instruments with allocated funding or the adoption of new legislation. In the latter case the financial impact will be determined and financial resources appropriately secured at the stage of preparing the draft legal provisions implementing the provisions of the Strategy.

Under the applicable regulations, entities performing public tasks are obliged to include cybersecurity expenditures in their financial plans. Financial planning should also cover the tasks included in the Action Plan. The Strategy does not generate additional financial impact for the state budget. Financial resources for the implementation of tasks included in the Action Plan should be secured by the leading or cooperating institutions within their financial plans.

Sources of funding for the implementation of the activities described in the document will include, in particular:

1) the state budget and the financial plans of individual units involved in the implementation of the Cybersecurity Strategy;
2) financial resources from the Cybersecurity Fund;
3) funds from the National Centre for Research and Development;
4) European funds, including within the framework of the following programmes and funds:
    a) DEP,
    b) Horizon Europe,
    c) European Funds for Digital Development 2021–2027,
    d) National Recovery and Resilience Plan,
    e) European Funds for a Modern Economy 2021–2027,
    f) other regional programmes.

# Action Plan for the Implementation of the Cybersecurity Strategy of the Republic of Poland

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| **Specific goal 1 – Development of the National Cybersecurity System** | | | | | | | | |
| 1.1 Improvement of the National Cybersecurity System | 1.1.1 | Adoption of the amendment to the Act on the National Cybersecurity System implementing the NIS 2 Directive | 2025 (ongoing task) | 2026 | MC | Other government administration institutions | Implementation of the NIS 2 Directive, streamlining of the National Cybersecurity System | Passing of the act |
| | 1.1.2 | Establishment of the PCOC as an organisational unit of the Ministry of Digital Affairs (MC) | 2026 | 2027 | MC | – | Establishment of an organisational unit within the Ministry of Digital Affairs (MC) | Amendment to the Organisational Regulations of the Ministry of Digital Affairs (MC) |
| | 1.1.3 | Establishment of the PCOC as a central state institution | 2027 | 2029 | MC | NASK, ABW, MON, AW, SKW, SWW, RCB, Police | Establishment of the institution | Conferring of the statute |
| | 1.1.4 | Alignment of national regulations with the provisions of the Network Code | 2028 | 2029 | ME | MC | Ensuring legal bases for the effective implementation of the Network Codes | Passing of the act |
| | 1.1.5 | Ensuring the application of Regulation (EU) 2022/2554 | 2025 (ongoing task) | 2026 | MF | KNF | Increasing cybersecurity in the financial sector | Passing of the act |
| | 1.1.6 | Implementation of Directive (EU) 2022/2556 | 2025 (ongoing task) | 2026 | MF | KNF | Increasing cybersecurity in the financial sector | Passing of the act |
| | 1.1.7 | Adaptation of the MON cybersecurity system to the requirements of the amendment to the Act on the National Cybersecurity System | 2025 (ongoing task) | 2026 | MON | DKWOC | Implementation of the requirements of the amendment to the Act on the National Cybersecurity System | Amendment to the decision on the organisation and functioning of the cybersecurity system within the MON |

[31] Where an abbreviation of a ministry's name is used, this refers to the minister responsible for the relevant area of government administration.

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | (implementing the NIS 2 Directive) | | | | | | |
| | 1.1.8 | Adaptation of MON structures responsible for cybersecurity for the implementation of new tasks | 2025 (ongoing task) | 2026 | MON | Cyberspace Defence Forces Component Command (DKWOC), units subordinate to and supervised by the Minister of National Defence | Achieving the capability to implement tasks | Allocation/modification of staffing and scope of competence |
| | 1.1.9 | Adaptation of MON structures for the needs of early warning in cybersecurity, cyber crisis response, and large-scale crisis management in cybersecurity in the military dimension | 2025 (ongoing task) | 2027 | MON | DKWOC/CSIRT MON, Territorial Defence Forces Command | Achieving the capability to implement tasks | Allocation/modification of staffing and scope of competence |
| | 1.1.10 | Expansion of the Internal Security Agency's (ABW) competencies and powers through the amendment to the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, implemented under the supervision of the Minister Coordinator of Special Services (MKSS), and adaptation of the ABW structures responsible for cybersecurity for the implementation of new tasks, along with the expansion | 2025 (ongoing task) | 2029 | ABW | MKSS | Expansion of the ABW's competencies and powers in the field of cybersecurity | Passing of the act |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | of the ABW's institutional capacity | | | | | | |
| 1.2 Increasing the efficiency of the National Cybersecurity System | 1.2.1 | Connection of new entities to the S46 system and development of this system | 2024 (ongoing task) | 2026 | MC, NASK | – | Increasing the number of National Cybersecurity System entities connected to the S46 system and implementing new functionalities of this system | Achieving the indicator values specified in the application for project support |
| | 1.2.2 | Adaptation of the S46 system for the execution of tasks resulting from the implementation of the CER Directive | 2024 (ongoing task) | 2026 | NASK | RCB | Maintaining a register of critical entities referred to in the CER Directive in the S46 system | Covering all critical entities with the service |
| | 1.2.3 | Launching the Cyber.gov.pl portal | 2025 (ongoing task) | 2026 | MC | NASK | Ensuring support for citizens, enterprises, and public institutions in using cybersecurity services provided by the government administration | Making the Cyber.gov.pl portal available |
| | 1.2.4 | Establishment or development of sectoral CSIRTs | 2024 (ongoing task) | 2027 | Competent authorities | MC, national-level CSIRTs | Establishment of new sectoral CSIRTs or development of existing capacity | Achieving the indicator values specified in the application for project support |
| | 1.2.5 | Establishment of the NASK Cybersecurity Centre (CCN) | 2023 (ongoing task) | 2029 | NASK | MC | Strengthening the National Cybersecurity System through the establishment of a centre comprising qualitatively new, thematic, specialised centres, hubs, and laboratories, and the development of NASK's capacity | Achieving the indicator values specified in the application for project co-financing |
| | 1.2.6 | Establishment of voivodeship teams of | 2024 (ongoing task) | 2026 | MC | NASK, Police | Establishment of voivodeship teams | Achieving the indicator values specified in the |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | cybersecurity specialists | | | | | of cybersecurity specialists operating locally and supporting public entities in incident handling and data recovery, as well as conducting activities raising awareness about cybersecurity | application for project support |
| | 1.2.7 | Implementation of the "Cybersafe Local Government" project | 2023 (ongoing task) | 2027 | CPPC | MC, NASK | Increasing the level of information security of LGUs by strengthening resilience and capabilities to effectively prevent and respond to incidents in information systems | Achieving the indicator values specified in the application for project co-financing |
| | 1.2.8 | Establishment of Local Cybersecurity Centres at the local government level | 2025 (ongoing task) | 2029 | MC, LGUs | CPPC | Establishment of Local Cybersecurity Centres acting as Shared Services Centres in IT, which will ensure a high level of security for institutions operating at the local government level | Achieving the indicator values specified in the application for project co-financing |
| | 1.2.9 | Support for entities of the National Cybersecurity System, including those using industrial operational technologies (OT) | 2024 (ongoing task) | 2026 | MC | CPPC, NASK | Support for National Cybersecurity System entities in the modernisation and expansion of cybersecurity infrastructure in IT networks, including support for entities using IT and OT applied in industrial control systems (ICS) | Achieving the indicator values specified in the application for project support |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | 1.2.10 | Development and adoption of the National Large-Scale Cybersecurity Incident and Crisis Response Plan | 2025 (ongoing task) | 2029 | MC | RCB, national-level CSIRTs, and other ministries and central offices | The functioning of the "National Large-Scale Cybersecurity Incident and Crisis Response Plan" will result in the undertaking of appropriate actions and the ongoing analysis of events | Preparation of an annual report on responding to large-scale cybersecurity incidents and crises, and the development of recommendations to mitigate potential future events |
| | 1.2.11 | Establishment of teams of cybersecurity specialists acting for the benefit of selected State Treasury companies and supporting these companies in implementing information security, handling incidents, and conducting activities raising awareness of cybersecurity, i.e., utilising knowledge from ISAC-MAP | 2025 (ongoing task) | 2029 | MAP | – | Increasing the level of cybersecurity in State Treasury companies | The number of functioning teams of cybersecurity specialists acting for the benefit of selected State Treasury companies |
| | 1.2.12 | Establishment of ISAC Energia | 2025 (ongoing task) | 2029 | ME | CSIRT GOV, CSIRT NASK | Ensuring information sharing capabilities between OES in the energy sector | Establishment of ISAC Energia |
| | 1.2.13 | Establishment of ISAC Telko | 2025 (ongoing task) | 2028 | UKE | CSIRT GOV, CSIRT NASK | Ensuring information sharing capabilities between OES in the electronic communications subsector and producers of telecommunications equipment and software | Establishment of ISAC Telko |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | 1.2.14 | Development and adoption of the National Risk Assessment | 2025 (ongoing task) | 2026 | RCB | Ministries and central offices | Implementation of the EU Civil Protection Mechanism regarding the National Risk Assessment of identified significant threats, including cybersecurity | Adoption of the National Risk Assessment by the Council of Ministers by way of a resolution |
| | 1.2.15 | Development and adoption of the Strategy on the resilience of critical entities | 2025 (ongoing task) | 2026 | RCB | ABW, ministries and central offices | Increasing the resilience of critical entities by ensuring the uninterrupted provision of essential services by critical entities and the uninterrupted functioning of critical infrastructure | Adoption of the Strategy on the resilience of critical entities referred to in the CER Directive |
| | 1.2.16 | Establishment of the National Cyber Hub in accordance with the Cyber Solidarity Act | 2026 | 2029 | NASK | – | Creation of a national centre for sharing information on cyber threats in accordance with the provisions of the CSoA | Achieving the indicators specified in the applications for financing from the DEP |
| | 1.2.17 | Organisation of specialised cybersecurity exercises and workshops using modern CyberRange platforms, in particular for National Cybersecurity System entities | 2024 (ongoing task) | 2029 | MON | ECSC, MC, ABW | Increasing competencies and team building for cybersecurity teams, verification of acquired skills in direct operations/ competition | The number of organised exercises/workshops, number of participants |
| | 1.2.18 | Support for entrepreneurs carrying out tasks for the SZRP regarding | 2025 (ongoing task) | 2029 | MON | DKWOC/CSIRT MON, ABW | Increasing the cybersecurity of entrepreneurs | The number of supported entities |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | the protection of information systems used for their execution | | | | | carrying out tasks for the SZRP | |
| 1.3 Development of an integrated information sharing system to ensure the continuity of government administration, national security, and civil protection | 1.3.1 | Establishment of the State Secure Communications System (SBŁP) | 2025 (ongoing task) | 2028 (planned continuation) | MSWiA | Police, National Headquarters of the State Fire Service (KG PSP), National Headquarters of the Border Guard (KG SG), State Protection Service, ABW, MC, National Institute of Telecommunications (IŁ), RCB, Polish Medical Air Rescue | Reliable, secure, and robust telecommunications systems ensuring information flow services in times of peace, crisis, and conflict | The number of entities covered by the SBŁP and of systems serving to increase the level of information security |
| | 1.3.2 | Development and maintenance of the mobile communications system for classified information up to the "Restricted" (SKR-Z) classification level | 2022 (ongoing task) | 2025 (planned extension of the contract) | MC, NASK | – | Support for public administration and National Cybersecurity System entities, field entities, and uniformed services in classified communication at the "Restricted" level | Achieving the indicator values specified in the application for project co-financing |
| | 1.3.3 | Development of the Communicator | 2022 (ongoing task) | 2025 (planned extension of cooperation for 3 years) | MC | National Cloud Operator (OChK) | Support for National Cybersecurity System entities, including public administration and uniformed services, in overt, free, and secure official communication | The number of entities and users |
| | 1.3.4 | National communicator | 2025 (ongoing task) | 2029 | MC | MSWiA, ABW, NASK, MON, DKWOC | Support for public administration entities by providing an accessible communicator for secure overt communications | The number of users |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| 1.4 Increasing the cybersecurity of entities supervised by authorities responsible for cybersecurity | 1.4.1 | Execution of supervisory tasks of the authority responsible for cybersecurity in the energy sector | 2025 (ongoing task) | 2029 | ME | – | Increasing the level of cybersecurity in the sector | The number of entities against which supervisory measures were applied |
| | 1.4.2 | Execution of supervisory tasks of the authority responsible for cybersecurity in the transport sector, excluding the water transport subsector | 2025 (ongoing task) | 2029 | MI | – | Increasing the level of cybersecurity in the sector | The number of entities against which supervisory measures were applied |
| | 1.4.3 | Execution of supervisory tasks of the authority responsible for cybersecurity in the water transport subsector | 2025 (ongoing task) | 2029 | MI | – | Increasing the level of cybersecurity in the sector | The number of entities against which supervisory measures were applied |
| | 1.4.4 | Execution of supervisory tasks of the authority responsible for cybersecurity in the banking sector and financial market infrastructure | 2025 (ongoing task) | 2029 | KNF | – | Increasing the level of cybersecurity in the sector | The number of entities against which supervisory measures were applied |
| | 1.4.5 | Execution of supervisory tasks of the authority responsible for cybersecurity in the healthcare sector, excluding the entities referred to in Article 26(5) of the Act on the National Cybersecurity System | 2025 (ongoing task) | 2029 | MZ | – | Increasing the level of cybersecurity in the sector | The number of entities against which supervisory measures were applied |
| | 1.4.6 | Execution of supervisory tasks of the authority responsible for | 2025 (ongoing task) | 2029 | MON | – | Increasing the level of cybersecurity in the sector | The number of entities against which supervisory measures were applied |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | cybersecurity in the healthcare sector covering the entities referred to in Article 26(5) of the Act on the National Cybersecurity System | | | | | | |
| | 1.4.7 | Execution of supervisory tasks of the authority responsible for cybersecurity in the drinking water supply and distribution sector | 2025 (ongoing task) | 2029 | MI | – | Increasing the level of cybersecurity in the sector | The number of entities against which supervisory measures were applied |
| | 1.4.8 | Execution of supervisory tasks of the authority responsible for cybersecurity in the digital infrastructure sector, excluding the entities referred to in Article 26(5) of the Act on the National Cybersecurity System | 2025 (ongoing task) | 2029 | MC | – | Increasing the level of cybersecurity in the sector | The number of entities against which supervisory measures were applied |
| | 1.4.9 | Execution of supervisory tasks of the authority responsible for cybersecurity in the digital infrastructure sector covering the entities referred to in Article 26(5) of the Act on the National Cybersecurity System | 2025 (ongoing task) | 2029 | MON | – | Increasing the level of cybersecurity in the sector | The number of entities against which supervisory measures were applied |
| | 1.4.10 | Execution of supervisory tasks of the authority responsible for cybersecurity for | 2025 (ongoing task) | 2029 | MC | – | Increasing the level of cybersecurity in the sector | The number of entities against which supervisory measures were applied |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | digital service providers, excluding the entities referred to in Article 26(5) of the Act on the National Cybersecurity System | | | | | | |
| | 1.4.11 | Execution of supervisory tasks of the authority responsible for cybersecurity for DSPs covering the entities referred to in Article 26(5) of the Act on the National Cybersecurity System | 2025 (ongoing task) | 2029 | MON | – | Increasing the level of cybersecurity in the sector | The number of entities against which supervisory measures were applied |
| | 1.4.12 | Execution of the tasks of the competent authority referred to in the Network Code | 2026 | 2029 | ME | – | Covering entities in the sector with regulations resulting from the Network Code | Identification of high-impact and critical-impact entities |
| 1.5 Development and implementation of a risk assessment methodology at the national level | 1.5.1 | Development of a new risk assessment methodology | 2025 (ongoing task) | 2026 | MC | NASK, IŁ | Risk assessment within the National Cybersecurity System | Development of the methodology |
| **Specific goal 2 – Preventing and combating cybercrime and achieving capabilities to conduct a full spectrum of operations in cyberspace** | | | | | | | | |
| 2.1 Introduction of regulations to more effectively combat cybercrime | 2.1.1 | Amendment to regulations concerning banking secrecy | 2025 (ongoing task) | 2026 | MS | MF, MSWiA, KNF, MC, ABW, SKW, Police | More effective combating of cybercrime | Passing of the act |
| | 2.1.2 | Introduction of obligations for banks and other financial institutions supporting the | 2025 (ongoing task) | 2029 | MF | MS, MSWiA, KNF, MC, ABW, SKW Police | More effective combating of cybercrime | Passing of the act |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | combating of cybercrime | | | | | | |
| | 2.1.3 | Implementation of legislative, organisational, and technical solutions to enhance the protection of internet users against harmful and dangerous content, with a particular focus on protecting children and youth (combating child sexual abuse material (CSAM), live-streamed abuse, grooming, etc.). | 2025 (ongoing task) | 2029 | MC, NASK | MC, UKE, Police | Establishment of a system of trusted flaggers; automatic systems for the protection of children against harmful and illegal content | Ongoing analysis of content harmful to children and youth and issuing warnings; establishment of a single structure within the Police dealing with CSAM-related crimes |
| | 2.1.4 | Review of the solutions contained in the Act on combating abuse in electronic communications | 2026 | 2027 | MC | NASK, UKE, Police | Analysis of the effectiveness of the solutions contained in the Act | Determination of the need for changes in the Act |
| | 2.1.5 | Adaptation of provisions countering identity theft to technological changes | 2025 (ongoing task) | 2029 | MC | MSWiA, MS, ABW, Police | Reducing identity theft online | Passing of the act |
| | 2.1.6 | Review of legislation and rationalisation of criminal liability for cybercrimes | 2025 (ongoing task) | 2029 | MS | MSWiA, MC, ABW, SKW, Police | More effective deterrence against committing cybercrimes | Amendment of legal acts |
| | 2.1.7 | Amendments to the governing acts of individual special services and the Penal Code regarding the combating of cybercrime, including cyberterrorism and cyberespionage | 2025 (ongoing task) | 2029 | MS, MSWiA, ABW, AW, SKW, SWW, Central Anti-Corruption Bureau (CBA), Police | – | Streamlining the combating of cybercrime | Passing of the act |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | 2.1.8 | Amendment of statutory provisions towards the introduction of statutory justifications for operational and analytical activities | 2026 | 2029 | MSWiA, PK | ABW, Police, SKW | Streamlining the combating of cybercrime and ensuring legal security for officers | Passing of the act |
| | 2.1.9 | Development and implementation of centralised IT tools supporting the fight against cybercrime | 2025 (ongoing task) | 2029 | MC | MKSS, ABW, Police, National Prosecutor's Office (PK), MS | More effective combating of cybercrime | Deployment of tools |
| 2.2 Strengthening specialised cybercrime combating structures | 2.2.1 | Creating and developing specialised human resources along with institutional and technical facilities for the needs of combating cybercrime | 2025 (ongoing task) | 2029 | PK, Police, ABW | MS | More effective combating of cybercrime | – |
| | 2.2.2 | Development of specialised organisational units for cybercrime within the prosecutor's office and the Police | 2025 (ongoing task) | 2029 | PK, ABW, Police | – | More effective combating of cybercrime | The number of established specialised organisational cells for cybercrime within the prosecutor's office and the Police |
| | 2.2.3 | Development of specialisation in the prosecution of cybercrime | 2025 (ongoing task) | 2029 | PK | MS | More effective combating of cybercrime | Introduction of the specialisation in the prosecutor's office |
| 2.3 Enhancing the analytical capabilities of law enforcement agencies, special services, and judicial authorities using new technologies | 2.3.1 | Enhancing the analytical capabilities in the fight against cybercrime | 2025 (ongoing task) | 2029 | PK, Police, ABW | | More effective combating of cybercrime using advanced technologies | Implementation of modern data analysis systems |
| | 2.3.2 | Training for law enforcement officers and representatives of the judicial authorities and the prosecutor's office on new technologies | 2025 (ongoing task) | 2029 | MS | PK, ABW, Police, MSWiA | More effective combating of cybercrime using new technologies | The number of organised training courses |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| 2.4 Increasing the effectiveness of law enforcement agencies through the exchange of knowledge and experience regarding cybersecurity and methods used by cybercrime perpetrators | 2.4.1 | Training of representatives of judicial authorities, the prosecutor's office, and law enforcement agencies on combating cybercrime | 2025 (ongoing task) | 2029 | MS | PK, ABW, Police | More effective combating of cybercrime | The number of organised training courses |
| | 2.4.2 | Cooperation with Interpol and Europol in combating cybercrime | 2025 (ongoing task) | 2029 | Police | MS | More effective combating of cybercrime | – |
| | 2.4.3 | Training on obtaining data from foreign entities used in combating cybercrime | 2025 (ongoing task) | 2029 | MS, Police | ABW, PK | The number of organised training courses | The number of trained officers and prosecutors |
| 2.5 Combating cyberterrorism and cyberespionage | 2.5.1 | Amendment to the acts regulating the functioning of special services in a manner enabling the effective conduct of operational activities in cyberspace | 2025 (ongoing task) | 2029 | MKSS | ABW, AW, SKW, SWW | Increasing effectiveness in combating cyberterrorism and cyberespionage | Passing of the act |
| | 2.5.2 | Strengthening specialised structures for combating cyberterrorism and cyberespionage within the ABW | 2025 (ongoing task) | 2029 | ABW | – | Increasing effectiveness in combating cyberterrorism and cyberespionage | Introduction of organisational changes within the ABW |
| | 2.5.3 | Development of a system for the retention of content generated by persons involved in terrorist activities using internet communicators and other means of communication | 2025 (ongoing task) | 2029 | ABW | MS, MSWiA, SKW, Police | Increasing effectiveness in combating cyberterrorism and cyberespionage | Deployment of the system |
| | 2.5.4 | Implementation of solutions limiting irregularities related | 2025 (ongoing task) | 2029 | MC | ABW, Police, UKE, MS | Increasing effectiveness in combating | Amendment of legal acts |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | to the registration of SIM cards | | | | | cyberterrorism and cyberespionage, as well as other cybercrimes | |
| | 2.5.5 | Building the capacity of CTI teams of institutions responsible for cybersecurity at the national level in the context of increasing the capabilities for distributing information to domestic and foreign recipients | 2025 (ongoing task) | 2029 | National-level CSIRTs, AW, ABW, SKW, SWW, MC, Police | – | Increasing the capabilities of entities cooperating in the subject area of operation | The number of provided information reports |
| 2.6 Achieving capabilities to conduct a full spectrum of operations in cyberspace | 2.6.1 | Organisation of specialised cybersecurity exercises and training courses using modern CyberRange platforms | 2024 (ongoing task) | 2029 | MON | ECSC, DKWOC, ABW, AW, SKW, SWW | Increasing the skills and knowledge of the SZRP personnel and special services in the field of cybersecurity, team building for cybersecurity teams, and verification of acquired skills in direct operations | The number of organised exercises and training courses, the number of participants |
| | 2.6.2 | Developing personnel competencies based on defined training paths | 2024 (ongoing task) | 2029 | MON | ECSC, DKWOC | Systematisation of the competency management and training process for MON cybersecurity personnel | The number of defined professional roles and development paths |
| | 2.6.3 | Certification of persons in the field of cybersecurity based on existing and future certification schemes | 2024 (ongoing task) | 2029 | MON | ECSC, DKWOC | Introduction of standardisation and harmonisation of competency assessment for MON cybersecurity personnel | The number of accredited certification schemes and issued certificates |
| | 2.6.4 | Coordination of the implementation of commitments under the Cyber Defence Pledge | 2025 (ongoing task) | 2029 | MON | DKWOC, MC, RCB, other public administration entities | Strengthening cyber resilience at the national level | Questionnaire – self-assessment |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | 2.6.5 | Development of the SZRP detection system (obtaining telemetry from systems essential for state defence) and building a threat information sharing network | 2026 | 2029 | DKWOC | SKW | Increasing situational awareness in cyberspace | The number of entities covered by detection |
| | 2.6.6 | Active operations in cyberspace aimed at obtaining information about the network infrastructure of adversaries and information affecting the security of Poland | 2025 (ongoing task) | 2029 | AW, ABW, SKW, SWW, CBA | Government administration institutions | Obtaining and transferring information essential for the security of Poland to competent organisations | Number and quality of provided information reports |
| | 2.6.7 | Active operations in cyberspace aimed at neutralising or limiting the functioning of individual structural elements (entities, tools, schemes) engaged by the adversary for operations against Poland | 2025 (ongoing task) | 2029 | Intelligence and counterintelligence special services | MON, national-level CSIRTs | Neutralisation of cyber threats originating from adversaries' infrastructure | The number of neutralised servers |
| **Specific goal 3 – Increasing the level of resilience of information systems in the public (including military) and private spheres** | | | | | | | | |
| 3.1 Increasing the level of resilience of information systems | 3.1.1 | Introduction of cybersecurity requirements in the Public Procurement Law | 2025 (ongoing task) | 2027 | MC | Government administration institutions | Creation of a uniform and effective approach regarding the cybersecurity of procured products and services | Passing of the act |
| | 3.1.2 | Introduction of a procedure for the procurement of | 2026 | 2027 | MC | Government administration institutions | Streamlining the process of executing urgent procurements | Passing of the act |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | cybersecurity-related services and products in urgent cases related to state security | | | | | for cybersecurity needs | |
| | 3.1.3 | Coordinated vulnerability disclosure | 2025 (ongoing task) | 2026 | NASK | ABW, MON | Ensuring a single point where any person can securely report a vulnerability | Implemented process for receiving and handling vulnerability reports |
| | 3.1.4 | Development of a training programme and tools for the practical verification of resilience against phishing threats within the MON | 2024 (ongoing task) | 2027 | MON | DKWOC, ECSC | Increased awareness among soldiers and employees | The number of conducted simulated phishing campaigns, the number of training courses |
| | 3.1.5 | Implementation of a data labelling policy within the MON | 2025 (ongoing task) | 2027 | MON | General Staff of the Polish Armed Forces, DKWOC | Increasing the security of information processed in MON information systems | Execution of the schedule |
| | 3.1.6 | Development/update of cybersecurity standards and guidelines within the MON | 2025 (ongoing task) | 2026 | MON | DKWOC | Increasing the security of information systems | The number of developed/updated documents |
| | 3.1.7 | Conducting security tests of ICT systems operated by the SZRP, including active testing of systems to verify computer incident response procedures and methods of countering attacks on MON ICT systems | 2025 (ongoing task) | 2029 | MON, DKWOC/CSIRT MON, SKW | Units subordinate to and supervised by the Minister of National Defence | Increasing the security of information systems | The number of conducted security tests |
| 3.2 Development of national cryptology, including the migration to | 3.2.1 | Development of a post-quantum cryptography migration plan | 2025 (ongoing task) | 2029 | MC | ABW, MON, MRiT, SKW, NASK, IŁ, DKWOC | Ensuring Poland's secure migration to post-quantum cryptography and securing data confidentiality in | Adoption of the Plan |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| post-quantum cryptography and the development of quantum technologies | | | | | | | the public and private sectors | |
| | 3.2.2 | Construction of a national quantum communication network based on the QKD mechanism – PIONIER-Q (participation in the EURO-QCI network) | 2023 (ongoing task) | 2029 | Participants of the PIONIER-Q consortium | MC, MNiSW, MRiT | Construction of a network for quantum encryption key exchange domestically and through international cooperation using optical networks and satellite communication | The number of international links; the number of entities with access to the QKD network |
| | 3.2.3 | Development and provision to citizens, organisations, and entrepreneurs of modern, national cryptographic tools (such as pseudonyms, domain signatures, anonymous attribute certificates, one-time tokens) | 2025 (ongoing task) | 2029 | NASK | MC, MRiT, academic centres | Introduction and dissemination of modern methods of cryptographic authentication, use of digital identity, and resilience to attacks on digital identity based on DLT, among other things | Availability of public-key-based digital identity for legal persons, availability of pseudonymous authentication for natural persons, availability of mechanisms for generating attribute attestations for natural persons, availability of DLT-based time-stamping, availability of mechanisms protecting against unauthorised use of signing and authentication keys and external cryptanalytic attacks |
| 3.3 Cloud computing services for strengthening the resilience of information systems | 3.3.1 | Common State IT Infrastructure | 2025 (ongoing task) | 2026 | MC | – | Increasing the resilience of information systems and the digital development of public administration; activities related to the development of cloud computing services will be undertaken | Introduction of the WIIP Initiative by way of an act |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | 3.3.2 | Classified cloud | 2026 | 2029 | MC | ABW, MON, NASK, SKW, DKWOC | Increasing the availability of classified systems and raising their resilience level | The number of entities with access to the classified cloud |
| | 3.3.3 | Development of a Plan for the Migration of Key IT Systems of Poland in the Event of a Crisis or War | 2026 | 2029 | MC | ABW, MON, SKW, NASK, DKWOC | Ensuring the capability for the secure migration of key information systems of Poland in the event of a crisis or war | Adoption of the Plan |
| 3.4 Development of capabilities for the effective prevention of and response to cybersecurity incidents | 3.4.1 | Cyber threat intelligence (CTI) | 2025 (ongoing task) | 2029 | MC | Entities ensuring cybersecurity at the national level | Increasing the level of cybersecurity at the national level | The number of National Cybersecurity System entities equipped with CTI systems |
| | 3.4.2 | Ensuring Anti-DDoS protection for public entities and entities essential from the perspective of national cybersecurity | 2025 (ongoing task) | 2029 | NASK | MC | Ensuring Anti-DDoS protection for public entities and entities essential from the perspective of national cybersecurity | The number of entities for which Anti-DDoS protection is ensured |
| | 3.4.3 | Conducting exercises and stress tests in the area of critical infrastructure operators | 2025 (ongoing task) | 2029 | RCB | Ministries and central offices, ABW, AW, CSIRTs, and authorities responsible for critical infrastructure | Strengthening the resilience of critical infrastructure operators to antagonistic threats, particularly in the area of cybersecurity | The number of conducted exercises and stress tests |
| 3.5 Development of standardisation in cybersecurity | 3.5.1 | Cybersecurity recommendations and standards | 2025 (ongoing task) | 2029 | MC | PWCyber partners | Strengthening the resilience of information systems in the public and private sectors through the implementation of cybersecurity standards and recommendations | The number of developed recommendations and standards |
| | 3.5.2 | Preparation of guidelines and promotion of good practices raising | 2025 (ongoing task) | 2029 | MC | NASK | Increasing awareness and skills in the field of cybersecurity | The number of implemented guidelines and of training and workshop participants |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | resilience to cyber threats | | | | | | |
| | 3.5.3 | Introduction of an obligation for critical infrastructure operators to apply minimum cybersecurity standards | 2025 (ongoing task) | 2026 | RCB | Authorities responsible for critical infrastructure | The Council of Ministers will define, by way of a regulation, minimum requirements for critical infrastructure operators in such areas as cybersecurity, aimed at implementing solutions adequate to the results of the conducted threat analysis | The number of reports on the state of critical infrastructure protection submitted to the ministers responsible for critical infrastructure |
| | 3.5.4 | Establishment of a national centre responsible for standardisation in cybersecurity | 2026 | 2027 | NASK | MC | Establishment of common standards applied by National Cybersecurity System entities | The number of issued standards, guidelines |
| 3.6 Public-private partnership in the area of cybersecurity | 3.6.1 | PWCyber | 2025 (ongoing task) | 2029 | MC | – | Promoting awareness and raising the competencies of National Cybersecurity System entities in the field of cybersecurity and modern technologies | The number of initiatives executed jointly with partners |
| | 3.6.2 | Organising regular cybersecurity seminars for critical infrastructure operators | 2023 (ongoing task) | 2029 | RCB | MC, NASK, ABW, MON, SKW | Increasing awareness and skills in the field of cybersecurity | The number of conducted seminars and of seminar participants |
| | 3.6.3 | Organisation of National Critical Infrastructure Protection Forums | 2023 (ongoing task) | 2029 | RCB | MC, NASK, ABW, MON, SKW | Promoting awareness in the field of cybersecurity and | The number of conducted forums and the number of forum participants |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | | | | | | modern technologies | |
| **Specific goal 4 – Increasing the potential of the national technological and industrial base and strengthening the technological sovereignty of the Republic of Poland in the area of cybersecurity** | | | | | | | | |
| 4.1 Strengthening supply chain security at the national and international levels | 4.1.1 | Obtaining the capability by the NASK national certification body to issue certificates under the EUCC scheme | 2024 (ongoing task) | 2026 | NASK | MC, IŁ, Łukasiewicz Research Network – Institute of Artificial Intelligence and Cybersecurity | Accreditation and notification for certification under EUCC for the NASK national certification body | The number of conducted certification processes |
| | 4.1.2 | Obtaining the capability of the security evaluation laboratory at IŁ to conduct security evaluations of ICT products under the EUCC scheme, at the "high" assurance level for the full scope of the EUCC scheme | 2025 (ongoing task) | 2026 | IŁ | NASK | Accreditation and notification for certification under EUCC | The number of conducted certification processes |
| | 4.1.3 | Introduction of amendments to the Act – Public Procurement Law facilitating cybersecurity procurements | 2025 (ongoing task) | 2026 | MC | Government administration institutions | Adoption of the amendment to the Act | – |
| | 4.1.4 | Obtaining the capability for certification under the European cybersecurity certification scheme for cloud services (EUCS) | 2026 | 2026 | NASK | MC, IŁ, MON, WIŁ | Authorisation and notification for conformity assessment bodies | The number of conducted certification processes |
| | 4.1.5 | Adoption of the first national cybersecurity certification scheme | 2025 (ongoing task) | 2026 | MC | NASK | Implementation of the national cybersecurity certification scheme | Adoption of the regulation defining the certification scheme |
| | 4.1.6 | Obtaining the capability for | 2025 (ongoing task) | 2026 | NASK | MC, IŁ, MON, WIŁ | Capability for certification | The number of certification schemes |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | certification compliant with the requirements of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) | | | | | compliant with the AI Act in the certification body at NASK | |
| | 4.1.7 | Obtaining the capability for certification compliant with the requirements of the Cyber Resilience Act | 2025 (ongoing task) | 2026 | NASK | MC, IŁ, ŁUKASIEWICZ-EMAG | Capability for conformity assessment against the requirements of the Cyber Resilience Act in conformity assessment bodies | The number of conducted assessments |
| | 4.1.8 | Obtaining the capability for certification under the European cybersecurity certification scheme for 5G solutions (EU5G) – preparation of national technical capabilities | 2025 (ongoing task) | 2029 | MC | NASK, IŁ | Obtaining the capability for certification | The number of conducted certification processes |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | 4.1.9 | Obtaining the capability of the national system for assessing the conformity of radio equipment against the cybersecurity requirements specified in the RED Directive | 2025 (ongoing task) | 2026 | IŁ | MC | Obtaining the capability for certification | The number of conducted certification processes |
| | 4.1.10 | Development and implementation of the MON security policy on countering cyber threats in the supply chain for the SZRP | 2025 (ongoing task) | 2027 | MON | DKWOC, Armed Forces Support Inspectorate, Armament Agency | Increasing supply chain security | Adoption of the MON security policy regarding countering cyber threats in the supply chain, the number of MON units that have implemented the policy |
| 4.2 Stimulating research, development, and innovation in the area of cybersecurity | 4.2.1 | R&D&I initiatives in the area of cybersecurity | 2025 (ongoing task) | 2029 | NCBR | MNiSW, MC, MON, MRiT | Building national technological and industrial competencies and technological sovereignty | The number of R&D&I projects launched in the field of cybersecurity |
| | 4.2.2 | Support for Polish entities in international R&D&I initiatives in the area of cybersecurity | 2025 (ongoing task) | 2029 | MC | MNiSW, NCBR, MON, MRiT | Building national technological and industrial competencies and technological sovereignty | The number of international R&D&I projects in the area of cybersecurity with the support of government institutions |
| | 4.2.3 | Building the Cybersecurity Competence Community | 2024 (ongoing task) | 2029 | MC | | Increasing the capability and competitiveness of Poland, and by extension Europe, regarding offered solutions aimed at ensuring cybersecurity, which will help to improve the EU's strategic autonomy | The number of applications to join the Competence Community |
| | 4.2.4 | Ensuring mechanisms of data security, non- | 2024 (ongoing task) | 2029 | NASK, MC | MS, MF, UNKF, MNiSW, MS, National Health | Construction and maintenance of resilient blockchain | The number of use cases in public sector |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | repudiation, integrity, and privacy – construction, maintenance, and development of use cases of the EBSI Europeum (blockchain) European network node in Poland | | | | Fund, Social Insurance Institution | infrastructure for providing cross-border public sector services | services, the number of cross-border use cases |
| **Specific goal 5 – Building the awareness, knowledge, and competencies of the staff of the National Cybersecurity System entities, as well as of citizens and entrepreneurs** | | | | | | | | |
| 5.1 Increasing awareness and knowledge, and strengthening the competencies of the staff of the National Cybersecurity System entities | 5.1.1 | Training courses for National Cybersecurity System entities | 2025 (ongoing task) | 2029 | MC | NASK, PWCyber partners | Increasing awareness and knowledge, and strengthening the cybersecurity competencies of the staff of National Cybersecurity System entities | The number of organised training courses |
| | 5.1.2 | Training courses for public administration | 2025 (ongoing task) | 2029 | MC | NASK, PWCyber partners | Increasing awareness and knowledge, and strengthening the cybersecurity competencies of public administration staff | The number of organised training courses |
| | 5.1.3 | Training courses for local administration | 2025 (ongoing task) | 2029 | MC | NASK, PWCyber partners | Increasing awareness and knowledge, and strengthening the cybersecurity competencies of local administration staff | The number of organised training courses |
| | 5.1.4 | Development of a training programme and tools for verifying the knowledge and awareness of MC employees regarding | 2024 (ongoing task) | 2029 | MC | – | Increased employee awareness | Percentage of employees covered by training and knowledge verification tests |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | cyber hygiene and cyber threats | | | | | | |
| | 5.1.5 | Financial support for persons performing tasks in the field of cybersecurity, within the framework of the functioning of the Cybersecurity Fund | 2024 (ongoing task) | 2030 | MC | – | Limiting the outflow of cybersecurity specialists from the public sector and levelling out remuneration in relation to the private sector | The number of undertaken initiatives (granted support) |
| | 5.1.6 | Preventive and educational activities. Certification of competencies based on the European Cybersecurity Skills Framework in public administration and in local government units | 2025 (ongoing task) | 2029 | MC, NASK | NASK | Increasing awareness and strengthening the competencies of the most important persons in the state, as well as employees of central offices, LGUs, and others. Harmonisation of the competency assessment for the management personnel of National Cybersecurity System entities | The number of executed training courses/issued certificates |
| | 5.1.7 | Establishment of an institution responsible for the harmonisation and validation of the personnel education process in the area of cybersecurity | 2026 | 2028 | NASK | – | Establishment and operationalisation of a unit responsible for the harmonisation and validation of the education process in the field of cybersecurity | The number of validated education programmes |
| | 5.1.8 | Development of the skills of technical personnel by conducting exercises and competitions based on the | 2025 (ongoing task) | 2029 | NASK, MC | – | Generating interest among young cybersecurity enthusiasts – school and university students – in participating in | – |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | experience of ECSC competitions | | | | | competitions and exercises requiring technological knowledge, including subject-specific competitions and olympiads in the field of cybersecurity | |
| | 5.1.9 | Creating communication strategies related to responding to the consequences of cybersecurity incidents | 2025 (ongoing task) | 2029 | NASK | MC | Harmonising the method of responding to cybersecurity incidents so that key information reaches all stakeholders | Ongoing notification about current trends visible in incidents – propagating knowledge |
| | 5.1.10 | Conducting Cooperation Programmes with National Cybersecurity System entities serving to share experiences, transfer knowledge, and undertake joint initiatives – as a continuation of the PdC (Partnership for Cybersecurity) Programme | 2025 (ongoing task) | 2029 | NASK | MC | Increasing the awareness and knowledge, and strengthening the competencies in the area of cybersecurity among the personnel of entities forming the National Cybersecurity System, who are participants of the PdC | The number of organised meetings |
| | 5.1.11 | Countering cyber threats and strengthening the cybersecurity system by the Hybrid Threats Team established at the Government Crisis Management Team | 2025 (ongoing task) | 2029 | RCB | Public administration entities, services, and critical infrastructure operators | Early identification of hybrid threats and support for the coordination of activities in the area of cybersecurity | The number of team meetings |
| | 5.1.12 | Coordination of information sharing between administration, | 2025 (ongoing task) | 2029 | RCB | Public administration entities, services, and critical | Ongoing coordination of information sharing between entities | – |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | services, and critical infrastructure operators | | | | infrastructure operators | | |
| | 5.1.13 | Creating regular reports on the state of execution of tasks resulting from introduced CRP alert levels. Creating reports on events and incidents occurring while the CRP alert levels apply | 2025 (ongoing task) | 2029 | RCB | Public administration entities and critical infrastructure operators | Coordination of activities and creating reports related to the introduction of CRP alert levels | The number of reports |
| | 5.1.14 | Building a personnel certification system, including the implementation of personnel certification programmes, including those based on the competency profiles of the European Cybersecurity Skills Framework and the NIST Framework in public administration, local government units, and the MON | 2025 (ongoing task) | 2029 | MC, MON | ECSC, NASK | Increasing awareness and strengthening the competencies of the most important persons in the state, as well as employees of central offices, LGUs, and others. Harmonisation of the competency assessment for the management personnel of National Cybersecurity System entities | The number of accredited certification schemes and issued certificates |
| | 5.1.15 | Organisation of specialised, technical training courses in the area of cybersecurity using modern CyberRange platforms | 2024 (ongoing task) | 2029 | MON | ECSC, MC | Increasing the cybersecurity skills and knowledge of the personnel of National Cybersecurity System entities, particularly public administration entities | The number of organised training courses and trained persons |
| | 5.1.16 | Organisation of cybersecurity training courses/conferences | 2025 (ongoing task) | 2029 | MON | Units subordinate to and supervised by the Minister of National Defence | Increasing the cybersecurity awareness and knowledge of | The number of informative and educational |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | (dissemination of good practices in the field of cybersecurity) directed at National Cybersecurity System entities within the scope of responsibility of the Minister of National Defence | | | | | National Cybersecurity System entities | undertakings, the number of participants |
| 5.2 Developing the cybersecurity awareness and knowledge of citizens and entrepreneurs | 5.2.1 | Publicly available training courses on cybersecurity and digital hygiene | 2025 (ongoing task) | 2029 | MC | NASK, PWCyber partners (commercial companies), CPPC | Increasing awareness and knowledge, and strengthening the cybersecurity competencies of citizens | The number of organised training courses |
| | 5.2.2 | Training courses on cybersecurity and digital hygiene for children and youth, as well as teaching staff | 2025 (ongoing task) | 2029 | MC | MEN, NASK, UKE | Increasing the cybersecurity awareness and knowledge of children and youth and improving digital hygiene through the continuation of the Cyberlekcje 3.0 (Cyberlessons 3.0) project, together with NASK and MEN | The number of schools, representatives of teaching staff (teachers, educators, psychologists), and students covered by the project |
| | 5.2.3 | Information and education campaign – Cybersecurity and digital hygiene for seniors | 2025 (ongoing task) | 2029 | MC | NASK, CPPC, UKE | Increasing the awareness and knowledge of seniors in the field of digital hygiene by conducting an information and education campaign | The number of organised information and education campaigns |
| | 5.2.4 | Education and information campaign for entrepreneurs, disseminating the | 2025 (ongoing task) | 2029 | MRiT | NASK | Increasing the awareness and knowledge, and strengthening the competence among | End product indicators: The number of education and information campaigns concerning ICT – 3. |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | benefits of using digital technologies (KEI MŚP) | | | | | SMEs in the field of cybersecurity and digital hygiene by conducting training courses | The number of internet campaigns – 3.<br>The number of PR campaigns – 3.<br>The number of special actions – 20.<br>End result indicators:<br>Reach of education and information activities/campaigns – approx. 8 million (persons).<br>The total number of submitted applications for e-services concerning the establishment and running of business activity – min. 7.8 million.<br>The number of visits to the website of the campaign concerning cybersecurity for companies – 1.5 million. |
| | 5.2.5 | Cybersecurity knowledge base on the gov.pl government portal | 2025 (ongoing task) | 2029 | MC | – | Developing the cybersecurity knowledge base on the gov.pl government portal | The number of published new articles at gov.pl |
| | 5.2.6 | Development of educational solutions to enhance the protection of internet users against harmful and dangerous content, with a particular focus on protecting children and youth (combating child sexual abuse material (CSAM), live- | 2025 (ongoing task) | 2029 | MC, NASK | – | Dissemination of knowledge about the harmfulness of specific content – applies to both CSAM and other content harmful to children and youth. Limiting the access of children and youth to harmful content | The number of informative and awareness-raising actions, launching a dedicated team within NASK under Dyżurnet.pl to identify and combat harmful content other than CSAM |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | streamed abuse, grooming, etc.). | | | | | | |
| | 5.2.7 | Lectures at higher education institutions raising awareness of resilience to current cyber threats | 2025 (ongoing task) | 2029 | AW | – | Increased awareness among students and academic staff in the area of cybersecurity. Increase in the number of students pursuing a career in cybersecurity and interested in the subject – leading to a larger number of available specialists on the market | The number of conducted lectures |
| | 5.2.8 | Conducting simulated social engineering tests for the benefit of interested public sector units and enterprises | 2025 (ongoing task) | 2029 | AW | – | Increased awareness among employees based on the results of the conducted tests. Diagnosis of the real scale of threats resulting from social engineering attacks | The number of conducted tests |
| | 5.2.9 | Communication on websites and publishing on social media profiles of information campaigns regarding cybersecurity | 2024 (ongoing task) | 2029 | RCB | NASK, MC | Increased awareness among citizens. Information campaigns concerning cyber threats conducted at the national level bring measurable benefits, which lead to an increase in awareness of cyber threats. The activities are accompanied by the publication of infographics related to cyber threats and the obligations of administration and citizens in | The number of published messages and the number of views |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | | | | | | connection with the introduced CRP alert levels | |
| | 5.2.10 | Implementation of the CYBER.MIL Academy project | 2025 (ongoing task) | 2029 | MON | DKWOC, ECSC | Increasing interest in service in the SZRP/work in the MON in the area of cybersecurity and computer science | The number of higher education institutions participating in the project |
| | 5.2.11 | Implementation of the "CyberMil z klasą" (CyberMil with Class) workshops | 2025 (ongoing task) | 2029 | Central Military Recruitment Centre | DKWOC, Polish Naval Academy, Military University of Technology, General Tadeusz Kościuszko Military University of Land Forces | Generating interest in military cybersecurity, improving the project participants' knowledge of cybersecurity and computer science | The number of schools participating in the project |
| | 5.2.12 | Organisation of the Marian Rejewski Prize competition for the best engineering, bachelor's, master's thesis, and doctoral dissertation devoted to cybersecurity and cryptology | 2025 (ongoing task) | 2029 | MON | – | The number of laureates employed in the SZRP | The number of works submitted to the competition |
| | 5.2.13 | Increasing the digital maturity and cybersecurity of companies by making digital services available at Biznes.gov.pl | 2025 (ongoing task) | 2026 | MRiT | NASK | Increasing the digital maturity and cybersecurity of companies | Users of new and modernised public digital services, products, and processes – 30,000.<br>Completion of the process of developing new or improving existing e-services – 3.<br>Completion of the process of developing new or expanding existing public information systems – 1.<br>Percentage of companies that have implemented the received |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | | | | | | | recommendations, out of those that have executed e-services – 15%. |
| **Specific goal 6 – Strengthening the Republic of Poland's solid international standing in the field of cybersecurity** | | | | | | | | |
| 6.1 Active international cooperation at the strategic, political, and legal levels | 6.1.1 | Participation in the Tallinn Mechanism – running the Back Office | 2023 (ongoing task) | - | MC | MSZ, competent authorities | Support for Ukraine in the area of cybersecurity | The number of executed activities |
| | 6.1.2 | Participation in international events in the area of cybersecurity and relevant international law | 2025 (ongoing task) | 2029 | MC | MSZ, competent authorities, NASK | Increasing the awareness and competencies of personnel, strengthening the international presence of Polish experts | The number of events and the nature of participation |
| | 6.1.3 | Support in the organisation of cybersecurity events involving foreign entities | 2025 (ongoing task) | 2029 | MC | MSZ, competent authorities, CSIRTs | Strengthening the image of the Republic of Poland as a vital and active entity in the area of cybersecurity, strengthening the international presence of Polish experts | The number of joint activities |
| | 6.1.4 | Conceptualisation and implementation of selected projects within existing G2G agreements | 2025 (ongoing task) | 2029 | MC | – | Deepening international cooperation, measurable benefits in accordance with the assumptions of projects or undertaken actions | The number of joint activities |
| | 6.1.5 | Establishing bilateral dialogue and cooperation based on Memoranda of Understanding | 2025 (ongoing task) | 2029 | MC | MSZ | Bilaterally strengthening international cooperation, primarily in the areas of sharing threat information, | The number of developed agreements or consultations within the signed Memoranda of Understanding |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | | | | | | sharing good practices, and cooperating in response to incidents and attacks | |
| | 6.1.6 | Participation in legislative work in the area of cybersecurity at the EU level | 2025 (ongoing task) | 2029 | MC | Competent authorities | Monitoring legislative processes and responding in accordance with national priorities | - |
| | 6.1.7 | Participation in working and expert groups at the EU and international levels in the area of cybersecurity and relevant international law | 2025 (ongoing task) | 2029 | MSZ, competent authorities | MC | Strengthening the image of Poland as a vital and active entity in the area of cybersecurity | - |
| | 6.1.8 | Drafting positions to be presented by Poland's representatives at meetings, or drafting and submitting written positions in the area of cybersecurity and relevant international law | 2025 (ongoing task) | 2029 | MSZ, competent authorities | MC | Strengthening the image of Poland as a vital and active entity in the area of cybersecurity | - |
| | 6.1.9 | Participation in exercises in the area of cybersecurity and relevant international law | 2025 (ongoing task) | 2029 | Competent authorities | MSZ, MC, NASK, national-level CSIRTs | Improving coordination and communication at the national and international level | The number of exercises |
| | 6.1.10 | Conducting intergovernmental consultations on cybersecurity policy and relevant international law | 2025 (ongoing task) | 2029 | MC | MSZ, competent authorities | Bilateral strengthening of intergovernmental cooperation | The number of joint activities or consultations |
| | 6.1.11 | Promoting Polish candidacies for key positions in working groups and in | 2025 (ongoing task) | 2029 | MSZ | MC, MON | Strengthening the image of Poland as a country with a | - |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | international organisations in the area of cybersecurity | | | | | high level of professionalism and expertise in the area of cybersecurity | |
| | 6.1.12 | Supporting the development of the resilience of third countries | 2025 (ongoing task) | 2029 | MSZ, MC | NASK, competent authorities, academic centres, and NGOs | Increasing the level of security of Poland's strategic environment | The number of executed aid projects |
| | 6.1.13 | Establishing bilateral and multilateral dialogue and cooperation based on agreements in the military dimension | 2025 (ongoing task) | 2029 | MON | DKWOC | Bilateral/ multilateral strengthening of international cooperation, primarily in the areas of sharing threat information, sharing good practices, and cooperating to address incidents and attacks | The number of developed agreements or consultations within existing agreements |
| | 6.1.14 | Organisation of military cybersecurity events involving foreign entities | 2025 (ongoing task) | 2029 | MON | DKWOC, ECSC | Strengthening the image of the Republic of Poland as a vital and active entity in the area of cybersecurity, strengthening the international presence of Polish experts | The number of undertakings |
| 6.2 Active international cooperation at the operational and technical levels | 6.2.1 | Operating as a single point of contact for cybersecurity within international organisations | 2025 (ongoing task) | 2029 | MSZ, competent authorities | – | Sharing information on threats, sharing good practices, and cooperating to address incidents and attacks | – |
| | 6.2.2 | Information sharing and cooperation within international technical forums in | 2025 (ongoing task) | 2029 | MC, CSIRTs | MSZ | Raising the level of cybersecurity of Poland and building trust between | – |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | the area of cybersecurity | | | | | international partners | |
| | 6.2.3 | Participation in international initiatives and projects, as well as cooperation networks, such as EBSI/Europeum (blockchain), development of eIDAS, EuroQCI, IRIS2, and others | 2024 (ongoing task) | 2029 | NASK, MC | – | Deepening international cooperation regarding standardisation and shaping secure technical, legal, and service solutions common to the entire EU | The number of use cases identified as indicators in international projects |
| | 6.2.4 | Cooperation within the European Cybersecurity Alert System | 2026 | 2029 | NASK | National-level CSIRTs, sectoral CSIRTs, Local Cybersecurity Centres, ISACs | Creation of a cross-border hub for sharing cyber threat information in accordance with the provisions of the CSoA | Achieving the indicators specified in the applications for financing from the DEP |
| | 6.2.5 | Coordination of activities and organisational and technical support for cooperation with partner special services | 2025 (ongoing task) | 2029 | AW, ABW, SKW, SWW | Government administration institutions | Increasing the efficiency and effectiveness of actions through the coordination of activities | The number of and effectiveness of undertakings executed in cooperation with partners |
| | 6.2.6 | Establishing cooperation in the cyber domain with a larger number of foreign entities | 2025 (ongoing task) | 2029 | National Cybersecurity System entities as per to their scope of responsibility | Authorised foreign authorities | Increasing the informational potential in the cyber domain relevant for the intelligence service | The number of provided information reports |
| | 6.2.7 | Participation in international PACE exercises | 2025 (ongoing task) | 2029 | RCB | Ministries and central offices, ABW, AW, CSIRTs, and authorities responsible for critical infrastructure | Planning, preparing, and coordinating exercises at the national level and in relations between international stakeholders | – |
| | 6.2.8 | Organisation of specialised technical training courses in the area of cybersecurity using | 2024 (ongoing task) | 2029 | MON | ECSC, MC | Building recognition and the strong position of Poland in the international arena. | The number of conducted training courses and the number of participants |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| | | modern CyberRange platforms, intended for cooperating entities from EU/NATO member states and Ukraine | | | | | Improving the level of knowledge and skills of the personnel responsible for maintaining the security of the infrastructure entrusted to them | |
| | 6.2.9 | Organisation of international specialised cybersecurity exercises using modern CyberRange platforms | 2024 (ongoing task) | 2029 | MON | ECSC, MC | Testing knowledge and verifying acquired skills, as well as team building for cybersecurity teams in direct operations – defensive and offensive alike | The number of conducted exercises and the number of participants |
| | 6.2.10 | Running the National Point of Contact for cooperation with NATO | 2025 (ongoing task) | 2029 | DKWOC/MON | SZRP | Strengthening cybersecurity cooperation with the competent NATO bodies and member states | The number of joint undertakings/activities |
| | 6.2.11 | Active participation in the CSIRT Network, particularly regarding information sharing | 2025 (ongoing task) | 2029 | National-level CSIRTs | MC, MSZ, competent authorities | Effective and active sharing of threat information, sharing good practices, and cooperating in response to incidents and attacks | – |
| | 6.2.12 | Participation in working and expert groups at the EU and international level in the area of cybersecurity | 2025 (ongoing task) | 2029 | MC, MSZ | National-level CSIRTs, competent authorities | Effective and active expert cooperation in various areas of cybersecurity and threats, sharing good practices, and cooperating to address incidents and attacks | – |
| 6.3 Coordination of international activities | 6.3.1 | Coordination activities of the Government Plenipotentiary for | 2025 (ongoing task) | 2029 | Government Plenipotentiary for Cybersecurity | MC, MSZ, MON | Coordination of national activities related to civil-military cooperation | – |

| Area of action | Task No. | Task name | Schedule | | Competent institution(s)[31)] | | Expected results | Metric |
|---|---|---|---|---|---|---|---|---|
| | | | Start date | End date | Leading institution | Cooperating institution(s) | | |
| related to civil-military cooperation in the field of cybersecurity | | Cybersecurity in the field of international civil-military cooperation on cybersecurity | | | | | in the field of cybersecurity | |
| | 6.3.2 | Coordination of activities and information sharing with partner special services | 2025 (ongoing task) | 2029 | AW, ABW, SKW, SWW | Government administration institutions | Increasing the efficiency of actions through the coordination of activities | The number of and effectiveness of undertakings executed in cooperation with partners |
| | 6.3.3 | Participation in international CMX exercises | 2025 (ongoing task) | 2029 | MC, RCB, competent authorities, national-level CSIRTs | Ministries and central offices, AW, authorities responsible for critical infrastructure | Planning, preparing, and coordinating exercises at the national level and in relations between international stakeholders | – |