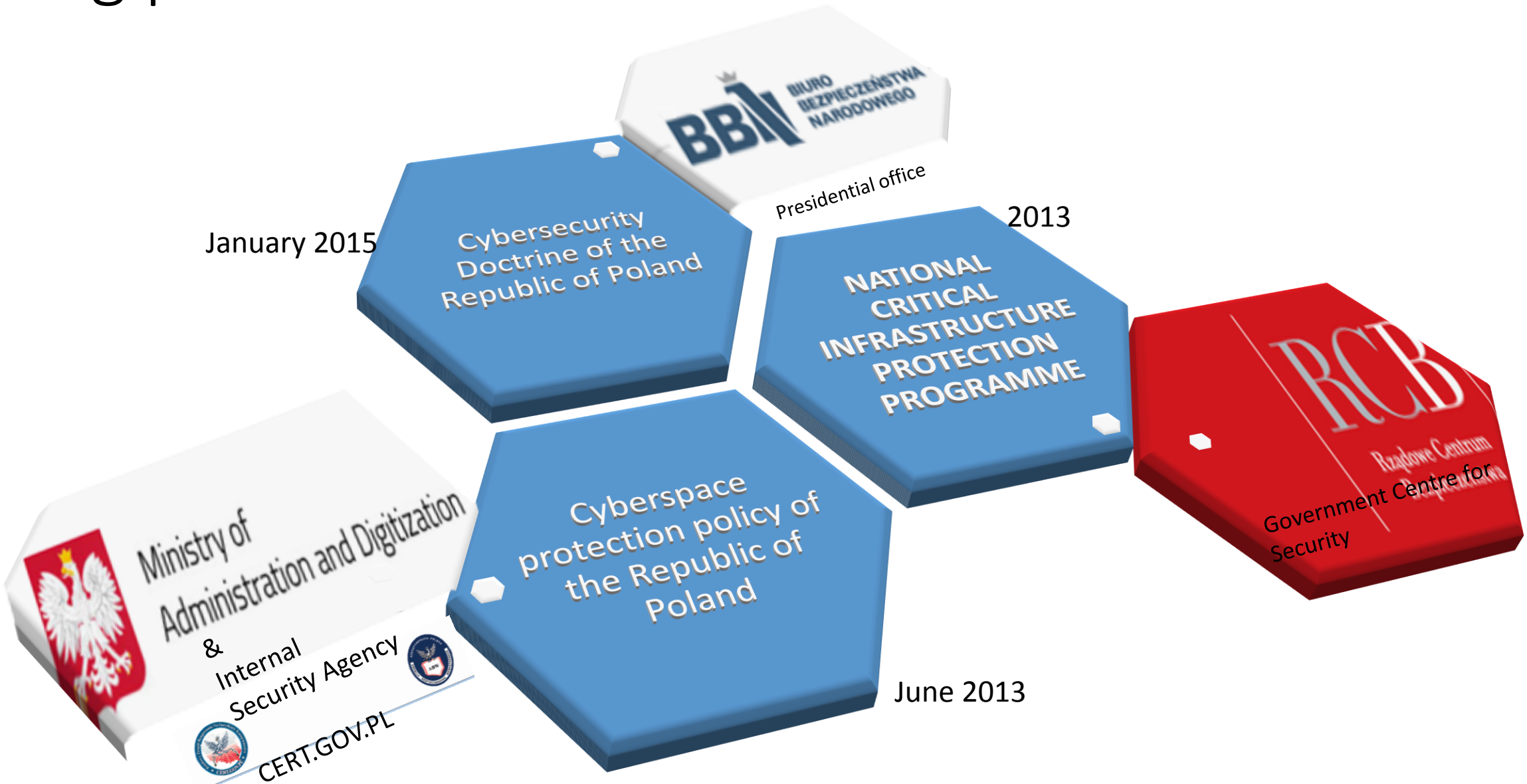
Cyber Security Strategic Level Landscape in Poland

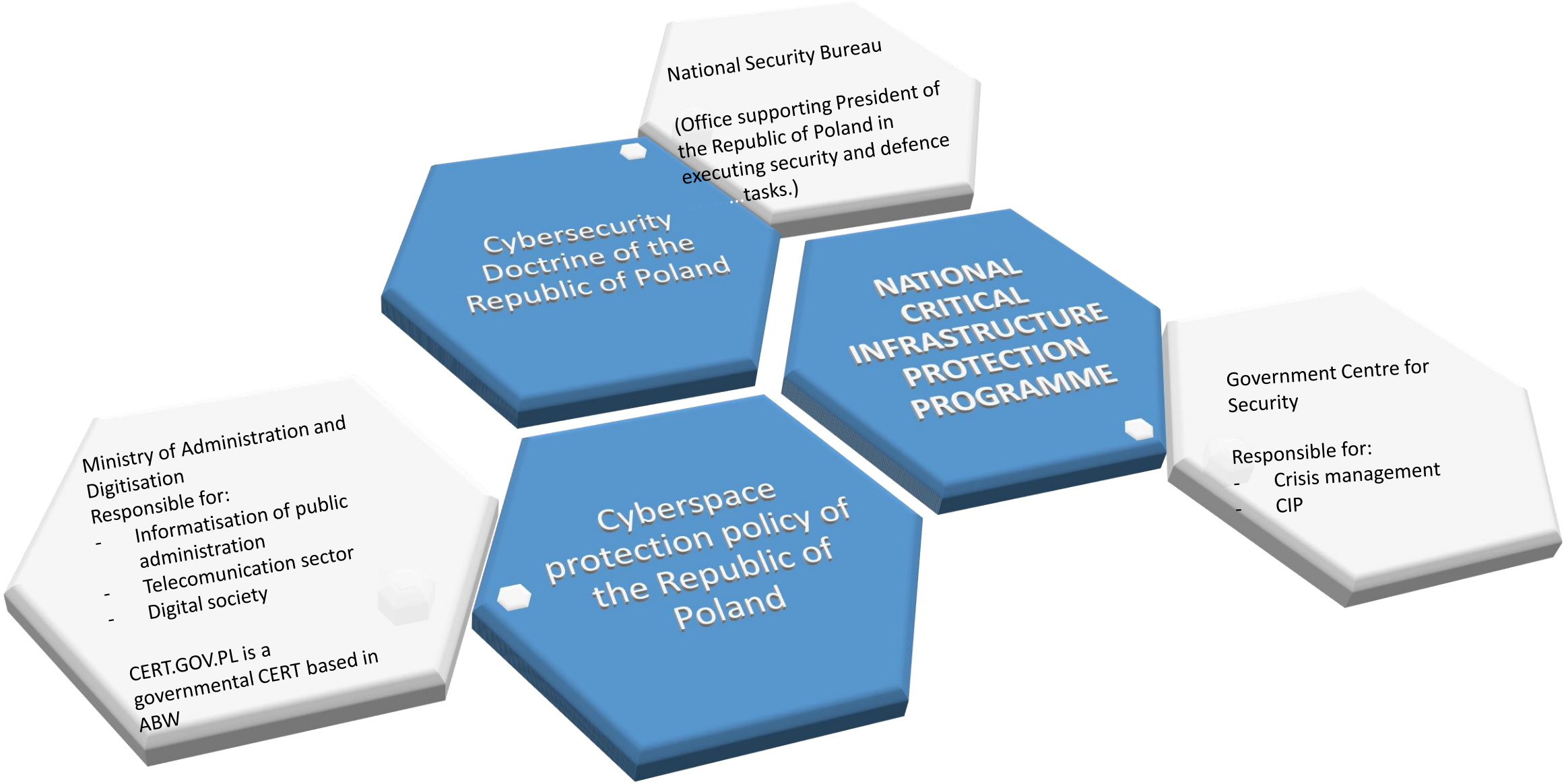
Krzysztof Silicki

NASK Institute, Poland

ENISA MB, EB

Big picture


BBN
BIURO BEZPIECZEŃSTWA NARODOWEGO
Presidential office
January 2015
Cybersecurity Doctrine of the Republic of Poland
2013
NATIONAL CRITICAL INFRASTRUCTURE PROTECTION PROGRAMME
RCB
Rządowe Centrum Bezpieczeństwa
Government Centre for Security
Ministry of Administration and Digitization
&
Internal Security Agency
CERT.GOV.PL
Cyberspace protection policy of the Republic of Poland
June 2013


National Security Bureau
(Office supporting President of the Republic of Poland in executing security and defence ...tasks.)
Cybersecurity Doctrine of the Republic of Poland
NATIONAL CRITICAL INFRASTRUCTURE PROTECTION PROGRAMME
Government Centre for Security
Responsible for:
- Crisis management
- CIP
Ministry of Administration and Digitisation
Responsible for:
- Informatisation of public administration
- Telecomunication sector
- Digital society
CERT.GOV.PL is a governmental CERT based in ABW
Cyberspace protection policy of the Republic of Poland

CSIRTs in Poland

CERT.GOV.PL - Governmental CERT
est. 2008 in ABW (Internal Security Agency)

CERT Polska - de facto national CERT
est. 1996 in NASK

MIL-CERT-PL - Military CERT
est. 2009 in Ministry of National Defence

- Other CSIRTs (academic, telco, ISP…)

NATIONAL CRITICAL INFRASTRUCTURE PROTECTION PROGRAMME

Government Centre for Security (RCB) is responsible for the preparation of the National Critical Infrastructure Protection Programme in close collaboration with the ministers and heads of central offices competent in matters of national security as well as responsible for the following systems:

a) Energy, fuel and energy resources supply systems,

b) Communication systems,

c) Tele-information network systems,

d) Financial systems,

e) Food supply systems,

f)Water supply systems,

g) Health protection systems,

h) Transportation systems,

i) Rescue systems,

j) Systems ensuring the continuity of public administration activities,

k) Systems of production, storing and use of chemical and radioactive substances, including pipelines for dangerous substances;

NATIONAL CRITICAL INFRASTRUCTURE PROTECTION PROGRAMME

The Programme shall specify among others:

- national priorities, objectives, requirements and standards, to ensure the smooth functioning of critical infrastructure;
- detailed criteria which enable to identify objects, installations, facilities and services included in the critical infrastructure systems, taking account of their importance for the functioning of the state and satisfying the needs of the citizens

In short **critical infrastructure** shall be understood as both real and cybernetic systems (including objects, facilities or installations) necessary for minimal operation of the economy and the state.

The legal basis is: the Act of 26 April 2007 on crisis management,

Every second year the Programme is a subject of an evaluation

NATIONAL CRITICAL INFRASTRUCTURE PROTECTION PROGRAMME

CIP public-private Forum

The Forum's objective :

- creating a platform conducive to exchange the views as well as work on sensitive issues related to critical infrastructure protection;

- reporting and developing of new legal solutions for critical infrastructure protection;

- exchange of views and comments of stakeholders at an early stage of legislative work in the field of critical infrastructure;

- organization of workshops, seminars and conferences devoted to critical infrastructure protection;

- creating a database of experts on issues related to the subject of critical infrastructure in the various systems – financial, communication, tele-information network systems, energy, fuel and energy resources supply system.

A mechanism to protect critical infrastructure will be established within the framework of the Forum:

- Information sharing about threats
- Coordination of actions in case of emergency
- Participation in the exercises on critical infrastructure protection.

Cooperation with private sector

Cyberspace Protection Policy

- Established in June 2013 by Ministry of Public Administration and Digitisation (MAC) and Internal Security Agency (ABW)
- Since 2009 there were works on cyberspace protection programmes but two preceding documents did not received enoungh formal status

Policy applies to the government administration

At the same time the *Policy* is recommended for local government administration of communes, districts and provinces and other offices (units which do not belong to the state and local government administration), including:

a) Chancellery of the President of the Republic of Poland;
b) Chancellery of the Sejm of the Republic of Poland;
c) Chancellery of the Senate of the Republic of Poland;

The *Policy* is at the same time a guide to actions for all other users of cyberspace who are not mentioned above.

Cyberspace Protection Policy

1) Increasing the level of security of the State ICT infrastructure.
2) Improving the capacity to prevent and combat threats from cyberspace.
3) Reducing the impact of incidents threatening the ICT security.
4) Determining the competence of entities responsible for the security of cyberspace.
5) Creating and implementing a coherent system of cyberspace security management for all government administration entities and establishing guidelines in this area for non-state actors.
6) Creating a sustainable system of coordination and exchange of information between the entities responsible for the security of cyberspace and the cyberspace users.
7) Increasing awareness of the cyberspace users on the methods and safety measures in cyberspace.

Objectives

Cyberspace Protection Policy

Minister for digitisation on behalf of Council of Ministers is responsible for implementation of the Policy

Supervising body: Council of MInisters

To help realise this mission – a special team (interdepartment task force) is established (Task Force for Cybersecurity Protection)

Main action lines defined in the document:

- Risk assesment
- Security of e-government infrastructure
- Legislation
- Organisational and procedural security (e.g. the role of security officers)
- Developing technical and response capabilities (eg. CERTs, EWS)
- Cooperation
- Research programmes

Responsibility and main action lines

Task Force for Cybersecurity Protection

Main tasks:

- Preparation of the action plan according to Policy provisions
- Recommendation of standards and good practices for institutions
- Creation of forum of information sharing between public and private sector
- Coordination of implemenbtation of the Policy
- Coordination of harmonisation with EU strategies and regulations

Action plan

Main lines of action: Risk assesment

Each governemt administration institution shall submit to MAC report summarizing the results of the risk assesment (in accordance with the model developed by MAC)

Annual report contains information on types of risks, threats and vulnerabilities diagnosed by individual participating institutions

MAC determine the uniform methodology for performing risk analyses

Governmental CERT is providing information about general threats, possible risks in cyberspace and also incident response

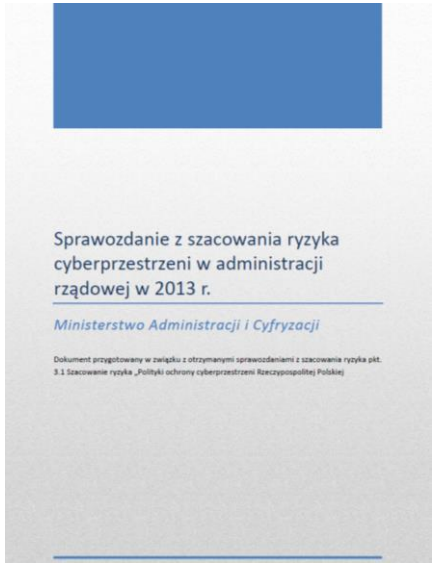
Two editions of risk assesment reports were performed for 2013 and for 2014

Risk assesment outcome is constituting the basis (during preparation stage) for developing the key indicators of proper implementation of the Policy

BOTTOM-UP approach — every institution is advised to suggest indicators of objectives which would be then aggregated and global indicators will be developed

Inventory of key systems, threats and risks

- Each year MAC is preparing a report, aggregating data from public institutions (first report for 2013, second edition currently under preparation)
- Consists of:
  - Identification of key information systems
  - Catalogue of threats identified
  - Risk analysis output (register)
  - Set of recommendations for risk mitigation
- MAC performs revision (if necessary) of the methodology guidelines for the consecutive year



Annual report

Cyberspace security officers (PCS)

3.4.3. The role of plenipotentiaries for cyberspace security

The organizational units of government administration should define the role of a plenipotentiary for cyberspace security (hereinafter referred to as PCS).

The tasks of a plenipotentiary within the scope of cyberspace security shall include in particular:

1) implementation of the obligations arising from the provisions of legal acts relevant to ensure cyberspace security;
2) development and implementation of procedures for responding to computer incidents which will apply in the organization;
3) identification and conducting periodic risk analyses;
4) preparation of emergency plans and testing them;
5) development of procedures to ensure information of appropriate CERTs about:
   a) the occurrence of computer incidents,
   b) the relocation of an organizational unit, contact information, etc.

Cyberspace security officers (PCS)

The *Policy* does not indicate the location of a plenipotentiary for cyberspace security in the structure of an organizational unit, however, the role of a plenipotentiary should be assigned to the person responsible for carrying out the process of ICT security.

During risk analysis process organisations are sending reports to MAC once a year – including contact data for cyberspace security officers (named: *plenipotentiaries - PCS*)

There are several trainings, seminars and workshops organised every year for PCS by MAC.

Apart of this contact data for new PCSs are provided by e-mail to the ministry (database is maintained to be up-to-date)

Curently near 130 PCS are estabished and registered in the database

Cybersecurity Doctrine of the Republic of Poland

Published by National Security Bureau (BBN) – office of the President of Poland - in 2015

Higher level document: National Security Stategy of RP

Doctrine is describing not only aspect of cybersecurity and but also the need for cyberdefence capabilities

National Security Council

Cybersecurity Doctrine of the Republic of Poland

- **The National Security Bureau (BBN) published the Polish cybersecurity doctrine in 2015**, after more than a year of studies and drafting. The document outlines further lines of work on improving national security in cyberspace.
- The doctrine maps out tasks for state institutions, notably security agencies and armed forces, private sector and NGOs.
- The threats coming from cyberspace and identified in the doctrine include cybercrime, like "cyberviolence, destructive cyberprotests and cyberdemonstrations," attacks against telecommunications systems important for national security, data and ID theft, and hijacking of private computers.
- External threats listed by the doctrine are cybercrises and cyberconflicts, cyberwar included, as well as cyberespionage involving states and other entities. "Threats (for Poland) coming from cyberspace include extremist, terrorist and international criminal organizations whose attacks in cyberspace can have ideological, political, religious, business or criminal motivations," the document points out.
- It emphasizes the need for "pursuing active cyberdefence, including offensive actions in cyberspace, maintaining readiness for cyberwar," protection and defence of Polish teleinformation systems and accumulated data, and supporting key private firms in their cybersecurity efforts.

Current and Future work

- Ministry of Digitisation is launching preparation work for development of the optimal cybersecurity governance model in Poland
  - considering country specific conditions and current landscape,
  - to be prepared for future NIS directive

- NASK institute is actively involved in this proces
- We are interested in any life experience of cybersecurity governance models in other countries

Thank you for your attention

Krzysztof.Silicki@nask.pl