Ministry
of Digital Affairs

CYBERSECURITY STRATEGY OF THE

REPUBLIC OF POLAND

FOR 2019 – 2024

Marek Zagórski
Minister of Digital Affairs

Ladies and gentlemen,

Hereby I present to you a Cybersecurity Strategy of the Republic of Poland for 2019-2024. It is a result of analysis of current and future challenges and threats to the increasingly vigorous digital transformation of the Polish economy and public administration.

The strategy defines the areas of activities supporting the implementation of the main objective, which is to increase the level of resilience to cyber threats and to strengthen data protection through the development of the National Cybersecurity System, which consists of professional staff, threat-conscious users, safe and effective processes along with modern and security-checked information technologies.

The adoption of the Act on the national cybersecurity system in 2018 created the legal and organisational basis for building, for the first time in history, a comprehensive cybersecurity system in Poland. This system will be continuously developed, as clearly indicated in one of the specific objectives set out in the Strategy. Moreover, the priorities of the Polish government in the area of information security were indicated. These include raising public awareness on cyber threats, supporting initiatives aimed at creating innovative solutions and tools, strengthening cooperation with the private sector and developing digital services using new generations of mobile networks and large-scale data collection and analysis systems.

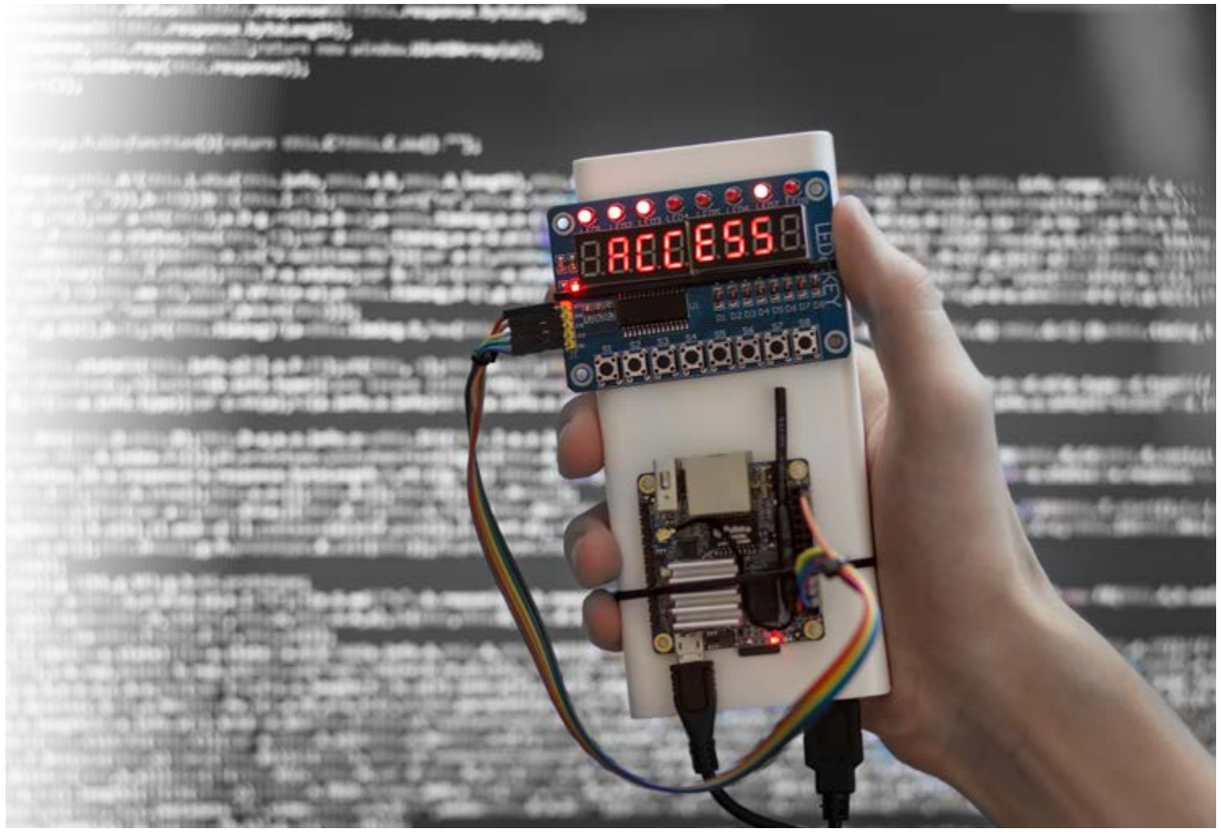
A high level of cybersecurity can be achieved through the wide application of best practices, implementation of new legislative and organisational solutions, as well as through international operational cooperation and information sharing.

The strategy is also a starting point for the development of a detailed Action Plan, which will include specific projects with key performance indicators and identification of financing sources.

The Act, the Strategy and the future Action Plan are a set of tools for public administration. The tools that have one common goal - to ensure safe, undisturbed access to the opportunities resulting from the digital transformation, serving the rapid development of the economy and raising citizens' living standards.

CYBERSECURITY STRATEGY OF THE REPUBLIC OF POLAND

Table of contents



1. Introduction – rationale for actions to increase cybersecurity

Fast and unhindered access to information which is used in the management, production, services and the public sector has more and more impact on social and economic growth. Dynamic progress of information systems serves the development of the national economy, in particular communications, commerce, transport and financial services. Digital technologies that comprise cyberspace[1] are used for shaping social relationships. Moreover, online services have become a tool for effecting on the behaviour of social groups, as well as exerting influence in the political sphere.

Any significant disruption to the functioning of cyberspace, whether global or local, will have an impact on economic activity, citizen's sense of security and safety, the efficiency of public sector institutions, production and service processes, and as a result on national security in general.

Protection of information systems and information processed therein is a challenge for all entities of the national cybersecurity system, i.e. businesses providing services using information systems, public authorities, institutions responsible for the national security, and specialised entities dealing with cybersecurity at the operational level. It is even more important as Poland is closely connected with other countries through international cooperation within organisations such as the European Union (EU), the North Atlantic Treaty Organisation (NATO), the United Nations (UN) and the Organisation for Security and Cooperation in Europe (OSCE). This cooperation plays an important role in responding to the increasing number of incidents caused by illegal activities in cyberspace that are leading to tangible and reputational damages which are growing by the year. Criminal activities are being taken by individuals, organised crime groups, as well as, groups sponsored by governmental institutions and armed forces of countries which conduct offensive actions focused specifically on cyberespionage and gathering intelligence on other states' defence capabilities.

[1] Cyberspace is the space for processing and exchanging information formed by ICT systems defined in Article 3(3) of the Act of 17 February 2005 on the computerisation of activities of entities performing public tasks (Journal of Laws of the Republic of Poland of 2019, items 700, 730, 848 and 1590), including relations between them and relationships with the users – in accordance with Article 2(1b) of the Act of 29 August 2002 on the martial law and competences of the Supreme Commander of the Armed Forces and the rules of his subordination to the constitutional authorities of the Republic of Poland (Journal of Laws of the Republic of Poland of 2017, item 1932).

CYBERSECURITY STRATEGY OF THE REPUBLIC OF POLAND

2. Strategic context of cybersecurity in the Republic of Poland

The Cybersecurity Strategy of the Republic of Poland for 2019–2024 is a continuation and extension of actions taken by the government administration to increase the level of cybersecurity in the Republic of Poland. As part of actions taken to date, the Act of 5 July 2018 on the national cybersecurity system (Journal of Laws of the Republic of Poland, item 1560)[2] entered into force and the government beforehand also adopted the following documents:

- **in 2013, the Policy for the Protection of Cyberspace of the Republic of Poland,**
- **in 2017, the National Framework of Cybersecurity Policy of the Republic of Poland for 2017–2022.**

The Cybersecurity Strategy of the Republic of Poland for 2019–2024 supersedes the National Framework of Cybersecurity of the Republic of Poland for 2017–2022 adopted under Resolution no. 52/2017 of the Council of Ministers of 27 April 2017 regarding the National Framework of Cybersecurity of the Republic of Poland 2017–2022.

The purpose of this document is to define strategic objectives and relevant political and regulatory measures to achieve a high level of cybersecurity, principally a resilience to cyber threats of information systems used by operators of essential services , critical infrastructure operators, digital service providers and the public administration, as well as to increase information protection in the information systems by means of standardised safeguards. The achievement of the strategic objectives shall also contribute to increasing the national security, improving the effectiveness of law enforcement agencies and judicial authorities in detecting and combating cybercrime, events of a hybrid nature (including events of a terrorist nature) and cyberespionage.

The Cybersecurity Strategy of the Republic of Poland for 2019–2024 is aligned with ongoing operations related to ICT systems used by critical infrastructure operators. It also takes into account the need to enable the Armed Forces of the Republic of Poland - in domestic, alliance and coalition contexts - to conduct military operations in the event of cyber threat which requires defensive operations.

By implementing the Cybersecurity Strategy of the Republic of Poland for 2019–2024, the government will fully guarantee the right to privacy and hold the position that free and open Internet is an important element of the functioning of a modern society.

[2] The Act of 5 July 2018 on the national cybersecurity system implements 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 (Official Journal of the EU L 194, 19.07.2016, p. 1).
[3] Applies to operators of essential services referred to in Article 5 of the Act of 5 July 2018 on the national cybersecurity system.
[4] Applies to digital service providers referred to in Article 17 of the Act of 5 July 2018 on the national cybersecurity system.

CYBERSECURITY STRATEGY OF THE REPUBLIC OF POLAND

3. Scope of the Cybersecurity Strategy of the Republic of Poland for 2019–2024

The Strategy takes into account, in particular[5]:

1. **cybersecurity objectives and priorities;**
2. **entities involved in the implementation and deployment of the Strategy;**
3. **measures used to achieve the objectives of the Strategy;**
4. **specification of means for readiness, response and restoration, including principles of public-private cooperation;**
5. **risk assessment approach;**
6. **activities related to educational, information and training programmes regarding cybersecurity;**
7. **activities related to research and development plans regarding cybersecurity.**

Furthermore, the Strategy takes into account international cooperation regarding cybersecurity.

Introduced by way of a resolution of the Council of Ministers, the Cybersecurity Strategy of the Republic of Poland for 2019–2024 directly affects entities of the government administration and, indirectly, after the adoption of applicable general law on the initiative of the Council of Ministers, other public authorities, businesses and citizens.

[5] Article 69(2) of the Act 5 July 2018 on the national cybersecurity system.

4. Vision, main goal, specific objectives

4.1 Vision

The efficient and safe operation of information systems and means of electronic communication are resulted in the successful growth of the Republic of Poland, the increasing t effectiveness of the economy and performance of institutions and entities, including also its social activity and everyday functioning of individual members of the society. Therefore, as part of actions planned in the Cybersecurity Strategy by the year 2024, the government shall systematically enhance and develop the national cybersecurity system. The said actions include systemic organisational, operational, technological and legal measures as well as shaping social attitudes and conducting research and development projects to ensure achievement of high cybersecurity standards of software, hardware and digital services. The government shall take these actions by building confidence between the private sector and the public administration while respecting the rights and freedoms of the citizens.

4.2 Main goal

Increasing the level of resilience to cyber threats[6] and protection of information in the public, military and private sectors, as well as promoting knowledge and good practices to enable the citizens to better protect information.

[6] "Cyber threat" means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons – in accordance with Regulation (EU) No. 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (Official Journal of the EU, L 151, 07.06.2019, p. 15).

4.3 Specific objectives

Specific objective 1.
Development of the national cybersecurity system.

Specific objective 2.
Increasing the level of resilience of information systems of the public administration and private sector, and achieving the capacity to effectively prevent and respond to incidents.

Specific objective 3.
Increasing the national capacity in the area of cybersecurity technology.

Specific objective 4.
Building public awareness and competences in the area of cybersecurity.

Specific objective 5.
Building strong international position of the Republic of Poland in the area of cybersecurity.

5. Specific objective 1 – Development of the national cybersecurity system

5.1 Implementation and evaluation of the functioning of the provisions regarding the national cybersecurity system

The development of the national cybersecurity system is based on full implementation and evaluation of the functioning of provisions establishing the system, by reference to other regulations, in particular the Act of 26 April 2007 on crisis management (Journal of Laws of the Republic of Poland of 2019, item 1398), the Act of 5 August 2010 on the protection of classified information (Journal of Laws of the Republic of Poland of 2019, item 742) and the National Security Strategy of the Republic of Poland. The evaluation may entail the necessity to introduce respective amendments of provisions which remove barriers to effective information sharing and responding to incidents in a coordinated and unhindered manner.

Amendments to regulations regarding the functioning of the national cybersecurity system shall arise also from practical functioning of Directive (EU) No. 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 (Official Journal of the EU, L 194, 19.07.2016, p. 1), hereinafter referred to as „the NIS Directive", at the European level. Experience arising from application of regulations in this respect shall also be a premise to request amending the provisions of the NIS Directive itself at the EU level in order to improve its effectiveness. Among areas requiring such amendments shall be further specification of responsibilities of digital services providers, specifically ones that provide cloud computing services which will be increasingly used as a data processing model for essential services.

The responsibility for drafting amendments to regulations in the area of cybersecurity within their respective remits shall rest on competent ministers as defined in the Act of 4 September 1997 on divisions of the government administration (Journal of Laws of the Republic of Poland of 2019, items 945, 1248 and 1696) and competent authorities in accordance with the Act of 5 July 2018 on the national cybersecurity system.

As part of the legislative work, the minister competent for digitalisation, in cooperation with other ministries and competent authorities responsible for supervision of ICT systems in respective sectors, shall review sectoral and specific regulations which address the subject in question, as well as regulations which might affect other areas, for example personal data protection or critical infrastructure in the context of the National Critical Infrastructure Protection Programme. It shall also be necessary to undertake legislative work to regulate the area of development, acquisition and operation of specialised dual-use tools for the purpose of defensive and offensive operations in cyberspace.

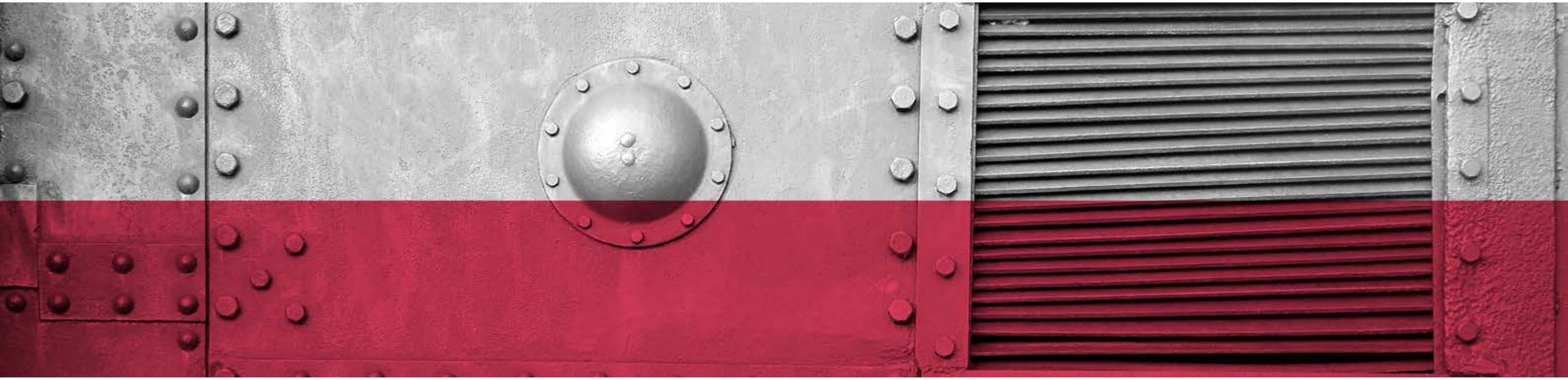
The implementation of the Cybersecurity Strategy shall involve regulating the issues of operational cooperation, including proper coordination of actions and information sharing between authorities responsible for the national security, counter-terrorist efforts as well as internal security and public order.

Due to rapid pace of changes occurring in area of cybersecurity, it will be necessary to continuously monitor the phenomena taking place there and initiate possible amendments in the law. Proposed directions and plans regarding counteracting cyber threats shall be reviewed by the Advisory Committee for Cybersecurity under the Council of Ministers. It is a consultative and advisory body of the Council of Ministries in cybersecurity matters. Among its remits is also evaluation of operations of CSIRT MON, CSIRT NASK, CSIRT GOV as well as sectoral cybersecurity teams and competent authorities for cybersecurity.

5.2 Enhancing the efficiency of the functioning of the national cybersecurity system

The efficiency of the national cybersecurity system shall be enhanced by means of launching by 1 January 2021, by the minister competent for digitalisation, an ICT system supporting:

1. cooperation of entities of the national cybersecurity system;
2. generation and transfer of recommendations of activities increasing the level of cybersecurity;
3. incident reporting and handling;
4. risk assessment at the national level;
5. cyber threat warnings.



Competent authorities responsible for supervision of ICT systems in sectors where essential and digital services are provided shall take actions to support the operators and providers in ensuring the security of their services. To this end, the competent authorities shall have a right to issue organisational and technical recommendations and provide tools and knowledge regarding the best sectoral and cross-sectoral practices which increase cybersecurity. Development of the national cybersecurity system also entails the further increasing of capacity of institutions dealing with cybersecurity at the operational level, including the three CSIRTs at the national level and cooperating with them sectoral cybersecurity teams as well as information sharing and analysis centres. It is necessary to set up systemic solutions to share information and e knowledge about vulnerabilities, threats and incidents between all stakeholders.

Within the framework of cooperation of government administration and local administration, the government shall recommend and act for local administration units in the area of increasing their competences in designing cybersecurity enhancing processes, specifically the selection, deployment and maintenance of technical assets that increase cybersecurity, including the utilise of state-of- the-art and secure cloud computing models, development of secure applications and utilise of secure mobile systems.

Efficiency of the functioning of the national cybersecurity system shall also be increased by introducing standardisation of security solutions, including introduction of minimum security requirements for ICT networks and systems operated by the public administration. The standardisation and cybersecurity requirements, developed and used by the public administration as part of the National Cybersecurity Standards, should also become a determinant of good practices for the private sector and citizens.

Sectoral and national exercises, initiated by the Government Plenipotentiary for Cybersecurity, shall verify the efficiency of the functioning of the national cybersecurity system. Moreover, the capabilities of the Armed Forces of the Republic of Poland to conduct defensive operations in cyberspace will be increased through participation in national and international cybersecurity exercises.

5.3 Development of an information sharing system for the purpose national security management

In order to increase the efficiency of management of national security, actions shall be taken to ensure information sharing and consultation of responses both at the strategic and operational level, in particular between the civilian and military spheres. It is necessary to set up an information sharing system for the public administration that would be resilient to cyber threats and based on state-of-the-art information sharing technologies taking into account the need for high mobility. The system shall be used in various states of exception and states of national defence readiness.

5.4 Enhancing cybersecurity of essential and digital services and critical infrastructure

Information technologies (IT) used by operators of essential services, digital service providers, critical infrastructure operators (including telecommunications operators) are a critical element in

ensuring citizens security and continuity of operation of the state. Moreover, security of the most important sectors of the economy, specifically the energy sector, depends on ensuring undisturbed operation of industrial operational technologies (OT). This is why the government shall take ensuring of IT and OT cybersecurity as a priority. This has already been reflected in analyses regarding specification of security requirements that must be met by telecommunications operators, specifically when building the 5G network which will become the backbone for the functioning of the state in the area of mobile telecommunications. It is assumed that some legal amendments must be taken in this area in order to enable an appropriate control of ensuring cybersecurity.

Furthermore, bearing in mind that the sole responsibility for ensuring security of services relies primarily on providers, the government shall take supporting actions to increase capacity and competences in cybersecurity of operators of essential services, critical infrastructure operators and digital service providers. These actions, for ensuring its adequacy, shall take into account their different specifics and their different cybersecurity maturity. In addition, the government shall support all these entities in responding to significant, critical and substantial incidents, especially in the event of cross-sectoral incidents.

Firstly, consistent actions shall be taken to develop criteria of identification of critical infrastructure operators and operators of essential services, taking into account the need for including them into the crisis management system. This process shall be carried out in cooperation with all sectors. Based on mechanisms provided for by a law, minimum cybersecurity requirements shall be recommended with a particular focusing on business continuity management.

Digital service providers shall be covered by a similar regime. However, the government is fully aware of the international nature of these entities and of the need to ensure such a regulations that support the development of a digital market in Poland. Therefore, actions in this area shall be conducted at the European level, particularly within the NIS Cooperation Group, and within the framework of transatlantic cooperation with British and American institutions which stir improvement of cybersecurity standards among digital service providers.

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

A joint static and dynamic risk assessment methodology that take into account the specificity of individual sectors, critical infrastructure operators, operators of essential services and digital service providers, shall be introduced for the purpose of cybersecurity management at the national level. This shall ensure comparability

of assessment, also regarding risk levels, in particular for the purpose of the national security risk reports, developed in accordance with the crisis management regulations. Risk assessment shall become a continuous process that will enable depicting the risk level in near real time.

The methodology and tools enabling static and dynamic risk assessment in ICT systems are being developed as part of the National Cybersecurity Platform project funded by the National Centre for Research and Development – the completion of work is scheduled by the end of 2020.

5.6 Increasing capacity to counteract cybercrime, including cyberespionage and incidents of a terrorist nature

With regard to increasing the capacity to counteract cybercrime, including cyberespionage and events of a hybrid nature (including events of a terrorist nature), it is important to provide support to operators of essential services, digital service providers and critical infrastructure operators so that they can detect and combat incidents at any stage. To this end, cooperation and coordination of actions of law enforcement agencies is required irrespective of the motives of the perpetrators, and appropriate preservation of digital evidence is particularly important.

Increasing the effectiveness of procedural and operational activities requires establishing and broadening the interaction of law enfo rcement agencies with other entities that may have knowledge which is helpful to determine the substance of an offence or identify the perpetrator. This includes cooperation with national and international private sector entities, in particular in the telecommunications, banking and insurance sectors. It is also necessary to ensure continuous information sharing on threats and vulnerabilities, both at the national and international level.

Given the nature of cyberspace, combating cybercrime requires cross-border cooperation of law enforcement agencies and CERT/CSIRT units. The time factor is critical in procedural actions and operational investigation related to offences committed in cyberspace.

This means that efficient and reliable information sharing channels between law enforcement agencies of different countries are required.

Given the dynamic nature of cyberspace offences and the related need to take procedural and operational actions, it is necessary to introduce regulations that enable processing and transfer of electronic procedural documents.

Rapidly changing methods of crime require development of research in the field of combating cybercrime, the results of which will provide support to law enforcement agencies. The results of this research will be used in the work of law enforcement and judicial authorities, and will provide material to develop preventive measures. Awareness campaigns shall be enrolled to inform the public about cybercrime threats and methods to prevent or mitigate them. Operators of essential services, providers of digital and Internet access services as well as NGOs and public entities shall play an important role in this type of activity.

[7] The methodology and tools enabling static and dynamic risk assessment in ICT systems are being developed as part of the research project titled „The National Cybersecurity Platform", carried out by the Research and Academic Computer Network (NASK) and funded by the National Centre for Research and Development as part of the CyberSecIdent Programme – Cybersecurity and e-Identity.

6. Specific objective 2 – Increasing the level of resilience of information systems of the public administration and private sector, and achieving the capacity to effectively prevent and respond to incidents

6.1 Development and implementation of National Cybersecurity Standards and disseminate of good practices and recommendations

Based on the expertise of technical committees of the Polish Committee for Standardisation, research centres, academia and research institutes as well as public and private entities concerned, new standards shall be developed or the existing norms and standards shall be translated into specific recommendations regarding their implementation.

In order to increase the resilience to cyber threats of information systems used by the public administration it is necessary to develop National Cybersecurity Standards as a set of organisational and technical requirements regarding, in particular, the security of:

- applications;
- mobile devices;
- workstations;
- servers and networks;
- cloud computing models.

In order to ensure secure and cost-effective processing infrastructure of the public administration's IT systems, which will soon start using new forms of processing and storage of information, including cloud computing, it will be necessary to develop recommendations and disseminate good practices which increase the resilience to potential cyber threats. Execution of public tasks, in particular, ones connected with cybersecurity, shall be supported by application of Polish Standards based on the European and international standards. References to standards should also be widely used over the entire life cycle of the ICT systems. It is also important to support execution of recommendations issued by market regulators.

6.2 Supply chain security

Ensuring cybersecurity requires application of organisational and technical protections over the entire life cycle of the ICT systems. These actions comprise the so-called secure supply chain and include designing, developing, deploying, operating and disposing g. The term supply chain means a system which consists of subsystems of production, distribution, transport, storage and recycling of ICT systems components, as well as their installation, launch, ongoing maintenance, servicing and repairs.

An important element of ensuring a quality assurance in the supply chain is the evaluation and certification of products (software, hardware and services in particular). The priority in this regard shall be to establish, and subsequently maintain and develop, a national s cybersecurity evaluation and certification scheme based on operations of accredited conformity assessment bodies, which shall enable the Republic of Poland to achieve full and internationally recognised status of an Authorizing Member country in providing cybersecurity solutions.

The Republic of Poland shall actively participate in the work on establishing European cybersecurity certification schemes in accordance with Regulation (EU) No. 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act).

Actions at the national level shall include, in particular, designation of the national cybersecurity certification authority which shall issue European cybersecurity certificates, supervise national conformity assessment bodies which assess compliance of products, services and processes with the requirements set forth in the European cybersecurity certification schemes and cooperate with the national accreditation body – the Polish Centre for Accreditation in order to monitor and supervise activities of accredited national conformity assessment bodies which assess compliance with respect to the requirements of Regulation (EU) No. 2019/881 of the European Parliament and of the Council.

These actions shall result in achieving, at the national level, the ability to support Polish manufacturers which, when holding European cybersecurity certificates, will be able to compete more efficiently on the of the European Union's Digital Single Market.

6.3 Security tests and audits

Periodic audits are among measures that enable assessment of the effectiveness of the currently implemented information security management systems and the adequacy of the safeguards introduced. Audit methodologies should take into account applicable standards, good practices and specificity of respective sectors. The aim of such an approach is to achieve comparability of audit outcomes.

Periodic tests (including penetration testing), which provide for a real assessment of the system's resilience to threats, are another security assessment measure. Outcomes of these tests are the basis for verification of the safeguards deployed. In order to utilise the public capacity in the area of cybersecurity, the so-called bug-bounty[8] testing shall be disseminated.

[8] Bug-bounty – search for software vulnerabilities conducted by people not associated with the software developer, usually with the general consent of the developer.

7. Specific objective 3 – Increasing the national capacity in the area of cybersecurity technology

7.1 Development of industrial and technological resources for the purposes of cybersecurity

The government aims to invest in development of industrial and technological resources for the purpose of cybersecurity by creating the conditions needed for the development of businesses, in particular SMEs and start-ups, as well as research and development institutes which are dealing with a development of new solutions in the area if cybersecurity. The priorities include increased capabilities in the area of designing and producing software, hardware and services used in all branches of the Polish industry to improve its competitiveness.

The acquisition of new technologies for development of domestic ventures shall also be realised through participation in international initiatives that emphasise innovation, and through bilateral cooperation and within international organisations, including the European Cybersecurity Industrial, Technology and Research Competence Centre planned by the European Commission and the EU's Member States. Moreover, the government shall strive to actively disseminate knowledge and trainings among Polish entrepreneurs and to implement cybersecurity technologies enabling full use of the capabilities of other state-of-the-art digital technologies, including AI-based autonomous systems, in production and service provision processes.

Actions shall be taken to stir the increase of cybersecurity competences of research and higher education institutions. By means of legal instruments, the government shall stir higher education institutions to provide teaching helpful in attracting cybersecurity specialist, including as part of first and second-cycle studies, doctoral schools and post-graduate programmes.

In order to even the chances of Polish entrepreneurs on the global market, the government shall support development of digital competences of Polish businesses and ensure assistance in applying for funding of innovative solutions as well as consultancy regarding access to new markets and assistance in establishing cooperation with other businesses.

7.2 Focus on developing of public-private cooperation

Ensuring security in cyberspace requires joint efforts of the private sector, the public sector and the citizens. The government shall continue to establish an effective public-private partnership system based on trust and shared responsibility for cybersecurity.

[9] Among examples of actions aimed at developing the Polish industry and its competitiveness in the digital transformation era is the „Industry 4.0" programme run by the minister competent for economy. As part of this programme, Digital Innovation Hubs will be selected by way of a competitive process which will provide standardised support to entrepreneurs in digital transformation, including in the area of cybersecurity.

CYBERSECURITY STRATEGY OF THE REPUBLIC OF POLAND

At the same time, public administration shall improve its capacity in initiating and running cybersecurity projects. The government shall also actively participate in the existing and emerging forms of European public-private cooperation, thus promoting Polish business internationally.

In implementing a new vision of the country's development and supporting the innovation of the Polish economy, it will be important to set up a system of support for research and development projects in the area of cybersecurity conducted in cooperation with the academia and businesses.

7.3 Stimulating research and development in the area of cybersecurity

In view of the dynamically growing IT market, especially in view of the shift to IPv6 communication protocol, and in connection with development of the Internet of Things, Smart Cities, Industry 4.0 as well as Cloud Computing, broadband mobile communication network (5G and next generations) and Big Data, it is necessary to intensify research, development and manufacturing activities in the area of cybersecurity. To this end, research programmes[10] aimed at development and implementation of new methods of protection against cyber threats shall be continued in cooperation with the National Centre for Research and Development.

In the face of the dynamical development of technologies related to inter alia the Internet of Things, special attention should be paid to the need to ensure product, service and process security as early as at the design stage (Security by Design)[11] as well as data protection and privacy (Privacy by Design)[12].The government shall disseminate and support the security-by-design approach.

In addition, research programmes shall be developed in cooperation with the scientific and academic community in order to, in particular:

- assess the effectiveness of protections and resilience to cyber threats;
- assess the effectiveness of responding to incidents;
- develop methods of detecting and analysis new types of cybercrime, cyberterrorism and cyberespionage;
- study methods of attacks (including attacks of a hybrid nature) and measures to counteract these attacks and mitigate their effects;
- protect democratic processes against disruption by cyber threats.

[10] The Ministry of Digital affairs will continue to cooperate with the National Centre for Research and Development in inter alia the CyberSecIdent – Cybersecurity and e-Identity Programme.
[11] Security by design – an approach to the product or system development which consists in considering security and integration of security features from the point of conception. Commission Communication „A European Security Research and Innovation Agenda – Commission's initial position on ESRIF'S key findings and recommendations"/*COM(2009)691 final/.
[12] Privacy by design – an approach to data and privacy protection involving appropriate technical and organisational measures, which are designed to implement data-protection principles taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing. Based on Article 25 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) - Official Journal of the EU, L 119, 04.05.2016, pp 1).

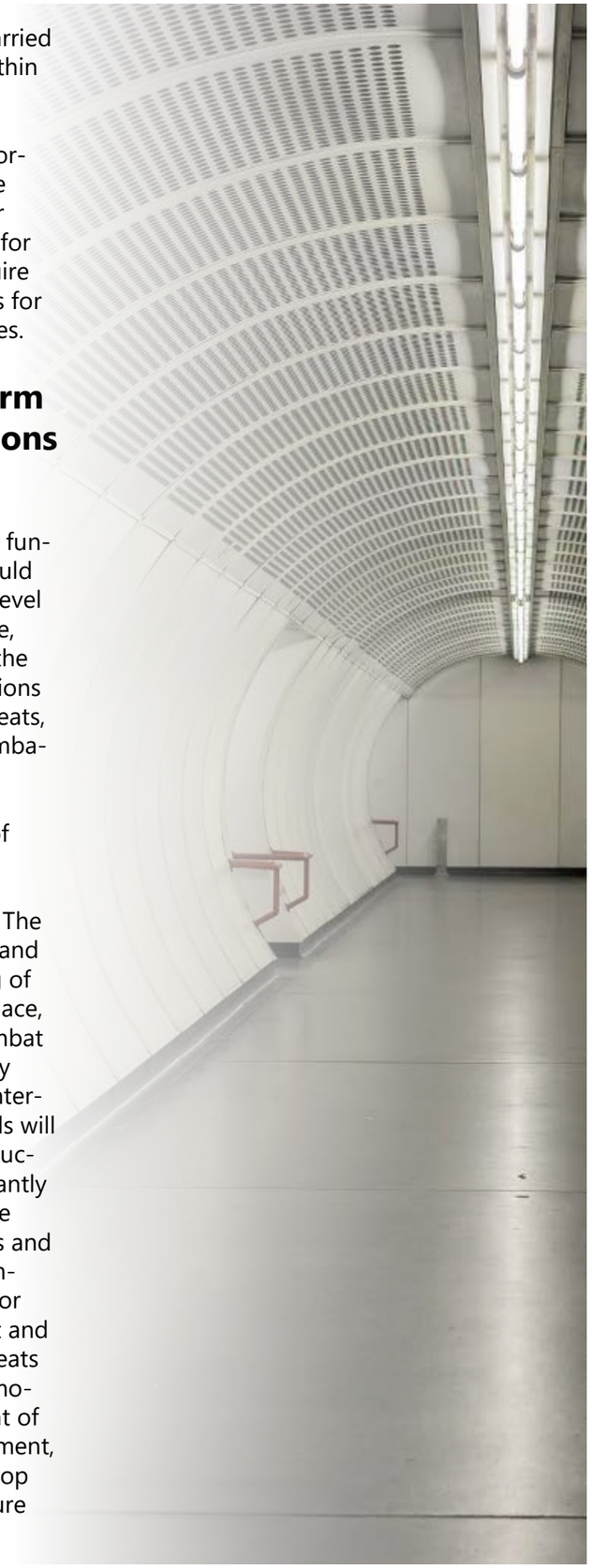
The research and development activities shall be carried out also in the area of international cooperation within the EU and the NATO.

Important tasks for ensuring cybersecurity are performed by non-governmental organisations, which are very efficient organisers of educational activities for the society and providers of analyses and opinions for the public administration. It is also possible to acquire experts with unique skills through analytical centres for the purposes of solving complex cybersecurity issues.

7.4 Gaining the capacity to perform a full spectrum of military operations in cyberspace

The Armed Forces of the Republic of Poland, as the fundamental element of the state defence system, should be involved in activities in cyberspace at the same level as in the air, on the ground and at sea, in peacetime, during war and in crisis situations alike. Therefore, the ability to conduct a full spectrum of military operations in cyberspace must include the identification of threats, the protection and defence of ICT systems, and combating cyber threats.

Activities in cyberspace represent an integral part of planned operations to be conducted by the Armed Forces of the Republic of Poland both on their own and in co-operation within alliances and coalitions. The structure of the Armed Force of the Republic of Poland will be improved by establishing and strengthening of formations tasked with conducting tasks in cyberspace, which have capabilities to identify, prevent and combat cyber threats. Readiness to military and non-military interoperability in cyberspace at the national and international level within alliances, coalitions and accords will be developed. Qualifications of the personnel conducting military operations in cyberspace will be constantly improved by means of training courses. At the same time, threats will be identified on an on-going basis and the situation will be assessed – also in terms of compliance with international law – which will provide for selecting appropriate methods and tools to protect and defend own resources and eliminate sources of threats to ICT networks and systems, both stationary and mobile. Bearing in mind the rapid pace of development of technologies that make up the cyberspace environment, the Ministry of National Defence will strive to develop or acquire an innovative methods and tools to ensure operational effectiveness in this domain.



8. Specific objective 4 – Building public awareness and competences in the area of cybersecurity

8.1 Increasing competence of the staff of entities relevant to ensuring cybersecurity of the Republic of Poland

Competences of the staff of entities relevant to ensuring cybersecurity of the Republic of Poland shall be increased through establishing and introducing of such a model of the academic education and professional development which will ensure appropriate qualifications of employees. To this end, model academic programmes shall be developed for a dedicated field of cybersecurity.

Within the framework of the broadly understood expert education, in order to more effectively counteract growing cybercrime, the system of training for all employees of entities relevant to ensuring cybersecurity and for representatives of law enforcement agencies and the judiciary shall be enhanced by putting in place a dedicated educational programme including both theoretical and practical trainings based on real examples of threats.

In order to retain highly qualified employees in public administration, alongside the use of other instruments supporting their activity, actions shall be taken to bring their salaries closer to the level they could obtain when working in the private sector.

At the same time, the government shall develop and implement a systemic support for increasing competences of employees of the local government administration units in the area of cybersecurity.

The managerial staff of local government administration units shall dynamically define responsibilities and authorisations of persons who play important roles in cybersecurity management and appropriately communicate these decisions to all stakeholders.

8.2 Creating conditions for the safe use of cyberspace by citizens

Cybersecurity education should be available as early as possible in the process of accessing digital services by children and youth – preferably even before they enter the digital world,. In practice, it is often required at the stage of early childhood education. Having regard to the issue of safe use of cyberspace, it is assumed that teachers shall receive support in execution their respective teaching programme, specifically in updating their teaching programmes through various activities conducted in accordance with the current knowledge regarding safe use of modern technologies.

In addition, actions shall be taken to support continuous professional development of teachers in the area of modern technologies and cybersecurity, taking into account diagnosed needs of a given school or establishment.

Higher education institutions shall be encouraged to develop interdisciplinary specialisations covering inter alia information security management, assessment and evaluation of ICT system safeguards, protection of personal data, protection of intellectual property on the Internet as well as issues related to the development of new technologies and the related challenges.

8.3 Developing public awareness towards the safe use of cyberspace

In cooperation with NGOs, academia and private sector, the public administration shall continue systemic actions to raise public awareness of the cyber threats. Educational actions shall be taken regarding the rights and freedoms in the digital environment and the rights of cyberattack victims and individuals who suffered losses as a result of on-line privacy breaches. Public campaigns aimed at various target groups, including children, parents and elders, shall also be continued.

In the face of increasingly numerous threats aimed at exerting specific influence on the society, and having regard to consequences of intentional use of social engineering tools to carry out manipulative actions, such as disinformation campaigns and inspirational or disintegration actions, it is required to take systemic measures to develop public awareness in the context of verifying authenticity of information and responding to attempts to distort in. As regards defence against manipulative actions, which may be an element of a hybrid nature operations, it is important to build capabilities among the society to identify actions aimed at affecting awareness or converting or disintegrating specific communities.

9. Specific objective 5 – Building strong international position of the Republic of Poland in the area of cybersecurity

9.1 Active international cooperation at the strategic and political level

In the face of the widespread globalisation processes and the related interdependence between countries, international cooperation is crucial for achieving security of global cyberspace.

While carrying out these tasks at the European level, the Republic of Poland shall intensify its efforts to ensure the security of the EU's Digital Single Market - the driving force behind economic growth and innovation. Moreover, it is important to strive to take greater account of the aspects of cybersecurity in the work on development of the Common Foreign and Security Policy of the European Union.

Poland's membership in the North Atlantic Treaty Organisation is an important pillar of the country's security, as well as the security of entire Euro-Atlantic area. Ever more intensive attacks of a hybrid nature make it essential to invest in deterrence and defence capabilities, including increasing of the resilience and ability to respond quickly and effectively to cyberattacks.

Through cooperation within the United Nations system, the Republic of Poland shall strive to continue the debate on an effective system of governance of the world wide web and issues related to the legal aspects of cyberattacks in order to develop coherent solutions that ensure the reliability of international information sharing on the Internet. In the legal and international context, it is crucial for individual countries to strive to achieve the widest consensus possible regarding the manner in which international law applies to cyberspace activities. The Republic of Poland – in cooperation with like-minded partners – shall promote the position that international law, now in force, most importantly the United Nations Charter, applies to cyberspace. The Republic of Poland acknowledges its commitment to the voluntary principles of responsible state behaviour in cyberspace developed by the UN Group of Governmental Experts, and calls for application of the entire international law to state activities in cyberspace and implementation of confidence building measures to mitigate the risk of conflicts arising from cyber threats. The Republic of Poland shall actively participate in strengthening security and confidence building measures within the existing international fora, including the OSCE. The government shall also join the efforts to effectively combat cybercrime internationally.

Particular importance is attached to cooperation with the countries of the region, including strengthening of cooperation within the Visegrad Group and Three Seas Initiative. Implementation of the Polish foreign policy can also include signing bilateral and multilateral international agreements or legally non-binding understandings regarding co-

operation in the area of cybersecurity with countries of developed technological capacity.

Strengthening of international position of the Republic of Poland will only be possible through internal close collaboration between Polish institutions and agencies responsible for ensuring cybersecurity, especially between the Ministry of Digital Affairs and the Ministry of Foreign Affairs, which is solely responsible for the coordination of the foreign policy of the Republic of Poland.

Achieving a strong international position of the Republic of Poland in the area of cybersecurity will not be possible without having the necessary domestic expertise. Staff resources supported by adequate funding shall be the basis for building the image of the Republic of Poland as a competent player at the international area. In this context, it is important for Polish experts to actively participate in discussions in regional and global fora and perform a key roles in international organisations, thus contributing to the successful execution of foreign policy in the area of cybersecurity. In order to acquire skills, develop knowledge and share best practices, the Republic of Poland shall attach ever greater importance to international bilateral and multilateral cooperation in matters of education, training and exercise, as well as awareness building.

In the area of international cooperation, the Republic of Poland will actively participate in exercises conducted by national organisations, EU and NATO as well as other international agencies.

9.2 Active international cooperation at the operational and technical level

International cooperation at the operational and technical level shall be carried out inter alia within the CSIRT Network at European Union level, in other fora for information sharing and analysis of the IT security situation of a given sector, through other international cooperation networks, like the FIRST or TF-CSIRT, information sharing platforms, like the MISP or n6, and within bilateral and multilateral cooperation. In this context, it shall be particularly important to develop common operational procedures within the EU and NATO, and the Visegrad Group. Cooperation at this level will not only serve to effectively counteract cyber threats , but will also contribute to the share of experience between technical staff in joint ventures. It shall also be an opportunity to promote Polish technological solutions and Polish expert staff.

Development of international cooperation is also possible through participation of public institutions involved in ensuring cybersecurity in international fora for information sharing on threats and vulnerabilities.

10.Managing the Cybersecurity Strategy of the Republic of Poland

The Cybersecurity Strategy is adopted for a period of 5 years.

The implementation of the Cybersecurity Strategy is coordinated by the minister competent for digitalisation.

The document is subject to review and evaluation two years after its adoption and in the fourth year of its term. The outcomes of the review are presented to the Council of Ministers. As a result of the review, the minister competent for digitalisation shall draft a proposal of corrective actions or a draft document for the next five-year period. Where justified, the Cybersecurity Strategy may be updated at dates other than said above.

Within six months of the adoption of the Cybersecurity Strategy, the Coordinator - in cooperation with members of the Council of Ministers, heads of central offices, Director of the Government Centre for Security and other authorities listed in the Act of 5 July 2018 on the national cybersecurity system - shall develop an Action Plan for the Implementation of the Cybersecurity Strategy and submit it to the Council of Ministers for approval. When developing the Action Plan, the above-mentioned authorities shall take into account in their activities the issues of cybersecurity in accordance with their statutory remit. The Action Plan shall include, in particular:

- name of a specific objective;
- name of the task;
- name of the action serving the accomplishment of the task;
- type of action – legislative, organisational, technological, educational, informational, promotional, other;
- schedule – the start and end date of the initiative concerned;
- authority or authorities – the leading authority and authorities cooperating in the execution of the task (if any);
- expected impacts;
- estimated cost.

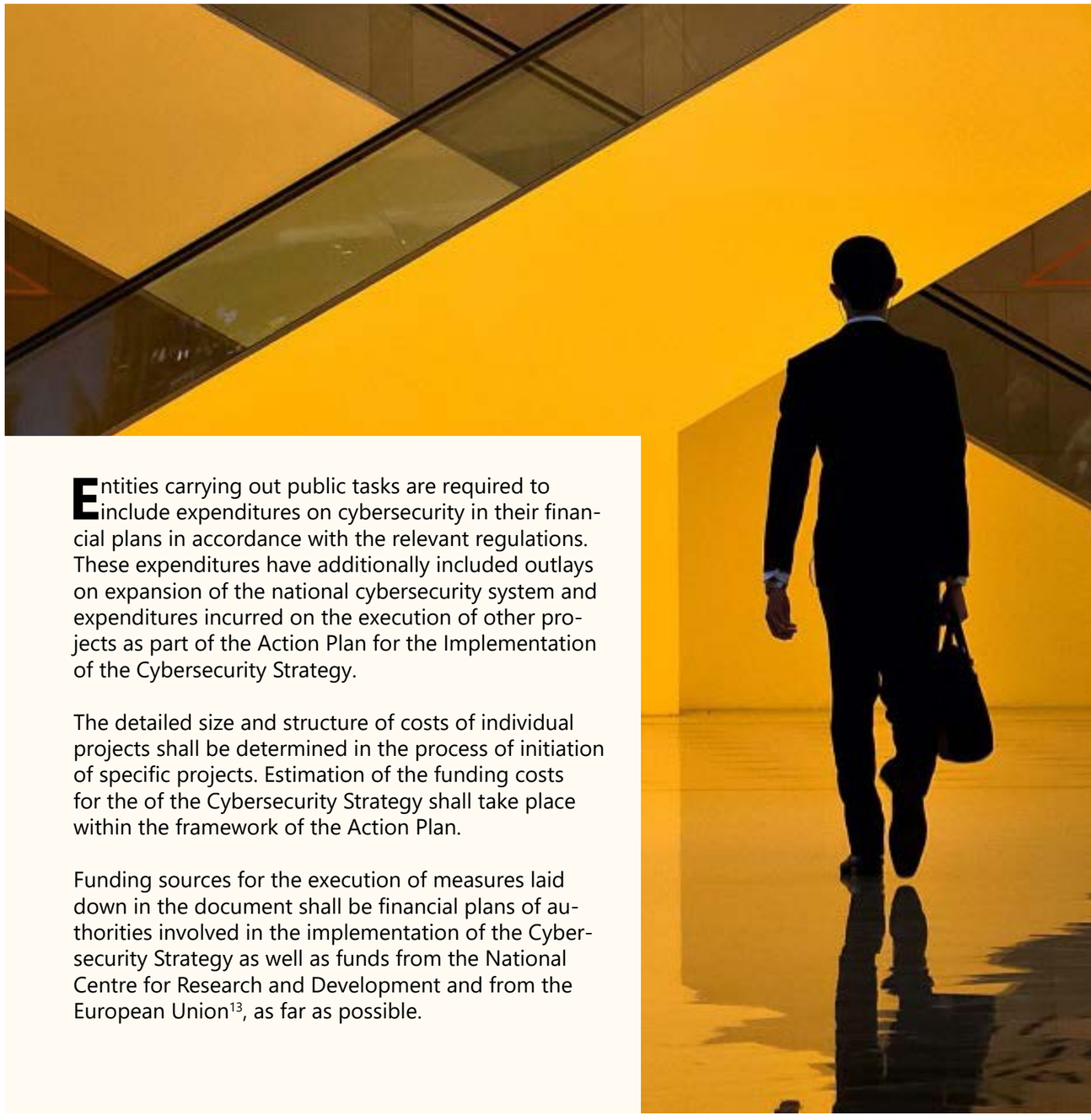
The Action Plan includes project-type actions with the start and end date of execution and deliverables.

The Minister of National Defence may, in consultation with the Coordinator, develop a separate Action Plan which is subject to an approval by the President of the Council of Ministers. Elements of the Action Plan which contain classified information are subject to the provisions of the Act of 5 August 2010 on the protection of classified information (Journal of Laws of the Republic of Poland, item 742). The Minister of National Defence sends, for the purposes of information and coordination, the accepted Action Plan to the minister competent for digitalisation and the Government Plenipotentiary for Cybersecurity.

The Coordinator shall annually develop a progress report on the implementation of the Cybersecurity Strategy for the previous year on the basis of information received from the entities involved in its execution. The reports shall be submitted to the Council of Ministers by 30 September.

If a separate Action Plan is developed, the Minister of National Defence submits a report on the execution of that Action Plan to the Council of Ministers via the Coordinator.

11. Funding



Entities carrying out public tasks are required to include expenditures on cybersecurity in their financial plans in accordance with the relevant regulations. These expenditures have additionally included outlays on expansion of the national cybersecurity system and expenditures incurred on the execution of other projects as part of the Action Plan for the Implementation of the Cybersecurity Strategy.

The detailed size and structure of costs of individual projects shall be determined in the process of initiation of specific projects. Estimation of the funding costs for the of the Cybersecurity Strategy shall take place within the framework of the Action Plan.

Funding sources for the execution of measures laid down in the document shall be financial plans of authorities involved in the implementation of the Cybersecurity Strategy as well as funds from the National Centre for Research and Development and from the European Union[13], as far as possible.

[13] EU programmes providing for funding of cybersecurity-related projects include, in particular: Horizon 2020 and Connecting Europe Facilities (CEF Telcom) – both conducted as part of the EU multiannual financial framework 2014–2021. Other two large programmes are scheduled for launch within the next EU financial perspective (2021–2028) - they are Digital Europe and Horizon Europe.

Ministry
of Digital Affairs