NASK

Cyber POLICY

Cybersecurity A.D. 2018

Strategic and legal aspects of cybersecurity and emerging technologies

www.cyberpolicy.nask.pl

NASK
Cyber POLICY

TABLE OF CONTENTS

Introduction

For many years now, the NASK National Research Institute (NASK PIB) has been working to improve the level of information and communication security in Poland. Since 1996, the first Polish computer emergency response team, CERT Polska, has been operating in the Institute's structure. After the NIS Directive adoption, we have started building policy level competences. As a result, one year later, we launched the CyberPolicy portal (https://cyberpolicy.nask.pl/), a compendium of strategic and legal aspects of cybersecurity and emerging technologies.

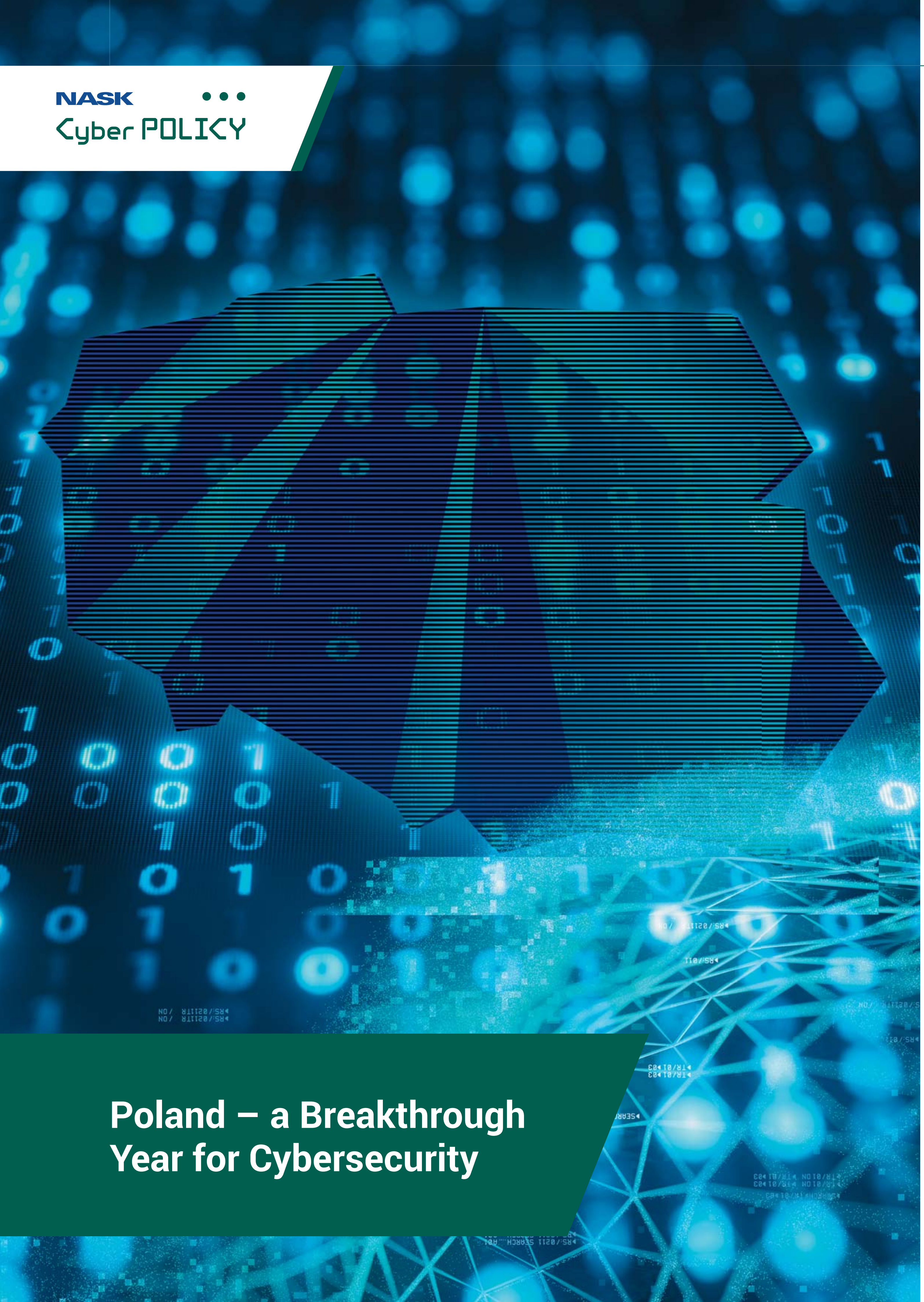
The Act on the National Cybersecurity System has imposed the role of CSIRT NASK (one of the three CSIRTs at the national level) on NASK PIB. Apart from operating activities, the Act also imposes policy level duties: performing strategic analyses, building cross-sectoral cooperation, creating good practice, developing recommendations, and providing support in capacity building.

The *Cybersecurity A.D. 2018* publication summarises strategic and legal aspects of cybersecurity and emerging technologies in 2018. It provides an overview of policy level activities in Poland, the European Union, the United Nations, the North Atlantic Alliance (NATO), and the Organisation for Security and Co-operation in Europe.

Enjoy reading!

Krzysztof Silicki, Deputy Director for Cybersecurity and Innovation, NASK PIB

NASK
Cyber POLICY



Poland – a Breakthrough Year for Cybersecurity

2018 was certainly a breakthrough year for cybersecurity in Poland.

On 10 May, the Personal Data Protection Act was adopted, taking into account provisions of the General Data Protection Regulation (GDPR). This is a revolution ensuring much stronger protection of privacy than before. The adoption of the Act was preceded by lengthy public and interministerial consultations.

On 5 July, the Act on the National Cybersecurity System was adopted, implementing provisions of the NIS[1] Directive of July 2016 into the Polish legal system. This Act (together with delegated acts) outlines the shape of the cybersecurity ecosystem in Poland. An interministerial group of experts worked on provisions of the Act; the process also involved extensive consultations with market sectors.

Both legal acts are extremely important and challenging for both the public and private sectors.

With the PSD2 Directive entering into force, changes have also been introduced to the Payment Services Act. Hence, the financial sector has gained even stronger cybersecurity regulations.

2018 also marks the beginning of work on the Polish Artificial Intelligence strategy. Efforts that took experts several months have resulted in the publication of the strategic pillars. The next step will be drafting the relevant document.

Act on the National Cybersecurity System

The Act on the National Cybersecurity System is the first legal act concerning this issue in Poland. It implements the NIS Directive. Since the NIS Directive is a minimum harmonisation, the Member States have the possibility to create stronger regulations on national level. In Poland this possibility has been used. Therefore, the public administration and (indirectly) the telecommunications sector have been also included in the Act.

The Act creates the structure of the new cybersecurity system in Poland. It designates three national level CSIRTs with clear constituency, establishes supervision in cybersecurity (competent authorities, introduction of financial penalties), and creates a political and strategic framework for cybersecurity management in Poland (Cybersecurity Policy of the Republic of Poland, appointment of Cybersecurity Ombudsman and Council).

The Act has been in force since 28 August 2018.

Scope of the Act

The Act includes three types of entities: essential services operators, digital service providers and public entities.

Essential Services Operators

Essential services operators are enterprises and institutions providing services that are essential for the maintenance of critical societal or economic activities, dependent on information systems[2]. The Act lists the sectors in which essential services operators will be identified: **energy, transport, banking and financial market infrastructures, health, drinking water supply (and distribution), and digital infrastructure**[3]. The implementing regulation to the Act[4] lists the essential services in detail. **The list of essential services operators is kept by the minister in charge of digital affairs.** Operators may be registered on the list and removed from it if requested by the authority in charge of cybersecurity. Operators are identified by competent authorities[5] then issuing an administrative[6] decision based on the following three criteria:

1. the provision of an essential service in one of the listed sectors,
2. the service must depend on information systems,
3. the occurrence of an incident has a significant disruptive effect on the provision of this service.

The assessment of a disruptive effect depends on the disruptive effect thresholds that have been set by the Council of Ministers in the Regulation[7].

[1] Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union; https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148.

[2] Essential services operators (ESO) are not operators of critical infrastructure (CI). Critical infrastructure protection is regulated by the Crisis Management Act of 27 April 2007. The definition included in the Act defines CI as "systems and their functionally related facilities, including civil structures, equipment, systems, services essential for the security of the state and its citizens, and ensuring the efficient functioning of public administration bodies as well as of institutions and enterprises". Currently, the Government Centre for Security is working to replace the object model with the service model in respect of CI security.

[3] Internet exchange points, top-level domain name registry and DNS services are indicated as part of the digital infrastructure.

[4] Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and disruptive effect thresholds of an incident in respect of provision of essential services.

[5] Article 5 of the Act on the National Cybersecurity System.

[6] If an operator has already been identified as an operator of critical infrastructure, its obligations under the Crisis Management Act (e.g. preparation of security documentation) will be deemed as having been fulfilled.

[7] Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and disruptive effect thresholds of an incident in respect of provision of essential services.

Obligations of Essential Services Operators

An essential services operator must implement security management in the information system used to provide the essential service. It is also obliged to **implement risk management** and **adapt security measures accordingly**. Furthermore, it maintains cybersecurity documentation of the information system, keeps it up to date, and stores it for at least 2 years[8].

It is operator's responsibility to handle the incidents. Therefore, it must:

- classify the incident based on the criteria set out in the Regulation[9],
- report a **significant incident** to the relevant CSIRT at the latest within **24 hours** after its detection,
- cooperate with CSIRT in addressing the incident, including ensuring access to information and removing vulnerabilities of the system.

If a **sectoral cybersecurity team** is established, the operator additionally provides a report to the team. The operator cooperates with the team by sending the necessary data. Moreover, it makes sure the team has access to the information on recorded incidents.

In order to fulfil the tasks set out in the Act, the operator creates internal structures responsible for cybersecurity. **The Act also permits outsourcing of cybersecurity services** by way of an agreement with an external entity. Conditions for cybersecurity service providers, as well as for the operator's internal structures are set out in the Regulation of 10 September 2018[10].

Every 2 years, the Operator **must carry out**[11] **a security audit of the information system used to provide the essential service.** The first audit should take place within one year after the decision on considering the operator as an essential services operator is served.

Essential services operators are supervised by competent authorities for cybersecurity matters in respect of their obligations under the Act. As part of the supervision, such bodies may carry out inspections and impose fines.

Digital Service Providers (DSP)

Digital services providers include: **online marketplaces, cloud computing services and online search engines**. The scope of the Act does not apply to micro- or small enterprises[12].

DSP definitions:

Online marketplace – means a digital service that allows consumers and/or traders to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace.

Cloud computing service – means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

Online search engine – means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found[13].

DSPs are not subject to regulation as strict as that applying to essential services operators. This is caused by the cross-border nature of digital services and the international nature of DSPs.

Apart from the adequate risk management of the information systems used to provide a digital service, DSPs must perform activities to enable detection, recording, analysis and classification of incidents. **In case of a substantial incident, a digital service provider must supply the information to the competent CSIRT at the latest within 24 hours after its detection.**

DSPs, just like essential services operators, are supervised by competent authorities that may carry out inspections and impose fines.

[8] This provision excludes operators who have facilities, systems, equipment or services included in the critical infrastructure, and who have an approved critical infrastructure protection plan and documentation.

[9] Regulation of the Council of Ministers of 31 October 2018 on the thresholds for considering an incident as significant.

[10] Regulation of the Minister of Digital Affairs of 10 September 2018 on the organisational and technical conditions for cybersecurity service providers, and for internal organisational structures of essential services operators responsible for cybersecurity.

[11] Guidelines for the audit are set out in the Act.

[12] Article 104 of the Act on Freedom of Economic Activity of 2 July 2004 defines a **microenterprise** as an enterprise where, in at least one of the last two financial years, **the annual average employment amounted to less than 10 employees** and the achieved annual net turnover from the sale of goods, products and services, and from financial operations did not exceed the PLN equivalent of 2 million euros, or where the total assets of its balance sheet drawn up at the end of one of these years did not exceed the PLN equivalent of 2 million euros.

Article 105 of the Act on Freedom of Economic Activity of 2 July 2004 defines a **small enterprise** as an enterprise where **the annual average employment amounted to less than 250 employees** and the achieved annual net turnover from the sale of goods, products and services, and from financial operations did not exceed the PLN equivalent of 50 million euros, or where the total assets of its balance sheet drawn up at the end of one of these years did not exceed the PLN equivalent of 43 million euros.

[13] Annex 2 to the Act on the National Cybersecurity System.

Public Entities

The national cybersecurity system also includes such public entities as: National Bank of Poland – central bank of the Republic of Poland (Narodowy Bank Polski); National Economy Bank – state development bank whose mission is to support the social and economic development of Poland (Bank Gospodarstwa Krajowego); Office of Technical Inspection; Polish Air Navigation Services Agency; Polish Centre for Accreditation; National Fund for Environmental Protection and Water Management; and provincial funds for environment protection and water management, as well as research institutes and commercial law companies, performing public utility tasks.

Pursuant to Article 21, **each of the above-mentioned entities must appoint a contact person responsible for maintaining communication with entities of the national cybersecurity system in respect of public tasks that depend on information systems**.

Additionally, each of the public entities is obliged to manage an incident in a public entity, including ensuring its handling. The **time for reporting an incident to the relevant CSIRT cannot exceed 24 hours after the time of detection**.

Incident Reporting

Three CSIRTs at the National Level

The Act sets out **three CSIRTs at the national level: CSIRT NASK in the structures of the NASK National Research Institute; CSIRT GOV in the structures of the Internal Security Agency; and CSIRT MON in the structures of the Ministry of National Defence.** Each national CSIRT has a clearly defined constituency, i.e. the range of entities that are obliged to report to it and to which the CSIRT provides support.

CSIRT MON coordinates handling of incidents reported by entities subordinated to the Minister of National Defence and enterprises of special economic and defence importance[14]. CSIRT GOV coordinates incidents reported by government administration, National Bank of Poland (Narodowy Bank Polski), National Economy Bank (Bank Gospodarstwa Krajowego) and critical[15] infrastructure operators. CSIRT NASK coordinates incidents reported by other entities, including essential services operators[16], digital service providers and local government authorities. Incidents may also be reported to CSIRT NASK by natural persons, i.e. ordinary citizens. It can be said that CSIRT NASK is the so-called CERT of last resort[17]. CSIRT MON and CSIRT GOV (in accordance with provisions of the Act on Counter-Terrorism Measures and the Act on Military Counterintelligence Service and Military Intelligence Service) are competent in the case of terrorist incidents. CSIRT MON is always responsible in the case of national defence incidents. The following diagram shows the constituency division among the three CSIRTs of the national level.

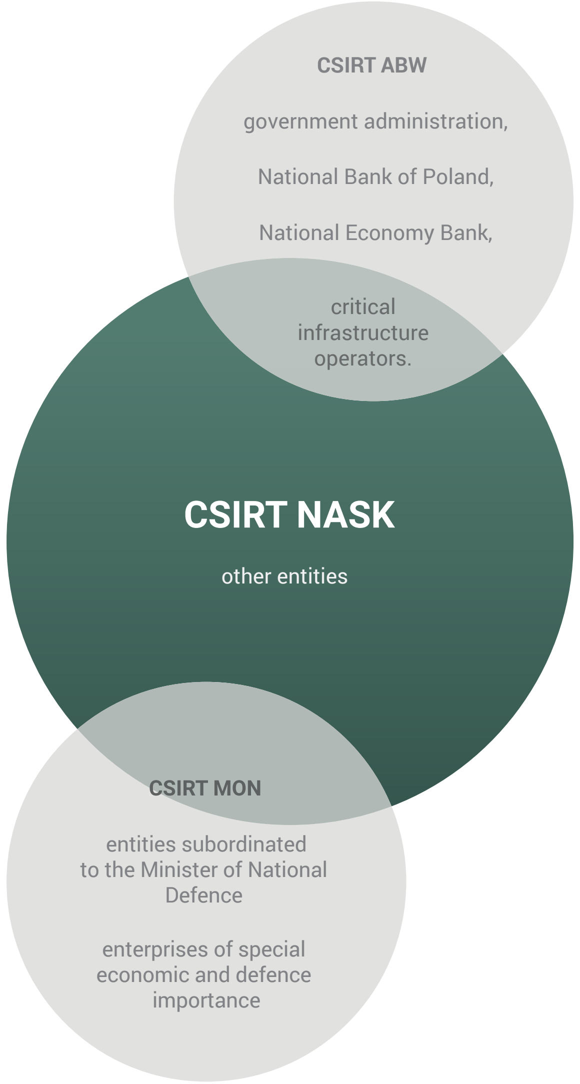

CSIRT ABW
government administration,
National Bank of Poland,
National Economy Bank,
critical infrastructure operators.
CSIRT NASK
other entities
CSIRT MON
entities subordinated to the Minister of National Defence
enterprises of special economic and defence importance

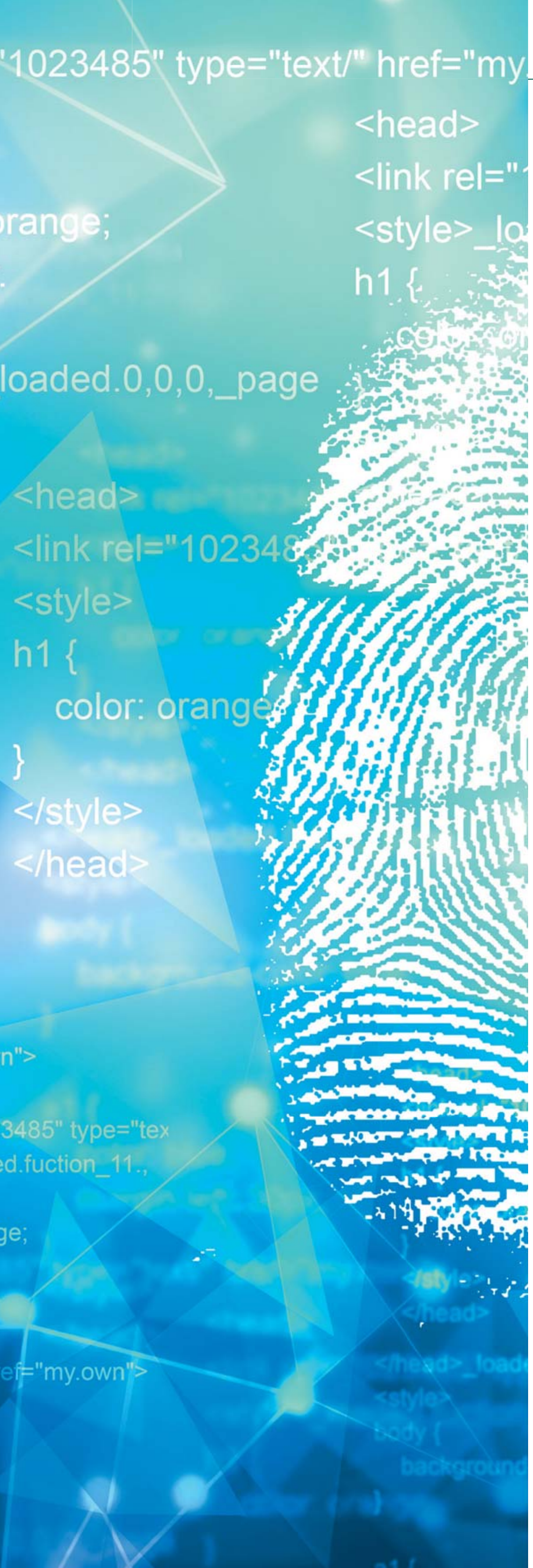
Fig. 1. Constituency division among the three CSIRTs at the national level.

[14] These entities have been specified in the Regulation of the Council of Ministers of 3 November 2015 on the list of enterprises of special economic and defence importance.

[15] In accordance with the Act of 26 April 2007 on Crisis Management.

[16] Not being critical infrastructure operators.

[17] According to the ENISA nomenclature included in *Deployment of Baseline Capabilities of National/ Governmental CERTs*, this means that if an entity is unable to obtain direct contact with or expected assistance from an entity that is directly involved in an incident, the reporting entity submits a query to the CSIRT of last resort.



All the three national CSIRTs are to cooperate with the competent authorities, the minister responsible for digital affairs and the cybersecurity officer. Furthermore, their tasks include, among others, monitoring of cybersecurity threats and incidents at the national level; nationwide risk estimation; communication of incidents and risks to other entities of the national cybersecurity system; publication of announcements regarding identified cybersecurity threats and responding to reported incidents.

Besides, national CSIRTs provide analytical and R&D facilities for the country's cybersecurity system. In this respect, they conduct advanced analysis of malware and vulnerabilities. They also monitor threat indicators as well as develop tools and methods to detect and combat threats to cybersecurity.

The national CSIRTs may also perform the necessary technical tasks related to threat analysis and coordination of handling a significant, substantial and critical incident.

During incident handling, the competent authority may request an essential services operator or digital service provider to remove the vulnerabilities.

Types of Incidents

The Act introduces three levels of incidents.

The first level are all events that have or may have an adverse effect on cybersecurity.

The second level includes significant incidents[18] that involve essential services operators; substantial incidents[19] that involve digital service providers; and incidents in public entities[20] that involve public entities. These incidents are classified by essential services operators, digital service providers and public entities. The classification is based on specific criteria. For essential services operators, the criteria are set out by the Regulation of the Council of Ministers of 31 October 2018 on the thresholds for considering an incident as significant. For digital service providers – the thresholds are set out in the Commission Implementing Regulation (EU) 2018/151[21].

The third level are critical incidents[22]. These are large-scale incidents that pose a greater threat than those mentioned above. **An incident is classified as critical by the relevant CSIRT at the national level (CSIRT MON, CSIRT NASK or CSIRT GOV)**. The table below presents the levels of incidents.

Incident level	Definition	Classification determination	Reporting necessary
First level	incident – an event that has or may have an adverse effect on cybersecurity;	no	no
Second level	significant incident – causes or may cause a significant reduction in the quality or interruption in continuity of supplying an essential service;	essential services operator	CSIRT GOV – operators of critical infrastructure CSIRT MON – entities subordinate to the Ministry of National Defence CSIRT NASK – other based on the criteria from the Regulation to the Act on the National Cybersecurity System
	substantial incident – has a significant effect on the provision of a digital service	digital service provider	CSIRT NASK
	an incident in a public entity – causes or may cause a deterioration of quality or interruption of the performance of a public task	public entity	CSIRT GOV CSIRT NASK CSIRT MON (according to the constituency)
Third level	critical incident – results in a major detriment to the public security or public order, international interests, economic interests, operation of public institutions, civil rights and freedoms, or human life and health	CSIRT MON CSIRT GOV CSIRT NASK	yes, but the reporting operator/ service provider will not always be aware that this is a critical incident (e.g. it will report a second level incident and the competent CSIRT at the national level will change its classification)

Table 1. Incident levels under the Act on the National Cybersecurity System

Cooperation of CSIRTs at the National Level

The Act provides legal framework for the close cooperation between national level CSIRTs. It includes the development of incident management procedures whose coordination requires the involvement of more than one CSIRT.

[18] Significant incident – an incident that causes or may cause a significant reduction in the quality or interruption in continuity of supplying an essential service; Article 2.7 of the Act on the National Cybersecurity System.

[19] Substantial incident – an incident that has a significant impact on the provision of a digital service within the meaning of Article 4 of the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (OJ EU L 26, 31.1.2018, p. 48), hereinafter referred to as "Implementing Regulation 2018/151"; Article 2.8 of the Act on the National Cybersecurity System.

[20] An incident that causes or may cause a deterioration of quality or interruption of the performance of a public task carried out by a public entity referred to in Article 4, items 7-15; Article 2.9 of the Act on the National Cybersecurity System.

[21] https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32018R0151

[22] Critical incident – an incident that results in a major detriment to the public security or public order, international interests, economic interests, operation of public institutions, civil rights and freedoms, or human life and health, classified by competent CSIRT MON, CSIRT NASK or CSIRT GOV; Article 2.6 of the Act on the National Cybersecurity System.

[23] According to the Act on Crisis Management, Prime Minister is GCMT's Chairperson, whereas relevant departmental ministers are members of the team. The introduction of the format of the Team for Critical Incidents enables a quick transfer of information on the so-called critical incidents, i.e. "resulting in substantial damage to the security or public order, international interests, economic interests, activities of public institutions, civil rights and freedoms, or human life and health" to the level of the Council of Ministers, via GCS. This will make it easier to manage a crisis that is likely to have kinetic effects in the case of critical incidents.

Furthermore, the Act introduces the format of the **Team for Critical Incidents** that coordinates critical incidents handling. It consists of national level CSIRTs and the Government Centre for Security as a secretariat. This format ensures the cooperation with the Government Crisis Management Team (GCMT)[23]. Furthermore, representatives of competent authorities may be invited to participate in the work of the team.

During its meetings, the Team for Critical Incidents decides which national level CSIRT will be the leading one in the critical incident handling process. The team also distributes the tasks related to the process. During the meeting a decision may be made to call together the Government Crisis Management Team. This mechanism makes it possible to include cybersecurity issues in the Polish crisis management framework.

GDPR vs. Incident Handling

The Act on the National Cybersecurity System takes into consideration the new regulations introduced by the General Data Protection Regulation (GDPR). National level CSIRTs (MON, NASK, GOV), as well as sectoral cybersecurity teams process personal data obtained in connection with incidents and cybersecurity threats. These include, among others, information about users of IT systems or telecommunication terminal equipment, or data of essential services operators, digital service providers and public entities.

National CSIRTs and sectoral cybersecurity teams may process only information that is necessary for the performance of the task. The data must be deleted or anonymised within 5 years after the end of handling the incident to which they relate.

The Act also obliges to publish, on a website, e.g. the contact details of the personal data controller, the purpose and legal basis of the processing, the category of the processed data, and the period of processing or the source of the data. Importantly, the entities must also inform of the **restrictions on obligations and rights of data subjects**.

CSIRTs may also process legally protected information, e.g. company secrets, if this is necessary for the performance of their tasks. However, they must keep the information secret. This means that the legislature has made use of Article 23 GDPR that makes it possible to exclude certain entities from some of GDPR provisions.

Incident Handling vs. Access to Public Information

The Act on Access to Public Information does not refer to information on vulnerabilities, incidents and risk of their occurrence, and cybersecurity threats. Therefore, CSIRTs cannot be expected to report incident data by making them available as public information. The solution is all about building trust within the system. However, CSIRT MON, CSIRT NASK or CSIRT GOV may publish information about incidents in the Public Information Bulletin if it is **necessary to prevent or handle them**. In advance, this decision should be consulted with the essential service operator or that digital service provider who has reported the incident.

Supervision

Competent Authorities

The act introduces sectoral approach to the cybersecurity supervision in Poland. Each of the essential sectors of the economy is supervised by a competent authority. Because of that, the 11 sectors listed in the Act are included in the capacity of competent departmental ministers[24], as shown in the table below:

Competent authority for cybersecurity matters	Sector/subsector
Minister competent for energy matters	Energy sector
Minister competent for transportation matters	Transportation sector
Minister competent for maritime economy and minister competent for inland waterway transport	Water transport sub-sector
KNF – Polish Financial Supervision Authority	Banking sector and financial market infrastructure
Minister competent for health matters	Health sector
Minister competent for water management	Drinking water supply and distribution sector
Minister competent for digital affairs	Digital infrastructure sector
	Digital service providers
Minister of National Defence (entities subordinate of the Ministry of National Defence and enterprises of special economic and defence importance)	Health sector
	Digital infrastructure sector
	Digital service providers

Table 2. Competent authorities for individual sectors

Competent authorities are the ministers competent for specific sectors of administration. Under an agreement, they may request subordinate or supervised entities to perform certain tasks. **This means that a sectoral regulatory authority operating in a relevant sector may represent the minister as the competent authority.**

The competent authority for cybersecurity is responsible for analysing entities in a relevant sector. Afterwards, it **issues a decision which of the entities will become an essential services operator**. Then the competent authority prepares recommendations for action to strengthen the cybersecurity of the sector. It also conducts inspections of its subordinate operators.

Sectoral Cybersecurity Team

Competent authorities may decide to establish sectoral cybersecurity teams. Such a team will know the specific nature of a relevant sector. This is a major advantage because it will help adjust the support provided to essential services operators. The team will be responsible for: sectoral incident reporting and handling, as well as analysing their impact, and developing recommendations. It also cooperates with the national CSIRT. The team can also share information on significant incidents with other EU countries.

Minister of Digital Affairs

The minister competent for digital affairs is responsible for civil aspects of cybersecurity in Poland. The minister monitors the implementation of the Polish National Cybersecurity Strategy, recommends areas of cooperation with the private sector and provides information on good practices, educational programmes and cybersecurity awareness training.

The minister competent for digital affairs also works towards the development and maintenance of the ICT system to support entities within the national cybersecurity system. The minister also keeps the Single Point of Contact (SPC). SPC cooperates with the European Commission, provides annual reports, liaises with other Member States in the field of cybersecurity, and coordinates cooperation between the competent authorities in Poland.

Minister of National Defence

The Minister of National Defence handles the cybersecurity-related cooperation of Poland's Armed Forces with the relevant institutions of the NATO, the EU and international organisations. The Minister also empowers the Polish Armed Forces to carry out military operations in cyberspace by organising specialised cybersecurity training projects for the Armed Forces and managing incident-related activities during martial law.

Penalties

The Act introduces penalties for non-compliance with legal provisions. Essential services operators and digital service providers may be fined between PLN 1,000 and PLN 1,000,000,000. The fine is a result of a decision of the competent authority for cybersecurity matters. The proceeds go to the state budget.

Strategy and Coordination of Policy in the Field of Cybersecurity

Polish National Cybersecurity Strategy

Under the Act, Poland has to adopt the National Cybersecurity Strategy. The Strategy is developed by the minister competent for digital affairs, who cooperates with the Plenipotentiary for Cybersecurity and other ministers. The Council of Ministers adopt the Strategy by a resolution for 5 years. The resolution is reviewed every 2 years.

Plenipotentiary and Advisory Committee for Cybersecurity

In order to coordinate the policy on a national scale, the Act introduces the Advisory Committee for Cybersecurity and the Plenipotentiary for Cybersecurity.

The Plenipotentiary is appointed and dismissed by the Prime Minister as a Secretary of State or Undersecretary of State. The Plenipotentiary is supervised by the Council of Ministers. The tasks of the Plenipotentiary include:

- analysing and assessing the functioning of the national cybersecurity system;
- supervising the risk management process of the national cybersecurity system;
- issuing opinions on government documents, including draft legal acts, which affect the implementation of cybersecurity-related tasks;
- disseminating new solutions and initiating cybersecurity activities at the national level;
- initiating national cybersecurity exercises;
- issuing recommendations on the use of IT devices or software at the request of CSIRT.

[24] The Act of 4 September 1997 on sectors of government administration (Journal of Laws of 1997 no. 141 item 943) determines a total of 28 sectors of government administration in Poland. The document describes their scope and the competence of the ministers in charge of individual sectors.

Additionally, the Plenipotentiary cooperates with other states, supports research and development of cybersecurity technologies, and undertakes activities to increase public awareness of cybersecurity threats and safe Internet use.

The Advisory Committee for Cybersecurity, with the Prime Minister as the Chair, provides consultations and advice to the Council of Ministers. The Advisory Committee consists of the minister competent for internal affairs, the minister competent for digital affairs, the Minister of National Defence, the minister competent for foreign affairs, the Head of the Chancellery of the Prime Minister, the Head of the National Security Bureau, and the minister competent for coordinating the activities of special services. The Director of the Government Centre for Security, the Head of the Internal Security Agency or his deputy, the Head of the Military Counterintelligence Service or his deputy, and the Director of the Research and Academic Computer Network – National Research Institute also attend the meetings of the Advisory Committee.

Implementing Regulations of the Act on the National Cybersecurity System

The Act on the National Cybersecurity System is complemented by a number of implementing regulations that provide details concerning the provisions of the Act. These include:

1. **Regulation on the organisational and technical conditions for entities providing cybersecurity services, and for internal organisational structures of essential services operators responsible for cybersecurity** of 10 September 2018. The Regulation sets out guidelines for essential services operators (ESO). According to provisions of the Act, ESO may ensure the security of the provided services themselves or entrust this task to an external entity providing services in the field of cybersecurity.
2. **Regulation on the list of essential services and disruptive effect thresholds of an incident in respect of provision of essential services** of 11 September 2018. This is the most significant regulation that gives the basis for the competent authorities to appoint essential services operators in sectors included in provisions of the Act.
3. **Regulation on the scope and mode of operation of the Advisory Committee for Cybersecurity** of 2 October 2018. The Advisory Committee for Cybersecurity is a consultative and advisory body of the Council of Ministers in the field of cybersecurity. The Regulation stipulates the mode of operation of the Advisory Committee, obligations of the Secretary, and how the Advisory Committee adopt its position.
4. **Regulation on the list of certificates entitling to carry out the audit** of 12 October 2018. The Regulation provides requirements for the audit that essential services operators must carry out every 2 years. The audit may be conducted by a conformity assessment body[25], at least two auditors who have relevant experience[26], or at least two auditors who have the certificates specified in the Regulation.
5. **Regulation on types of documentation on cybersecurity of the information system used to provide the essential service** of 16 October 2018. Essential services operators are required to develop, apply and update documentation on the cybersecurity of the information system used to provide the essential service. The documentation consists of normative and operational parts.
6. **Regulation on the thresholds for considering an incident as significant** of 31 October 2018. The Regulation determines the thresholds for classifying incidents as significant for individual sectors and sub-sectors of the economy. It is mandatory to report such incidents.

[25] A conformity assessment body must be accredited in accordance with the provisions of the Act of 13 April 2016 on Conformity Assessment and Market Surveillance Systems (Journal of Laws of 2017 item 1398, and of 2018 item 650), to the extent as relevant for security assessments of information systems being undertaken. (Article 15 paragraph 2 item 1 of the Act on the National Cybersecurity System of 5 July 2018)

[26] An auditor should have at least a three-year experience in the field of auditing the security of information systems, or at least a two-year experience in the field of auditing the security of information systems, and hold a diploma of post-graduate studies in the field of information systems security audits, issued by an organisational unit that was entitled, as of the day of graduation, to grant doctoral degrees in economics, technology or law (Article 15 paragraph 2 item 2 of the Act on the National Cybersecurity System of 5 July 2018)

GDPR implementation – the new Personal Data Protection Act

General Data Protection Regulation

The GDPR was adopted on 27 April 2016 and replaced Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Regulation significantly increases natural persons' control over data concerning them:

- data subjects possess new rights: the right to data portability and the right to be forgotten;
- the data controller must now comply with an extended information obligation in respect of the data subject;
- profiling is regulated: now, in certain cases, the data subject will have the right to obtain e.g. human intervention, so that the decision concerning the subject is not made only by an algorithm;
- there is a new solution relating to data protection by design and data protection by default (Privacy by Design and Privacy by Default, respectively):
  - Privacy by Design means that the data controller must implement appropriate technical and organisational measures, 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;
  - Privacy by Default means that the data controller must implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed;
- the risk-based approach was introduced. According to this approach, data protection obligations vary depending on the risks arising from specific processing activities. Therefore, the data controller decides for itself which organisational and technical measures it should take to protect personal data;
- the data controller must notify the supervisory authority of a personal data breach not later than 72 hours after having become aware of it, in the case of breaches that may pose a risk to rights and freedoms of data subjects. Furthermore, it might also be obliged to notify the person whose rights or freedoms may have been infringed;
- administrative fines for infringements of GDPR provisions were introduced: infringements of the following provisions are subject to fines up to EUR 10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:
  - the obligations of the data controller and of the processor listed in the GDPR, e.g.: failure to verify the consent of the holder of parental responsibility over the child that is below the age of 16 years to the processing of his or her personal data; failure to maintain a record of processing activities; failure to appoint a Data Protection Supervisor in mandatory cases; failure to notify the supervisory authority of personal data breaches; failure to comply with the obligations related to the certification of an enterprise by the relevant entity;
  - the obligations of a certification body listed in GDPR;
  - the obligations of a monitoring body to take appropriate actions if an enterprise is found to have infringed an approved code of conduct;
  - infringements of the following provisions are subject to fines up to EUR 20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:
  - the basic principles for processing, including conditions for consent set out in GDPR;
  - the data subjects' rights;
  - the transfers of personal data to a recipient in a third country or an international organisation;
  - non-compliance with an order of the supervisory authority to temporarily or definitively limit the processing or suspend data flows or failure to provide access;
  - any obligations resulting from any Member State's law adopted under GDPR;
  - non-compliance with corrective actions imposed by the supervisory authority.

GDPR's entry into force and the need to ensure the effective application of its provisions was a significant legislative challenge. The Personal Data Protection Act of 10 May 2018 (Journal of Laws of 2018 item 1000) does not duplicate or implement the solutions of GDPR. Instead, it complements the new personal data protection provisions, making them compliant with the provisions and standards adopted at the EU level. The most important of the new regulations include:

- establishing the office of the President of the Personal Data Protection Office (PUODO), which replaced the Inspector General for Personal Data Protection (GIODO). The President is appointed and recalled by the Polish Parliament upon the consent of the Senate, for a term of office of 4 years. The same person cannot be the President of the Office for more than two terms of office;
- introducing the single-instance procedure before the President of the Office;
- designating the Personal Data Protection Council. The Council is a consulting and advisory body affiliated to the President of the Office, consists of 8 members, and is appointed for a two-year term of office;
- obliging data controllers and processors who are public entities to designate a data protection officer by 31 July 2018[1];
- specifying the conditions and mode of accrediting a certification body;
- determining the mode of approving the code of conduct;
- defining the procedure in the case of an infringement of personal data protection provisions, the inspection of compliance with personal data protection provisions, and the civil and penal liability for infringements;
- restricting, in comparison to GDPR provisions, the amount of administrative fines imposed on certain public authorities and bodies (entities of the public finance sector, research institutes and the National Bank of Poland – up to PLN 100,000; cultural institutions – up to PLN 10,000).

GDPR vs. CERTs/CSIRTs

The new personal data protection law is also a challenge for CSIRTs. Under the GDPR, **'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data**. However, 'processor' means a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller**.

Therefore, a CSIRT is the data controller whenever it processes personal data. If the team acts on behalf of law enforcement or other authorities (e.g. by providing technical support), the CSIRT acts as a processor because it does not determine the purposes or the means of the processing of personal data. Sharing and exchange of information between CSIRTs may also be considered the processing of personal data.

This means that when reporting incidents, CSIRTs are subject to the NIS Directive as well as GDPR. The following tables show requirements for incident notification under both legal acts.

[1] Exceptions involve the cases where AIS (administrators of information security) were previously designated and who, as of the date when the Act entered into force, become data protection officers.

GDPR

Type of incident	Notifying body	Notification recipient	Time limit
Personal data breach	Processor	Data controller	Without undue delay
Personal data breach	Data controller	Competent personal data protection authority	Without undue delay, where possible, not later than 72 hours after receiving the notification
Personal data breach with a high risk to the rights and freedoms of natural persons	Data controller	Competent personal data protection authority and data subjects	Without undue delay

Table 3. Notification of breaches according to GDPR

NIS

Type of incident	Notifying body	Notification recipient	Time limit
Incident having a significant impact on the continuity of essential services	Essential services operators	Competent data protection authority or CSIRT	Without undue delay
Incident having a substantial impact on the provision of a service	Digital service providers	Competent data protection authority or CSIRT	Without undue delay

Table 3. Incident reporting according to the NIS Directive

Therefore, the CSIRT should analyse to what extent it can process personal data within its constituency, and whether it is the processor (i.e. it processes personal data) or the controller. It must also document how it processes personal data, carefully analyse the period and principles of data processing, and anonymise personal data. However, when transferring personal data, it will be necessary to evaluate the constituency of both CSIRTs: the team which transfers the data and the one that is to receive the data.

The competences of the CSIRT at the national level in this respect are regulated by the Act on the National Cybersecurity System.

In Search of the "Polish" Artificial Intelligence (AI)

In 2018, the Polish government initiated work on Artificial Intelligence (AI) for the first time. Even before the publication of the Communication from the Commission: Artificial Intelligence for Europe[27], at the initiative of Poland, the Visegrad Group (V4) adopted a common position on Artificial Intelligence. V4 countries called on EC to further engage in the AI development, emphasising its potential to European enterprises. At the same time, they pointed out the need for in-depth analyses of legal, economic and social aspects important for the AI development. At the EU level, 9 priorities were defined:

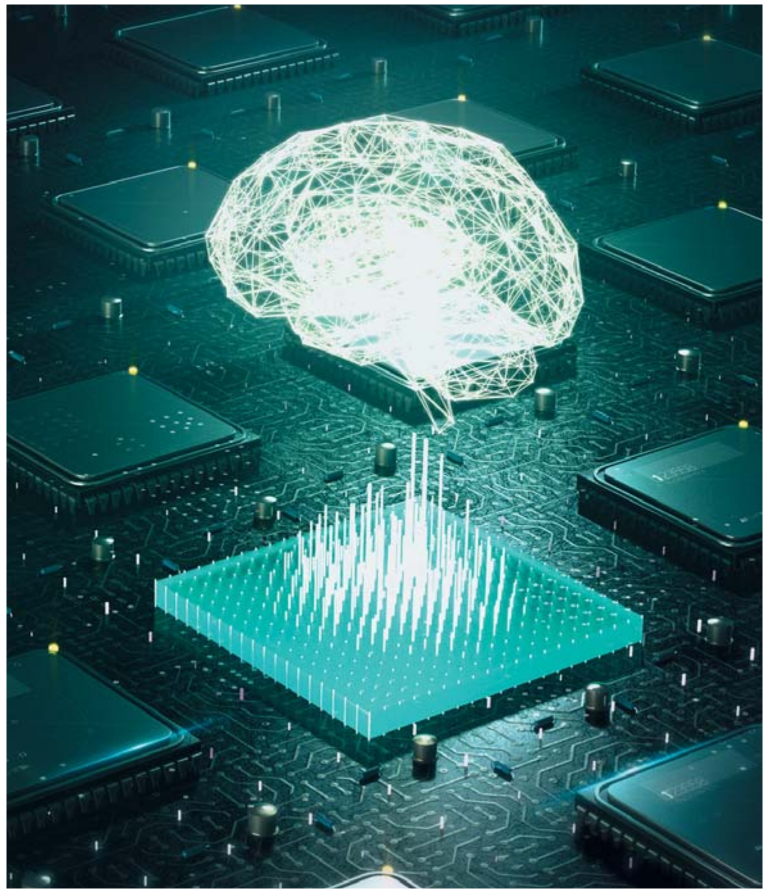
1. including Artificial Intelligence in discussions on digital transformation and making AI one of the EU's priorities for 2020 and beyond;
2. launching pan-European initiatives in the form of virtual data warehouses (this would enable to open up industrial data and speed up research, development and implementation of Artificial Intelligence);
3. launching a debate on the proper financing mechanism for digital technologies;
4. developing "regulatory sandbox" at the EU level to support R&D in key sectors, such as medicine, law, financial markets, services, automotive market, agriculture, environment protection, water management or food industry;
5. analysing the use of the AI technology in reforming the decision-making process by state administration;
6. supporting education and research, and creating academic environments supporting the AI development;
7. creating the European Artificial Intelligence Observatory;
8. ensuring cybersecurity and trust;
9. investigating the impact of Artificial Intelligence on the labour market in Europe[28].

The next step was to establish the four Artificial Intelligence working groups at the Ministry of Digital Affairs: data economy; R&D funding; education; ethics and law. For several months, experts had worked on recommendations that they ultimately presented in early November 2018 as *Foundation of AI Strategy in Poland.*

The document summarises activities of the working groups, and presents the action plan for 2018-2019. It also defines the following priorities:

- developing a new cooperation programme dedicated to AI in the economy;
- creating DIH (Digital Innovation Hub)[29] for Artificial Intelligence;
- supporting non-governmental organisations in disseminating knowledge about AI;
- creating an AI public educational portal;
- launching a virtual AI institute;
- establishing the virtual chair of AI law and ethics (at the Ministry of Digital Affairs);
- developing a catalogue of criteria for AI ethics[30].

Work on the national AI strategy will continue in 2019.



[27] For more information on the Communication from the Commission Artificial Intelligence for Europe, see page 39.

[28] https://www.gov.pl/web/cyfryzacja/stanowisko-grupy-wyszehradzkiej-dotyczace-sztucznej-inteligencji

[29] For more information on DIH, see page 43.

[30] https://www.gov.pl/web/cyfryzacja/sztuczna-inteligencja-polska-2118

Amendments to the Payment Services Act

On 10 May 2018, the Act amending the Payment Services Act and certain other acts[31] was adopted. It implements the PSD2 Directive[32] into the Polish legal system.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC **(PSD2 Directive) was adopted in November 2015**. It increases customer protection and cooperation in the European payments market by:

- including the payment services not previously regulated by the Directive;
- ensuring equal opportunities for a new type of payment services;
- increasing the protection and security of payments by e.g. stronger authentication mechanisms;
- increasing competitiveness and, as a result, encouraging lower prices for customers.

The PSD2 Directive regulates a new type of payment services based on access to "third parties". In a way, this is a revolution in the financial market: it introduces the obligation to permit "third parties" to provide intermediary services without the need of a contract between an account servicing institution (e.g. a bank) and the "third party" (a payment service provider).

Third-party action

Instead of logging in directly to electronic banking services, a customer logs in to an external payment service provider ("third party"). Then, the payment service provider logs in, on behalf of the customer, to the account servicing institution (e.g. a bank) and executes relevant transactions (e.g. payment initiation).

The most important issue regulated by the Act is the security of payment service providers who must take mitigation measures and introduce control mechanisms to manage the operational and security risks.

The Act defines an incident as "an unexpected event having an adverse impact on integrity, availability, confidentiality, authenticity or continuity of the payment services provision, or creating a significant probability that this event will have such an impact; or a series of such events"[33]. Payment service providers must immediately report significant operational and security incidents (including ICT incidents) to the Polish Financial Supervision Authority (KNF). Furthermore, if such an incident could affect financial interests of users, the provider must inform them as well.

Providers must also supply KNF with the annual data on frauds related to payment services.

Moreover, the Act introduces the obligation of strong authentication. It ensures the protection of users' confidentiality in the following three cases: when the user accesses his or her account online; when he or she initiates an electronic payment transaction; and, via a remote channel, when he or she takes an action that may involve the risk of fraud related to the provided payment services or other abuses[34]. These provisions will enter into force on 14 September 2019.

[31] The Act also amends the following: the Act of 29 August 1997 – Tax Law; the Act of 29 August 1997 – Banking Law; the Act of 16 November 2000 on Counteracting Money Laundering and Terrorist Financing; the Act of 24 August 2001 on Settlement Finality in Payment Systems and Securities Settlement Systems and on Supervision of such Systems; the Act of 21 July 2006 on Financial Market Supervision; the Act of 5 November 2009 on Credit Unions; the Act of 12 May 2011 on Consumer Credit; the Act of 5 August 2015 on Handling Complaints by Financial Market Entities and on the Financial Ombudsman; the Act of 15 December 2017 amending the Value Added Tax Act and certain other acts; and the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing.

[32] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ EU L 337 of 23 December 2015, p. 35).

[33] Article 9 c of the Act amending the Payment Services Act and certain other acts.

[34] Article 32 i of the Act amending the Payment Services Act and certain other acts.

European Union – Cybersecurity and Development of Modern Technologies in the Context of Building the Digital Single Market

The European Union (EU) was established in 1993 as an economic and political union. Since 2009, it has been operating as an international organisation. It consists of 28 Member States. The most important bodies of the EU are the European Commission (EC) (the executive authority with legislative initiative); the Council of the European Union (the main decision-making body); and the European Parliament (the body of legislative authority elected by direct universal suffrage).

The EU has been implementing the *Digital Single Market Strategy* (DSM)[35] since 2015. The purpose of DSM is to remove barriers between Member States, which could bring 415 billion EUR annually[36] to the EU economy, according to EC estimates. The Commission believes that the implementation of the actions set out in the DSM Strategy will contribute to the economic growth across the EU and make the daily lives of individual citizens easier. The very operation of the Digital Single Market will contribute to the creation of many new jobs. The DSM Strategy aims to enable Member States to take full advantage of the digital revolution and to achieve rapid economic growth.

A Digital Single Market Strategy for Europe – DSM Strategy

On 6 May 2015, the European Commission published the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe.

The document provides for the abolition of regulatory restrictions on digital issues to enable the creation of the European Digital Single Market. The purpose is to help accelerate the development of digital services and, as a result, build the competitiveness of European enterprises. One of the DSM-related actions involves cybersecurity. The Commission emphasises that citizens will only use secure digital services.

The foundation of the strategy is built on three main pillars with a list of concrete actions assigned to them. Their implementation will ensure the development of a single legal framework for the EU's digital single market:

1. **Better access for consumers and businesses to online goods and services**
   - Introduction of cross-border e-commerce rules that consumers and business can trust;
   - Introduction of affordable high-quality cross-border parcel delivery;
   - Preventing unjustified geo-blocking;
   - Better access to digital content – a modern, more European copyright framework;
   - Reducing VAT-related burdens and obstacles when selling across borders;
2. **Creating the right conditions for digital networks and services to flourish**
   - Making the telecoms rules fit for purpose;
   - A media framework for the 21st century;
   - A fit for purpose regulatory environment for platforms and intermediaries;
3. **Maximising the growth potential of the Digital Economy**
   - Building a data economy;
   - Boosting competitiveness through interoperability and standardisation;
   - An inclusive e-society;

The second pillar includes cybersecurity activities.

[35] https://ec.europa.eu/digital-single-market/en

[36] http://europa.eu/rapid/press-release_IP-15-4919_en.htm

Implementation of the NIS Directive

2018 witnessed mainly work related to the implementation of the NIS Directive[37]. The Cooperation Group[38] established in 2016 coordinated the process (Member States had time to implement it by 9 May 2018). As part of its work, the Group prepared and published a number of documents to support Member States:

- Reference document on security measures for Essential Services Operators
- Reference document on incident notification for Essential Services Operators (circumstances of notification)
- Compendium on cybersecurity of election technology
- Cybersecurity incident taxonomy
- Guidelines on notification of Essential Services Operators incidents (formats and procedures)
- Guidelines on notification of Digital Service Providers incidents (formats and procedures)

Reference document on the identification of Essential Services Operators (modalities of the consultation process in cases with cross-border impact)[39]

Member States also regularly develop cooperation through the CSIRTs network[40].

The NIS Directive, i.e. 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, is the first pan-European legal act involving cybersecurity. The regulation includes two types of entities: essential services operators – ESO (entities from the energy, transport, banking, finance, health, drinking water supply and digital infrastructure sectors) and digital service providers – DSP (online marketplaces, cloud computing services and online search engines). The objective of the NIS Directive is to increase the ICT security both in the Member States and in the EU as a whole. It aims to do so through:

- mandatory incident reporting by essential services operators, and ex post supervisory measures for digital service providers;
- the obligation to estimate cybersecurity risks;
- the obligation for Member States to designate a CSIRT (Computer Security Incident Response Team) that receives incident reports from ESOs and DSPs;
- the obligation to establish competent authorities for cybersecurity matters in the Member States to supervise ESOs and DSPs;
- cooperation between Member States through the Cooperation Group (cooperation mechanism at the political level) and the CSIRTs network (cooperation mechanism at the operational level).

[37] 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.

[38] The Cooperation Group is a political and strategic cooperation mechanism established under Article 11 of the NIS Directive. Its purpose is to support and facilitate strategic cooperation among Member States. The Group is composed of representatives of the Member States, the Commission and ENISA. The Commission provides the secretariat.

[39] https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[40] The CSIRTs network is a mechanism created under Article 12 of the NIS Directive. It consists of representatives of the Member States' CSIRTs and CERT-EU, whereas the Commission participates in the CSIRTs network as an observer. ENISA provides the secretariat. The task of the CSIRTs network is to strengthen operational cooperation between Member States. Under the decision of the minister competent for digital affairs, CERT Polska, which is part of the structure of the NASK National Research Institute, represents Poland in the CSIRTs network.

Negotiations on the Cybersecurity Act

One of the key events of 2018 were the negotiations on the *Cybersecurity Act*. The proposed act was presented in September 2017 as part of the so-called cybersecurity package. The package also included Communication of the European Commission: *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. The document is an update of the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace of 7 February 2013.

The Communication of the EC *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* builds on three pillars which set out concrete measures:

Building EU resilience to cyberattacks

- Strengthening the European Union Agency for Cybersecurity (ENISA);
- Developing towards the Single Market for cybersecurity;
- Full implementation of the Directive on network and information security (the NIS Directive);
- Resilience through rapid response in a crisis situation;
- Establishing a cybersecurity competence network and the European Cybersecurity Research and Competence Centre;
- Building a strong EU cybersecurity skills base;
- Promoting cyber hygiene and risk awareness;

Creating effective EU cyber deterrence

- Identifying malicious actors;
- Stepping up the law enforcement response;
- Stepping up public-private cooperation against cybercrime;
- Stepping up political response;
- Building cybersecurity deterrence through the Member States' defence capabilities;

Strengthening international cooperation on cybersecurity

- Cybersecurity in external relations;
- Building cybersecurity capacity;
- Deepening EU-NATO cooperation.

In the Communication, the European Commission also announced a strong rapprochement between military and civilian issues related to cybersecurity.

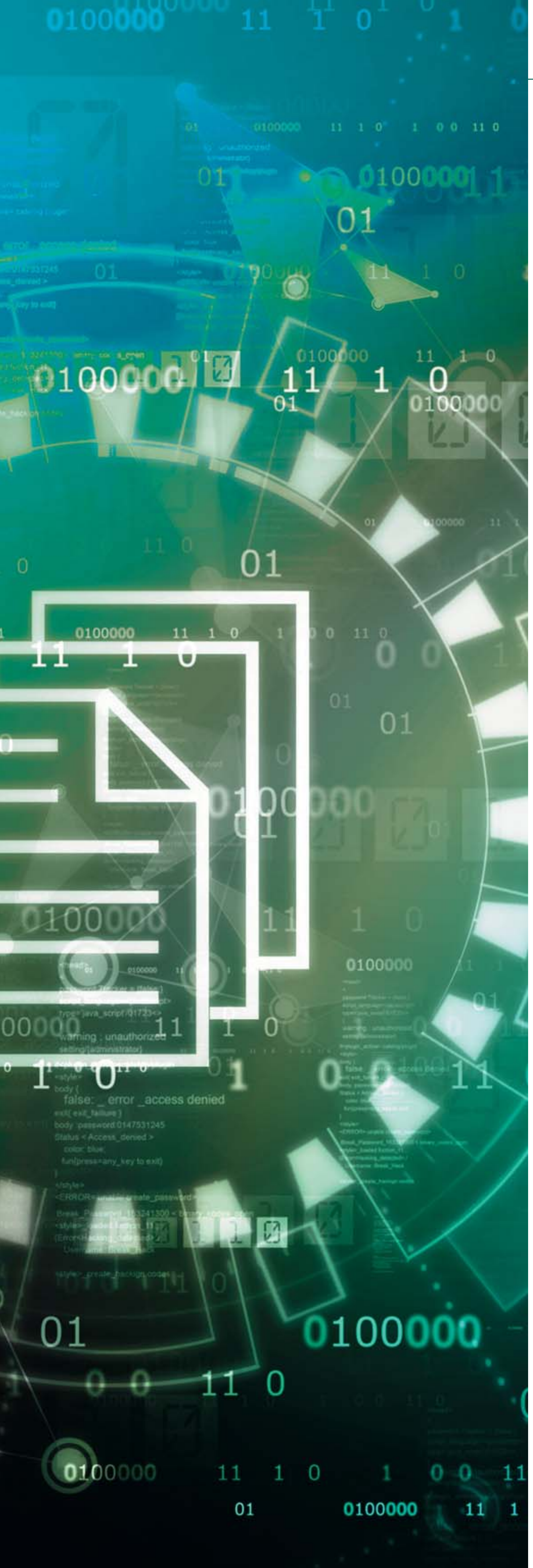
The European Parliament and Commission reached agreement on the package on 10 December 2018, whereas the official publication of the document is expected in March/April 2019. The *Cybersecurity Act* (CA) is the second (following the NIS Directive) legal regulation on cybersecurity at the European level. It aims to increase the resilience of the EU and Member States to ICT risks, and to build a strong cybersecurity system to strengthen the Digital Single Market.

The CA consists of two parts. The first one is a new permanent mandate for the European Union Agency for Cybersecurity (ENISA), whose role has been considerably strengthened. The other one is a regulation creating an EU cybersecurity certification framework for ICT products and ICT services. This crucial change will significantly affect the existing certification model, dominated by SOG-IS (Senior Official Group Information Security Systems)[41].

Regulation on Information and Communications Technology Cybersecurity Certification

The Regulation introduces the **European cybersecurity certification framework.** It sets out a mechanism for establishing European cybersecurity certification schemes and for confirming that products or services meet certain security requirements. The result will be the **mutual recognition of certificates** within the Union. The European Commission also assumes that **certification will increase confidence among consumers** because they will be able to choose tested and compli-

[41] The SOG-IS agreement was concluded in 1997 in response to the EU Council Decision of March 1992. The signatories to the agreement may independently evaluate and certify ITC products and ITC services in accordance with the international standard ISO/IEC 15408, which makes it possible to officially verify the security of ICT systems. Poland joined the group of signatory states of the SOG-IS agreement in 2017.



ant devices and solutions. Moreover, enterprises will save time and money because they **will no longer need to apply for a certificate in every Member State** where they would like to offer their services or products. Additionally, those enterprises that will invest in cybersecurity will gain a significant competitive advantage.

The adoption of the Cybersecurity Act also poses challenges to those Member States that have not yet taken any steps to create a national cybersecurity certification system. Those states that do not need to build the necessary competences and infrastructure from scratch in order to test e.g. certified equipment will be in a much better position.

The European Commission, ENISA and the European Cybersecurity Certification Group are involved in the certification process at the European level.

The European Cybersecurity Certification Group (ECCG) is one of the most important bodies established by CA. The Group consists of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities. ECCG is chaired by the European Commission that, with ENISA's assistance, provides the group's secretariat. ECCG's main task is to cooperate with EC and ENISA by advising on the preparation of certification schemes. Furthermore, the Group is expected to improve cooperation between national certification authorities.

Certification Process Step by Step

Either the European Commission or the European Cybersecurity Certification Group can initiate the certification process. The difference is that **ENISA has to prepare a European certification candidate scheme only at EC's request**. If ECCG requests the preparation of a candidate scheme, ENISA may reject such a request, but must specify the reasons for the rejection.

Step 1: Preparation of a candidate scheme

ENISA is responsible for preparing a certification candidate scheme. During its work, the Agency must consult all stakeholders on the candidate scheme, and set up a working group composed of Member State experts to prepare the scheme. The developed candidate scheme is then submitted to the European Commission.

Furthermore, ECCG provides assistance and expert advice. The Group also gives their opinion on the prepared candidate scheme. This opinion is not binding, and its absence does not prevent the candidate scheme from being submitted to the European Commission. However, ENISA should take utmost account of ECCG's opinion. This way, the public sector has a say in the preparation of European certification schemes.

Step 2: Acceptance of the proposed candidate scheme

On the basis of the candidate scheme received, the Commission **may adopt implementing acts** to establish European cybersecurity certification schemes for ICT processes, ICT products and ICT services.

Step 3: Scheme review

At least every 5 years, ENISA **assesses** the usefulness and relevance of the **adopted European cybersecurity certification schemes**. The European Commission or ECCG may request the Agency to develop an amended candidate scheme.

Step 4: Information on the European cybersecurity certification schemes

ENISA is responsible for setting up **a dedicated website on cybersecurity certification**. The website will contain information, among others, about valid, expired or withdrawn schemes, certificates or statements of conformity. It should also include a repository of links to information provided by ICT manufacturers and suppliers.

The following diagram illustrates the certificate preparation process:

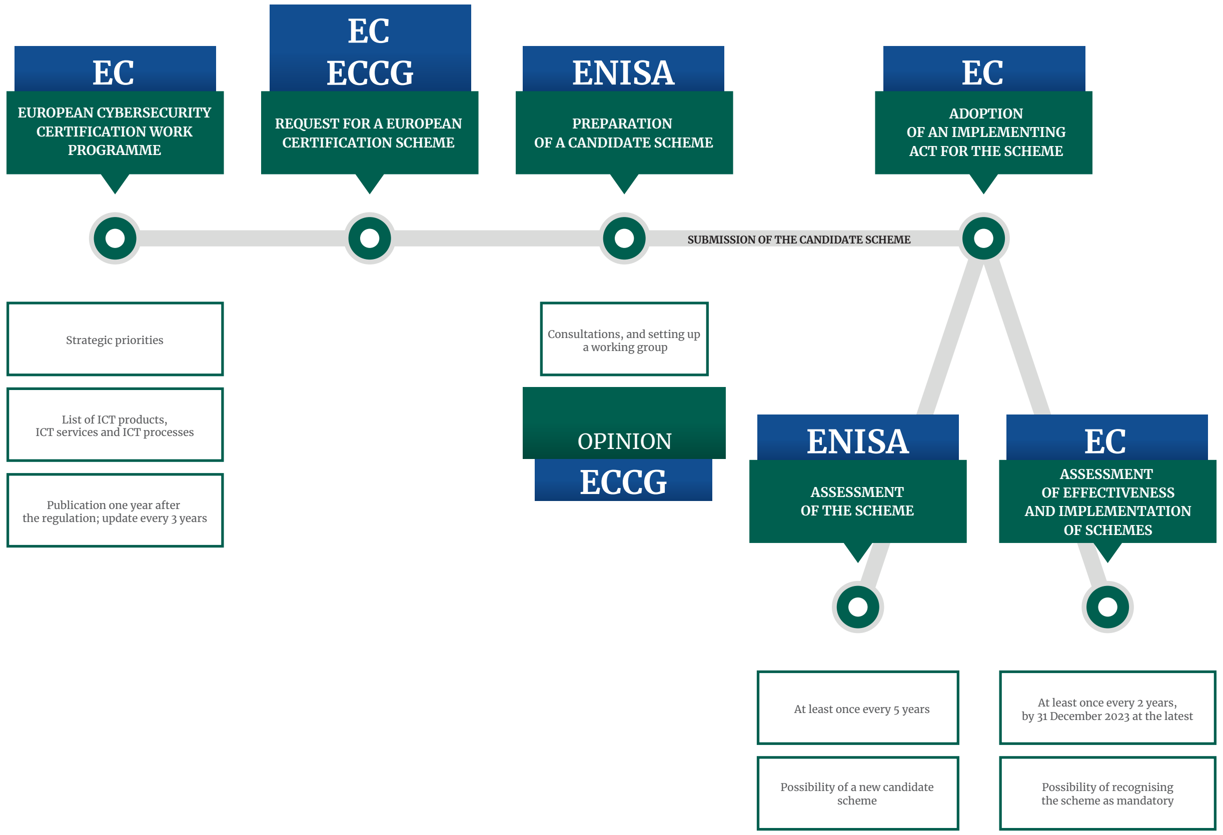

EC
EUROPEAN CYBERSECURITY CERTIFICATION WORK PROGRAMME
EC
ECCG
REQUEST FOR A EUROPEAN CERTIFICATION SCHEME
ENISA
PREPARATION OF A CANDIDATE SCHEME
EC
ADOPTION OF AN IMPLEMENTING ACT FOR THE SCHEME
SUBMISSION OF THE CANDIDATE SCHEME
Strategic priorities
List of ICT products, ICT services and ICT processes
Publication one year after the regulation; update every 3 years
Consultations, and setting up a working group
OPINION
ECCG
ENISA
ASSESSMENT OF THE SCHEME
EC
ASSESSMENT OF EFFECTIVENESS AND IMPLEMENTATION OF SCHEMES
At least once every 5 years
Possibility of a new candidate scheme
At least once every 2 years, by 31 December 2023 at the latest
Possibility of recognising the scheme as mandatory

Fig. 2. Preparation of European cybersecurity certification scheme

A European cybersecurity certification scheme may specify **assurance levels: basic, substantial and high**. The assurance level for a relevant ICT product or service should be **proportional to the level of the risk** in terms of, among others, the probability and impact of an incident.

A certificate issued at a specific level assures that ICT products, ICT services and ICT processes meet the corresponding security requirements, and have been evaluated in accordance with the guidelines applicable at that level.

Assurance level	Risk	Evaluation required
Basic	known basic risks of incidents and cyberattacks	technical documentation
Substantial	known cybersecurity risks risk of incidents and cyberattacks carried out by actors **with limited skills and resources**	absence of publicly known vulnerabilities ICT products or ICT services correctly implement the necessary security functionalities
High	risk of state-of-the-art cyberattacks carried out by actors with **significant skills and resources**	absence of publicly known vulnerabilities ICT products or ICT services correctly implement the necessary security functionalities **resistance to skilled attackers, using penetration testing**

Table 5. Assurance levels and required evaluation according to the Cybersecurity Act

The European cybersecurity certification scheme also permits a **conformity self-assessment.** It is **the sole responsibility** of a manufacturer or a provider of ICT products and ICT services. The self-assessment should be permitted only for the products and services if they correspond to **assurance level ‘basic’**[42].

Mandatory Certification

CA introduces mandatory certification for the ICT products, ICT processes and ICT services that EC identifies as requiring such certification as a result of a review. EC starts the assessment from the particularly vulnerable sectors listed in Annex II to the NIS Directive: energy, transport, banking and financial market infrastructures, health, drinking water supply and digital infrastructure. They undergo assessment at the latest two years after the first scheme is adopted.

Certification at National Level – Obligations of Member States

While the preparation of cybersecurity certification schemes takes place at the European level, the **certification process occurs at the national level**. CA imposes specific obligations on Member States to help build an efficient national cybersecurity certification system. It is necessary to designate the following authorities and bodies to enable the certification process:

1. A national cybersecurity certification authority (NCCA)

NCCA should be established **within 24 months after the publication of the Regulation**. A Member State may also designate a national cybersecurity certification authority in the territory of another Member State, after agreeing with that Member State.

A national certification authority has a twofold role: **it issues certificates** (certification body) and carries out **supervisory activities**. Both functions must be separated and independent of each other. National authorities must also be **independent of the entities they supervise**.

Their main tasks include **monitoring compliance of** ICT products, ICT processes and ICT services with requirements of the certificates issued in their Member States. They also support national accreditation bodies in the **supervision of conformity assessment authorities**. In order to perform their tasks, they may, among others, carry out audits, impose penalties or even withdraw a certificate that does not comply with the European certification scheme.

National certification authorities cooperate with each other and with EC; they **also participate in works of the European Cybersecurity Certification Group**. Moreover, they are subject to **peer review**. It is carried out **at least once every five years**, by at least two national cybersecurity certification authorities of other Member States and the Commission. ENISA may participate in the peer review.

2. National accreditation body

Under the prior Regulation[43], each Member State designates a single national accreditation body. In Poland, the Polish Centre for Accreditation **accredits conformity assessment bodies** provided that they meet specified requirements[44]. Accreditation is issued for a **maximum of five years** and should be renewable on the same conditions provided that the conformity assessment bodies still meet the requirements.

3. Conformity assessment body

Conformity assessment bodies **may issue certificates for assurance level ‘basic’ or ‘substantial’** and, after being required to do so by NCCA, even for assurance level ‘high’.

If a national cybersecurity certification authority issues a European cybersecurity certificate, then the authority’s certification body will be accredited as a conformity assessment body.

European cybersecurity certification schemes may also set out **specific or additional requirements.** In such a case, NCCA authorises conformity assessment bodies that meet those requirements.

National Cybersecurity Certification Scheme and Cybersecurity Certificates

The Cybersecurity Act will affect current certification systems in the Member States. However, previously issued national certificates will remain effective. Even if they are covered by new European certification schemes, **they will keep their validity until the expiry date specified in the relevant certificate.**

The national cybersecurity certification schemes **covered by** European certification schemes **will cease to be effective** from a date established in an implementing act of the relevant European scheme. However, if the national scheme **is not covered** by the European equivalent, it will continue to **exist**.

Member States do not introduce new national cybersecurity certification schemes for ICT products, ICT services or ICT processes that are already covered by an existing European cybersecurity certification scheme.

Issuance of Cybersecurity Certificates

The required assurance level for a relevant ICT product or ICT service, defined by the certification scheme, determines which body may issue a European cybersecurity certificate, as shown in the table below.

Assurance level	Issuing authority or body	Exceptions
Basic/Substantial	Conformity assessment bodies	The scheme may determine that the certificate can **only** be issued by a **public body**: national cybersecurity certification authority public body that is accredited as a conformity assessment body
High	National cybersecurity certification authorities (NCCA)	**The certificate can be issued by** a conformity assessment body: upon prior approval by the national cybersecurity certification authority for each individual certificate issued by a conformity assessment body; upon prior general delegation of this task to a conformity assessment body by the national cybersecurity certification authority.

Table 6. Issuance of cybersecurity certificates.

[42] The issuing of an EU statement of conformity is voluntary, unless otherwise specified in Union law or Member State law. EU statements of conformity are recognised in all Member States.

[43] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93

[44] The requirements are set out in the Annex to the above-mentioned Regulation.

The following diagram shows the certificate issuance process:

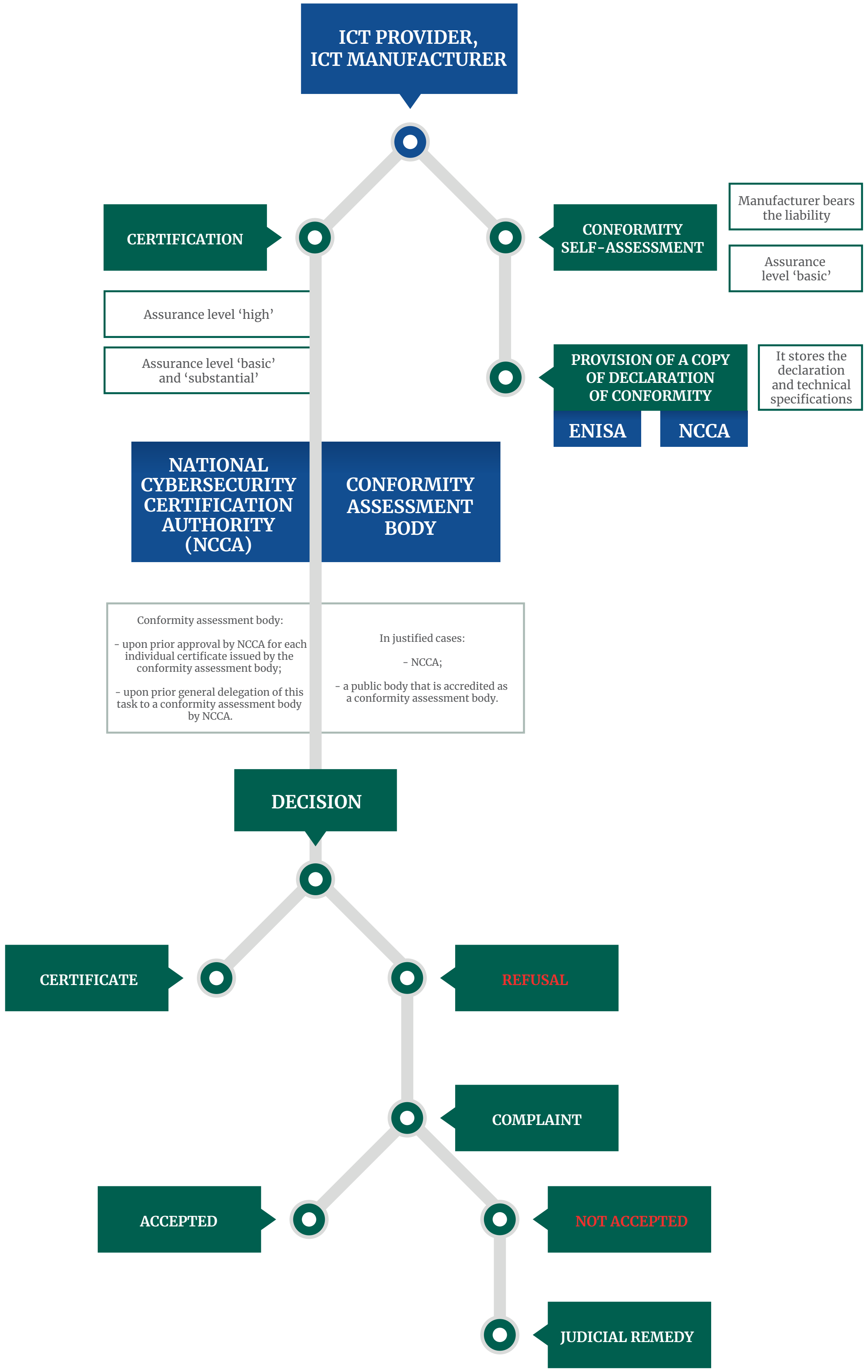

ICT PROVIDER,
ICT MANUFACTURER
CERTIFICATION
Assurance level 'high'
Assurance level 'basic' and 'substantial'
CONFORMITY SELF-ASSESSMENT
Manufacturer bears the liability
Assurance level 'basic'
PROVISION OF A COPY OF DECLARATION OF CONFORMITY
It stores the declaration and technical specifications
ENISA
NCCA
NATIONAL CYBERSECURITY CERTIFICATION AUTHORITY (NCCA)
CONFORMITY ASSESSMENT BODY
Conformity assessment body:
- upon prior approval by NCCA for each individual certificate issued by the conformity assessment body;
- upon prior general delegation of this task to a conformity assessment body by NCCA.
In justified cases:
- NCCA;
- a public body that is accredited as a conformity assessment body.
DECISION
CERTIFICATE
REFUSAL
COMPLAINT
ACCEPTED
NOT ACCEPTED
JUDICIAL REMEDY

Fig. 3. Certification issuance process.

Under the Regulation, Member States can impose penalties for infringements of its provisions. The same is applicable to breaches of European cybersecurity certification schemes. The penalties must be effective, proportionate and discouraging.

ENISA's New Mandate

The European Union Agency for Cybersecurity (ENISA) was established in 2004. So far, ENISA's mandate has been temporary and due to end in June 2020. With the introduction of the *Cybersecurity Act*, ENISA gained a permanent and clearly defined mandate, a greater impact on EU's cybersecurity ecosystem, and a higher budget.

ENISA, located in Greece, is an independent centre of expertise on cybersecurity. The Agency's principal aim is to ensure a high level of cybersecurity in the EU. ENISA completes tasks resulting from EU provisions and ensures that no work performed by Member States is duplicated.

When established in 2004 (Regulation (EC) No 460/2004), the Agency received a mandate for 5 years. However, it was renewed twice: in 2009 and in 2011. ENISA was the only European agency with a temporary mandate valid until June 2020. In the July 2016 communication, the European Commission revised the Agency's mandate. The result was the legislative act presented on 13 September 2017 as part of the "Cybersecurity package".

ENISA's main tasks include the following:

1. **Development and implementation of EU policy and law**

ENISA is to provide its independent opinion and analysis. The Agency should also contribute to EU policy, sector-specific policy and law initiatives if they refer to cybersecurity. ENISA is also expected to support Member States in the development of national cybersecurity policies, and in the implementation of the related EU guidelines and the law relating to data protection and privacy.

2. Capacity-building

ENISA's new task is to assist Member States, EU institutions, bodies and agencies in prevention of cyber threats. In this respect, it cooperates with the CERT-EU team[45]. The Agency also supports national CSIRTs in raising their capabilities and organising cybersecurity exercises at EU level on at least a biennial basis (*CyberEurope*).

ENISA also has specific tasks related to the implementation of the NIS Directive: it assists the Cooperation Group in identification of essential services operators in relation to cross-border dependencies, provides the secretariat for the CSIRTs network, and supports the cooperation of national CSIRTs; it supports information sharing in and between key sectors, and provides best practices and guidance for the sectors.

3. **Operational cooperation at EU level**

ENISA's role is also strengthened by another new task. The Agency supports cooperation among Member States, EU institutions, bodies, offices, agencies and stakeholders. In this respect, ENISA works on synergies between these entities and CERT-EU, services dealing with cybercrime, and supervisory authorities dealing with the protection of privacy and personal data. The Agency advises on how to improve CSIRT's capabilities. It also assists Member States in assessing incidents and analysing vulnerabilities. ENISA prepares a regular Cybersecurity Technical Situation Report on incidents and cyber threats based on reports shared by the Member States, the CSIRTs network, the single points of contact and the European Cybercrime Centre (EC3) at Europol. Finally, it contributes to developing a cooperative response to large-scale cross-border incidents or crises related to cybersecurity[46].

4. **Market, cybersecurity certification, and standardisation**

With the introduction of the European cybersecurity certification scheme, ENISA has been given a number of competences and obligations. ENISA is to support and promote the implementation of cybersecurity certification of ICT products, ICT services and ICT processes by monitoring developments in related areas of standardisation on an ongoing basis. Another task is recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes. ENISA prepares candi-

[45] The Computer Emergency Response Team (CERT-EU) for the EU Institutions, bodies and agencies is composed of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, European Economic and Social Committee). The CERT-EU cooperates with other CERTs in the Members States and with specialised IT security companies.

[46] In this respect, ENISA aggregates reports from Member States, ensures the efficient flow of information in the CSIRTs network, provides support in the public communication relating to incidents or crises, and tests the cooperation plans for responding to cross-border incidents at EU level.

date European cybersecurity certification schemes to be provided to the European Commission. Together with EC, ENISA chairs the Cybersecurity Certification Group, which consists of experts representing the relevant stakeholders[47]. Furthermore, ENISA compiles and publishes guidelines and develops good practices in respect of the certification, and contributes to the related capacity-building in Member States, e.g. by organising workshops or conferences.

5. Knowledge and information

As part of the new tasks, ENISA is expected to perform analyses of emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity. ENISA performs strategic analyses of incidents in order to identify emerging trends and help prevent incidents. It provides advice, guidance and best practices in respect of cybersecurity of the critical infrastructure, essential services operators and digital service providers.

6. Awareness-raising and education

The new mandate also strengthens ENISA's role in the field of education. ENISA provides individual guidance on good practices aimed at citizens, organisations and businesses, and, in cooperation with the Member States, organises regular awareness campaigns. Every year, in October, ENISA coordinates the European Cybersecurity Month[48]. It also supports local education activities of the Member States.

7. Research and innovation

ENISA contributes to the strategic research and innovation agenda in the field of cybersecurity by advising on research needs and priorities. At the Commission's request, the Agency also participates in the implementation phase of research and innovation funding programmes.

8. International cooperation

ENISA contributes to EU's efforts to cooperate with third countries and international organisations on issues related to cybersecurity. It engages as an observer in the organisation of international exercises, and facilitates the exchange of best practices. Together with MSCG (Member States Certification Group), ENISA provides expertise on matters concerning agreements for the mutual recognition of cybersecurity certificates with third countries.

Organisation of ENISA

ENISA's administrative structure is composed of Management Board, Executive Board, Executive Director, ENISA Advisory Group, and National Liaison Officers Network. The following table shows ENISA's structure.

Management Board	The Management Board is composed of one member appointed by each Member State, and two members appointed by the Commission. All members have the right to vote. Each member of the Management Board has an alternate; the alternate represents the member in case of absence. Members of the Management Board and their alternates are appointed on the basis of their knowledge in the field of cybersecurity, taking into account their relevant managerial and administrative skills. The Management Board makes its decisions by a majority of its members. A majority of two-thirds of the members of the Management Board is required for the adoption of the single programming document[49] and of the annual budget, and for the appointment, extension of the term of office or removal of the Executive Director. The Management Board establishes the general direction of the operation of ENISA, adopts the proposed budget, and prepares the annual report on ENISA's activities, which is submitted to the European Parliament, to the Council, to the Commission and to the Court of Auditors. The Management Board also appoints the Executive Director.
Chairperson of the Management Board	The Management Board elects a Chairperson and a Deputy Chairperson from among its members, by a majority of two thirds of the members. Their term of office is four years, which is renewable once. Meetings of the Management Board are convened by its Chairperson. There are at least two meetings a year.
Executive Board	The Management Board is assisted by an Executive Board. The Executive Board is composed of five members and a representative of the Commission. The term of office of the members of the Executive Board is four years, and it is renewable. The Executive Board meets at least once every three months. The Executive Director may take part in the meetings of the Executive Board, but has no right to vote. The Executive Board prepares decisions to be adopted by the Management Board and assists the Executive Director in implementing the decisions.
Executive Director	ENISA is managed by its Executive Director, who is independent in the performance of his or her duties. The Executive Director is accountable to the Management Board. The Executive Director may set up **working groups** composed of experts from the Member States. The procedures regarding the appointment of the working groups are specified in ENISA's internal rules of operation.
ENISA Advisory Group	The ENISA Advisory Group operates within ENISA. It is established, upon a proposal from the Executive Director, for the term of office of two-and-a-half years. It is composed of experts representing the relevant stakeholders, such as providers of electronic communications networks or ICT services, SMEs, operators, consumer groups, academic experts, and representatives of law enforcement and data protection supervisory authorities. The Group is chaired by the Executive Director or by any person whom the Executive Director appoints on a case-by-case basis. The ENISA Advisory Group advises ENISA and the Executive Director.
National Liaison Officers Network	ENISA also has a **National Liaison Officers Network** composed of representatives of all Member States (each Member State appoints one representative). The Network's task is to facilitate the exchange of information between ENISA and the Member States; support ENISA in disseminating its activities, findings and recommendations; and act as a point of contact between ENISA and national experts in the field of cybersecurity.

Table 7. Organisation of ENISA

[47] The Commission selects, on the basis of a proposal from ENISA, members of the Stakeholder Cybersecurity Certification Group.

[48] ENISA coordinates the European Cybersecurity Month, a recurring initiative of the European Commission that takes place every year in October. The 6th edition of the ECSM was held in 2018. The NASK National Research Institute coordinates this campaign in Poland.

[49] The single programming document contains ENISA's annual and multiannual programming, which includes detailed objectives and expected results, including performance, to evaluate ENISA's operations.

Cooperation with Member States, Third Countries and International Organisations

ENISA may cooperate with Member States or international organisations. ENISA may also establish working arrangements, subject to the prior approval of the Commission, which do not create legal obligations incumbent on EU and its Member States. ENISA is open to the participation of third countries that have concluded agreements with EU. Relevant provisions of such agreements establish working arrangements, specifying in particular the nature, extent and manner in which those third countries are to participate in ENISA's work. The Management Board adopts a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent.

European Cybersecurity Competence Centre and the Network of National Coordination Centres – New EC Proposal

On 12 September 2018, the European Commission presented a proposal for a regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. The proposal aims to stimulate the European cybersecurity technological and industrial ecosystem, and strengthen cooperation in the field of cybersecurity between different industry and research communities. According to EC's proposal, the European Cybersecurity Competence Centre, the Network of National Coordination Centres and the Cybersecurity Competence Communities are to be part of the new ecosystem.

The **European Cybersecurity Competence Centre** is a new institution and has the following tasks:

- facilitate and help coordinate the work of the Network of National Coordination Centres;
- enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities;
- contribute to the wide deployment of state-of-the-art cybersecurity products and solutions across the economy;
- improve the understanding of cybersecurity and contribute to reducing skills gaps in EU related to cybersecurity;
- contribute to the reinforcement of cybersecurity research and development in EU;
- enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity;
- enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund.

Principally, the Centre is to distribute European funds allocated for cybersecurity from the European to the Member State level. The Centre is also expected to build knowledge and expertise.

According to the EC proposal, the structure of the Competence Centre consists of the following:

- a **Governing Board**, composed of one representative of each Member State, and five representatives of the Commission;
- an **Executive Director**, engaged by the Competence Centre and appointed by the Governing Board from a list of candidates proposed by the Commission;
- an **Industrial and Scientific Advisory Board**, consisting of no more than 16 members. The members are appointed by the Governing Board from among the representatives of the entities of the Cybersecurity Competence Community.

Network of National Coordination Centres – the centres will be designated by Member States and accredited by the European Commission. They are to support activities of the Competence Centre. Furthermore, the tasks of the Network are as follows:

- facilitating the participation of industry and other actors at the Member State level in cross-border projects;
- contributing, together with the Competence Centre, to identifying and addressing sector-specific cybersecurity industrial challenges;
- acting as contact point at the national level for the Cybersecurity Competence Community and the Competence Centre;
- seeking to establish synergies with relevant activities at the national and regional level;
- implementing specific actions for which grants have been awarded by the Competence Centre;
- promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at the national or regional level;
- assessing requests for becoming part of the Cybersecurity Competence Community submitted by entities established in the same Member State as the Coordination Centre.

The **Cybersecurity Competence Community** will cooperate with the European Cybersecurity Competence Centre and disseminate expertise. This diverse group of actors illustrating different viewpoints will represent, among others, industry, academic and non-profit research organisations, associations, and public entities. Accredited entities accepted into the Community must demonstrate that they have cybersecurity expertise with regard to at least one of the following domains:

- research;
- industrial development;
- training and education.

The accreditation is given by the European Competence Centre. Relevant organisations are established under national law as members of the Cybersecurity Competence Community after an assessment made by the National Coordination Centre of the Member State. Furthermore, relevant EU bodies, agencies and offices may be appointed as members of the Cybersecurity Competence Community.

The members of the Cybersecurity Competence Community:

- support the Competence Centre in achieving its mission and objectives and, for this purpose, work closely with the relevant National Coordinating Centres;
- participate in activities promoted by the Competence Centre and National Coordination Centres;
- participate in working groups established by the Governing Board of the Competence Centre to carry out specific activities from the Competence Centre's work plan;
- where relevant, support the Competence Centre and the National Coordination Centres in promoting specific projects;
- promote and disseminate the relevant outcomes of the activities and projects carried out within the Community.

The proposal for the Regulation on the European Cybersecurity Industrial, Technology and Research Competence Centre raises many controversies. It is difficult to see justification for the dominant role of the European Commission in the Governing Board and the dependence of Member States' voting rights in the Board on the funds paid into the Centre. Furthermore, part of the Centre's tasks clearly overlap with the new mandate of the European Union Agency for Cybersecurity (ENISA).

European Electronic Communications Code – Telecommunications Law Reform

The European Electronic Communications Code[50] (the Code) was adopted on 11 December 2018. The proposal of the relevant directive has been underway since September 2016. It is a comprehensive reform of telecommunication provisions from 2009 and **one of the most important proposals in respect of the Digital Single Market**. Changes involve the access to the infrastructure, the regulation of radio spectrum, and the definition and regulation of electronic communications services. Furthermore, the European Commission has proposed a new objective for the regulatory framework: **widespread access to and use of very high capacity connectivity**.

The Directive also increases the cybersecurity of the telecommunications sector. In accordance with Article 40, operators must ensure appropriate technical and organisational measures to manage the risks posed to security of networks and services. The level of security of these measures must be appropriate to the risk in order to prevent and minimise the impact of security incidents. Furthermore, undertakings must guarantee the integrity of their networks, and notify the competent national regulatory authority of breaches of security. In order to determine the significance of a security incident, the following parameters must, in particular, be taken into account:

- the number of users affected by the security incident;
- the duration of the security incident;
- the geographical spread of the area affected by the security incident;
- the extent to which the functioning of the network or service is disrupted;
- the extent of impact on economic and societal activities.

These parameters are in conformity with the NIS Directive and, therefore, with the Act on the National Cybersecurity System.

[50] Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

However, in accordance with Article 41 of the Code, competent national authorities may require undertakings:

- to provide information needed to assess the security and integrity of their services and networks, including documented security policies;
- to submit to a security audit carried out by a qualified independent body or a competent authority, and make its results available to the competent authority. The undertaking pays the cost of the audit[51].

ePrivacy Negotiations

The proposal of the ePrivacy[52] Regulation was presented on 10 January 2017. The regulation was to enter into force together with GDPR, and become a special regulation concerning Internet privacy (the so-called *lex specialis* to GDPR). However, the negotiations have been longer than expected.

The proposal of the regulation covers communications service providers, Internet providers and such entities as: Facebook, Messenger, Skype, Gmail, WhatsApp or Viber. The regulation also applies to entities not established in the EU, but which provide services to citizens of an EU country.

The project extends the definition of Internet marketing, and introduces protection for both natural and legal persons. A few of its important elements are the increased transparency of cookies (used to store information about preferences and personalise websites), the need to anonymise electronic messages sent by users, and the protection of metadata that provide highly sensitive information, such as location, the websites visited or the time and date when an individual sent a message.

Council Conclusions on Malicious Cyber Activities – EU Diplomacy in the Service of Cybersecurity

On 16 April 2018, the Council of the European Union adopted conclusions on malicious cyber activities[53]. In the document, the Council expressed its serious concern about the increased ability and willingness of third states and non-state actors to pursue their objectives by undertaking malicious cyber activities. It firmly condemned the malicious use of information and communications technologies. It specifically listed Wannacry and NotPetya attacks as having caused significant damage and economic loss in the EU and beyond. The Council stressed that the use of ICTs for malicious purposes is unacceptable. It expressed its willingness to continue working on the further development and implementation of the voluntary non-binding norms, rules and principles for the responsible state behaviour in cyberspace, e.g. within the UN and other appropriate international fora.

The Council's activities are a continuation of the initiative launched in 2017 when EU adopted the Framework for a Joint EU Diplomatic Response (the so-called *diplomacy toolbox*). The document provides for the use of EU diplomacy as a response to malicious cyber activities (appropriately to the extent, scale, duration, intensity, complexity, sophistication and impact of the activities)[54].

Artificial Intelligence for Europe

In 2018, the European Commission focused particularly on the issues related to Artificial Intelligence (AI) and the ethical aspects of its development.

Communication from the Commission Artificial Intelligence for Europe

EC presented the Communication Artificial Intelligence for Europe on 25 April 2018. The document determines actions in the field of technology, ethics, law and economics. AI has been identified as a significant strategic challenge. EC stresses differences in the funds allocated for AI in Europe and worldwide: European investments in AI amount to only between EUR 2.4 and 3.2 billion, whereas in Asia and North America between EUR 6.5 and 9.7 and between EUR 12.1 and 18.6, respectively. The AI challenge has been addressed in the following three aspects:

[51] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018L1972&from=it

[52] Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

[53] *Council conclusions on malicious cyber activities*, 7517/18.

[54] https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=uriserv%3AOJ.L_.2017.239.01.0036.01.ENG

1. **Boosting the EU's technological and industrial capacity and AI uptake across the economy**

   Principally, the European Commission aims to increase spending on AI, which is to reach EUR 20 billion by the end of 2020. However, this applies to public and private sectors combined, while EC's investments in AI amount only to EUR 1.5 billion under the research and innovation framework programme Horizon 2020.

2. **Preparing for socioeconomic changes**

   New jobs will emerge as a result of AI. Other jobs will be replaced. Therefore, the Commission encourages the modernisation of education and plans to set up dedicated (re-)training schemes in connection with the Blueprint on sectoral cooperation. Furthermore, EC has announced that it will continue activities related to the development of digital skills.

3. **Ensuring an appropriate ethical and legal framework**

   The emergence of AI is also a legal and ethical challenge. Therefore, EC has announced the development of a guidance document on the interpretation of the Product Liability Directive.

Expert Group on Artificial Intelligence

In June 2018, EC appointed a group of 52 AI experts. It consists of representatives of academia, civil society, as well as industry. The Group's objective includes the elaboration of recommendations on future-related policy development. On 18 December, the Group proposed the **Ethics Guidelines for the Development and Use of Artificial Intelligence[55],** in which it put forward a structure of trustworthy AI. The document has been the subject of public consultations, and its final version is expected to be published in March 2019.

Coordinated Plan on Artificial Intelligence

EC published the Coordinated Plan on Artificial Intelligence[56] on 7 December 2018. The document has seven main objectives:

1. **Common objectives and complementary efforts**

   The Commission has presented a framework for national AI strategies, and encouraged the Member States to develop their national AI strategy by mid-2019. The strategies are expected to outline e.g. investment levels. The European Commission is particularly interested in scaling up public and private investments in order to reach the target of EUR 20 billion per year.

2. **Towards a European AI public-private partnership and more financing for start-ups and innovative small and medium-sized enterprises**

   The Commission would like to reinforce cooperation between the private sector and the public sector, particularly in respect of research and creation of new AI technologies and applications. This should foster the collaboration between academia and industry. The Commission also aims at making available resources for start-ups and innovators in AI in the amount of EUR 100 million in 2020.

3. **Strengthening excellence in trustworthy AI technologies and broad diffusion**

   In order to foster collaboration between the best research teams in Europe, the Commission has announced the creation of networks of European AI research excellence centres. Furthermore, EC plans to reinforce Digital Innovation Hubs towards Artificial Intelligence, where it considers farming, smart cities, and connected and autonomous vehicles as key sectors.

4. **Adapting learning and training programmes and systems to better prepare our society for AI**

   Technological changes modify the skills required of young people, those who are still learning and those who are already in the labour market, meaning they need to up-skill. Thus, more focus needs to be put on life-long learning and education of those workers who will actually implement the AI solutions of the future. The Commission will support Masters and PhDs in AI through the research programmes.

5. **Building up the European data space essential for AI in Europe, including for the public sector**

   EC stresses that further developments in AI require a well-functioning data ecosystem built on trust, data availability and infrastructure. In 2020, the Commission will continue the development of a common database of health images. Furthermore, the Commission will support cybersecurity solutions.

6. **Developing ethics guidelines with a global perspective and ensuring an innovation-friendly legal framework**

EC emphasises that the development of AI in Europe must respect fundamental rights and follow ethical rules. Thus, the experts will present their final version of the Ethics Guidelines for the Development and Use of Artificial Intelligence in March 2019.

[55] https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_draft_ethics_guidelines_18_december.pdf

[56] https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence

7. **Security-related aspects of AI applications and infrastructure, and international security agenda**

   According to the Commission, there is a need to better understand how AI can impact security in three dimensions:

   - how AI could enhance the objectives of the security sector;
   - how AI technologies can be protected from attacks;
   - how to address any potential abuse of AI for malicious purposes.

Disinformation

In 2018, anti-disinformation activities in the European Union increased, resulting in the publication of four important documents.

According to the EU Hybrid Fusion Cell[57], disinformation by the Russian Federation poses the greatest threat to the EU in the context of the European Parliament elections scheduled for May 2019[58]. By 2020, Member States will have held a total of more than 50 national, presidential and local elections[59]. Meanwhile, according to the Commission, disinformation campaigns have had a clear effect on the elections held in the EU[60] in recent years.

EC Communication: Tackling Online Disinformation: a European Approach

The Communication, published on 26 April, presents the scope, scale and analysis of disinformation, describes the risks associated with its dissemination, and proposes specific measures to tackle it. The document was developed as a result of a report delivered by the High-Level Expert Group: *A multi-dimensional approach to disinformation*[61].

The Commission highlights the following main areas of actions:

1. **A more transparent, trustworthy and accountable online ecosystem**

   The Commission encourages online platforms to become more involved in tackling online disinformation as part of self-regulation. This can be done by creating an independent European network of fact-checkers.

2. **Secure and resilient election processes**

   With a view to the 2019 European Parliament elections, the Commission has announced that particular attention will be paid to the security of Network and Information Systems.

3. **Fostering education and media literacy**

   Critical and digital competences are crucial to the resilience of our societies to disinformation. The Commission emphasises the importance of extending digital education and the need to strengthen new media literacy.

4. **Support for quality journalism as an essential element of a democratic society**

   There is a need to strengthen the role of journalism and reinforce trust in journalists. They should also further embrace the opportunities offered by new technologies and develop the necessary digital skills to enable fact-finding and verification.

5. **Countering internal and external disinformation threats through strategic communication**

   In 2015, the East Stratcom Task Force was set up to address Russia's ongoing disinformation campaigns. The EU Hybrid Fusion Cell was established in 2016 within the EU Intelligence and Situation Centre, whereas the European Centre of Excellence for Countering Hybrid was launched in 2017.

Code of Practice on Disinformation

In September 2018, the European Commission published the Code of Practice on Disinformation. The document is a self-regulatory standard of the business sector, developed by representatives of online platforms, leading social networks, advertisers and the advertising industry, with the support of academia and civil society. The Code includes five key actions:

[57] The EU Hybrid Fusion Cell was established within the EU Intelligence and Situation Centre of the European External Action Service in 2016. It analyses information concerning hybrid threats and shares assessments and briefings within EU institutions, ensuring to inform EU decision-making. In respect of cyber threats, the Cell relies on information received, among others, from CERT-EU.

[58] Action Plan against Disinformation, p. 4

[59] Action Plan against Disinformation, p. 2

[60] Information Manipulation, a challenge to our democracies. A report by the Policy Planning Staff and the Institute for Strategic Research

[61] The High-Level Expert Group on fake news and online disinformation consists of 39 experts. Its members have different backgrounds, including academia and journalism, written press and broadcasting organisations, and online platforms. The group is chaired by Prof. Dr. Madeleine de Cock Buning from the University of Utrecht. The The Group is to advise the European Commission on fake news. The tasks of HLEG included, among others, defining the scope of the phenomenon, identifying the roles and responsibilities of relevant stakeholders, and formulating recommendations. The Group was set up in January 2018, whereas the report: A multi-dimensional approach to disinformation was published in March 2018. The full report is available at: https://publications.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1

- Transparency of advertisement placements;
- Identification of false accounts and bots;
- Transparency and verifiability of algorithms;
- Access to different news sources;
- Monitoring by academic researchers and public authorities.

In October 2018, the Code was signed by the largest online platforms. **The first evaluation is planned after one year. If EC decides that the impact of this regulation is unsatisfactory, it may propose further actions, including the regulatory ones.**

Commission Communication on Securing Free and Fair European Elections (Election Package)

In September 2018, the European Commission proposed measures to increase transparency of political advertisements, and to impose sanctions for unlawful use of personal data to deliberately influence the outcome of European elections.

Recommendations of the European Commission to secure free and fair European elections:

- **Establishing a national elections network** (engaging law enforcement authorities, cybersecurity authorities and data protection authorities) and **appointing a contact point** to take part in a European cooperation network for elections;
- **Enhancing transparency in online political advertisements** – European and national political parties should make information on advertising campaigns available online (expenditure, positioning criteria, entities behind them); otherwise, Member States should impose sanctions on the parties;
- Protection of networks and information systems against cyber threats;
- **Applying EU data protection rules** – in particular in view of the increasing impact of micro-targeting in electoral context based on personal data;
- **Strengthening the rules on funding of European political parties** – enabling penalties for breaching personal data protection if such breaches are to deliberately affect the outcome of European elections; the sanctions could amount to 5% of the annual budget of the relevant European political party or foundation;
- Establishing a cybersecurity competence network.

Action Plan against Disinformation

The Action Plan against Disinformation was announced on 5 December 2018. In the Plan, the European Commission specified the actions EU institutions and Member States must carry out before the 2019 European Parliament elections. The most important tasks presented in the Action Plan include the following:

- **Reinforcing the Strategic Communication Task Forces:** provision of additional specialised staff and necessary tools **(a budget increase for strategic communication from EUR 1.9 million in 2018 to EUR 5 million in 2019);**
- Establishing a **Rapid Alert System** for addressing disinformation campaigns by March 2019;
- Implementing the **Code of Practice on Disinformation;**
- Supporting **the creation of teams of multi-disciplinary independent fact-checkers and researchers;**
- Ensuring effective follow-up of the Elections Package, notably the Recommendation.

Digital Innovation Hubs – New Concept for Cross-Sectoral Collaboration

Digital Innovation Hub (DIH) is a concept developed by the European Commission in several stages. The first one involves Competence Centres that produce a specific technology used to support the digital transformation in Europe. The new concept, resulting from completed analyses, sees Digital Innovation Hubs in a new light. They will build an ecosystem of digital innovations by bringing together different environments and sectors. They will also help exchange knowledge, experience and technology. According to the Commission DIH will play the following roles:

- a one-stop-shop that provides support and advice to enterprises in respect of business processes, applications of digital technology in manufacturing, etc.;
- a competence centre that acts as an intermediary between enterprises and investors, and provides knowledge, expertise and technology to enterprises in the relevant state;
- a point of contact in the relevant state that strengthens innovation and creates a platform for collaboration between various stakeholders[62].

The figure below illustrates the DIH concept:

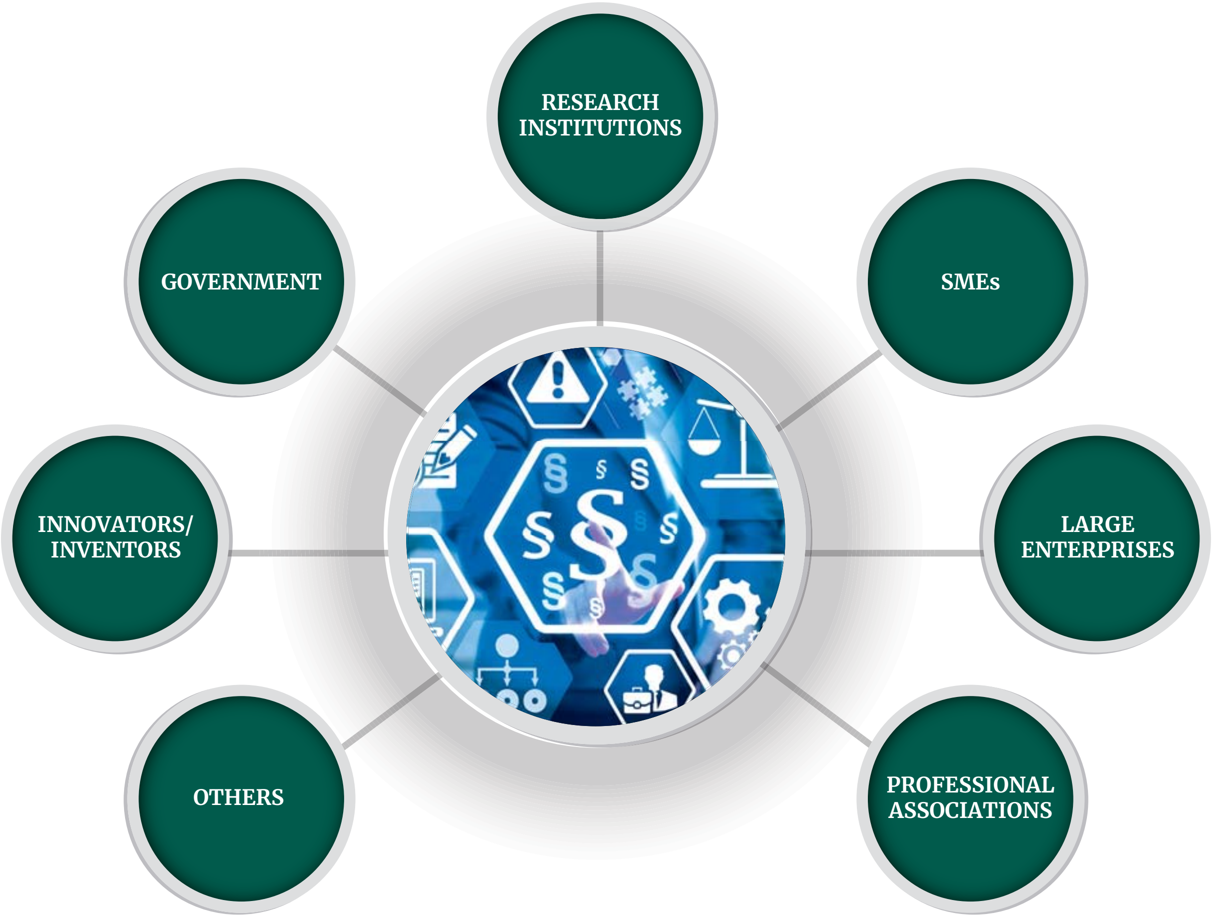
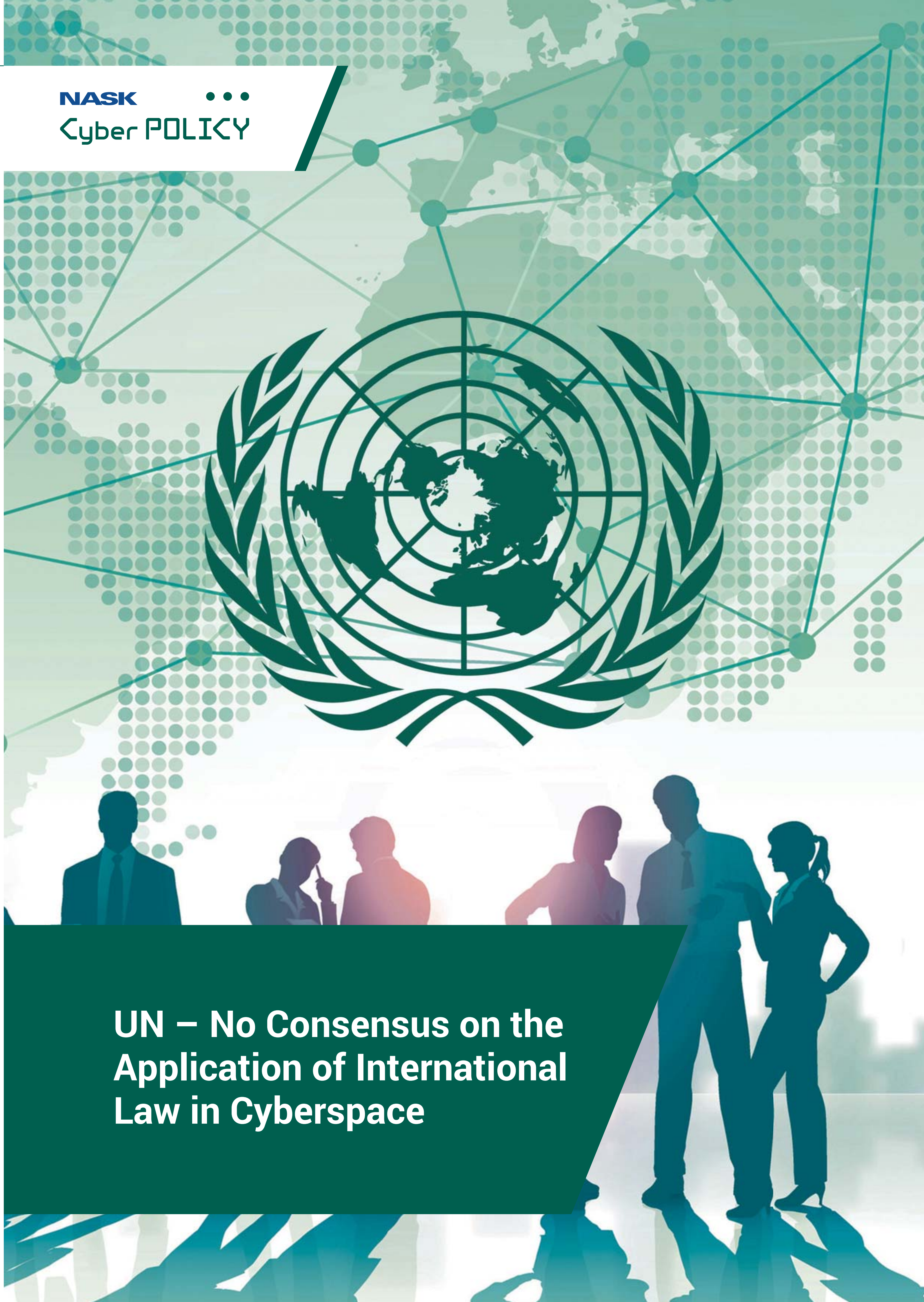


Fig. 4. Digital Innovation Hub concept

In 2017, EC conducted a pilot project to prepare staff for the development of DIH in Central and Eastern Europe. In 2018, the concept was still under discussion. It was agreed that Member States would be the ones to report DIHs to EC (until now, they could individually submit a relevant application by filling out the questionnaire on the EC website). The Commission also assumes that DIHs will become the main centres for the development of Artificial Intelligence in Europe.

[62] https://ec.europa.eu/digital-single-market/en/digital-innovation-hubs



UN – No Consensus on the Application of International Law in Cyberspace

The United Nations (UN) is the largest international organisation with 193 Member States. It was founded in 1945 to maintain international peace and security. The UN is central in global efforts to solve problems which challenge humanity in the 21st century: climate change, sustainable development, human rights, terrorism, humanitarian aid, health security, gender equality, food production, the rule of law, and many others[63]. The UN also provides a platform for dialogue, enabling governments to find areas for consensus and cooperation. The UN consists of the General Assembly, the Security Council, the Economic and Social Council, the Trusteeship Council, the International Court of Justice, and other organisations, committees and groups established within it.

The UN addressed cybersecurity for the first time in 1990 when the General Assembly adopted Resolution 45/121[64] during the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. The Resolution stressed the need to introduce computer-related crime into the legislation of states, and was the basis for the 1994 edition of the International review of criminal policy – United Nations Manual on the prevention and control of computer-related crime, which concerned the prevention and control of cybercrime[65]. Since 1998, cybersecurity has been a fixed item on the agenda of the UN General Assembly, and the subject of several resolutions issued not only by the General Assembly, but also by organisations operating within the UN, in particular the International Telecommunication Union (ITU).

Resolutions of the General Assembly and the Economic and Social Council of the United Nations:

- Resolution 55/63, January 2001 – ensuring that laws and practices in Member States eliminate safe havens for those who criminally misuse information technologies;
- Resolution 56/121, January 2002 – combating the criminal misuse of information technologies.
- Resolution 57/239, January 2003 – creation of a global culture of cybersecurity.
- Resolution 58/32, December 2003 – developments in the field of information and telecommunications in the context of international security.
- Resolution 58/199, January 2004 – creation of a global culture of cybersecurity and the protection of critical information infrastructures.
- Resolution 64/211, March 2010 – creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures.
- UN Economic and Social Council Resolution 2011/33, July 2011 – prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children.

Resolutions of the International Telecommunication Union:

- Resolution 181, Guadalajara 2010 – definitions and terminology relating to building confidence and security in the use of information and communication technologies.
- Resolution 58, Dubai 2012 – encouraging the creation of national computer incident response teams, particularly for developing countries.
- Resolution 45, Dubai 2014 – mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam.
- Resolution 130, Busan 2014 – strengthening the role of ITU in building confidence and security in the use of information and communication technologies.
- Resolution 174, Busan 2014 – ITU's role with regard to international public policy issues relating to the risk of illicit use of information and communication technologies.
- Resolution 179, Busan 2014 – ITU's role in child online protection.
- Resolution 50 Hammamet 2016 – cybersecurity.
- Resolution 52, Hammamet 2016 – countering and combating spam.
- Resolution 67, Buenos Aires 2017 – the role of the ITU Telecommunication Development Sector in child online protection.
- Resolution 69, Buenos Aires 2017 – facilitating creation of national computer incident response teams, particularly for developing countries[66].

UN GGE Group – To What Extent Does International Law Apply in Cyberspace?

The most important international treaties had been adopted even before the Internet was operational. Therefore, one of the biggest challenges for international relations is the application of the existing international law in cyberspace. In 2003, the General Assembly of the United Nations asked the Secretary-General to analyse potential threats to information security, and to publish possible measures of prevention and cooperation that would help minimise these threats. The **United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security** (**UN GGE**) was established at the time. Since then, there have been five GGEs[67].

- The first GGE was called in 2004, but, due to disagreements, no consensus was reached on the final report. Therefore, a brief procedural report was issued instead;
- The second GGE started its work in 2009. It came out with a report that encouraged the cooperation among States, the public and the private sectors with the aim to increase cybersecurity. The report also outlined recommendations on risk analysis, exchange of information and best practices, such as further dialogue between States to reduce cybersecurity risks and protect critical infrastructure; building mutual trust; and stabilisation and reduction of risks arising from the use of ICT by States, also in the context of international conflicts[68];
- The third GGE met three times in 2012-2013, and the report presented much more far-reaching conclusions than the previous documents. The experts stressed that **international law applies to cyberspace. The Charter of the United Nations, State sovereignty and international norms and principles that result from this sovereignty as well as other provisions of law apply to ICT-related activities of the States.** This concerns also the operation of information and communication infrastructure situated within the territory of a State[69]. This means, among others, that both the Member States and the entities supervised by them **are restricted from using proxies to commit internationally wrongful acts in cyberspace.** The States should also ensure that their territories are not unlawfully used by non-State actors in terms of ICT.

Key conclusions of the 2013 final report:

Recommendations on norms and principles of State conduct:

- the need to use norms of the applicable international law to cyberspace, including the Charter of the United Nations,
- adoption of an international code of conduct for information security,
- respect for human rights and fundamental freedoms specified in the international law when taking cybersecurity measures,
- intensification of work against criminal activity in cyberspace,
- restriction of use of proxies to commit wrongful acts in cyberspace,
- involvement of society and the private sector in efforts to increase the level of cybersecurity.

[63] The principles of the United Nations are enshrined in Article 1 of the Charter of the United Nations. The Charter of the United Nations is available in Polish on the website of the United Nations Information Centre in Warsaw at: http://www.unic.un.org.pl/dokumenty/karta_onz.php

[64] Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (A/45/756) http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/45/121

[65] UN. Centre for Social Development and Humanitarian Affairs; "International review of criminal policy". No. 43-44, 1994; https://digitallibrary.un.org/record/162804

[66] A summary of the UN cybersecurity documents has been published under the Digital Blue Helmets programme at https://unite.un.org/digitalbluehelmets/resources

[67] Each time, the composition of the group was different. The first group, established in 2004, consisted of 15 people; the second one in 2009 was also composed of 15 people. In 2014, the fourth GGE was expanded to 20 experts and coordinated by a Brazilian representative; in 2016, the number of experts increased even more, to 25; *United Nations Groups of Governmental Experts*, https://www.nti.org/learn/treaties-and-regimes/united-nations-groups-governmental-experts/#communications; *Developments in the field of information and telecommunications in the context of international security*, https://www.un.org/disarmament/topics/informationsecurity/

[68] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*; http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf

[69] The United Nations Charter is the founding document of the United Nations. The Charter was signed on 26 June 1945 in San Francisco by 50 Member States, including the Permanent Five: China, France, the United States, the United Kingdom and the USSR. The Charter articulated a commitment to universal respect for, and observance of, human rights and worth of human dignity. It also stressed the need to promote social progress and better standards of life in larger freedom. The countries that signed the Charter have committed themselves to abide by its provisions. (source: *Charter of the United Nations*; *United Nations portal*; http://www.un.org/en/charter-united-nations/index.html)

- **The fourth GGE operated in 2014-2015.** The published report was largely based on recommendations of previous groups, promoting open, safe and secure cyberspace. Above all, it emphasised the need to further build international safety and security, using state-of-the-art technologies and engaging the academia and the business sector in activities ensuring cybersecurity; and the need to include the academia communities in analyses related to the development of ICT. The General Assembly adopted the report in December 2015 and called on the Member States to abide by it[70].
- **The last UN GGE worked in 2016-2017.** A meeting of 25 experts coordinated by a German representative took place in June 2017. They failed to reach consensus. The dialogue disintegrated mainly between representatives of the United States and of Cuba. The United States expected GGE to develop clear and specific guidelines for the applicability of international law in state-of-the-art technologies, including international humanitarian law, the right to self-defence and the right to State responsibility and preventive measures. Currently, under the international law, States may lawfully use force in self-defence in response to a serious armed attack and in proportion to the damage suffered. This is also the case with international humanitarian law, which contains a distinction between civilians and military personnel. In the case of cyberattacks, it is extremely difficult to identify a single perpetrator, victims, civilians or military personnel. According to Cuban representatives (unofficially, Russia and China took a similar stance), the applicability of these rules in cyberspace could lead to its militarisation. This GGE failed to reach a common position. So far, the UN has not called for the continuation of the group[71].

Cybersecurity Activities of the International Telecommunication Union

The International Telecommunication Union (ITU) is a specialised organisation of the UN that focuses its activities on information and communication technologies. ITU is the only organisation of the UN for representatives of both the public and private sectors. It brings together 193 Member States, regulators, academic institutions and around 700 enterprises from all over the world[72].

Guide to Developing a National Cybersecurity Strategy

In 2018, ITU published its “Guide to developing a national cybersecurity strategy[73]”. The document supports States in the development of their cybersecurity strategies. The Guide describes the various phases of the development: from identification of needs, through analysis and implementation, to evaluation. Furthermore, the Guide presents good practices in management, risk assessment, critical infrastructure, and legal and educational solutions. The document was drafted with the support of representatives of international organisations, private sector, academic institutions, and in cooperation with NATO and the European Union Agency for Cybersecurity (ENISA[74]). The figure below presents the lifecycle of a National Cybersecurity Strategy.

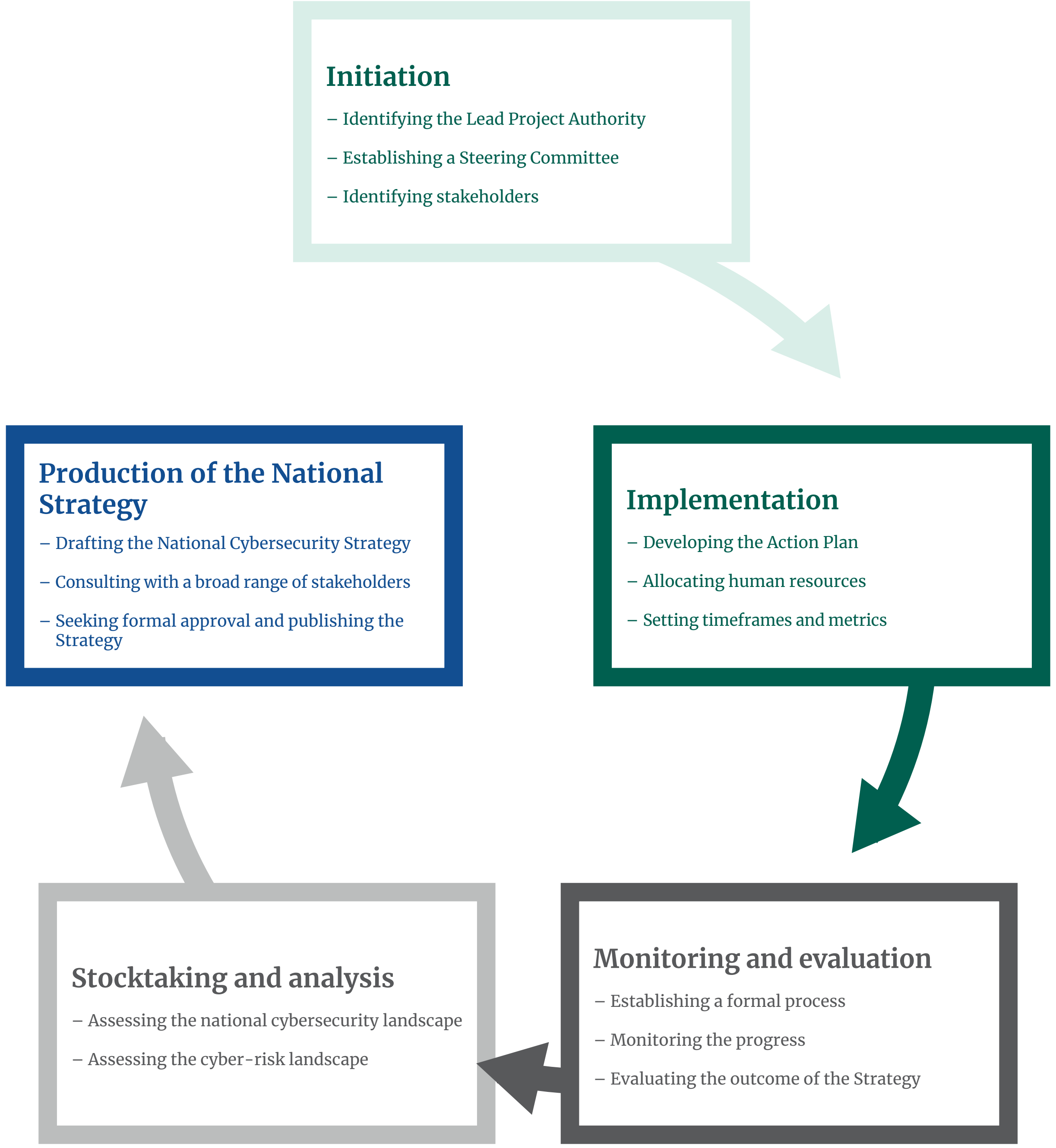

Initiation
– Identifying the Lead Project Authority
– Establishing a Steering Committee
– Identifying stakeholders
Implementation
– Developing the Action Plan
– Allocating human resources
– Setting timeframes and metrics
Monitoring and evaluation
– Establishing a formal process
– Monitoring the progress
– Evaluating the outcome of the Strategy
Stocktaking and analysis
– Assessing the national cybersecurity landscape
– Assessing the cyber-risk landscape
Production of the National Strategy
– Drafting the National Cybersecurity Strategy
– Consulting with a broad range of stakeholders
– Seeking formal approval and publishing the Strategy

Fig. 5. Lifecycle of a National Cybersecurity Strategy according to the Guide[75]

[70] James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey, “*Developments in the Field of Information and Telecommunications in the Context of International Security*”; https://www.nti.org/learn/treaties-and-regimes/united-nations-groups-governmental-experts/#communications)

[71] Korzak E., *UN GGE on Cybersecurity: The End of an Era*?, The Debate; https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/

[72] More information on the International Telecommunication Union is available at: https://www.itu.int

[73] “*Guide to developing a national cybersecurity strategy*”, International Telecommunication Union (ITU) 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

[74] In September 2018, ENISA also developed a tool enabling to evaluate Member States’ national cybersecurity strategies. The tool consists of simple questions that allow to implement a strategy step-by-step, and help set priorities for the future. It also supports the achievement of the NIS Directive goals. Together with the publication of the tool, ENISA has updated its interactive map of national strategies. Source: *ENISA launches the Cybersecurity Strategies Evaluation Tool*; https://www.enisa.europa.eu/news/enisa-news/enisa-launches-the-cybersecurity-strategies-evaluation-tool

[75] “Guide to developing a national cybersecurity strategy”, International Telecommunication Union (ITU) 2018, p. 17; https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Principles supporting the development of a National Cybersecurity Strategy:

1. Vision

The strategy should set a clear whole-of-government and whole-of-society vision. The clearer the vision, the easier it will be to coordinate and implement the Strategy amongst the relevant stakeholders. The objectives should be formulated at a sufficiently high level and consider the dynamic nature of the digital environment.

2. Comprehensive approach and tailored priorities

Cybersecurity is a complex multi-faceted issue, and it is important to understand all its aspects together with the relevant country's specific context. Based on an analysis, it is possible to define priorities in line with the objectives and implementation timeline of the Strategy, and allocation of the necessary resources. The priorities included in a National Cybersecurity Strategy will vary by country.

3. **Inclusiveness**

The Strategy should be developed with the active participation of all the relevant stakeholders, and it should address their needs. Cybersecurity has become critical to government, businesses and individuals. Engaging all the relevant stakeholders is essential to the development of a National Cybersecurity Strategy.

4. **Economic and Social Prosperity**

The Strategy should foster economic and social prosperity, maximise the contribution of ICT to sustainable development and social inclusiveness, and lead to building the trust and confidence necessary to protect the relevant country from cyber threats.

5. **Fundamental human rights**

The Strategy should respect and be consistent with fundamental values, including, but not limited to, the ones found in the United Nations' Universal Declaration of Human Rights[76], the International Covenant on Civil and Political Rights[77], as well as relevant multilateral or regional legal frameworks. Rights that people have offline must also be protected online.

6. **Risk management and resilience**

While the digital environment provides stakeholders with economic and social opportunities, it also exposes them to cybersecurity risk. It is impossible to entirely eliminate the cybersecurity risk, but it is possible to effectively manage it. The Strategy should encourage the adoption of measures to minimise the risk, and include recovery plans in the case of incidents.

7. **Appropriate set of policy instruments**

The Strategy should use the most appropriate policy instruments available. These include legislation, regulation, incentive programmes and mechanisms, education programmes, sharing best practices, etc. For each of the objectives, the most appropriate policy instrument should be selected, considering the country's specific circumstances.

8. **Clear leadership, roles, and resource allocation**

The Strategy should be set at the highest level of the government, which will then assign relevant roles and responsibilities and allocate sufficient human and financial resources. All parties involved should have a clear understanding of their respective roles and responsibilities. Moreover, the strategy should ensure accountability and allocation of relevant resources to each phase.

9. **Trust environment**

Building trust is essential to realise the full potential of the social, political and economic opportunities offered by the use of ICTs. The Strategy should ensure protection of users' interests and security of data, systems and services. The principle of trust should apply not only among the general population but also within those public and private organisations that will offer their ICT-related services to citizens[78].

Computer Incident Response Teams

ITU supports Member States in establishing National Computer Incident Response Teams (CIRTs[79]) that coordinate handling of cyberattacks. First, it assesses the readiness of the relevant State to implement the national CIRT. Next steps involve assistance in training, planning, implementing and operating the team. After establishing the CIRT, ITU offers support and possibilities for further development. Until now, 75 countries have been evaluated and 18 CIRTs have been established in, among others, Uganda, Zambia, Ghana, Kenya and Cyprus.

Global Cybersecurity Index (GCI)

The Global Cybersecurity Index is the ITU's initiative to raise awareness of cybersecurity. GCI measures the commitment of countries to cybersecurity, and their ability to maintain it at global, regional and international levels. ITU experts conduct evaluation together with partners from the private, public and academic sectors. The aim is to identify current problems and gaps as well as areas for improvement[80]. It is also to motivate the countries to boost their score. The ranking includes various levels of cybersecurity development, as reflected by the overall level of ICT services. The concept is based on the assumption that the more advanced the cybersecurity solutions, the higher the level of ICT services.

The initiative started in 2013. After publishing the 2014 report and collecting feedback, the second edition was planned. This time, it received support from more partners (e.g. World Bank, FIRST, INTERPPOL, UNICRI, UNODC, etc.) and used a new data analysis model. It included 25 indicators measured by 157 questions, evaluating the level of the relevant country's commitment in respect of 5 cybersecurity pillars: legal, technical, organisational, capacity building, and cooperation.

The main objectives of GCI are to measure:

- the type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- progress in cybersecurity commitment of all countries from a global perspective;
- progress in cybersecurity commitment from a regional perspective;
- the cybersecurity commitment divide (i.e. the difference between countries in terms of their level of engagement in cybersecurity initiatives).

Therefore, countries have been split into three groups according to their level of cybersecurity commitment. The heat map shows the results, illustrating the level of commitment from high (green) to low (red).

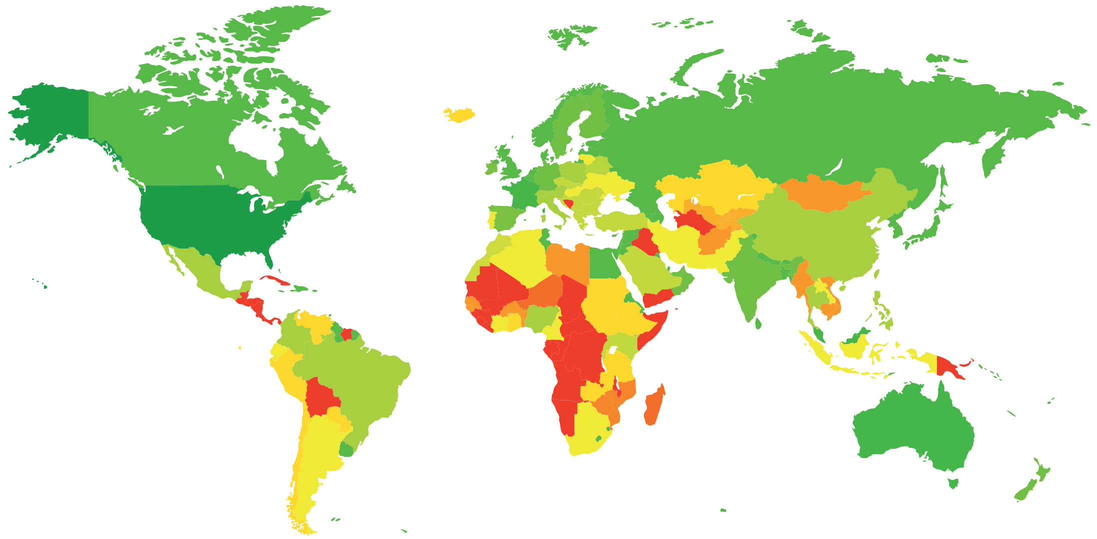


Fig. 6. GCI Heat Map (December 2018)[81]

The analysis of individual countries based on GCI took place for the third time in 2018[82]. The report and the latest ranking will be published in 2019.

[76] The third General Assembly of the United Nations adopted the Universal Declaration of Human Rights in 1948. The declaration includes a set of human rights and rules of their application. The document is one of the UN's greatest achievements. Source: Universal Declaration of Human Rights; http://www.unesco.pl/fileadmin/user_upload/pdf/Powszechna_Deklaracja_Praw_Czlowieka.pdf

[77] The United Nations adopted the International Covenant on Civil and Political Rights in 1966. Unlike the Universal Declaration of Human Rights, the Covenant is legally binding. It contains a list of fundamental human rights and freedoms, and States' obligations towards their citizens. The Covenant establishes the Human Rights Committee, which ensures compliance with provisions of the document. The same year, the UN also adopted the International Covenant on Economic, Social and Cultural Rights. Source: *International Covenant on Civil and Political Rights* (ICCPR); Information Platform humanrights.ch; https://www.humanrights.ch/en/standards/un-treaties/iccpr/

[78] "*Guide to developing a national cybersecurity strategy*", International Telecommunication Union (ITU) 2018, pp. 30-34; https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

[79] The name varies depending on the institution: *National Computer Incident Response Team* (CIRT), *Computer Emergency Response Team* (CERT) or *Computer Security Incident Response Team* (CSIRT).

[80] *Global Cybersecurity Index* (GCI) 2017; ITU, p. 13; https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

[81] *Source: Global Cybersecurity Index (GCI) 2017; Fig. 4.1.1: GCI Heat Map; ITU, p. 25, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf*

[82] *Global Cybersecurity Index*; https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, Global Cybersecurity Index (GCI) 2017; ITU, pp. 15-16; https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

United Nations Office on Drugs and Crime (UNODC)

> The United Nations Office on Drugs and Crime (UNODC) was established in 1997. The UNODC work programme includes cooperation projects to help Member States to counteract international crime; research and analytical work, as well as normative work. UNODC assists States in implementing international treaties into domestic legislation on crime.
>
> UNODC also addresses cybercrime, which may be of an international nature or which may affect victims in different parts of the world. The Office supports national structures to promote cooperation between Member States and to build capacity in the fight against cybercrime. Specifically, UNODC draws upon its specialised expertise on criminal justice systems, and on its capacity in respect of education, data collection, research and analysis on cybercrime[83].

UNODC undertakes the following initiatives to support States in the fight against cybercrime:

- **Global Programme on Cybercrime** – it helps prevent and combat cybercrime by increasing the efficiency and effectiveness in its prosecution, coordinating national authorities, creating legal frameworks, strengthening international cooperation, and raising public knowledge of cybercrime risks.
- **Open-ended Intergovernmental Expert Group Meeting on Cybercrime** – extensively investigates cybercrime; collects data on national legislation, good practices and required technical assistance; and identifies areas for strengthening local and international activities.
- **Repository Cybercrime** – it is a central database of legislation and lessons learned on cybercrime[84].

Internet Governance Forum (IGF)

The Internet Governance Forum (IGF) was established in 2006. It enables open dialogue and exchange of information and experience for everyone interested in shaping the future of the Internet[85]. All WSIS (World Summit on Information Society) members participate in annual IGF meetings. Organisations and experts from different backgrounds are also invited to cooperate with IGF. Cybersecurity is an important part of discussions in the forum. **The most recent meeting took place in November 2018 in Paris.**

> Until 1998, the Advanced Research Projects Agency at the United States Department of Defense oversaw the Internet. However, it was clear that the Internet should become independent from the US government agency. This was the reason behind the formation of the Internet Corporation for Assigned Names and Numbers (ICANN). The Corporation is responsible for assigning and administering IP addresses, and managing domains and DNS servers. According to the *Memorandum of Understanding,* which founded ICANN, the Corporation is a not-for-profit, public-benefit organisation operating under the California law.
>
> Initially, ICANN was established as a step towards the privatisation of Internet governance. However, the US government's influence has never fully ceased. Representatives of individual States first expressed their opposition to American domination of the Internet at the World Summit on the Information Society held in Geneva in 2003 and, afterwards, in Tunis in 2005. They demanded the creation of a body that would oversee the Internet on behalf of the United Nations. In the spirit of compromise, the Internet Governance Forum was formed. However, it received a subsidiary role and was deprived of decision-making powers. Ultimately, ICANN has remained a not-for-profit organisation that operates in the United States and is governed by the US law[86]. It continues to be an institution that oversees global DNS servers and domains, delegating some of its responsibilities to national registrars.

> The Internet Assigned Numbers Authority (IANA) is part of ICANN. It coordinates some of the key elements that keep the Internet running smoothly, manages the Domain Name System, oversees IP address allocation, and maintains Internet protocol numbering systems. IANA does not engage in politics, but merely implements solutions overseen by ICANN[87].
>
> The Board of Directors is ICANN's most important decision-making body. It is elected annually by all Internet users in a voluntary vote. According to its principles, any user may become involved in ICANN's activities and express his or her opinion[88].

At the Forum, French President Emmanuel Macron called for a joint commitment to security in cyberspace. The declaration, dubbed the ***Paris Call for Trust and Security in Cyberspace,*** has been signed by 64 states, 328 private sector companies and 129 NGOs. The commitments of the Call are, among others, as follows:

- increase prevention against and resilience to malicious online activity;
- protect the integrity of the Internet;
- cooperate to prevent interference in electoral processes;
- work together to prevent the proliferation of malicious online programmes and techniques;
- improve the security of digital products and services as well as everybody's "cyber hygiene";
- work together to strengthen the relevant international standards, clamp down on online mercenary activities and offensive action by non-state actors[89].

High-level Panel on Digital Cooperation

On 12 July 2018, United Nations Secretary-General established the High-level Panel on Digital Cooperation. Its task is to make proposals on how to strengthen cooperation among Governments, the private sector, civil society, international organisations, academia and the technical community. Among other things, it should raise awareness about the transformative impact of digital technologies across the economy, and contribute to the broader public debate on ethical issues and changes in the digital future for all.

The Panel consists of 20 independent experts from different backgrounds, serving in their personal capacity. **The Panel met in person for the first time in September 2018.** The outcome of its work will be a report containing actionable recommendations, mapped trends in digital technologies, identified gaps, and opportunities for strengthening international cooperation. The experts are expected to work for 9 months, which means that the report should be published in the first half of 2019[90].

Cyber Policy Portal

In December 2018, UNIDIR[91] (United Nations Institute for Disarmament Research) launched a new online portal that maps the cybersecurity and cybersecurity-related policy landscape. It provides a rigorous, accessible and up-to-date overview of the cyber capacity of all 193 UN Member States, intergovernmental and regional organisations. It also draws from voluntarily provided and open-source material. Address of the portal: https://cyberpolicyportal.org/en/

[83] *Cybercrime*, http://www.unodc.org/unodc/en/cybercrime/index.html

[84] The repository is available at: https://sherloc.unodc.org/cld/v3/cybrepo/

[85] *The Internet Governance Forum* (IGF), Background paper, http://www.intgovforum.org/cms/2015/IGF.24.06.2015.pdf

[86] Morawski Ł., *Unia Europejska wobec procesu zarządzania Internetem* (European Union vs. the Process of Internet Governance), Institute of Political Studies of the Polish Academy of Sciences, pp. 114-120

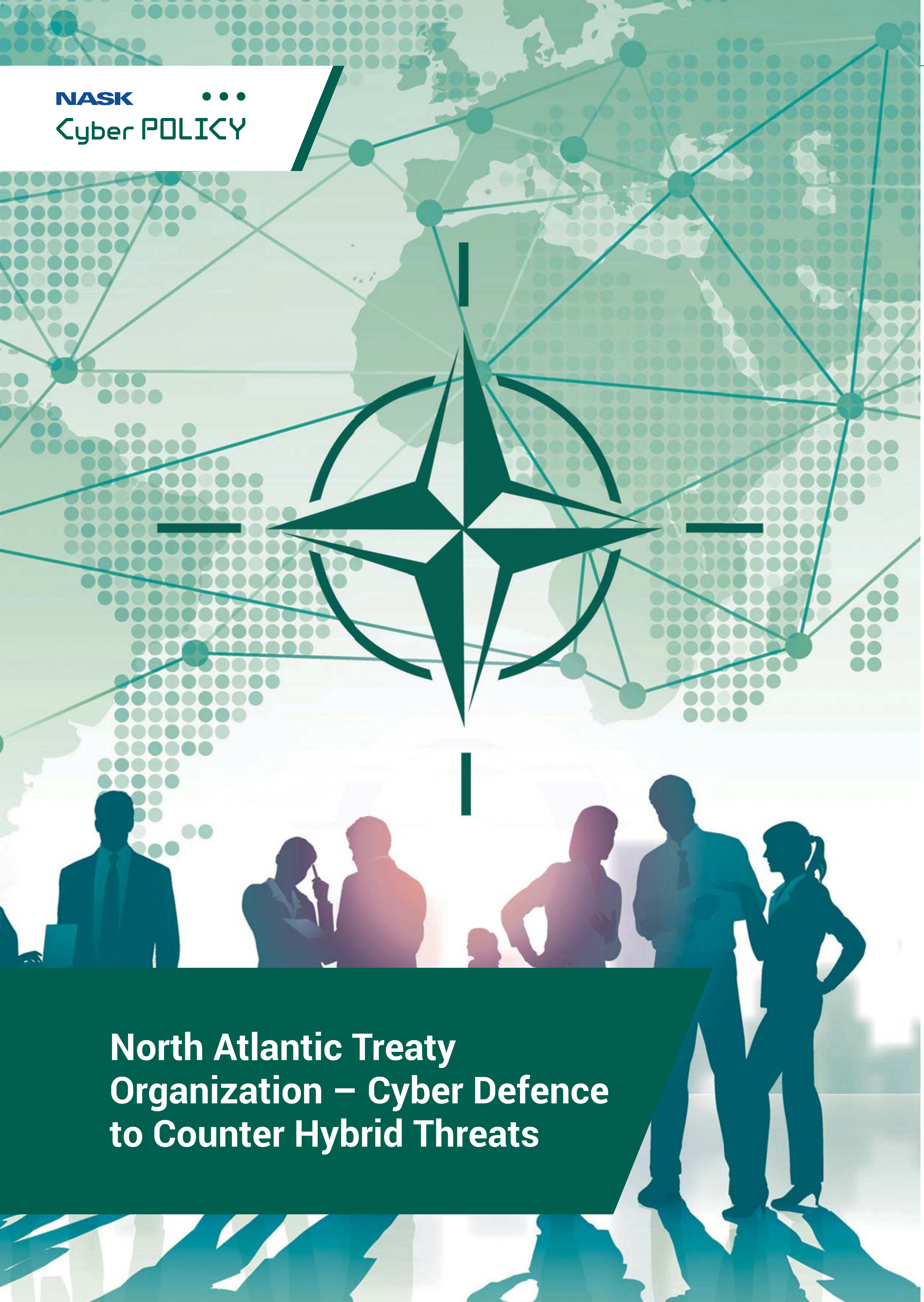
[87] IANA About us; https://www.iana.org/about

[88] Beginner's Guide to participating in ICANN; p. 2, https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf

[89] *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace. France Diplomatie*; https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

[90] *Secretary-General's High-level Panel on Digital Cooperation*; http://www.un.org/en/digital-cooperation-panel/

[91] Operating since 1980, the United Nations Institute for Disarmament Research (UNIDIR) is an autonomous institution within the United Nations that conducts independent research on disarmament and related problems, particularly international security issues; http://www.unidir.org/about/the-institute



North Atlantic Treaty Organization – Cyber Defence to Counter Hybrid Threats

The North Atlantic Treaty Organization (NATO) is a military alliance between 29 states. It was established in 1949 when representatives of 12 countries signed the North Atlantic Treaty in Washington. Poland joined NATO on 12 March 1999.

Initially, NATO was established to defend the West against the USSR. After the collapse of the Soviet Union, NATO's goal has become to preserve peace and stability. With the development of new technologies, cybersecurity is becoming an increasingly significant topic within the NATO forum. During the 2016 Warsaw Summit, NATO recognised cyberspace as the fourth operational domain. Today, NATO puts extensive efforts into securing its systems and networks, and into helping its allies to build effective cyber defence capacity.

NATO bodies responsible for cybersecurity[96]

The **North Atlantic Council**[97] (NAC) provides high-level political oversight on all aspects of implementation of NATO's cyber defence policy. The Council receives information on the most substantial incidents and cyberattacks, and plays a central role in the cyber defence crisis management.

The **NATO Cyber Defence Committee**[98] (NCDC), subordinate to the Council, plays a leading role in NATO's cyber defence policy. The Committee also provides advice to allied countries at the expert level.

At the working level, the **NATO Cyber Defence Management Board**[99] (CDMB) coordinates cyber defence throughout NATO civilian and military bodies.

The **NATO Consultation, Control and Command Board** (C3B) also plays an important role in the field of cybersecurity. It is responsible for consultation on technical aspects and implementation of cyber defence.

Evolution in NATO's approach to cyber defence

2002 – for the first time, Allied leaders acknowledged cyber defence at the Prague Summit.

2007 – a mass cyberattack hit Estonian state institutions, banks and media.

2008 – NATO approved the **first NATO Policy on Cyber Defence**[92]**,** adopted at the Bucharest Summit[93].

2008 – the conflict between Russia and Georgia illustrated how cyberspace activities might pose a threat no less than conventional warfare.

2010 – NATO adopted a new Strategic Concept at the Lisbon Summit. It gave the North Atlantic Council the task of developing a NATO in-depth cyber defence policy and preparing an action plan for its implementation[94].

2011 – NATO Defence Ministers approved the second NATO **Policy on Cyber Defence**[95].

2012 – NATO introduced cyber defence **into its Defence Planning Process**.

2014 – **NCIRC reached its full operational capability**, ensuring better protection to NATO's networks.

2014 – NATO launched its Industry Cyber Partnership, the first initiative to boost cooperation with the private sector.

2014 – at the Wales Summit, Allies supported the new cyber defence policy and approved an action plan. They recognised that **international law applied to cyberspace**, and that cyber defence was part of NATO's core task of collective defence.

2016 – at the Warsaw Summit, **States recognised cyberspace as a domain of operations**, in which NATO must defend itself as effectively as it did in the air, on land, and at sea. The summit also adopted the ***Cyber Defence Pledge***.

[92] Bucharest Summit Declaration; https://www.nato.int/cps/en/natolive/official_texts_8443.htm

[93] NATO's Cyber History (2008-2012); http://www.natolibguides.info/cybersecurity#s-lg-box-14363350

[94] Lisbon Summit Declaration; https://www.nato.int/cps/en/natolive/official_texts_68828.htm#cyber

[95] NATO Cyber Defence – Evolution; https://www.nato.int/cps/en/natohq/topics_78170.htm#

[96] NATO Cyber Defence – Governance; https://www.nato.int/cps/en/natohq/topics_78170.htm#

[97] The North Atlantic Council (NAC), NATO's principal political decision-making body, is the only body in NATO that operates and derives its authority explicitly from the Treaty. It is a primary consultation platform for Member States. The Council consists of representatives of all NATO Member States and the chairperson is the Secretary General. Numerous councils and committees support its work.

[98] In April 2014, NAC agreed to rename the Defence Policy and Planning Committee/Cyber Defence as the Cyber Defence Committee. It is a senior advisory body to the North Atlantic Council on cyber defence issues. It also ensures consultation with Allied countries, and manages NATO's internal cyber defence.

[99] The NATO Cyber Defence Management Board (CDMB) operates within the Emerging Security Challenges Division at NATO's Headquarters. It consists of representatives of all NATO's key cybersecurity stakeholders, such as the Allied Operational Command (ACO), the Allied Command Transformation (ACT) and NATO agencies. It is responsible for strategic planning and directions of development in NATO's network. It also supports Member States in their work to strengthen national cybersecurity systems.

Brussels Summit and Formation of the Cyberspace Operations Centre

The most important event of 2018 was **NATO's Brussels Summit in July**[100]. The final declaration stressed that cyber threats to NATO's security were becoming more frequent, complex and destructive. Therefore, NATO must be able to operate as effectively in cyberspace as it did in the air, on land, and at sea.

The most significant conclusions of the declaration:

Allies have agreed to **set up a new Cyberspace Operations Centre** as part of NATO's strengthened Command Structure (item 29). The new centre, responsible for cyber operations, should reach its full operational capability in 2023[101]. The Centre, situated at the Supreme Headquarters Allied Powers Europe (SHAPE) in Mons (Belgium), will host a 70-strong team of experts fed with military intelligence and real-time information on cyberattacks. This is a step towards creating the possibility of cyberspace operations. The Centre will ensure that the Supreme Allied Commander Europe is equipped with all the necessary tools to take actions in cyberspace.

NATO must **defend itself from hybrid challenges**, including cyberattacks or disinformation campaigns (item 2), which may also attempt at interfering with democratic processes, e.g. elections (item 6). Reaffirming its defensive mandate, NATO has also declared it will employ the full range of capabilities to deter, defend against, and counter cyber threats (item 20).

NATO is determined to deliver strong national cyber defences through full **implementation of the *Cyber Defence Pledge***. The implementation of the pledge is of key importance for enhanced cyber resilience of the Member States and for the costs of a cyber attack.

NATO has agreed how to integrate sovereign cyber effects into Alliance **operations and missions**. Allies would provide the solutions voluntarily under strong political oversight (item 20).

Individual Allies may consider **attributing malicious cyber activity** and responding in a coordinated manner (item 20).

The **dialogue between NATO and EU** remains essential to advance cooperation in respect of cybersecurity (item 70). The President of the European Council, the President of the European Commission and the Secretary-General of NATO signed the joint declaration on this matter the day before the Brussels Summit.

Implementation of the Cyber Defence Pledge

Cyber Defence was adopted at the Warsaw Summit in 2016. It results from the Alliance's efforts to build resilience to cyberattacks at the national level. Allies have pledged to increase their level of cybersecurity. The most important provisions of the Pledge include, among others:

- Strengthening cybersecurity of national networks and the infrastructure;
- Keeping pace with fast-growing cyber threats to enable NATO States to defend themselves effectively in cyberspace;
- Applying international law in cyberspace and cooperating with EU;
- Maintaining international cooperation through education, training and exchange of information.

The implementation of the Cyber Defence Pledge was first summarized during the conference in Paris on 15 May 2018. NATO Secretary General Jens Stoltenberg admitted that **almost every Ally upgraded their cyber defences**. The Allies managed to do it in less than two years after accepting the commitment. The United Kingdom is in the lead. It invested 1.9 billion GBP through the National Cybersecurity Strategy[102]. France follows suit, having invested 1.6 billion EUR[103].

The NATO Brussels Summit in July 2018 also evaluated the implementation of the Cyber Defence Pledge. Individual countries reported on the progress they had made.

<?> Brussels Summit Declaration; https://www.nato.int/cps/en/natohq/official_texts_156624.htm

<?> NATO Cyber Defence – Factsheet; https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf

<?> Why cyber space matters as much to NATO as land, sea and air defence; https://www.ft.com/content/9c3ae876-6d90-11e8-8863-a9bb262c5f53

<?> Cyber Defence Pledge Conference; https://www.nato.int/cps/en/natohq/opinions_154462.htm

Developing NATO's Cyber Defences

The **NATO Computer Incident Response Capability** (NCIRC) based in SHAPE, Mons, protects NATO's own networks by supporting cyber defence 24/7. Its team of 200 experts[104] plays a key role in responding to any cybersecurity incidents affecting NATO. It handles and identifies incidents, providing NATO and Allies with up-to-date analysis of the faced cyber challenges.

NCIRC operates as part of the **NATO Communications and Information Agency,** which also carries out other cyber defence initiatives. These include e.g. the NATO Industry Cyber Partnership, or rapid-reaction cyber defence teams.

- NATO helps Allies to boost their cyber defences by:
- Sharing real-time information about threats, as well as best practices on handling cyber threats;
- Maintaining rapid-reaction cyber defence teams that can be sent to help Allies in handling cyber challenges;
- Developing targets for Allies to facilitate a common approach to their cyber defence capabilities;
- Investing in education, training and exercises, such as Cyber Coalition.

Joint Declaration on EU-NATO Cooperation

The declaration of 10 July 2018 reaffirmed the commitment to advance the cooperation initiated in 2016 in Warsaw[105]. The seven key areas identified as requiring enhancement included e.g. countering hybrid threats (such as cyberattacks and disinformation) and cyber security and defence[106].

NATO and EU cooperate on several levels. In 2016, the two organisations signed a Technical Arrangement on Cyber Defence[107] that enabled NATO's (NCIRC) and EU's (CERT-EU) emergency response teams to exchange information and share best practices. NATO Secretary General demonstrated the actions taken in response to WannaCry and NotPetya attacks in 2017[108] as an example of good cooperation. Representations of both organisations also take part in joint exercises, e.g. Cyber Coalition or Locked Shields.

Exercises – Increasing Cooperation Among Allied States

NATO carries out many exercises, trying to prepare for potential contemporary challenges. The exercises are intended not only to help NATO test its strategies and mechanisms, but also to strengthen the cooperation between the Allied states.

- **Locked Shields** is an annual exercise organised by the NATO Cooperative Cyber Defence Centre of Excellence (**CCDCOE**) in Estonia. More than 1,000 experts from 30 countries participated in the event on 27 April 2018. 22 teams trained to preserve complex IT systems and handled large-scale cyberattacks. Locked Shields involved over 2,500 attacks. The winner was the team from NATO, followed by France and the Czech Republic[109].
- **Cyber Coalition**, NATO's cyber defence exercise, took place in Estonia between 26 and 30 November 2018[110]. In its eleventh year, it involved around 700 participants from 28 Allies and 4 partners, as well as from the private sector and academia. The aim of the exercise was to enhance coordination and collaboration between NATO and Allies, strengthen the ability to protect Alliance cyberspace, and conduct military operations in the cyber domain.

Important events

- **International Conference on Cyber Conflict (CyCon) 2018**

  CCDCOE[111] organised and held the 10th annual International Conference on Cyber Conflict **(CyCon) 2018** on 5 June 2018 in Tallinn. The event was attended by about 700 experts from over 40 countries. The Conference's core topic was maximising effects in cyberspace. Discussions and presentations were an opportunity to present original research papers and observations of renowned experts. Conference materials are published as IEEE *(Institute of Electrical and Electronics Engineers*) publications, and are an important contribution to the international technical literature.

[104] NATO Cyber Defence, Factsheet, December 2018; https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf

[105] EU-NATO Cooperation – Factsheet; https://cdn5-eeas.fpfis.tech.ec.europa.eu/cdn/farfuture/otambGc7_PZ7cDdMdQqQki4M3aTBIo6-efph8-K1vFI/mtime:1542899750/sites/eeas/files/eu-nato_cooperation_factsheet.pdf

[106] Joint Declaration on EU-NATO Cooperation; 2018 https://www.nato.int/cps/en/natohq/official_texts_156626.htm

[107] NATO and the European Union enhance cyber defence cooperation; https://www.nato.int/cps/en/natohq/news_127836.htm

[108] Cyber Defence Pledge Conference; https://www.nato.int/cps/en/natohq/opinions_154462.htm

[109] NATO Won Cyber Defence Exercise Locked Shields 2018; https://ccdcoe.org/nato-won-cyber-defence-exercise-locked-shields-2018.html

[110] Cyber Coalition helps prepare NATO for today's threats; https://www.nato.int/cps/en/natohq/news_160898.htm

[111] The 10th CyCon Hosts 700 Cyber Experts in Tallinn; https://ccdcoe.org/cycon/content/10th-cycon-hosts-700-cyber-experts-tallinn.html

- NIAS 2018 – Cyber Security Symposium

NIAS is the largest NATO cyber security conference. The 2018 event took place between 16 and 18 October 2018 in Belgium (NIAS18: *Securing NATO's Digital Endeavour*[112]). The Symposium stressed the importance of ensuring cybersecurity in every conventional operation of the Alliance. The exchange of critically important information in a secure manner is essential for military commanders and state leaders if they are to make the right decisions at the right time. The 2018 conference gathered more than 1,800 leaders and renowned cybersecurity specialists.

Disinformation – Activities of NATO StratCom COE

NATO is aware of the dangers posed to the Alliance by hybrid threats, such as cyberattacks or disinformation campaigns. The fact that NATO treats such actions very seriously was demonstrated e.g. by the declaration of the most recent NATO Brussels Summit in 2018[113]. As stated in the 2014 Wales Summit Declaration, Allies welcomed the establishment of the **NATO Strategic Communications Centre of Excellence** (NATO StratCom COE). It is a multi-nationally constituted and NATO-accredited international military organisation that is not part of the NATO Command Structure. Poland is one of its co-founders. Since its establishment, the Centre has been one of the leaders in building competences in strategic communication (including the fight against disinformation). Today, it has eleven member states, with three more that are finalising their accession procedure[114].

Other 2018 publications:

- ***Russia's Footprint in the Nordic-Baltic Information Environment***[115]

  It focuses on Russia's disinformation strategy in the Nordic-Baltic states. The analysis describes Russia's methods and objectives in the following four dimensions:

  1. **Political dimension**: maintaining the status of the great power, challenging Western values and subverting the unity of the Western states.
  2. **Information dimension**: developing its own global media system that promotes its worldview and its own perspective.
  3. **Military dimension**: countering NATO's expansion towards its borders.
  4. **Economic dimension**: the Arctic seen as a priority economic region for Russia.

- **Robotrolling**

  Robotrolling is a quarterly report that analyses social media manipulations related to NATO's presence in the Baltics. Its authors focus on disinformation actions taken by automated accounts (bots) and false accounts (trolls). Analyses have shown that bots created 46% of all Russian-language messages about NATO in the Baltic States and Poland[116] during the 4th quarter of 2018.

- **Executive summary. Fake News: A Roadmap**[117]

  It describes what fake news is and why the current information environment makes rapid spread of disinformation campaigns easier. Its authors demonstrate the actions to counteract this phenomenon.

- **Facebook game teaches how to spot disinformation**

  The game is designed to help Facebook users spot fake news[118]. Players run their own publishing business, earn virtual currency and gain readers by publishing reliable news. They are supported by a fact-finding screen that encourages players to verify sources and tells them how to distinguish true and false information.

[112] NIAS 18; http://nias2018.com

[113] Brussels Summit Declaration, items 2 and 21; https://www.nato.int/cps/en/natohq/official_texts_156624.htm

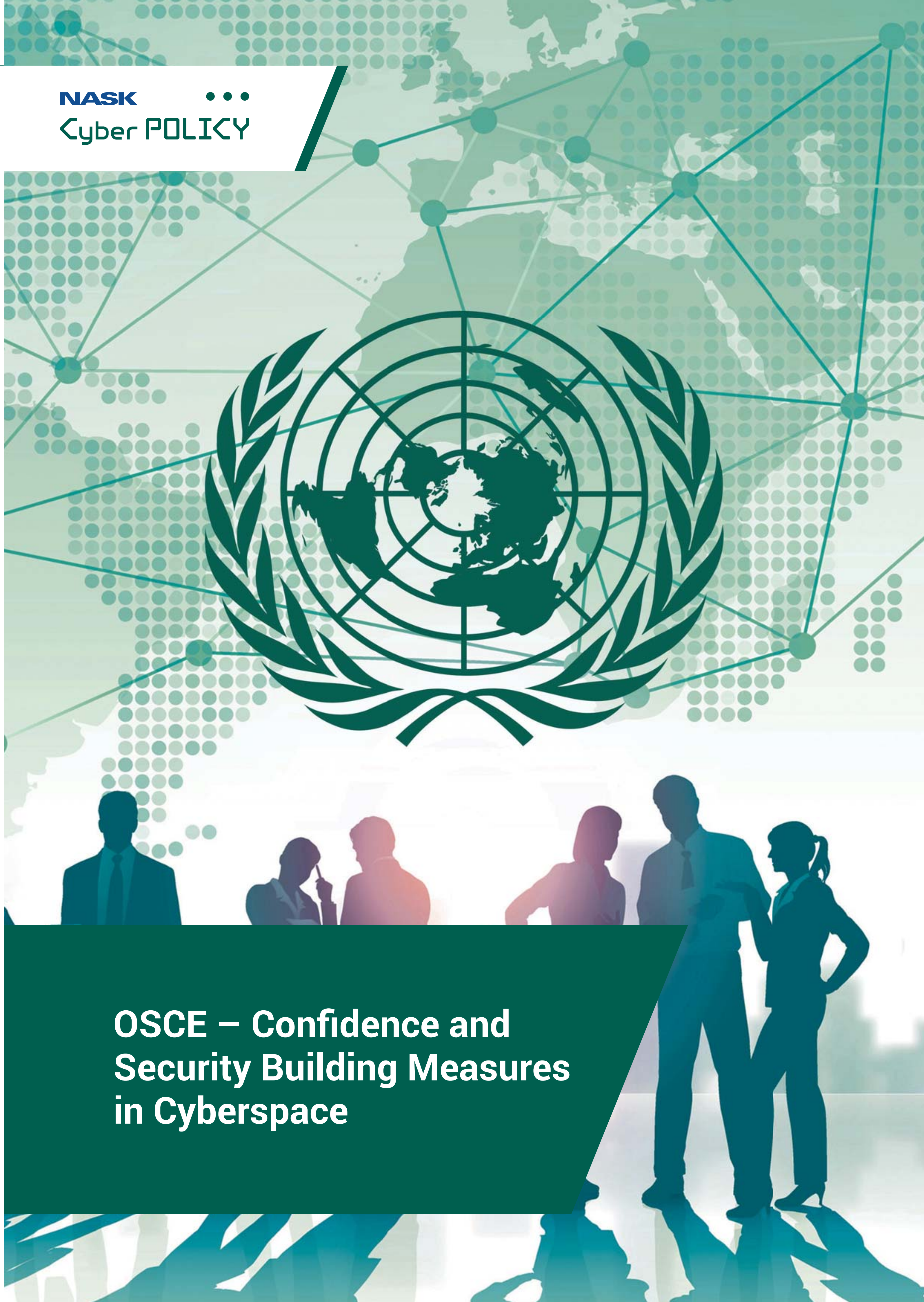
[114] NATO StratCom COE; https://www.stratcomcoe.org/about-us

[115] Russia's Footprint in the Nordic-Baltic Information Environment; https://www.stratcomcoe.org/russias-footprint-nordic-baltic-information-environment

[116] Robotrolling 2018/4; https://www.stratcomcoe.org/robotrolling-20184

[117] Executive summary. Fake News: A Roadmap; https://www.stratcomcoe.org/executive-summary-fake-news-roadmap

[118] Facebook game teaches how to spot disinformation; https://www.stratcomcoe.org/facebook-game-teaches-how-spot-disinformation



OSCE – Confidence and Security Building Measures in Cyberspace

The purpose of the **Organization for Security and Cooperation in Europe** (OSCE) is the prevention of conflicts in Europe. It was founded in 1995 and currently has 57 participating States (not only from Europe[119]). It addresses various concerns, including arms control, confidence- and security-building measures, human rights, national minorities, democratisation, counter-terrorism and environmental activities.

OSCE plays a significant role in raising the level of cybersecurity in the world by reducing the risk of conflicts among states. Cyberspace is now an additional dimension in complex inter-state relations. As a result, OSCE participating States have stepped up their efforts in confidence-building measures, in particular in respect of new technologies. This includes consultations on potential cybersecurity incidents, building platforms to exchange views and national cybersecurity policies, and cooperating in order to reduce vulnerabilities, e.g. in the area of critical information infrastructures.

OSCE – Confidence-Building Measures

OSCE has elaborated a set of 16 measures (confidence-building measures, CBMs) to build interstate confidence among participating states. The concept assumes that the best way to prevent conflicts is to create a direct communication system that clarifies misunderstandings and identifies potential disputes.

2013 CBM set of measures:

1. Participating States will voluntarily provide their national views on various aspects of cyber threats.
2. Participating States will facilitate cooperation among national cybersecurity bodies and exchange of information on cybersecurity.
3. Participating States will actively reduce the risks of possible emergence of political or military conflict that may stem from misunderstandings and the use of ICTs.
4. Participating States will share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet.
5. Participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building in the field of cybersecurity.
6. OSCE encourages participating States to have in place modern and effective national legislation to facilitate bilateral cooperation and information exchange between their respective governments and cybersecurity authorities.
7. Participating States will voluntarily share information on their national strategies and policies relevant to the security of ICTs.
8. Participating States will nominate a contact point to facilitate communications and dialogue among them.
9. In order to reduce the risk of misunderstandings, participating States will, as a first step, establish a list of common terminology related to security and use of ICTs.
10. Participating States will voluntarily exchange views and information using OSCE platforms.
11. Designated national experts from the participating States will meet at least three times each year, to discuss the current cybersecurity status and explore development of CBMs in the future.

The list was extended in 2016 by the following CBMs:

12. Participating States will voluntarily share information in different formats, including seminars, fora, and roundtables. They will exchange knowledge on processes and mechanisms to reduce the risk of conflict stemming from the use of ICTs. Participating States are encouraged to continue stable, transparent and predictable cooperation, as well as to complement international (e.g. UN) efforts. They should also take into account the needs and requirements of all stakeholders along with inviting representatives of the private sector, academia, centres of excellence and civil society to take part in such activities.
13. Participating States will voluntarily conduct information activities to support the access to authorised communication channels. The aim is to reduce the risks of misperception, escalation, and conflict; and to clarify technical and legal mechanisms to address ICT-related requests.
14. Participating States will promote public-private partnerships and develop mechanisms to exchange best practices of cybersecurity and the use of ICTs.
15. Participating States will voluntarily facilitate and/or participate in collaboration between authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to cybersecurity.
16. Participating States will encourage reporting of vulnerabilities affecting the security and share associated information on available remedies. Participating States agree that such information exchange, when occurring between States, should use appropriately authorised and protected communication channels and contact points[120].

CBMs were one of the topics discussed at the Rome conference in September 2018. 170 representatives of 57 OSCE participating States, partners, NGOs, academia and the private sector attended the conference. **The main discussion focused on mitigating the risks of conflict with the use of ICTs by applying the developed CBMs.** Attendees also had the opportunity to present topics related to local cybersecurity threats. They concentrated on **strengthening states' capacity to prevent incidents**. An important suggestion was to encourage **public-private partnerships.** As a result, countries could benefit from effective solutions of the private sector, raise cybersecurity awareness, and delegate tasks to cybersecurity companies[121].

Combating Cybercrime – Capacity-Building Project for South-Eastern Europe

In September 2017, OSCE launched its training capacity-building project aimed at developing knowledge and skills of criminal justice institutions in South-Eastern Europe. The project included a series of training courses and workshops, focusing e.g. on digital evidence, cryptocurrencies, the Dark Web, and Forensics[122]. The project will conclude in 2019 with a conference to identify areas requiring special attention in the future[123].

[119] OSCE consists of states from three continents: Europe, North America and Asia. Apart from participating States, the Organisation also consists of 6 Mediterranean Partners for Co-operation and 5 Asian Partners for Co-operation: "Who we are"; https://www.osce.org/whatistheosce

[120] Decision no. 1202 OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies, pp. 1-4; https://ccdcoe.org/sites/default/files/documents/OSCE-160310-NewCBMs.pdf

[121] New technological features, policy engagement and public-private partnerships as ways to lower risks of cyber conflicts in focus at Rome conference, OSCE Newsroom; https://www.osce.org/chairmanship/397853

[122] OSCE-hosted training course for South-Eastern Europe on handling digital evidence by first responders completed in Tirana, OSCE Newsroom, 26.01.2018; https://www.osce.org/secretariat/368056; OSCE hosts regional training course on Live Data Forensics in Tirana, OSCE Newsroom; https://www.osce.org/secretariat/374089; OSCE hosts training course for South-Eastern Europe on Dark Web and virtual currencies in Tirana; OSCE Newsroom; https://www.osce.org/presence-in-albania/372201

[123] OSCE launches project on combating cybercrime and cyber-enabled crime in South-Eastern Europe, OSCE Newsroom; https://www.osce.org/secretariat/341141

Authors

Rafał Babraj – Communications and Modern Technologies Specialist in the Strategic Analysis and Emerging Technologies Team at NASK PIB. Analyses disinformation and fake news, mainly in the context of EU and NATO policy. His research interests focus on the impact of the development of modern technologies on information security. Creator of the website: bezpiecznewybory.pl, preventing disinformation during elections.

Gained his professional experience as a journalist and web editor. Also worked for public administration press offices. Editor-in-chief of the Mazowieckie Province Office's website. Leader of the team introducing plain language standards at the Ministry of Health. Responsible for launching the Ministry of Health's website on the government portal: GOV.PL. Graduate of the Institute of Media Education and Journalism at the Cardinal Stefan Wyszyński University in Warsaw.

After hours, a writer and an avid fan of fantasy literature.

Justyna Balcewicz – "Human Factor" in Cybersecurity and Modern Technologies Analyst in the Strategic Analysis and Emerging Technologies Team at NASK PIB. Specialises in analyses of the impact of modern technologies on the development of society and the related challenges. Actively involved in the working group for education. The group aims to develop guidelines for the creation of an Artificial Intelligence for Poland strategy at the Ministry of Digital Affairs.

Gained her professional experience in the energy and financial sectors. There, she monitored anti-money laundering transactions. Previously Coordinator of EU projects financed from the Swiss-Polish Cooperation Programme and from the Norwegian Financial Mechanism.

Majored in Sociology in the Institute of Applied Social Sciences at the University of Warsaw. Graduated from the University of Finance and Management. Expert in interpersonal relationships and their impact on the functioning of the society and the development of digital competences in the world of modern technologies. In her spare time, writes children's and young adult books.

Magdalena Wrzosek – Head of the Strategic Analysis and Emerging Technologies Team at NASK PIB. Responsible for strategic, regulatory and organisational cybersecurity-related issues as well as development of modern technologies. Liaison Officer of the European Union Agency for Cybersecurity (ENISA). Coordinator of the European Cybersecurity Month in Poland. Creator of the CyberPolicy project (https://cyberpolicy.nask.pl). Worked in the interministerial team responsible for drafting the National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022 and the foundation for the Act on the National Cybersecurity System.

In 2014-2016, worked for the Ministry of Digital Affairs. Was responsible for e.g. negotiations on the NIS Directive, planning and coordination of European cyber crisis exercises – Cyber Europe (in 2014 and 2016). Organised international cooperation and implementation of provisions of the Cyberspace Protection Policy of the Republic of Poland.

Political scientist and cultural expert. Graduate of the University of Warsaw and the University of Konstanz in Germany. Completed postgraduate studies in project management, information security management, international law and foreign service. Also graduated from the George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen (Program on Cyber Security Studies (PCSS) and Seminar on Regional Security (SRS)). In 2016, took part in the US Department of State's International Visitor Leadership Program focusing on cybersecurity. Doctoral student at the War Studies University in Warsaw.

NASK

Cyber POLICY

Graphics partly developed by:

Harryartsrawpixel.com

rawpixel.com

Freepik.com

NASK

Cyber POLICY

NASK – National Research Institute

ul. Kolska 12, 01-045 Warszawa

Reception Desk

+48 22 380 82 00

+48 22 380 82 01

nask@nask.pl

Front Office

+48 22 380 82 04

+48 22 380 82 01

nask@nask.pl