NATIONAL FRAMEWORK OF CYBERSECURITY POLICY OF THE REPUBLIC OF POLAND FOR 2017-2022

RESPECTING THE RIGHTS AND FREEDOMS IN CYBERSPACE
COMPREHENSIVE APPROACH TO SECURITY
CYBERSECURITY AS AN IMPORTANT ELEMENT OF THE STATE POLICY

Ministry of Digital Affairs
Warsaw 2017

National Framework of Cybersecurity Policy of the Republic of Poland
for 2017-2022

Table of contents

1. Introduction

Social and economic development is more and more dependent on fast and unhindered access to information and its use in the management, production and service sector and by public entities. Continuous development of network and information systems, including analysing larger data sets, helps develop communications, commerce, transport, or financial services. We create and shape social relations in cyberspace, and the Internet has become a tool for influencing 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 ultimately on national security.

There is a risk to the availability integrity and confidentiality of information as a result of impact from various sources, including as a result of deliberate attacks, in the form of the distribution of malware, hacking ICT systems or blocking service provision. Attackers can be both criminal groups, acting for financial gain, for terrorist motives, and groups that may be backed by foreign states. The latter activities serve to obtain information, cause political or economic destabilisation, or induce social discontent.

Ensuring information security is a challenge for all entities that form the national cybersecurity system, i.e. business entities providing services using ICT systems, users, public authorities, and specialised entities dealing with ICT security at the operational level . It is therefore all the more important that Poland is closely linked with other states through international cooperation, within organisations such as the EU, the NATO, the UN and the OSCE. This cooperation plays an important role in the fight against the increasing number of incidents caused by illegal activities in cyberspace that are leading to material and reputational damages.

2. Strategic context

The National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022 is a strategic document in a continued process of actions taken by the governmental administration, aimed at raising the level of cybersecurity in the Republic of Poland, including the *Policy for the Protection of Cyberspace of the Republic of Poland* adopted by the government in 2013. The *National Framework* document was prepared by a group composed of representatives of the Minister of Digital Affairs, Minister of Defence and Minister of the Interior and Administration and representatives of the Internal Security Agency, the Government Centre for Security and the National Security Bureau.

The success of existing strategies in Poland, both national development strategies and those relating to national security and law and order depends on the use of ICT systems. Digitisation is not only a source of progress and innovation, but it also entails risks. In the light of the emerging threats, the widespread use of ICT systems, the increasing dependence of society and entrepreneurs on these systems, it is essential to expand the national cybersecurity system and ensure a consistent approach is taken across the Republic of Poland

The purpose of this document is to define framework activities aimed at achieving a high level of resilience of national ICT systems, essential service providers, critical infrastructure operators, digital service providers, and public administrations to cyber-incidents. The proposed strategic aims will also achieve increased effectiveness of law enforcement and judicial authorities in detecting and combating crimes, terrorist offences and espionage in cyberspace. The *National Framework of Cybersecurity Policy* is aligned with the ongoing operations related to critical infrastructure operators using ICT systems and takes into account the needs of the Armed Forces of the Republic of Poland.

When implementing the National Framework of Cybersecurity Policy, the Government will fully respect the right to privacy and the principal of a free and open Internet is an important element of the functioning of modern society.

3. Scope of the National Framework of Cybersecurity Policy

The National Framework of Cybersecurity Policy identifies, in particular:

- the ICT security objectives,
- the main actors involved in the implementation of the national framework of cybersecurity policy,
- management framework for achieving the objectives of the national framework of cybersecurity policy,
- the need to prevent and respond to incidents and to restore services to normal after an incident, including the principles of cooperation between public and private sectors,
- the approach to risk assessment,
- educational, information and training programmes related to cybersecurity,
- activities related to research and development plans in the field of ICT security,
- directions of international cooperation in the area of cybersecurity.

The National Framework of Cybersecurity Policy is adopted and introduced by the resolution of the Council of Ministers in May 2018. It directly affects entities of the government administration and, indirectly, other public authorities, entrepreneurs and citizens, after the adoption of a applicable cybersecurity law on the initiative of the Council of Ministers.

4. Vision, main goal, specific objectives

4.1. Vision

In 2022, Poland will be more resilient to attacks and threats from cyberspace. Thanks to a combination of internal and international activities, Poland's cyberspace will provide (constitute) a secure environment enabling the State to carry out their functions and allowing Poland to fully utilise the potential of the digital economy, while at the same time respecting the rights and freedoms of the citizens.

4.2. Main goal

Ensuring high level of security of the public and private sectors as well as citizens in a process of the provision or use of essential services and digital services.

4.3. Specific objectives

Specific objective 1. Increased capacity for nationally coordinated actions to prevent, detect, combat and minimise the impact of incidents which compromise the security of ICT systems vital to the functioning of the state.

Specific objective 2. Enhanced capacity to counteract cyberthreats.

Specific objective 3. Increasing the national potential and competence in the area of security in cyberspace.

Specific objective 4. Building a strong international position of the Republic of Poland in the area of cybersecurity.

5. Specific objective 1 – Increased capacity for nationally coordinated actions to prevent, detect, combat and minimise the impact of incidents which compromise the security of ICT systems vital to the functioning of the state

5.1. Adaptation of the legal environment to the needs and challenges in the area of cybersecurity

Development of the national cybersecurity system requires legal changes. Therefore, the existing legal provisions will be reviewed in order to harmonise them, increase efficiency and improve information flow among all stakeholders involved in building the national cybersecurity system.

The most far-reaching changes will result from the obligation to transpose *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*,[1] hereinafter referred to as the NIS Directive, into Polish law It contains security and notification requirements for operators of essential services[2] (such as energy or transport) and for digital service providers (e.g. cloud computing, search engines). and establishment of several cooperation or coordination mechanisms.

Ensuring effectiveness of the national cybersecurity system also requires the involvement of the public sector and telecommunications sector as well as Trust Service Providers[3], Competent ministers are responsible for preparing proposals of legal changes in the field of cybersecurity in their area of competence.

As part of improving the current cybersecurity system, the Minister of Digital Affairs, in cooperation with other Ministries, will review sectoral and specific regulations which address

[1] OJ EU 2016 L194

[2] See Appendix 2 of the NIS Directive for the full list of essential service providers

[3] As defined in the NIS Directive: 'a natural or legal person who provides any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals.'

the issues discussed to ensure they are fit for purpose. They will also consider how any changes to the existing cybersecurity system might affect other areas, such as personal data protection and the actions set out under the National Critical Infrastructure Protection Programme to ensure consistency. It will also be necessary to undertake legislative work to regulate how specialised tools in the field of military operations in cyberspace are developed, acquired and used by the Ministry of National Defence.

The issues of operational cooperation, including proper coordination of activities and exchanges of information between institutions responsible for national security, counter-terrorist efforts and internal security and public order, will be regulated.

Due to rapid pace of change occurring in area of cybersecurity, it will be necessary to periodically monitor the phenomena taking place there and initiate possible changes in the law.

5.2. Improving the structure of the national cybersecurity system

In view of the rapid pace of development of the information society, electronic administration and digital economy, and in the light of threats in cyberspace, the structure of the national cyberspace protection system will be improved so that it is able to cope with new challenges.

State Authorities will define the responsibilities of the entity coordinating the national cybersecurity system, the obligations and powers of the system participants, and the ways in which the coordinator may work with the system participants. The competence of the competent authorities responsible for supervision duties for essential services and digital services will also be specified.

Current activities of bodies in the civil and military sphere, and public and private sectors in the area of cybersecurity as well as institutions responsible for fighting cybercrime are currently scattered reducing the efficiency of the system. To improve this the tasks and responsibilities of the various institutions responsible for cybersecurity will be consolidated and harmonised. All the institutions involved in cybersecurity will work closely with each other to identify their roles and responsibilities as well as what resources they have at their disposal.

Development of the cybersecurity system at the national level also entails the further development of structures dealing with cybersecurity at the operational level, including the National Cybersecurity Centre (NC Cyber), the CSIRT at national level, sectoral incident response teams (sectoral CSIRT), information exchange and analysis centres (ISAC). To make these developments possible the Government will introduce new legislation setting out the revised competencies of the relevant institutions. In particular they will be amending the role of NC Cyber and the CSIRT capabilities at the national level. It is necessary to set up systemic solutions to exchange information between stakeholders and share knowledge about threats and incidents.

To ensure that the system is effective the relationship between various stakeholders in the national cybersecurity system, including bodies responsible for national security, counter-terrorist efforts, internal security and public order, the public prosecution service and the judiciary will also be the clarified.

In the framework of cooperation between the national government administration and the local government administration, the national government will strongly recommend that local governments create security clusters.

5.3. Increasing the effectiveness of cooperation of entities ensuring security in the cyberspace of the Republic of Poland

The basis for effective response to threats and attacks is effective functioning of reliable and secure mechanisms to exchange of information between stakeholders in the national cybersecurity system. On the other hand, a common issue is the reluctance of given entities to share information about identified threats, incidents and estimated losses. In addition to legal arrangements specifying mechanisms for the exchange of cybersecurity information, first, it is also necessary to create or expand the national CSIRT networks (national, sectoral, commercial and of entrepreneurs) which would exchange key information on security threats and incidents in a given sector or government department.

The information exchange system mechanisms will be designed in a way to ensure the protection of the interests of the participating entities, including protection of trade secrets, reputation and other relevant values.

Cybersecurity exercises and trainings are important factors in the process of enhancing the effectiveness of cooperation on the national and international level. This will improve our ability to work together to respond effectively to cybersecurity threats. At the national level, comprehensive exercises simulating the nationwide incidents will be simulated. Smaller-scale exercises, including sectoral ones, will also be organised in response to current events and incidents in order to continuously improve the staff knowledge, tools and procedures. The capabilities of the Armed Forces of the Republic of Poland to carry out military operations in cyberspace will be also increased as part of national and international exercises.

In the area of international cooperation, Poland will actively participate in exercises conducted by national organisations, the EU and the NATO bodies and other international actors.

Based on the exercises and trainings carried out, guidelines and recommendations will be developed to improve cybersecurity.

Improvement of the system is also possible through the participation in trusted international fora for the exchange of information on threats in cyberspace. Such fora are often informal or are created in the framework of non-profit organisations.

5.4. Enhancing ICT security of essential and digital services and critical infrastructure

Currently, information and communication technologies have become a foundation of economic development. Due to the fact that these technologies are used by essential service providers, digital service providers, and critical infrastructure operators, they are a critical element in ensuring citizens' security and continuity of operation of the state. For this reason, the Council of Ministers will treat ensuring ICT security as a priority. As the responsibility for ensuring security of services lies primarily with providers, the government will take action to improve their capacity and competence in cybersecurity. In particular this action will focus on helping

essential and digital service providers, critical infrastructure operators, and digital service providers to ensure they have the skills and knowledge they need, taking into account their diverse needs and their current cybersecurity skills. In addition, the government will support all entities in responding to serious incidents, especially in the event of cross-sectoral incidents.

Firstly, we will develop consistent criteria to determine which operators are to be classified as those providing essential services or responsible for critical infrastructure. This will be done so as to align as far as possible with the current crisis management system. This process will be carried out in cooperation with all sectors. Next, minimum requirements for ICT security will be developed, which will also cover the business continuity management. Digital service providers will be covered by a separate regime. The government is fully aware of the international nature of these entities and of the need to ensure regulations support the development of a digital single market in Poland.

Security clusters consisting of secure intranet networks, security services and secure Internet access, will become an important element of the structure of the national cybersecurity system. The first priority will be to build such a cluster for the central government administration.

5.5. Development and implementation of standards and good practices related to security of network and information systems

It is important that security is provided over the entire life cycle of the ICT systems, from production to use to disposal. Complying with the relevant Polish and International standards, recommendations from market Regulators and good practices should ensure that this is the case.

Especially entities performing tasks in the public interest are obliged to follow the relevant standards, and good practices.

The expertise of the technical committees of the Polish Committee for Standardisation, research and academic centres, research institutes, as well as other interested parties will help with the development of new standards where required. These will be aligned to international standards and Poland will continue to be active in the EU and international standard setting process.

Concrete recommendations for how these standards can be applied will be developed and the government will make every effort to ensure that this is done. The government will also support the implementation of recommendations issued by market regulators.

Recommendations on technical protections, system configuration, procedures for their safe operation and safe use will be developed. The recommendations will be voluntary and aim to help citizens and businesses. Information policies adjusted to the needs of individual target groups will also be prepared.

5.6. Development and implementation of a risk management system at the national level

A coherent risk assessment methodology, taking into account the specificity of individual sectors and operators of critical infrastructure and key services and digital service providers, will be developed for the purposes of improving national security. This will ensure comparability of assessment, of the level of risk, in particular for the national security risk reports, prepared in accordance with the crisis management regulations. In order to obtain data needed to estimate the risk, it will be necessary to develop a dependency model that describes the impact of an incident in one entity on the performance of services by other entities.

The Minister for Digital Affairs will be responsible for the analysis system and current risk management system. In the operational area, information from the system will be passed on to the relevant parties online. Access to this system will be given to the institutions responsible for security of cyberspace in the Republic of Poland and the institution coordinating crisis management.

A dynamic risk management system, resulting from globally identified vulnerabilities in software and hardware, will also be developed.

5.7. Ensuring a secure supply chain

Ensuring a high level of security of ICT systems requires a secure supply chain from design to production to operation to withdrawal. The term supply chain consists of subsystems of production, distribution, transport, storage and recycling of ICT systems components.

An important element of quality assurance in the supply chain is the evaluation and certification of products. The priority in this regard will be to create a national evaluation system, which will be conductive to gaining appropriate level of trust in the hardware, software and cryptography dimension.

Due to globalisation, it is important for Poland to be part of the international evaluation and certification system which is based on international norms and standards. Poland will actively participate in the establishment of a European system for evaluation and certification of products and services in the IT and communications sector. Poland aim to actively participate in international organisations gathering certifying bodies, such as the SOG-IS MRA[4] and the CCRA.[5]

5.8. Building a system warning cyberspace users about risks stemming from cyberthreats

A key requirement for ensuring the security of ICT systems is an access to information about threats and vulnerabilities as well as sharing of information about occurring or possible attacks. For this purpose, a system of management of cyberspace security on the national level will be built. This system will allow threats and vulnerabilities to be reported. This information will then be aggregated, analysed and correlated. Warnings based on this analysis will be given to stakeholders, informing them about potential threats and vulnerabilities taking into account the protection of trade secrets and other commercially sensitive information.

An additional information system for citizens will be created to protect end users from the effects of identified threats.

[4] SOG-IS MRA – Senior Officials Group Information Systems Security Mutual Recognition Agreement

[5] CCRA – Common Criteria Recognition Arrangement

6. Specific objective 2 – Enhancing capacity to counteract cyberthreats

6.1. Enhancing capacity to counteract cybercrime, including cyberespionage and incidents of a terrorist nature, occurring in cyberspace

With regard to enhancing the capacity to counteract cybercrime, including cyberespionage, incidents of a terrorist nature and hybrid threats, it is important to provide support to essential service providers, digital service providers and critical infrastructure operators so that they can detect and combat incidents. Cooperation and coordination of the activities of law enforcement agencies is required irrespective of the motives of the perpetrators It is also important to preserve electronic evidence.

Increasing the effectiveness of procedural or operational acts also requires broadening the interaction of law enforcement 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 essential to involve representatives of law enforcement agencies, including the police, in work of national and international fora for the exchange of information on threats and vulnerabilities.

Given the nature cyberspace, combating cybercrime requires cross-border cooperation of law enforcement agencies and entities such as the CERT/CSIRT. Acting quickly Acting quickly is critical in the proceedings or the investigation related to crimes committed in cyberspace. This means that efficient and reliable information exchange channels between law enforcement agencies of different countries are required.

Rapidly changing methods of crime require development of research in the field of counteracting cybercrime, the results of which will provide support to law enforcement. 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 society about cybercrime threats and the means to prevent or mitigate them. Providers of essential services, digital services, Internet access services and NGOs will play an important role in this type of activity.

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

The Polish Armed Forces, as a basic element of the state's defence system, must act in cyberspace[6] as effectively as in the air, on land and at sea. Therefore, the ability to conduct a full spectrum of military operations in cyberspace must include: the identification of threats, the protection and defence of information systems, and combating the threats at source.

Activities in cyberspace will be included in operational planning and will form an integral part of operations conducted by the Polish Armed Forces itself and in co-operation within, alliances and coalitions. Military structures, will be improved to ensure more effective planning, command and management of resources, skills and capabilities. The skills of staff conducting military operations in cyberspace will be constantly improved through internal training as well as highly specialised external training prepared for the Ministry of National Defence. At the same time, threats will be identified and the situation assessed on an ongoing basis in order to take appropriate protection measures or proactively address threats. Bearing in mind the rapid pace of technological development the Ministry of National Defence will strive to produce or acquire an innovative set of tools that will improve their performance in this domain.

6.3. Build capacity in the area of threat analysis at the national level

An essential element of the cyberspace security system is to maintain and develop national analytical capabilities needed to carry out an overall assessment of situation in the area of cyberthreats, and the verification and in-depth analysis of specific threats and incidents.

The National Cybersecurity Centre will help increase Poland’s cybersecurity by carrying out analytical tasks based on information from national and foreign sources and own studies and research of cooperating bodies.

---

[6] Cyberspace was recognised by NATO as another domain of law enforcement operations at the NATO Summit in Warsaw in 2016.

6.4. Building a secure communication system for the purposes of national security

A secure communication system will be created. This will allow for effective information exchange between the relevant bodies in the national security command system. It will also cover users of public administration at various levels, providing for reliable communications in the national security management, at all phases of crisis management and national defence readiness. The system will ensure secure, timely and reliable exchange of information in internal and external relations, including NATO and the EU. It will provide the essential telecommunication services, such as telephony, data transmission, electronic mail, video and teleconferencing, Internet access, access to databases of national registers at required security level.

6.5. Security audits and tests

One of measures that makes it possible to assess the effectiveness of the currently implemented information security management systems and the adequacy of the protections established are periodic audits. On the basis of norms and good practices and taking into account the needs of individual sectors, coherent audit methodologies will be developed. The aim of this approach is to make the results of audits comparable.

Another measure of assessing security is penetration testing, which allows for a real assessment of the system's resistance to threats. The results of this can then be used to improve the security of these systems where necessary.

Testing protection measures requires specialised tools. It is therefore important to revise the existing regulations to allow us to adopt to the rapidly changing environment. For example, the use of bug-bounty approach can be considered. allowing use of bug-bounties[7].

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

7. Specific objective 3 – Increasing the national potential and competence in the area of security in cyberspace

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

Polish government aims to invest in development of industrial and technological resources for cybersecurity by creating the conditions needed for the development of enterprises, scientific research centres and start-ups which will create for example new cybersecurity solutions.

As part of efforts to support digital businesses in Poland we have created the *Cyberpark Enigma* programme. As a result of this programme, participants will be able to produce high quality hardware and software, building on their existing skills and knowledge. Cybersecurity will be a big part of this. This will allow Polish businesses to offer their ICT services throughout the EU on a competitive basis. The acquisition of new technologies for development of domestic ventures will also be realised through participation in European initiatives that emphasise innovation, through bilateral cooperation and within international organisations.

In order to increase the competence of research centres in the area of cybersecurity, a Scientific Cybersecurity Cluster (SCC) is planned to be created. It will be a scientific platform composed of higher education institutions and scientific research centres specialising in cybersecurity technologies.

In order to equalise the opportunities of Polish entrepreneurs in the global market and to support development of Polish businesses in acquiring digital capabilities, innovation hubs,[8] which will offer comprehensive services for companies and start-ups, including testing new solutions, market research, support in applying for funding for development of innovation solutions, advice on access to new markets and assistance in establishing cooperation with other entrepreneurs, will be created.

[8] Technological and organisational environment where people without resources can test their innovative solutions and get full support in commercialising this solution.

7.2. Building cooperation mechanisms between the public sector and the private sector

Ensuring security in cyberspace requires the joint efforts of the private sector, the public sector and the citizens. The government will strive to build an effective public-private partnership system based on trust and shared responsibility for security in cyberspace. At the same time, public administration will improve its capacity to provide advice to all economic sectors about ICT security. The government will also become actively involved in the existing and emerging forms of European public-private cooperation and thus promote Polish business internationally.

In implementing a new vision of the country's development and supporting the innovativeness of the Polish economy, it will be important to build a system of support for research and development projects in the field of cybersecurity, including projects implemented in cooperation with the research community and commercial enterprises.

7.3. Stimulating research and development in the field of security of ICT systems

In view of the dynamically growing IT market, especially in view of the prospect of change of the IPv4 currently used on the Internet for IPv6, and in connection with development of the internet of things, smart cities, Industry 4.0, as well as Cloud Computing, and Big Data, there is a needs to enhance research, development and manufacturing activities in the area of cybersecurity.

To this end, a research programme aimed at preparation and implementation of new methods of protection against novel threats from cyberspace will be launched jointly with the National Centre for Research and Development[9].

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

- assess the effectiveness of protections and resistance of Poland's cyberspace to cyberthreats,

[9] The National Centre for Research and Development is the implementing agency of the Minister of Science and Higher Education. It was appointed in the summer 2007 as an entity in charge of the performance of the tasks within the area of national science, science and technology and innovation policies. The activity of the Centre is funded by the national treasury and the European Union

- assess the effectiveness of response to threats,
- analyse new trends in cybercrime, cyberterrorism and methods of combating them,
- study methods of attacks and ways of counteracting these attacks.

Important tasks for ensuring cybersecurity are performed by non-governmental organisations, which may be useful as organisers of educational activities and as providers of analyses and opinions for public administration. It is also possible to acquire specialists with unique skills through analytical centres for the purposes of solving complex problems in the field of cybersecurity .

7.4. Increasing competence of the staff of entities relevant to the functioning of cyberspace security

Competence of the staff of entities relevant to ensuring cyberspace security in the Republic of Poland will be increased through the creation and implementation of a model of academic education and professional development system which will ensure qualifications of employees appropriate to challenges.

Higher education institutions will be encouraged to develop interdisciplinary specialisations including, among others, information security management, protection of personal data, protection of intellectual property on the Internet and issues related to development of new technologies and challenges that are the derivatives of this.

As part of broadly understood expert education, in order to effectively counteract growing cybercrime, the system of training for all employees of entities relevant to the functioning of security in cyberspace and for the representatives of law enforcement authorities and the judiciary will be enhanced.

In order to retain highly qualified employees in public administration, alongside the use of other instruments supporting their activity, incentive schemes, including the “Golden Hundred” governmental programme, will be launched. The programme will address IT and ICT security specialists employed in public administration, and will aim at retaining and promoting the

best-qualified professionals. The Minister of Digital Affairs will be responsible for the preparation and implementation of the programme.

In order to provide heads of government administration units with substantive support in the area of cybersecurity management, the principle of appointing Plenipotentiaries for cybersecurity security in these units will be maintained.

For the optimal use of human resources in cybersecurity, a management model for these resources will be developed.

7.5. Creating conditions for the safe use of cyberspace by citizens

Education in the area of cybersecurity should begin at the early stage of education. The safe use of cyberspace will form a core part of the curriculum. It is also planned to develop and launch refresher courses for computer science teachers and to implement adequate changes in postgraduate education for teachers.

In parallel, in cooperation with NGOs and academic centres, public administration will undertake systematic actions to raise public awareness of the threats of cyberspace, as well as educational activities on rights and freedoms in the digital environment. Among other things, social campaigns addressed to different target groups (including children, parents, seniors) will be launched.

Public administration will support all actions of both essential service providers and digital service providers in undertaking educational and information activities. The goal of the activities will be to provide end-users with access to knowledge to understand the threats of cyberspace and to use effective ways of protection from these threats.

8. Specific objective 4 – Building strong international position of Poland in the area of cybersecurity

8.1. 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, Poland will intensify its efforts to ensure the security of the Digital Single Market - a driver of 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.

Our membership in the NATO is an important pillar of Poland's security, as well as the security of entire Euro-Atlantic area. Increasing frequency of attacks of a hybrid nature make investing in deterrence and defence capabilities, including improving the resilience and ability to respond quickly and effectively to cyberattacks, indispensable.

Through cooperation within the United Nations system, Poland will seek to continue the debate on an effective Internet governance system and issues related to the legal aspects of cyberattacks in order to elaborate coherent solutions that ensure the security of international information exchanges on the Internet. Poland will actively participate in strengthening confidence and security building measures within the existing international fora, including the OSCE. The government will also join the efforts to effectively combat cybercrime internationally.

We attach particular importance to the cooperation with the countries of the region, including strengthening cooperation within the Visegrad Group and with the Baltic Sea countries.

Strengthening of Poland’s international position 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, with the latter being responsible for the overall coordination of the foreign policy of Poland.

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

8.2. Active international cooperation at the operational and technical level

International cooperation at the operational and technical level will be carried out, *inter alia*, within the CSIRT Network at European Union level, in other fora for information exchange 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 will 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 threats in cyberspace, but will also contribute to the exchange of experience between technical staff in joint ventures. It will also be an opportunity to promote Polish technological solutions and Polish expert staff.

9. Managing the National Framework of Security Policy

The National Framework of Cybersecurity Policy is adopted for a period of 5 years. The Ministry of Digital Affairs is coordinating the implementation of the National Framework of Cybersecurity Policy. The document is subject to review and evaluation two years after its adoption and in the fourth year of validity. The results of the review will be presented to the Council of Ministers. As a result of the review, the Minister of Digital Affairs will prepare a proposal of corrective actions or a draft document for the next five-year period. If needed the National Framework of Cybersecurity Policy may be updated before that time.

Within six months of the adoption of the National Framework of Cybersecurity Policy, in cooperation with members of the Council of Ministers, heads of central offices and the Director of the Government Centre for Security, the coordinator will develop an *Action Plan for the implementation of the National Framework of Cybersecurity Policy*. When developing the *Plan*, the above-mentioned bodies shall take into account in their activities the issues of cybersecurity in accordance with the statutory competence. The *Action Plan* will include, in particular:

1) name of a specific objective,
2) name of the task,
3) type of action: legislative, organisational, technological, educational, informational, promotional, other action,
4) initiatives or implementation tools,
5) schedule – the commencement date and the end date of the initiative,
6) body or bodies – leading authority and their partners
7) expected impacts,
8) estimated cost

The provisions of the Act on the protection of classified information apply to the items of the *Plan* containing classified information.

The coordinator will annually prepare a progress report on the implementation of the National Framework of Cybersecurity Policy for the previous year on the basis of information received

from the entities involved in its implementation. The reports will be submitted to the Council of Ministers.

10. Financing

Under current regulations, entities carrying out public tasks are already required to include expenditure on cybersecurity in their financial plans. Additional costs may be incurred as a result of integration activities related to the construction of the national cybersecurity system and expenditure incurred on the implementation of other projects of the *Action Plan for the implementation of the National Framework of Cybersecurity Policy*. The detailed size and structure of costs of individual projects will be determined in the process of initiation of specific projects. Estimation of the financing costs for the implementation of the National Framework of Cybersecurity Policy will take place within the framework of the *Action Plan*. Funding sources for the implementation of measures described in the document will be financial plans of individual units involved in the implementation of the National Framework of Cybersecurity Policy as well as funds from the National Centre for Research and Development and from the European Union, as far as possible.

Ultimately, it is necessary to establish within the national budget a Multiannual Programme dedicated to the construction and development of projects in the area of cybersecurity within the state budget.

11. Glossary

The following definitions apply for the purposes of this document:

1) "network and information systems" or "ICT systems" mean:
    a) electronic communications networks within the meaning of Article 2(a) of Directive 2002/21/EC,
    b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, perform automatic processing of digital data; or
    c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance,
2) "cyberspace" means the space of processing and exchanging information created by ICT systems, including relations between them and relationships with the users,
3) "security of network and information systems" or "cybersecurity" or "ICT security" means the resilience of ICT systems, at a given level of trust, to any actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted, or processed data or the related services offered by, or accessible via, those networks and information systems,
4) "operator of essential services" means a public or private entity of a type referred to in Annex II of Directive (EU) 2016/1148 of the European Parliament and of the Council which meets the criteria laid down in separate provisions,
5) "digital service" means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council which belongs to one of the types listed in Annex III to Directive (EU) 2016/1148 of European Parliament and of the Council,
6) "incident" means any event having an actual adverse effect on the security of network and information systems,
7) "serious incident" means an incident or a group of incidents which cause or may cause significant damage to public safety, international interests of the Republic of Poland, including economic interests, confidence in public institutions, civil liberties or health of the citizens of Poland,

8) “risk” means any reasonably identifiable circumstance or event that could have an adverse effect on the security of network and information systems,
9) “standard” means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012,
10) “cloud computing” means a digital service that enables access to a scalable and elastic pool of shareable computing resources,
11) “CSIRT” or “CERT”[10] or “Computer Incident Response Team” refers to a group of people composed of security analysts, who are responsible for developing, recommending and coordinating actions to detect, stop and combat the effects of incidents, and obtain information on the essence of these incidents,
12) “CSIRT Network” means the organisational structure referred to in Article 12 of the NIS Directive,
13) “National CSIRT” means a national body that has the role and competence of the CSIRT in relation to incidents and threats of cross-sectoral and international nature or large scale national incidents or threats.
14) “National cybersecurity system” means a system composed of national entities or organisational structures of entities, along with the relations between these entities or structures, which serves ensuring high level of security in cyberspace of Poland,
15) “National Cybersecurity Centre” means the part of the national cybersecurity system whose role it is to monitor cybersecurity at the national level, coordinate actions aimed at preventing, counteracting and analysing the essence and consequences of serious incidents,
16) “security cluster” means a dedicated intranet network, connecting entities belonging to that cluster, providing security services, including the service of secure Internet access.

[10] CERT (Computer Emergency Response Team) is a name registered by the Carnegie Mellon University and its use requires consent of this university. CERT Poland has such consent. The NIS Directive uses the name CSIRT.