CYBERSECURITY GOVERNANCE IN SLOVAKIA WITH FOCUS ON LEGISLATION AND PRACTICAL QUESTIONS...

Rastislav Janota

Director

National Cyber Security Centre SK-CERT

November 2022

Welcome

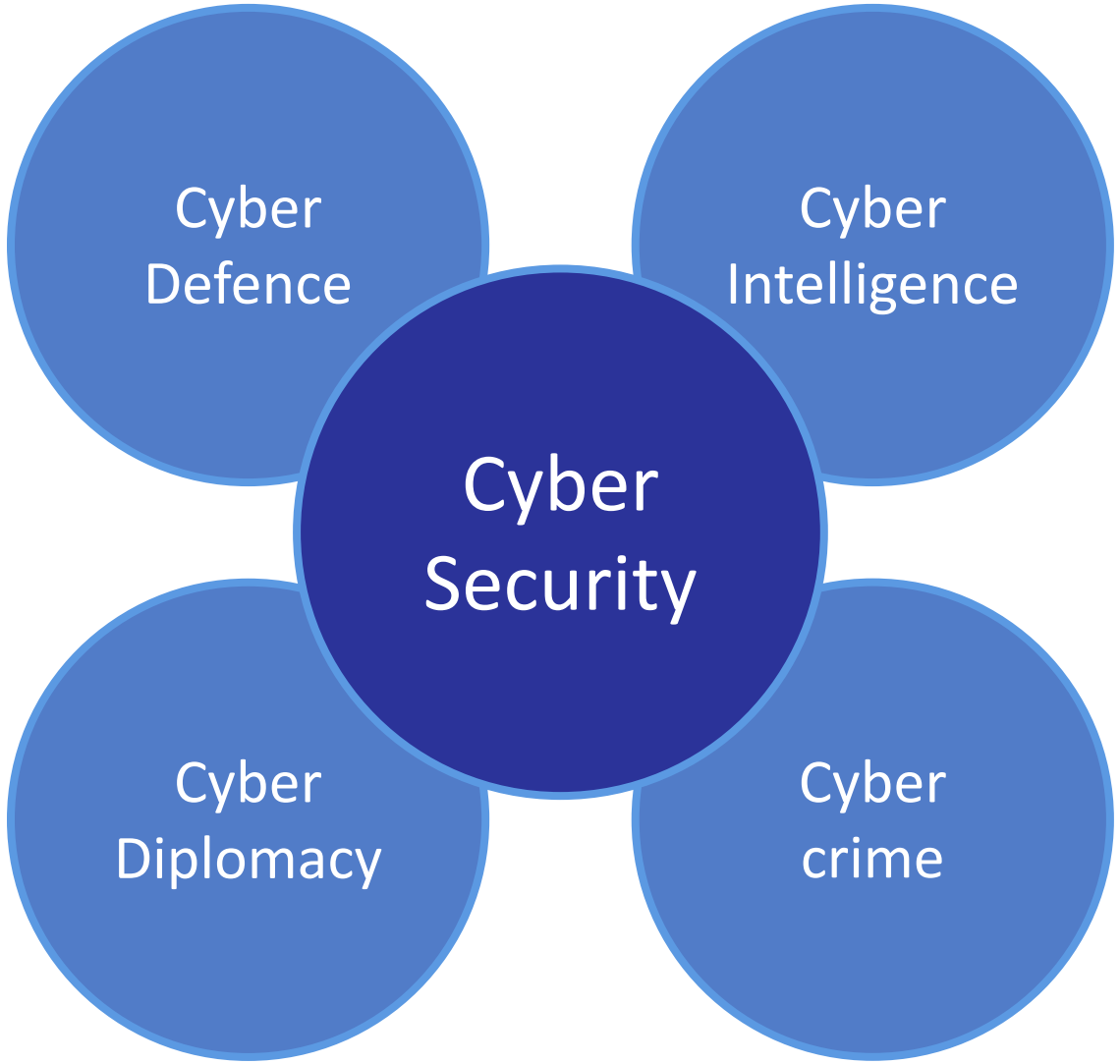
Motto:

Cybersecurity is topic we all should care

Where is Cybersecurity in Slovakia?

- Do not reshape usual roles in the government environment
- Fill the empty space between other areas
- Coordinate activities and foster cooperation between other players

- **Cyber Crime**
  - (***Ministry of Interior, police, crime investigators, prosecutors, courts***)
- **Cyber Defense**
  - (*Ministry of Defense, Army*)
- **Cyber Intelligence**
  - (*Intelligence services*)
- **Cyber Security**
  - (National Cyber Security Centre SK-CERT / *National Security Authority)*



DIFFERENT EU REGULATIONS

- **General Data Protection Regulation (GDPR) – 2016/679**
  - To strengthen and unify data protection for all individuals within the European Union (EU)
  - Regulator – Office for Personal Data Protection of the Slovak Republic
- **Payment Services Directive (PSD2) – 2015/2366**
  - To regulate payment services and payment service providers throughout the European Union (EU)
  - Regulator – National Bank of Slovakia
- **Regulatory framework for electronic communications – Telecoms Package (2009)**
  - To create a common set of regulations for the telecoms industry across all EU states
  - Regulator –Regulatory Authority for Electronic Communication and Postal Services

- **Network and Information Security Directive 2016/1148**
  - To force companies and organizations to protect their systems/data from cyber-attacks
  - Regulator – National Security Authority

New / proposed EU Cyber Security regulations

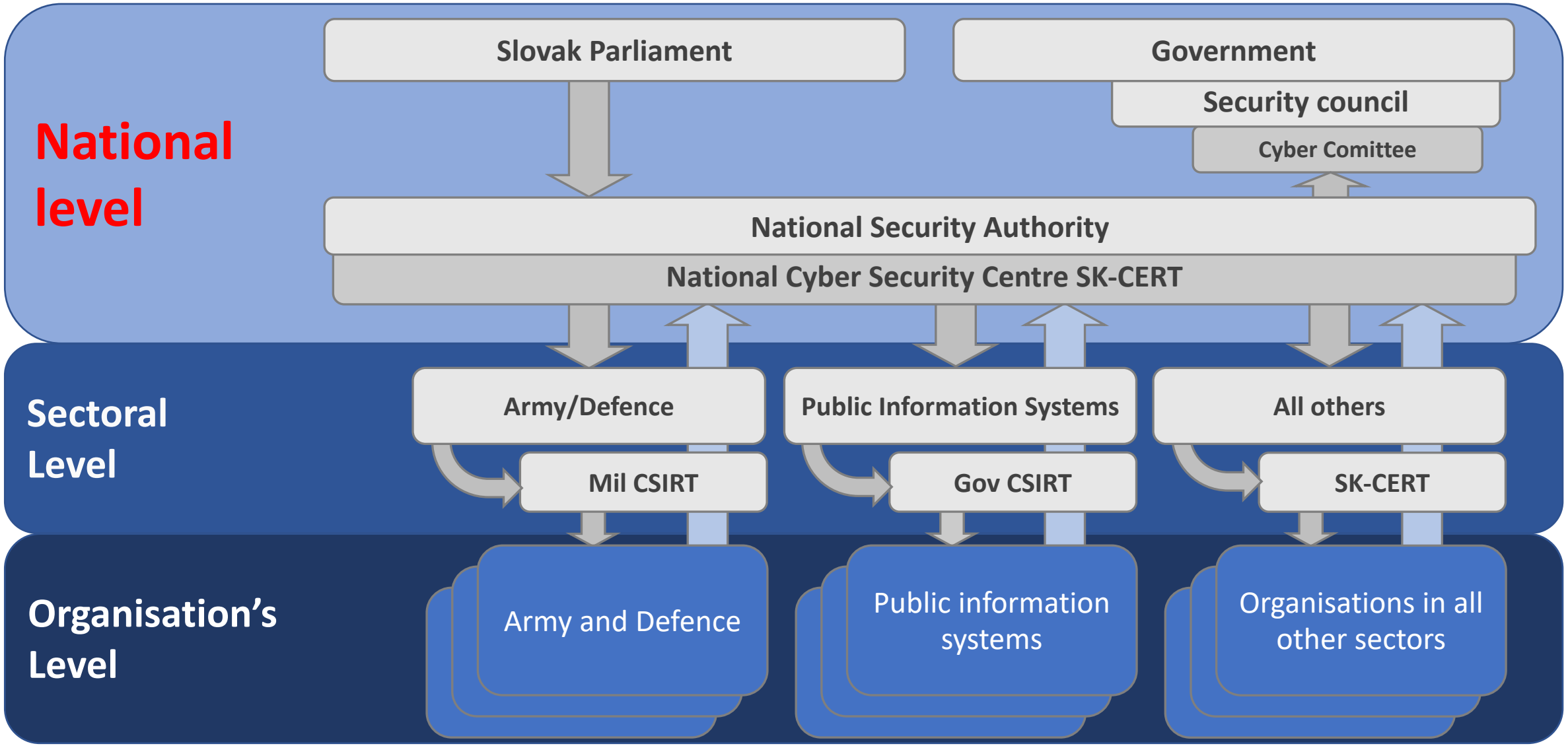
- Regulation on the Digital Operational Resilience of the Financial Sector (DORA Directive)

- Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities (CER)

- **Network and Information Security Directive 2**
  - New concept, great expansion of sectors and areas of responsibility
  - Very similar to our already valid KB law
  - Effective from 1.1.2023 (approx.)

- Big change: For the first time, mutual coordination of legislative acts. Both the DORA Directive and the CER Directive refer to NIS 2 and supplement it in the relevant areas

Slovak Cyber Security Governance



SK CERT

KEY RESPONSIBILITIES OF NSA

- Manages and coordinates carrying out of state administration
- Determines the principles for preventing cybersecurity incidents and principles for their handling
- Is a national point of contact for cybersecurity for foreign entities
- Systematically gathers, concentrates, analyses and evaluates information on the state of cybersecurity in the Slovak Republic
- Ensures and is responsible for coordinated cybersecurity incidents handling at the national level
- National CSIRT and SOC
- Is a national body for cyber security certification and a conformity assessment body according to a special regulation
- Assesses the supplier's security risks for the performance of activities that are directly related to the operation of networks and information systems in the Slovakia
- Perform close cooperation with all players in the cyber security space on national level
- Working with cyber security community

SK CERT

Cybersecurity law principles in Slovakia

- Minimum regulations approach used (only NIS duties)
- Practical approach to incident handling
- Opening voluntary ‘win-win’ cooperation with the market instead of mandatory duties

- Alignment with Critical Infrastructure Protection legislation
- Alignment with Intelligent Industry 4.0 government approach
- Definitions of sectors and subsectors for OES incl. competent bodies and their duties
  - (11 Sectors, 27+1 Sub Sectors, 11 Competent Authorities)
- Mandatory government CSIRTs for sectorial competent bodies, government outsourcing and last-resort option
- Independent auditing based on internationally notified schema

- Law is in force since April 1st, 2018u

SK CERT

Cybersecurity law principles in Slovakia

- Based on EU NIS Directive
- With some national priorities already incorporated into the law:
  - No additional duties (over NIS) at the beginning
  - More sectors / subsectors (7 sectors vs 11 sectors with 28 subsectors)
    - Including telecommunication sector
  - Well defined identification criteria
  - Including public administration, police and army
    - -> 1700+ organization under cyber security duties currently
  - Security measures based on combination of international standards (ISO 27t family + NIST + COBIT5)
  - Separation of civil servants from regular control processes
  - Introduction of strict certification schema for cyber security audits (and auditors), regular (at least every 2 years) mandatory audits, results to deliver to NSA
- Implementation of NIS2 is going to be a minor evolution in Slovakia

SK CERT

Various Decrees

On the basis of §32 of the Act (Authorizing Provisions), the NBU issued

- Decree 164/2018 determining the identification criteria of the operated service (essential service criteria)
- Decree 165/2018, which determines the identification criteria for individual categories of serious cyber security incidents and the details of reporting cyber security incidents
- Decree 166/2018 on details of the technical, technological and personnel equipment of the unit for solving cyber security incidents
- Decree 362/2018 establishing the content of security measures, the content and structure of security documentation and the scope of general security measures
- Decree 436/2019, which determines the rules and scope of the cyber security audit and details on the accreditation of conformity assessment bodies and the content of the final report on the results of the cyber security audit (according to § 29 sections 1 to 4)

Another decree is being prepared

- Decree determining security standards and knowledge standards in the field of cyber security (§ 5(1)(w), § 20(1))

OTHER/NEXT ACTIVITIES

- In January 2021, the Slovak Government approved the National Cyber Security Strategy for the years 2021 to 2025, followed by the Action Plan for the implementation of the Strategy for the years 2021 to 2025
  - The approved KB Strategy is based on
    - Security Strategy of the Slovak republic 2020
    - Defense Strategy of the Slovak republic 2020
- The Strategy (and therefore the Action Plan) has 7 key chapters
  - A trusted state prepared for threats
  - Effective detection and clarification of computer crime
  - A resilient private sector
  - Cyber security as a fundamental part of public administration
  - Strong partnerships
  - Educated professionals and an educated public
  - Research and development in the field of cyber security
- 2023-2024 – preparation of an amendment to the Act on Cyber Security – implementation of NIS2

DEFINITION OF SECTORS AND SUBSECTORS FOR OES (CURRENT SITUATION)

Sector	Subsector	Managing authority	CIP	NIS	CiiP
Banking		Ministry of Finance		✓	✓
Transport	Air transport	Ministry of transport and construction	✓	✓	✓
	Rail transport		✓	✓	✓
	Water transport		✓	✓	✓
	Road transport		✓	✓	✓
Digital Infrastructure		National Security Authority		✓	✓
Electronic Communication	Satellite communication	Ministry of transport and construction	✓		✓
	Electronic communications networks and electronic communications services		✓		✓
Financial market infrastructures		Ministry of Finance		✓	✓

SK CERT

DEFINITION OF SECTORS AND SUBSECTORS FOR OES (CURRENT SITUATION)

Sector	Subsector	Managing authority	CIP	NIS	CIIP
Postal services		Ministry of trans & const	✓		✓
Energy	Mining	Ministry of Economy	✓		✓
	Electricity		✓	✓	✓
	Oil		✓	✓	✓
	Gas		✓	✓	✓
	Heat-power				✓
Other Industries	Pharmaceutical	Ministry of Economy	✓		✓
	Metallurgical		✓		✓
	Chemical		✓		✓
	Intelligent Industry (4.0)				✓
Health	All medical facilities (incl. Hospitals and private clinics)	Ministry of Health	✓	✓	✓

DEFINITION OF SECTORS AND SUBSECTORS FOR OES (CURRENT SITUATION)

Sector	Subsector	Managing authority	CIP	NIS	CIIP
Water and Atmosphere	Weather service	Ministry of the environment	✓		✓
	Water works		✓		✓
	Drinking water supply and distribution		✓	✓	✓
Public Administration	Public order and security	Ministry of interior			✓
	Information systems of public administration	Deputy Prime Minister's Office for Investments and Informatization	✓		✓
	Defense	Ministry of defense			✓
	Intelligence services	Intelligence services			✓
	Classified Information Protection	National Security Authority			✓

SK CERT

IDENTIFICATION CRITERIA – EXAMPLES (BANKING)

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Credit institutions whose business is to receive deposits or other repayable funds from the public and to provide loans on their own account	a) Number of clients exceeding 25 000. b) Market share exceeding 1% of the balance sheet total.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

IDENTIFICATION CRITERIA – EXAMPLES (DIGITAL INFRASTRUCTURE)

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Internet exchange point service provider for switching networks that are technically and organizationally separate.	Organization administers an autonomous system (AS) or operates data lines in the Internet network, where these interconnect the AS with two and more other AS in the overall transmission capacity of network interfaces of at least 2 Gbps. For these purposes an AS is considered only an AS with a public AS number (public ASN), not an AS	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss or material damage to at least one user exceeding 250 000 EUR. 4. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

BASIC DUTIES FOR OES FROM CYBER SECURITY ACT / NIS

Two important group of duties for Operators of Essential Services

- **Preventive duties**
  - Follow minimum security baselines defined by law
  - Do proper management of supply chain (suppliers of products/services)
- **Reactive duties**
  - Report cybersecurity incident to Cybersecurity Authority (NCSC SK-CERT)
  - Handle cybersecurity incidents
  - Cooperate with the Cybersecurity Authority and the competent body (sectoral authority) when handling the reported cybersecurity incident
  - At the time of the cybersecurity incident, to provide proof or means of proof so that they may be used in a criminal proceeding
  - Inform the law enforcement authority or the Police

Reporting Cyber Security Incidents to the NCSC SK-CERT

Allows the SK-CERT

- Have an overview of the state of cyber security in Slovakia in real time
- Obtain information and experience from abroad about a specific incident (if any)
- Warn other relevant SR entities against a similar problem
- Expand the knowledge base and prepare effective recommendations in the preventive area in order to minimize the risk of similar incidents in the future

It enables the sectoral central authority

- Have real-time insight into the state of cyber security within your sector
- Recommend effective ways of solving the given problem
- At the request of the subject, effectively assist/help in solving the incident

SK CERT

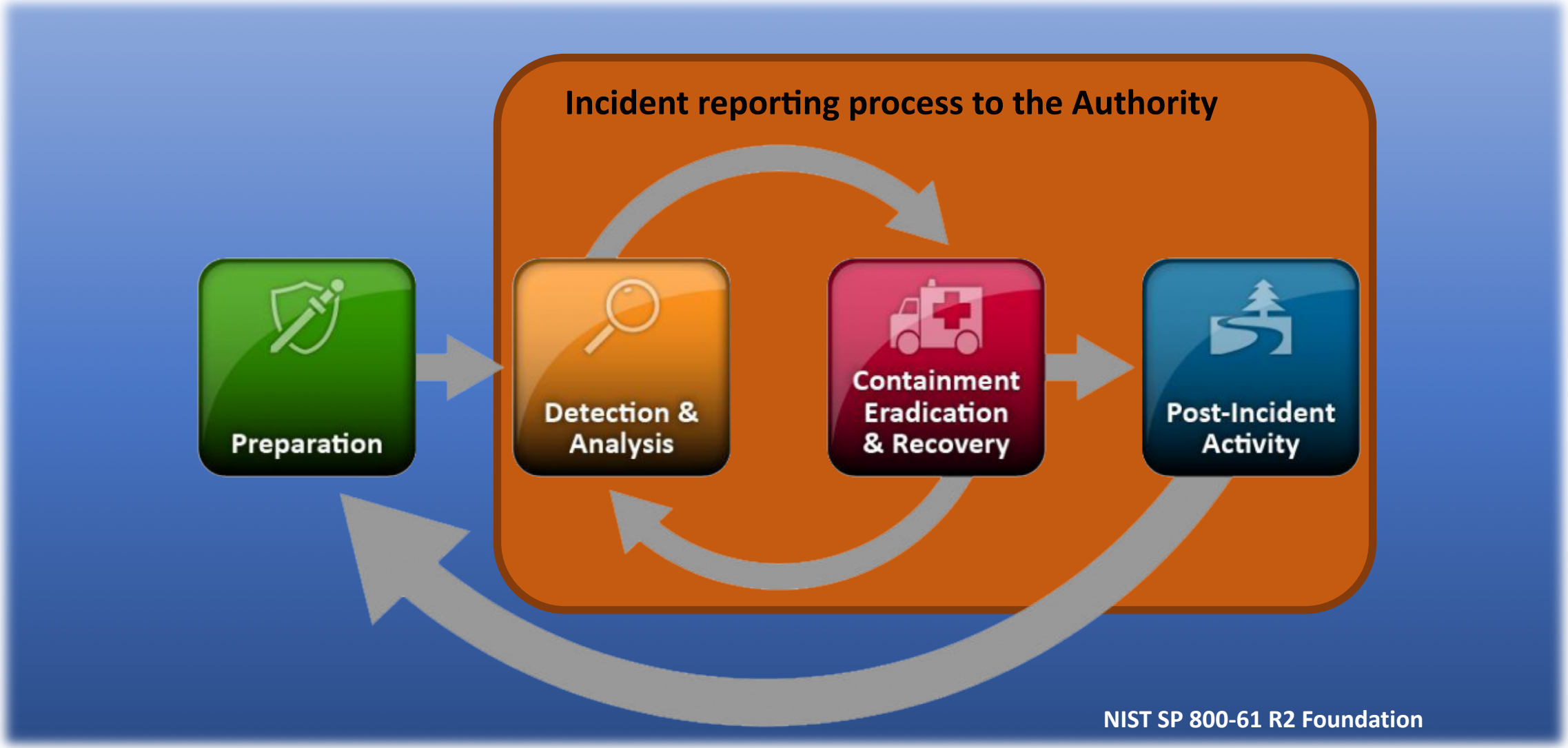
Categories of Incidents

- Incidents are categorized according to Decree of the National Security Authority
- Organisations have duty to report incidents as soon as they detect those to SK-CERT
- SK-CERT to oversee incident handling of all incidents
- Specific information about incidents to share with intelligence services

	Description	Escalation
Category I	Limited impact / affecting limited number of people/systems	-
Category II	Incidents with high impact on people/systems	-
Category III	Incident with potential critical (severe) impact	• To Military Intelligence • To Chairman of the Security Council of the Slovak Republic

SK CERT

Incident Response lifecycle



CSIRT = Computer Security Incident Response Team

- CSIRT is (according to §1 of the Act) a unit for dealing with cyber security incidents
  - There are many other synonymous abbreviations (CERT, CIRT, SIRT, PSIRT, SRC, CSC, IRT, CCS, etc.)

- We recognize three levels of CSIRT units
  - National unit SK-CERT (according to the law - part of the National Cyber Security Center)
  - CSIRT sector units (by law, or build by ministries and accredited by NSA)
  - "Real" CSIRT units (the law does not explicitly regulate them today)
    - Commercial, corporate, state, academic, etc.
    - They don't have to be called CSIRT, it can be, for example, an internal department/department/section of IS security and the like

ATTRIBUTIONS

- Attribution process (both Political/Strategic and Technical) oversee by National Security Authority
- in close cooperation with
  - Ministry of Foreign and European Affairs of the Slovak Republic
  - SIS (Civil intelligence)
  - Ministry of Defence (Military Intelligence)
  - Others (depends on situation)
- Results of attribution process (if any) to escalate to Cyber Security Committee of the Security Council of the Slovak republic

International Cooperation

- Council of Europe
  - HWP (Horizontal Working Party on Cyber)
- European Commission
  - NIS Cooperation Group
- EEAS - Cyber Diplomacy Toolbox
  - Framework for a joint response of EU states to malicious activities in cyberspace
  - It sets the legislative framework
  - Addresses sanctions against individuals and organizations/states as an EU response to cyber attacks (including attempted attacks)
  - The input is the results of the so-called Political and technical attribution of incidents from the level of CS
- ENISA – European Cyber Security Agency
  - The NBU represents the Slovak Republic in ENISA and ENISA bodies

International Cooperation

- Cyber Crises Liaison Organization Network (CyCLONE)
  - Initiative of the Member states
  - It deals with solving large-scale incidents and crises
  - It enables the cooperation of responsible organizations of individual CS
  - It also communicates with the CSIRT Network and the diplomatic level
  - It supports the national and political EU level for the implementation of informed decisions
  - Executive and Officer levels (national cyber authorities)

- EU CSIRT Network
  - Network of national units CSIRT + CERT-EU
  - EC as observer, ENISA - backoffice

International Cooperation

Other international organizations

- TF-CSIRT (CSIRT Task Force)
  - Wider Europe in particular, but also Asia, Africa, North and South America, etc.
  - Today approx. 400 CSIRTs
- FIRST (Forum of Incident Response and Security Teams)
  - A worldwide organization
  - Today 663 CSIRTs and 115 individual members (important persons)
- CERT.ORG - Software Engineering Institute, Carnegie Mellon University, Pittsburgh

International Cooperation

- Bilateral cooperation is extremely important for real operational capabilities
- Today, we have a highly developed bilateral cooperation, especially with
  - France - Agence nationale de la sécurité des systèmes d'information (ANSSI)
  - Germany - BSI
  - Luxembourg - GovCERT.LU, CIRCL.LU
  - Romania - National Cyber Security Directorate
  - The Netherlands - National Cyber Security Center the Netherlands (NCSC-NL)
  - Belgium - Center for Cyber Security Belgium
  - Austria - CERT.AT
  - CERT-EU
  - USA (selected organizations)
  - Czech Republic - National Office for Cyber and Information Security (NÚKIB)
  - Indonesia

KEY CHALLENGES

- Good legislation on all levels
  - Ability to fulfill security roles of key players
  - Regulation to motivate increase resiliency on all levels of organisations in SK
  - Not to increase bureaucracy on all levels, not to overdo regulation of private companies
  - While keeping important democratic principles
- Availability of staff – candidates for working in the field
- Government understanding / support / finance
- Good cooperation (all levels, all directions)
- Implementation of cyber security certification and a conformity assessment

Thank you

Rastislav Janota

rastislav.janota@nbu.gov.sk

NATIONAL SECURITY AUTHORITY

SK CERT