Infokommunikáció 2021

Information security issues for a future-proof EDR system

„Quis custodiet ipsos custodes? -Who will guard the guards themselves?

Tamás Kardos, Óbudai University

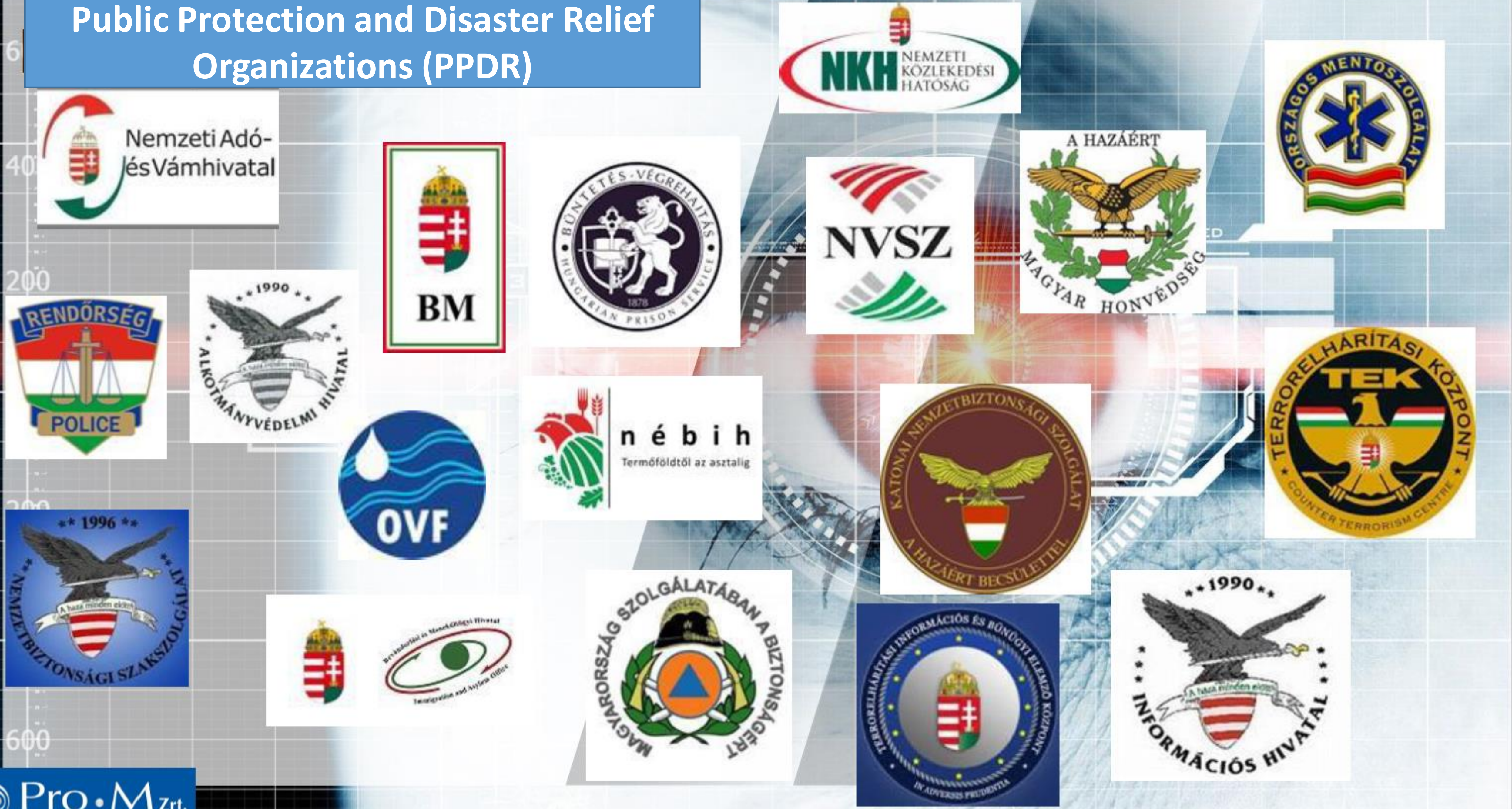
Doctoral School for Safety and Security Sciences, Supervisor: Zoltán Rajnai

Instructor: László Szabó, Head of Security Supervision, Pro-M Zrt.

BM Külső Gyakornoki Rendszer

2021. november 10.

Public Protection and Disaster Relief Organizations (PPDR)



Other Organizations (voluntary)

MOL

BKV ZRT

mvm group

BKK BUDAPESTI KÖZLEKEDÉSI KÖZPONT

MÁV

bud Budapest Airport

NEMZETI ÚTDÍJFIZETÉSI SZOLGÁLTATÓ ZRT.

NISZ NEMZETI INFOKOMMUNIKÁCIÓS SZOLGÁLTATÓ ZRT.

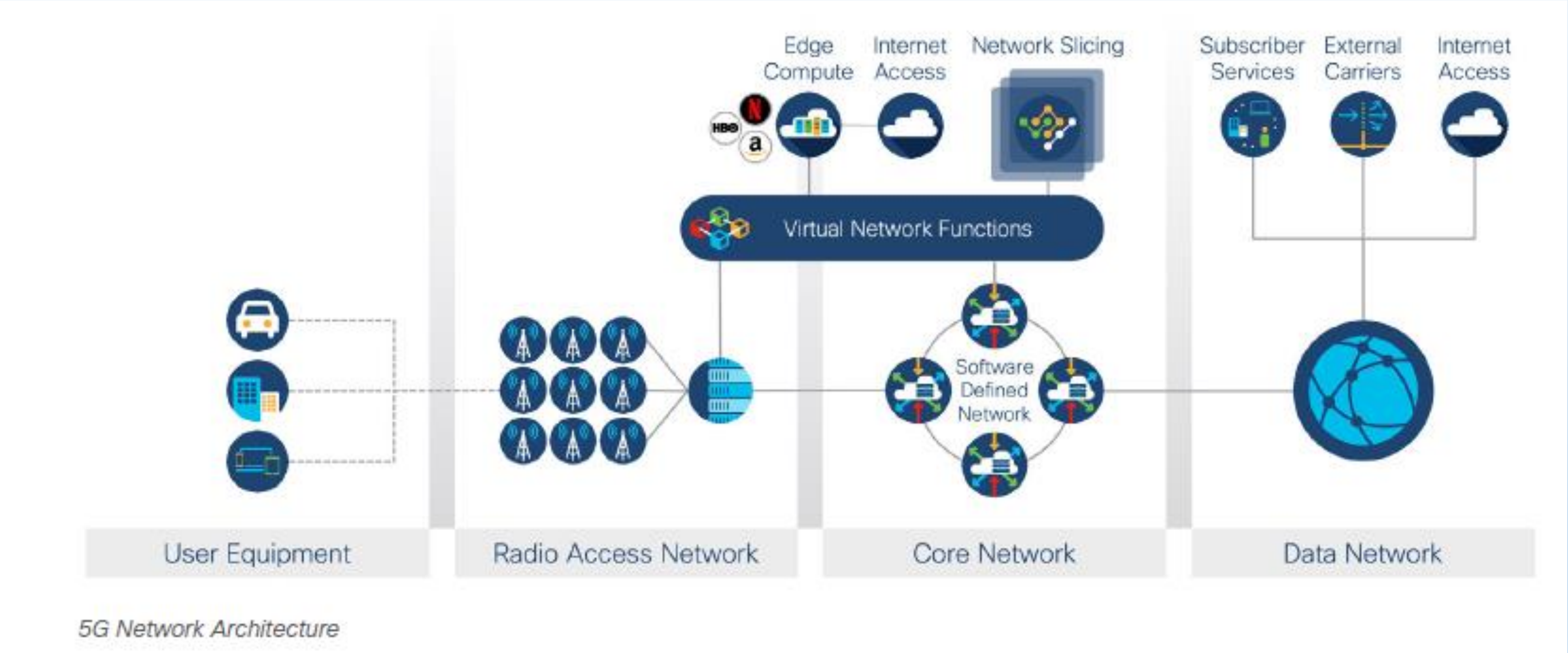
Introduction - EDR

- The TETRA-based system was built in 2006 (EDR 1.0)
- Decision about BB-PPDR in 2016, feasibility study and preparation (frequency and bandwidth allocated/reserved by NMHH), strategy was completed in 2020
- **Pro-M medium-term development strategy - EDR evolution**
  - **EDR 2.0 – BB data service (BB-PPDR) beyond TETRA voice**

    Hybrid network model, based 4G LTE technology. Own core and radio network (RAN) partly using the existing 4G/5G commercial mobile operator’s network.
  - **EDR 3.0 – Voice and Data service based on standard 3GPP network**

    The aim is to build the appropriate stand-alone, dedicated 4G/5G radio network (RAN), to integrate the TETRA radio network and to transfer traffic primarily to the dedicated radio network, and to maintain the use of the public radio network to meet ad-hoc needs.

Introduction – 4G/5G



5G Network Architecture

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-5g-cybersecurity-guidance.pdf

5G Cybersecurity Risks

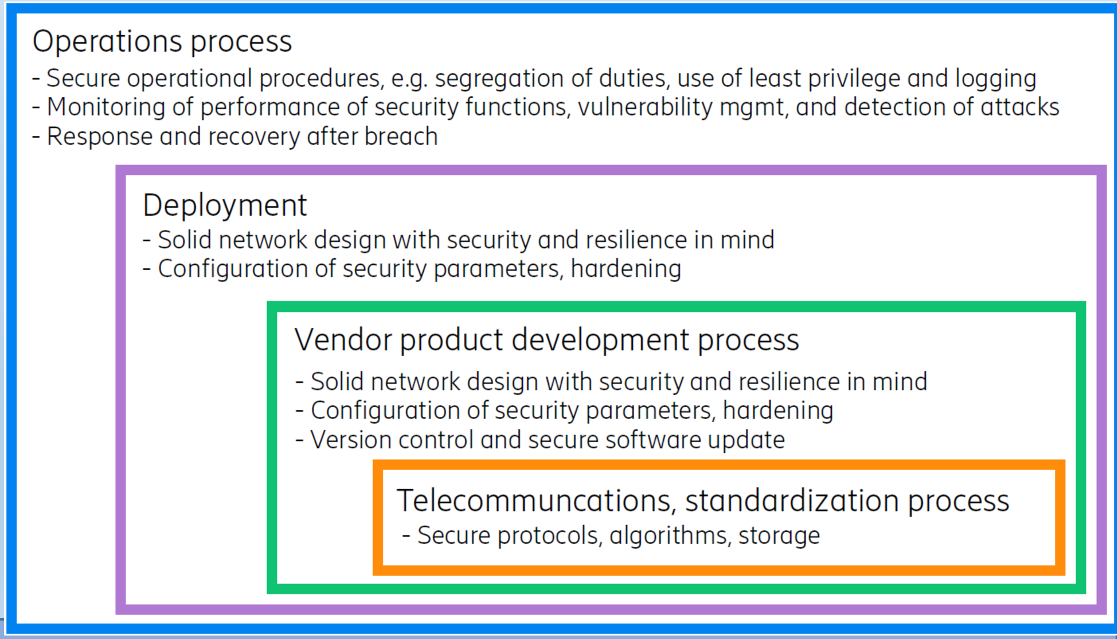
Telecommunications + enterprise networks existing cybersecurity risks + new avenues of attacks vs core network services – complex ecosystem of technologies/stakeholders/operations

- Service Based Architecture (decomposed, virtualized and distributed network functions)
- Application Based Programming IF (API)-Based Communication: communications between Service Functions for network optimization, configuration and management)
- Multi-Access Edge Computing for performance sensitive applications (operators distribute own infrastructure vs virtualized DC located near RAN access nodes vs enterprise customer DC and 3rd party cloud environments) + new attack vectors due to security management complexity

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-5g-cybersecurity-guidance.pdf

5G security challenges and considerations – Ericsson

- Comprehensive and risk-based
- Continuous process
  - Selection of suppliers– production of network elements– network operation (lifetime)
  - Consideration of non-technical factors as well – when developing the supplier's risk profile
  - Consideration of national security aspects as well
  - Minimize supply chain and supplier dependence
- Lifecycle security considerations
  - Standardization
  - Development
  - Deployment/Installation
  - O&M



Operations process

- Secure operational procedures, e.g. segregation of duties, use of least privilege and logging
- Monitoring of performance of security functions, vulnerability mgmt, and detection of attacks
- Response and recovery after breach

Deployment

- Solid network design with security and resilience in mind
- Configuration of security parameters, hardening

Vendor product development process

- Solid network design with security and resilience in mind
- Configuration of security parameters, hardening
- Version control and secure software update

Telecommuncations, standardization process

- Secure protocols, algorithms, storage

https://www.ericsson.com/en/security/a-guide-to-5g-network-security

6 recommendations for Mitigating 5G Cybersecurity Risks

Zero Trust
Integrity
Threat Protection
Visbility
Data Protection
Segmentation
5G
CYBERSECURITY

- **1. Zero Trust** – 5G infrastructure as untrusted environment – Authenticate and Authorize every assets in all areas (workforce/workplace/workload)
  - **Asset Hardening** – reduce attack surface with locking down local access controls, configuration and services
  - **AAA (authentication, authorization, accounting)** –contextual factors such: user identity, device type, geolocation. Non-user: device and application based certification-based AA
  - **Multi-Factor Authentication (MFA)** – for AA multiple and strong methods – contextual factors such device type geographical and/or network location
  - **Asset Profiling** – validate and track security posture – allow/deny based on assessed risk
  - **Traffic Encryption** –
- **2. Integrity** – validate vendor supply chain, security and secure development practices, monitor HW/SW and O&M integrity, detect infrastructure and service tampering
  - **Vendor Security Assessment:** vendor supply chain security program, secure product development and management lifecycle, vulnerability and data disclosure, overall information security practices. Direct assessment/testing of vendor
  - **Secure Boot and Runtime** – HW trust anchors SW image signing – integrity of HW/SW components. Runtime defenses against memory-based attacks such buffer overflows and code-injection
  - **Integrity Assurance**: monitor HW&SW to validate integrity and detect tampering – prompt corrective actions
  - **Operational Integrity**: policies, governance, and operational practices to detect and prevent insider abuse.

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-5g-cybersecurity-guidance.pdf

6 recommendations for Mitigating 5G Cybersecurity Risks - cont.

Zero Trust
Integrity
Threat Protection
Visibility
Data Protection
Segmentation
5G
CYBERSECURITY

- **3. Visibility:** Enable visibility across the infrastructure to identify all assets and monitor asset security logs and behavior and communication pattern analysis
    - **Asset Monitoring:** security tracking, logging, telemetry and centralized monitoring for all assets (network + endpoint + servers + applications)
    - **Anomaly Analysis:** machine learning based monitoring and behavior/communication pattern analysis. Even in encrypted traffic flows
- **4. Segmentation** end-to-end segmentation to reduce the attack surface, and limit the impact of compromise
    - **Software-Defined Segmentation:** Place assets into logical security groups that leverage network-integrated access controls and policy services to limit communication flows between groups. 5G network slicing features should be leveraged as a component of an end-to end segmentation strategy.
    - **Network and Application Firewalls**: Implement firewall gateways to inspect and explicitly allow or deny transactions between critical assets or asset groups.
- **5. Threat Protection** defensive security controls and continuous monitoring backed by machine learning capabilities, and establish incident response operations to detect and mitigate threats to assets
    - **Vulnerability Management**: effectively identify, mitigate, and remediate security vulnerabilities (e.g. software patching) in a timely manner.
    - **Denial-of-Service Defense Systems:** Monitor network traffic to detect and mitigate network flooding attacks.

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-5g-cybersecurity-guidance.pdf

6 recommendations for Mitigating 5G Cybersecurity Risks - cont.

5. Threat Protection (cont.)

- **Intrusion Detection and Prevention Systems**: Monitor network traffic to detect and mitigate unauthorized access or attempts to exploit system vulnerabilities.
- **Malicious Traffic Filtering Systems**: Monitor network traffic to block malicious or unwanted traffic such as spam or attempts to interact with malicious domains and websites.
- **Anti-Malware Systems**: Monitor network traffic and endpoint and server devices to detect and block malware files or malware execution.
- **Security Operations Center**: Establish a centralized security monitoring, incident response, and threat intelligence organization responsible for rapidly detecting and mitigating security breaches. Adopt integrated cybersecurity capabilities and automation tools that simplify and streamline security operations.

6. Data Protection and Privacy: application of policies, practices, and technical controls to protect user rights and secure data against unauthorized data access or use. Security policies and controls consistent with regulatory requirements and best practice. In the event of a breach or compromise and the mitigation and recovery procedures

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-5g-cybersecurity-guidance.pdf

EDR Evolution – Development Strategy

EDR 2.0

- ProSmart – Central data encryption and asset mgmt.
- LTE core (EPC) - own
- MVNO model - cooperation with public mobile networks (4G/5G)
- TETRA and LTE parallel used

EDR 3.0

- Deployment of a dedicated PPDR on a standard frequency
- Still use of the public radio network
- TETRA phasing out
- Integration of data and voice services

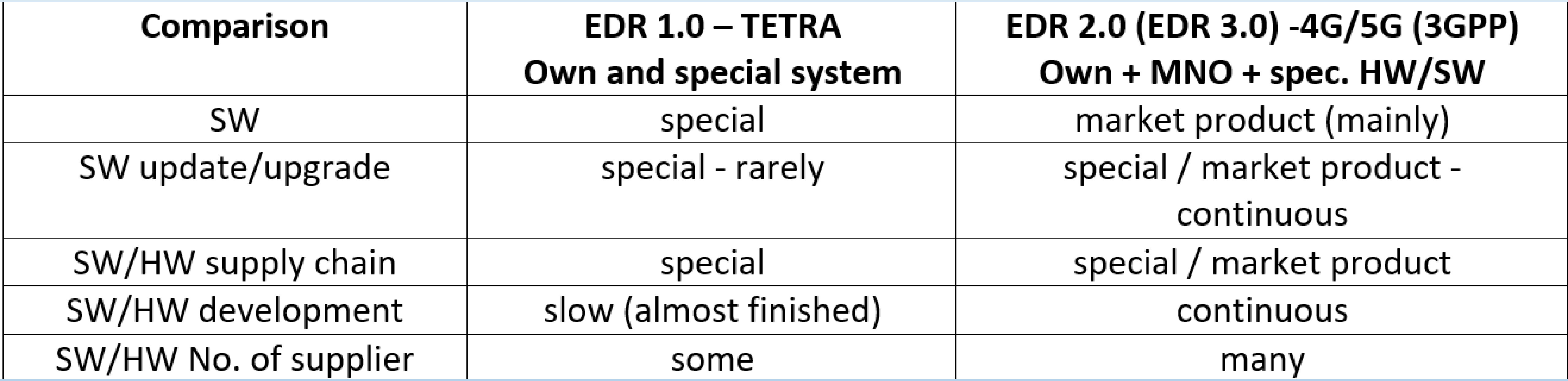
EDR 1.0 vs EDR 2.0 (3.0)

Comparison	**EDR 1.0 – TETRA** **Own and special system**	**EDR 2.0 (EDR 3.0) -4G/5G (3GPP)** **Own + MNO + spec. HW/SW**
Data stream (bit/data flow)	contains voice only	All data (voice + data)
Data validity	limited (command order)	data will remain (spoken words fly away, written words remain)
Scope of data	voice basically	voice/data/location/behavior/ special personal information personal data from Gov. DC, special personal data from health and criminal DB systems
Data Coding	special	market product/special
Data Storage	Own DB/cloud	Only in a government cloud, all data should be stored in a securely protected environment within the country

EDR 1.0 vs EDR 2.0 (3.0)?

Comparison	**EDR 1.0 – TETRA** **Own and special system**	**EDR 2.0 (EDR 3.0) -4G/5G (3GPP)** **Own + MNO + spec. HW/SW**
HW (endpoint) - TE	special	market product
HW (RAN) transmission + Radio Base Station	special	can be market product/special
HW (CORE)	special	can be market product/special
HW Owner	Own	Own/Provider (RAN/CORE)
HW infrastructure protection	Own	Own/Provider (RAN/CORE) + RAN endpoint (more intelligence)
HW size of the infrastructure	350 sites + 4 centers	RAN: even n* 100 radio sites (own + MNO provider), CORE: DC + Edge computing + Data Network

EDR 1.0 vs EDR 2.0 (3.0)?

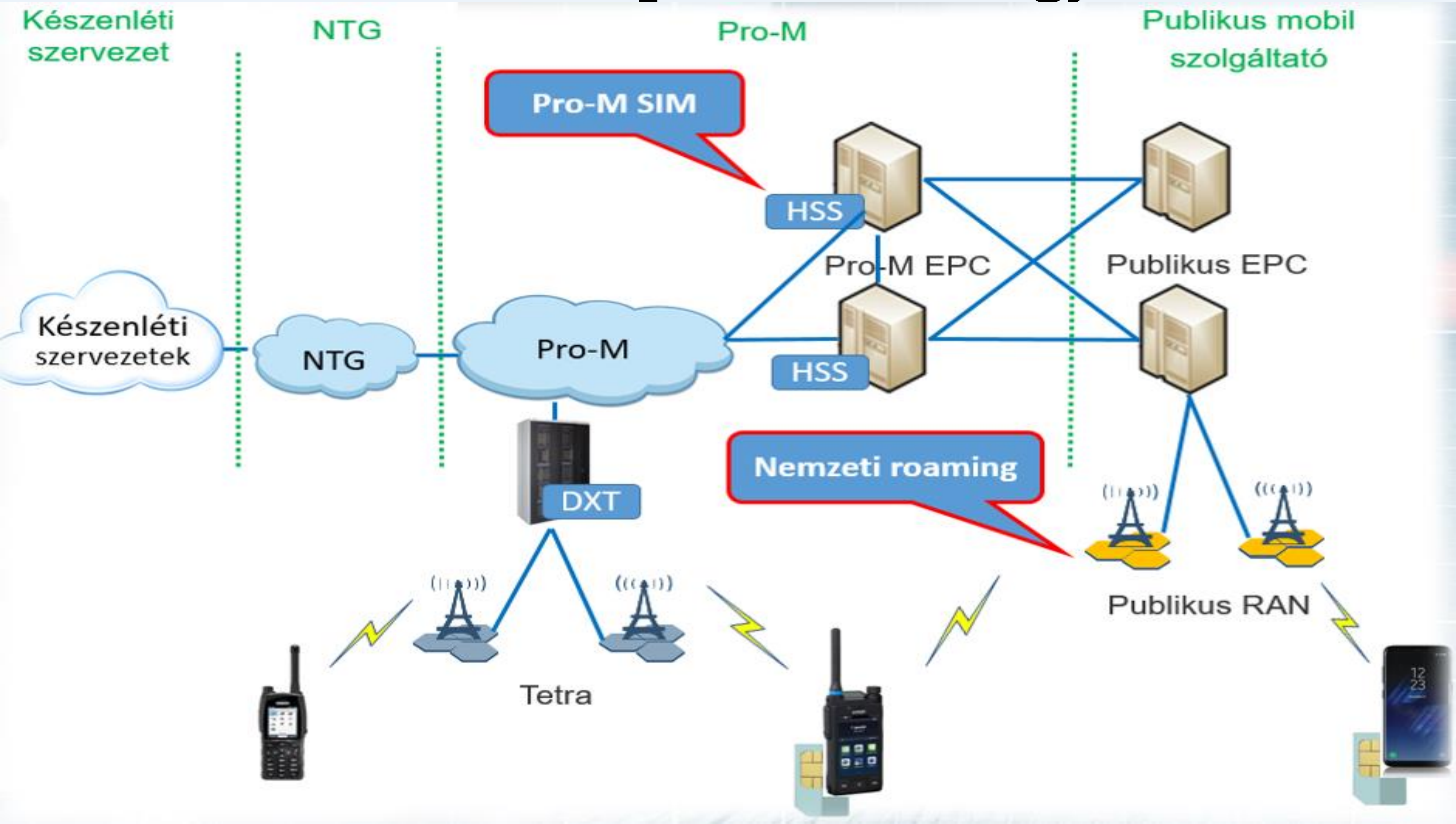


Comparison	**EDR 1.0 – TETRA** **Own and special system**	**EDR 2.0 (EDR 3.0) -4G/5G (3GPP)** **Own + MNO + spec. HW/SW**
SW	special	market product (mainly)
SW update/upgrade	special - rarely	special / market product - continuous
SW/HW supply chain	special	special / market product
SW/HW development	slow (almost finished)	continuous
SW/HW No. of supplier	some	many

EDR 1.0 vs EDR 2.0 (3.0)?

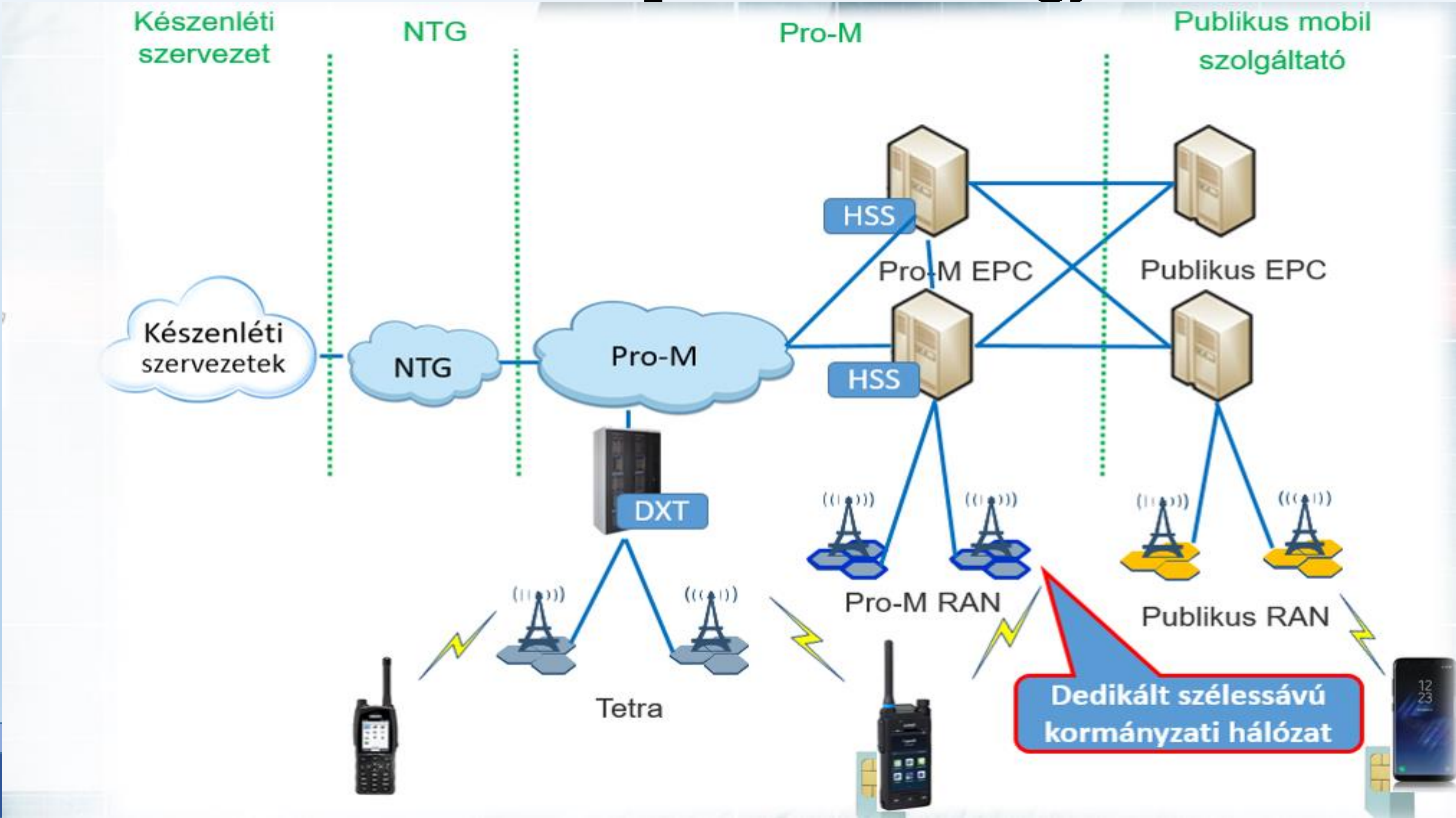
Comparison	**EDR 1.0 – TETRA** **Own and special system**	**EDR 2.0 (EDR 3.0) -4G/5G (3GPP)** **Own + MNO + spec. HW/SW**
Standardization	closed	continuous (3GPP)
Pursuit of security	continuous	continuous – part of a planned life cycle
Range of attackers	limited	can be the whole Word?
Supervision – Response/Prevention	mainly O&M – NOC + SOC response	O&M – NOC + SOC + EWS + CERTs supervision+ response + prevention + supply chain + continuous testing
Availability	Own competence, high	depend on provider (partially)
Operational safety	Own competence, high	depend on provider (partially)
Impact of system unavailability	significant	even more significant: A successful attack on the system has a significant social and political impact.

EDR 2.0 - Development Strategy

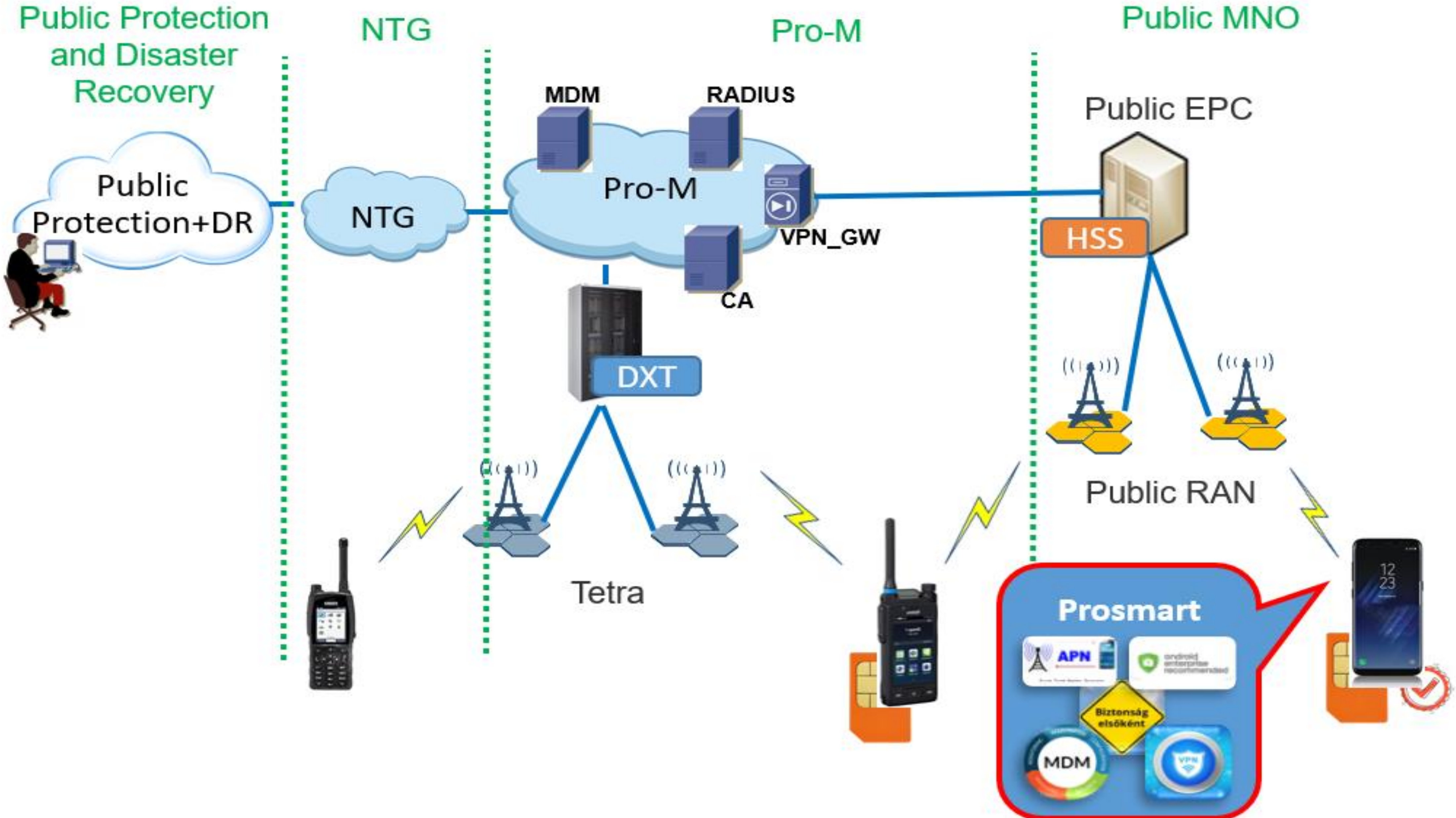


Pro • M Zrt.

EDR 3.0 - Development Strategy



EDR 2.0 – ProSmart framework



Conclusions? – Curiosities?

Paks 1 – EDR 1.0 - 346/2010. (XII. 28.) Korm. Rendelet a kormányzati célú hálózatokról

Paks 2 – ongoing change of 346/2010 - EDR 2.0/EDR3.0?

Thank you for your attention!

Questions?