ICCECIP 2023

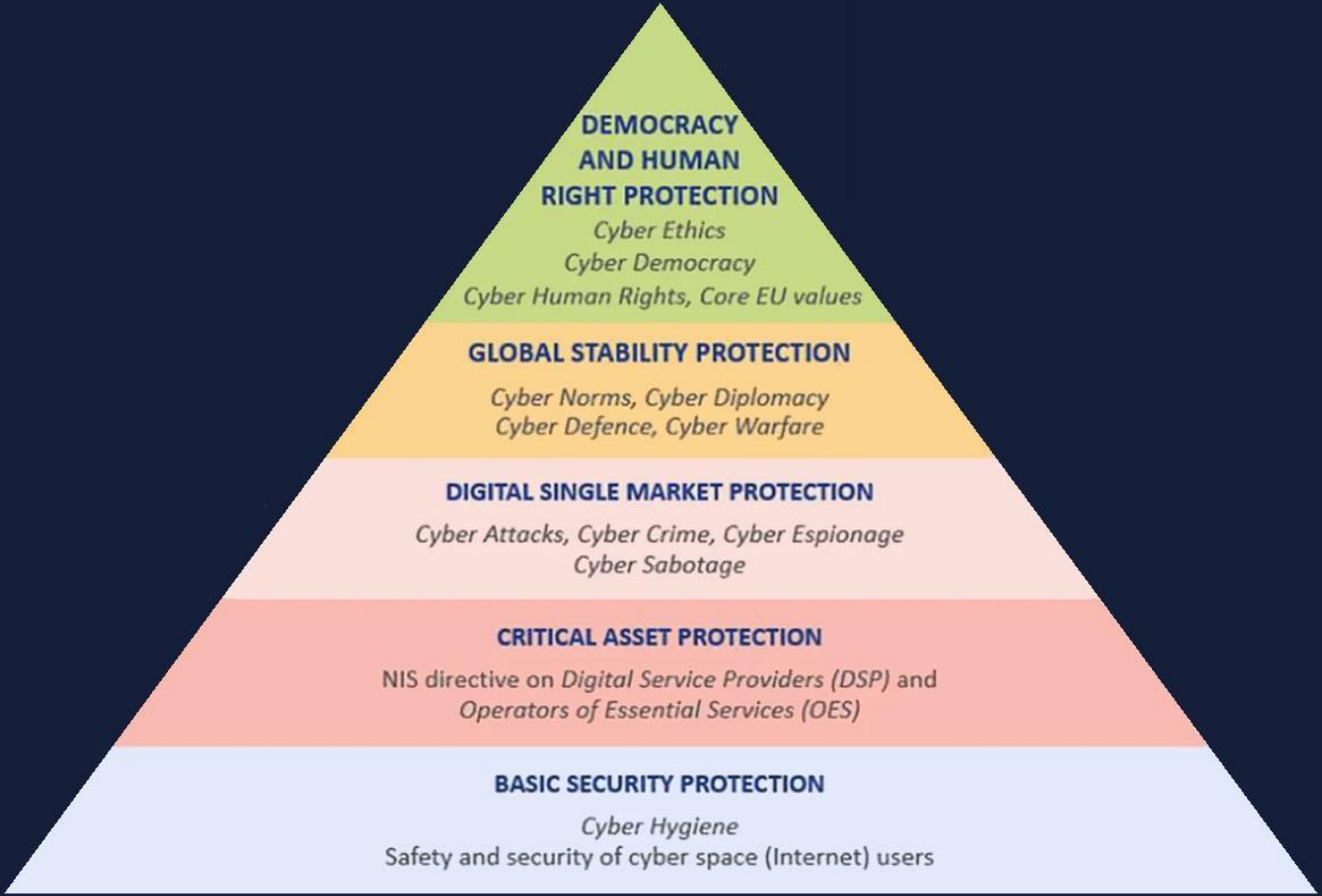
Hungarian legislation regarding of cyber security

Levente Durczy

PhD student, NIK / Óbuda University, Hungary

5th International Conference on Central European Critical Infrastructure Protection
13-14 November 2023 / Budapest, Hungary

Analysis of the European Union's Cyber Security Ecosystem



DEMOCRACY AND HUMAN RIGHT PROTECTION

Cyber Ethics
Cyber Democracy
Cyber Human Rights, Core EU values

GLOBAL STABILITY PROTECTION

Cyber Norms, Cyber Diplomacy
Cyber Defence, Cyber Warfare

DIGITAL SINGLE MARKET PROTECTION

Cyber Attacks, Cyber Crime, Cyber Espionage
Cyber Sabotage

CRITICAL ASSET PROTECTION

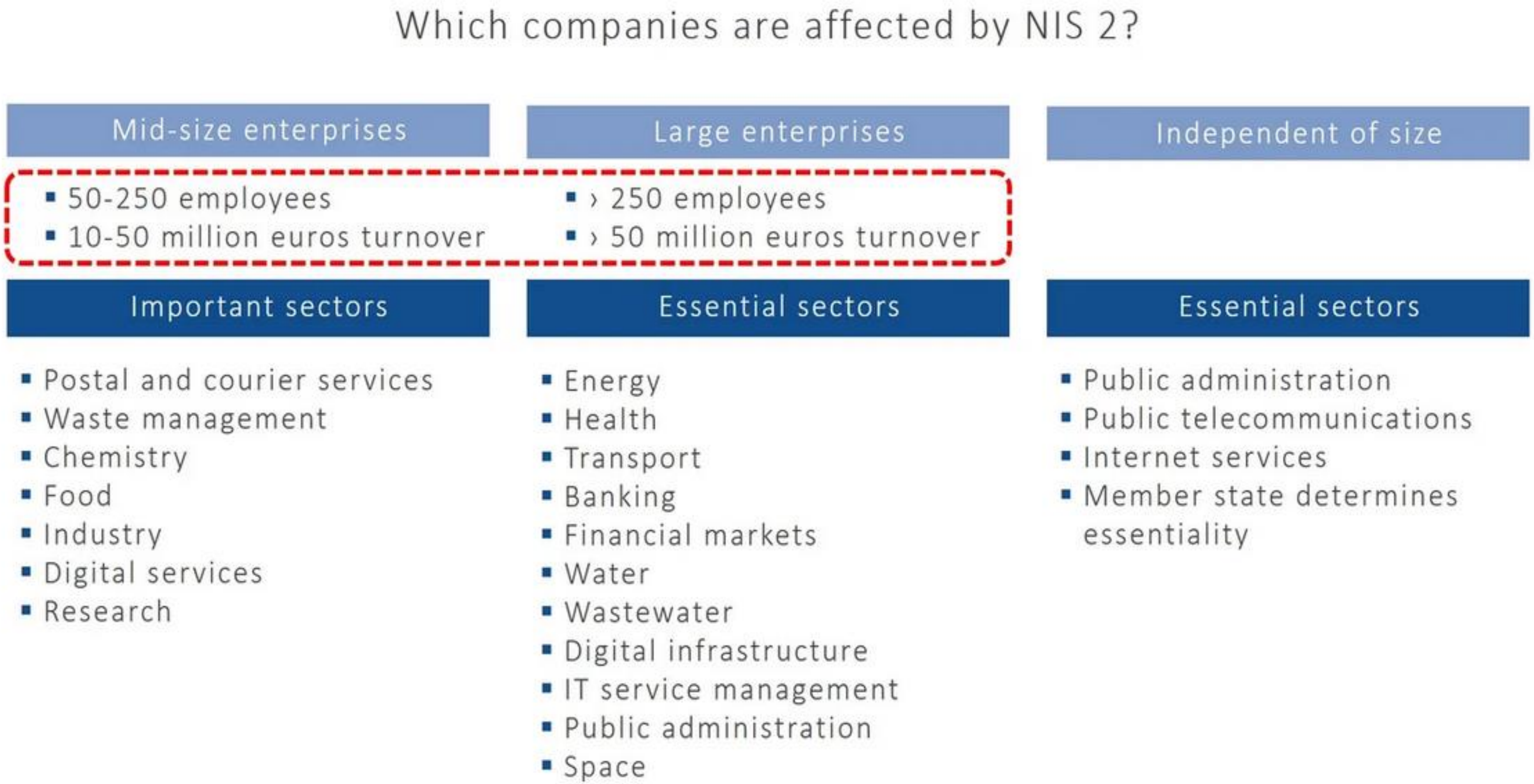
NIS directive on *Digital Service Providers (DSP)* and
Operators of Essential Services (OES)

BASIC SECURITY PROTECTION

Cyber Hygiene
Safety and security of cyber space (Internet) users

Zsolt Bederna · Zoltan Rajnai: Analysis of the cybersecurity ecosystem in the European Union

NIS2 Directive (EU 2022/2555)



Which companies are affected by NIS 2?

Mid-size enterprises	Large enterprises	Independent of size
▪ 50-250 employees ▪ 10-50 million euros turnover	▪ › 250 employees ▪ › 50 million euros turnover	
Important sectors	**Essential sectors**	**Essential sectors**
▪ Postal and courier services ▪ Waste management ▪ Chemistry ▪ Food ▪ Industry ▪ Digital services ▪ Research	▪ Energy ▪ Health ▪ Transport ▪ Banking ▪ Financial markets ▪ Water ▪ Wastewater ▪ Digital infrastructure ▪ IT service management ▪ Public administration ▪ Space	▪ Public administration ▪ Public telecommunications ▪ Internet services ▪ Member state determines essentiality

Hungarian regulation:

- 2013 "L." Act: on the electronic information security of state and local government bodies: National Cyber Defense Strategy
- Hungary's National Cyber Security Strategy (Government Decision 1139/2013 (III.21.)):

  Cyberspace is the electronic world that surrounds us, which is a combination of globally connected, decentralized, ever-growing electronic information systems, as well as social and economic processes in the form of data and information through these systems
- National Cyber Defense Institute (NKI, 2015)
- Data Protection Act (Act XXVIII of 2018):
- etwork and Information Security Strategy of Hungary (2018):
- National Cyber Security Coordination Council (Government Decree 484/2013 (XII. 17))
- Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision

Members of the National Cyber Security Coordination Council

- National Cyber Defense Institute (NKI);
- Government Incident Management Center (GovCERT-Hungary);
- National Electronic Information Security Authority (NEIH);
- Information Office independent event manager (IntCERT);
- Independent incident manager of the Military National Security Service;
- BM National Directorate General of Disaster Prevention (BM OKF/LRLIBEK);
- Hungarian Academy of Sciences – Computing and Automation Research Institute
- operates an information security incident management organization (HunCERT);
- Computer security incident management organization of the Government Information Technology Development Agency (NIIF CSIRT)

Act XXIII. of 2023 on Cybersecurity Certification and Cybersecurity Supervision

- The law set two main goals:

- Development of national cyber security certification systems

- Increasing cyber security preparedness among companies and organizations:

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

SZTFH
Szabályozott Tevékenységek
Felügyeleti Hatósága

Hungarian regulations from 2024 (NIS 2 compliance)

- **Obligations of the companies concerned (not complete):**
- in the event of an incident, the first notification obligation to the authorities within 24 hours
- Obligation to report events within 72 hours (attack assessment, severity, impact)
- They must carry out a risk analysis of their electronic information systems and the managed data
- They must classify their electronic information systems and the data handled in them into a security class (basic, significant, high)
- Developing an **Incident response plan** (IRP), and development of a **Business continuity plan** (BCP), and development of a **Disaster recovery plan** (DRP)
- Application of encryption solutions, carrying out security risk assessments
- Developing multi-factor authentication or continuous authentication solutions
- Monitoring and supervision of their network and the entire system
- Performing vulnerability tests, paying an annual cyber security monitoring fee

Conclusion:

What is security worth to the individual and the organization?

ARE WE SAFE?

Are we protected by legislation, "security policies", ...?

Passwords, two-key authentication, VPN, IOT device security holes, …

Which service provider can we trust?

How many places do we enter our data and password?

"Nice new world?"

What will become of this?

What is security worth to the individual and the organization?

ICCECIP 2023

Thank you for the kind attention!