The EECC and NIS2 impact on telecom operators

@ENISA Telecom Security Forum

Paolo Grassia, *Director of Public Policy*

Athens, 13 October 2021

@ETNOAssociation #ThinkDigital #ETNODigital

ETNO Members 2021

Albania

Austria

Belgium

Bosnia and Herzegovina

Bulgaria

Croatia

Cyprus

Denmark

Finland

France

France

Germany

Greece

Hungary

Iceland

Italy

Luxembourg

Macedonia

Malta

Netherlands

Netherlands

Norway

Poland

Portugal

Romania

Serbia

Slovakia

Slovenia

Spain

Sweden

Switzerland

UK

ETNO Observers 2021

Observers are telecommunication network operators from outside Europe or equipment manufacturers. They may attend all or part of ETNO activities, on an ad-hoc basis.

China

Finland

Italy

Sweden

USA

USA

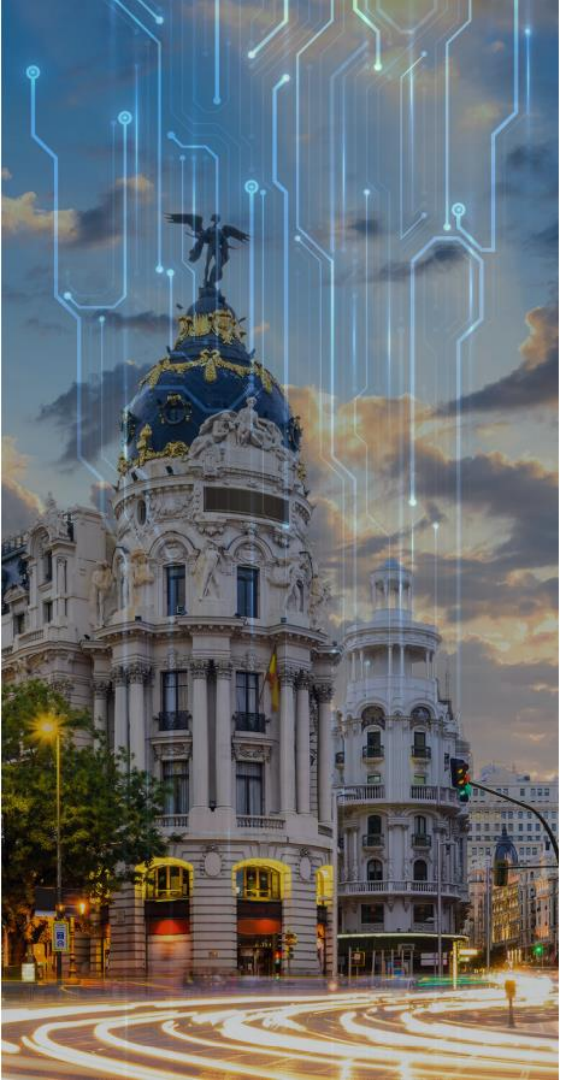
USA

USA

Overview

The EECC and NIS2 impact on telecoms

1. The EECC and its Implications
2. A complex legal environment
3. NIS2: opportunities & risks



1 | The EECC and its Implications

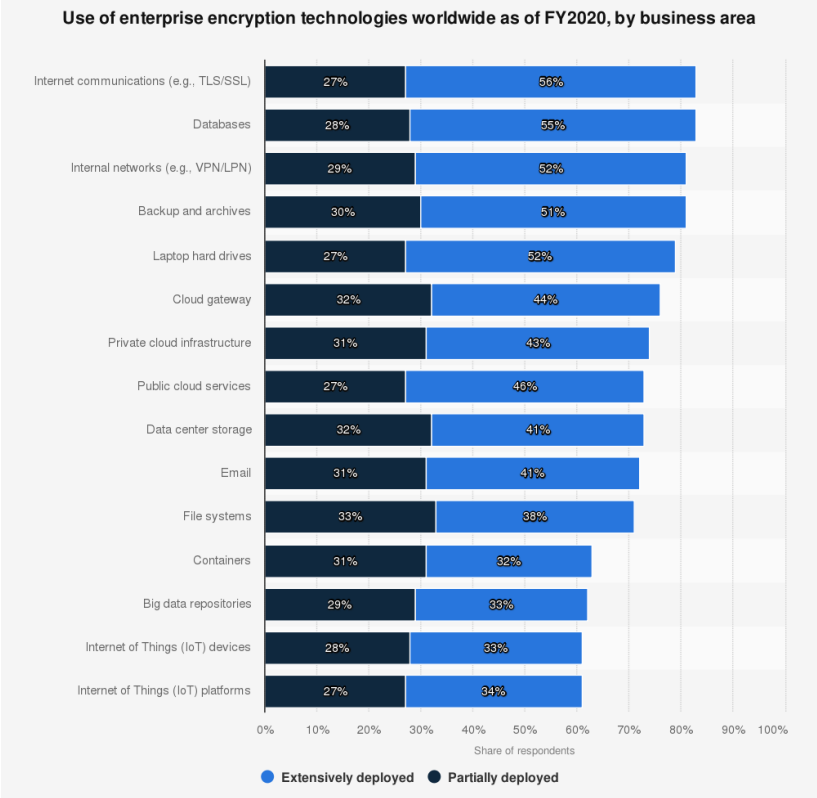
Evolution of the Legal Framework

Framework Directive *Art. 13a & 13b*	EECC *Art 40 & 41*
• Technical and organisational **risk management measures** ('state of the art'; risk-based approach) • Ensure continuity of service over telecom networks • **Notification** of security breach or integrity loss with significant impact • NRA notification to foreign NRAs, ENISA, and the public if needed • Commission implementing acts • NRAs empowered to issue **binding instructions**, e.g., on remedies • NRA information gathering, audit, and investigation powers	• Clear **definitions** of security and security incident, baseline measures • Emphasis on **encryption** • Notification **parameters** to appraise significance of the incident • Information to users about **significant threats** and remedies • Role of ENISA in promoting **harmonisation** • Stronger **cooperation** with LEAs, DPAs, other competent authorities, and CSIRTs • Contractual information requirements (Art 102)

etno

Encryption: an Unstoppable Reality

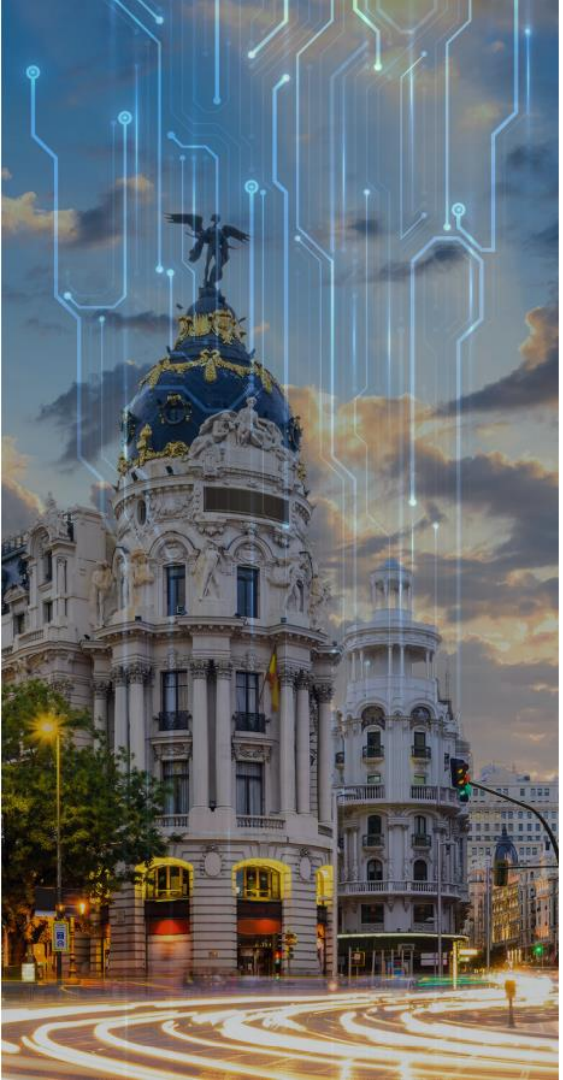
- **Encrypted web traffic** boom from some 50% in 2015 to over 90% today.
- **Key developments**: HTTPS and HTTP/2, TLS 1.3, optical encryption, 4G LTE networks.
- Leap forward with **5G**: encryption of user's identity and location



Source: Statista, 2021

Security Breach Reporting

- Current situation: **deadline** often immediate; specific X-hour deadline or ‘without undue delay’ in some countries.
- Telcos must typically notify **NRAs**. Cybersecurity agencies and (rarely) ministries and national CSIRT might also be notified.
- EECC: **Significance parameters** (users, duration, spread, functionality, broader impact) valuable, but no thresholds [see NIS].
- Challenges of **user information** about significant threats.



2 | A Complex Legal Environment

EECC Implementation Lagging Behind

24 Member States hit by infringement proceedings in February 2021

GREEN – all legislative steps taken and EECC is fully implemented
(**Bulgaria**, **Denmark**, **Finland, France, Hungary**)

ORANGE – EECC partially implemented, meaning that the main piece of legislation has been implemented / adopted, but either ancillary regulations need to be enacted to fully implement or the date for the legislation entering into force is in the future
(**Germany, Greece**, **Netherlands**, **Poland, UK**)

RED – no formal implementation of any EECC related legislation though the legislative process is being moved forward through public consultations or public circulation of draft legislation
(**Austria**, **Belgium**, **Croatia**, **Cyprus**, **Czech Republic**, **Estonia**, **Ireland**, **Italy**, **Latvia**, **Lithuania**, **Luxembourg**, **Malta**, **Portugal**, **Romania**, **Slovakia**, **Slovenia**, **Spain**, **Sweden**)

Source: Connect On Tech, 2021

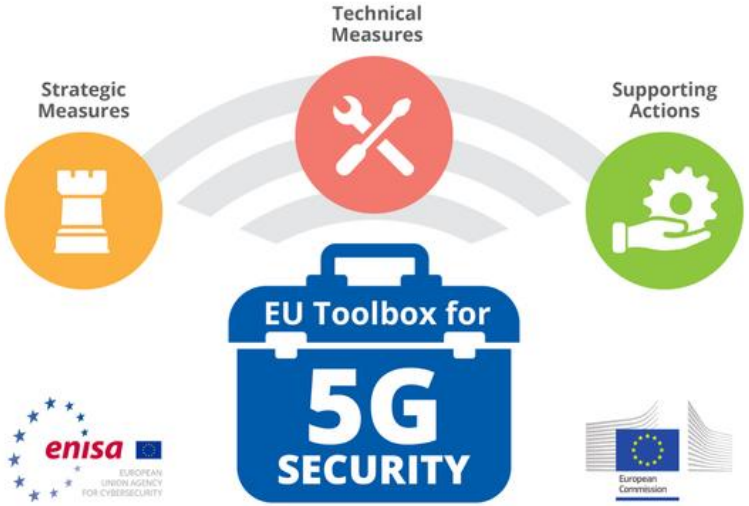
Intricacy of Applicable Rules

- Telcos can be regulated by the **NIS Directive** as IXPs or cloud providers (digital service providers). Some Member States have even identified telcos as Operators of Essential Services.
- Security breaches and **data breaches** frequently coincide. Compliance with GDPR and e-Privacy Directive.

Example: Reporting Obligations

- Different competent authorities and deadlines (data breaches: notification to DPAs within 72 hours).
- Different guidelines, procedures, report forms.

An Evolving Legal and Policy Framework

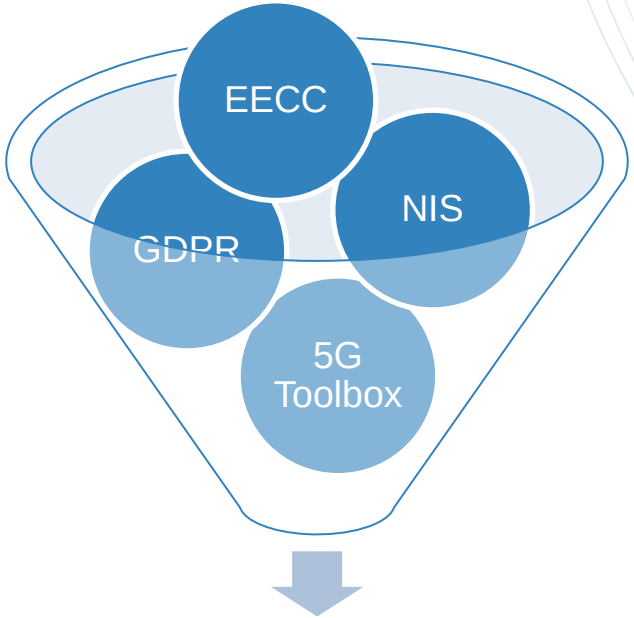


- Most EU countries have introduced new security rules for **5G networks**
- Minimum security requirements and restrictions on **high risk vendors**
- New initiatives or amendment to existing telecom law

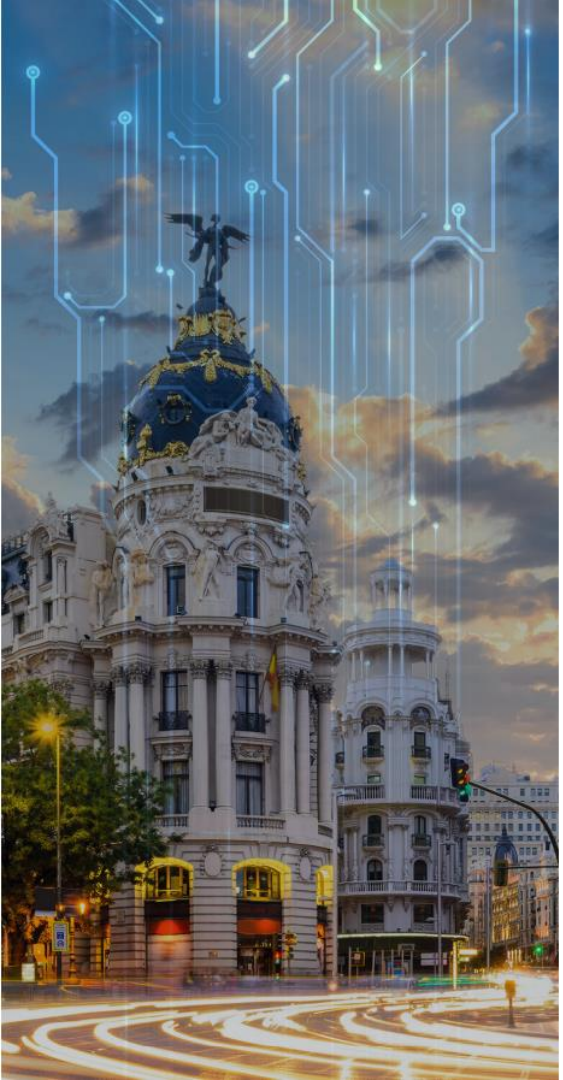
Source: ENISA, 2020

etno

An Evolving Legal and Policy Framework



Need for Consistency & Harmonisation



3 | NIS2: Opportunities & Risks

An Opportunity for Harmonised Rules

- Inclusion of electronic communication providers in scope of horizontal rules and repeal of the EECC security provision.
- National guidelines and legislation for the implementation of the EECC security provision can be maintained to apply NIS 2.

Need for EU-wide guidance and legislation to avoid inconsistency and promote greater harmonisation

Reporting obligations

A carefully drawn perimeter is the key to relevant and proportionate notifications

EECC *Art 40 & 41*	NIS 2 *Art 20*
• Notification of **security breach or integrity loss** with significant impact • Notification **parameters** to appraise significance of the incident • Information to users about **significant threats** and remedies • NRA notification to foreign NRAs, ENISA, and the public if needed • NRAs empowered to issue **binding instructions**, e.g., on remedies and threat prevention measures • Commission implementing acts • Clear **definitions** of security and security incident, baseline measures	• Notification of incident with significant impact and **significant cyber threats** to CA/CSIRT and users if needed • Definition **significance** of an incident • Staged deadlines (**24h** for initial notification; 1 month for final report) • Compulsory **feedback** by CA/CSIRT • CA/CSIRT notification to other Member States and ENISA, and the public if needed • Commission implementing acts to specify information, format and procedure of notification, and to define significance

The Crucial Role of ICT Supply Chain

Figure 5: Root cause categories – Telecom security Incidents in 2020

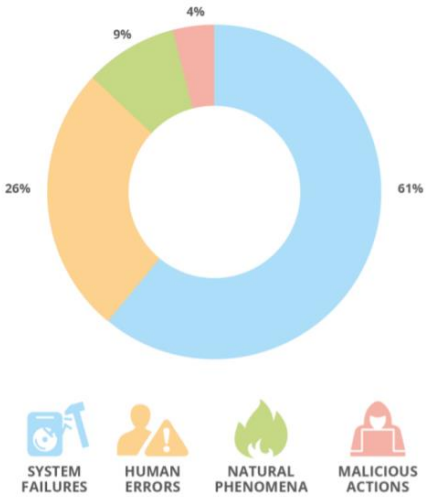


Figure 6: Root cause categories – Telecom security Incidents in 2020

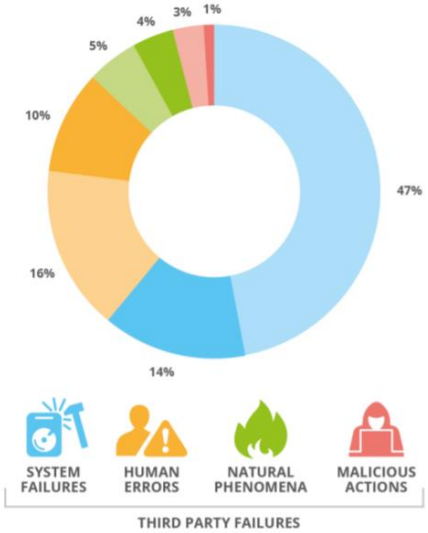
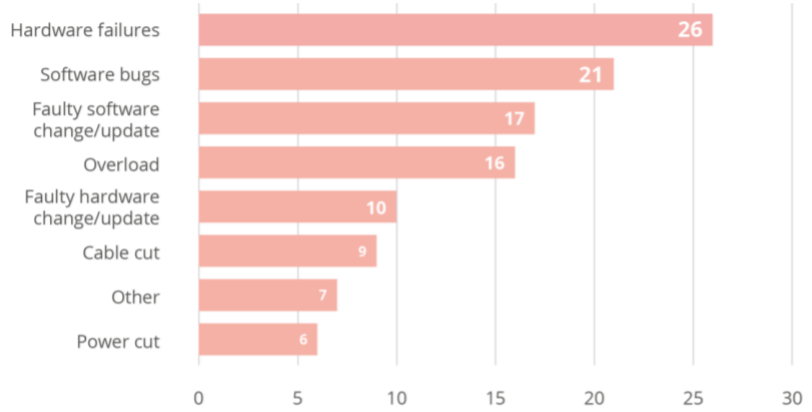


Figure 9: System failures – detailed causes



Source: ENISA Telecom Security Incidents 2020

Closing the ICT Supply Chain Gap

- EU coordinated risk assessments of critical supply chains and involvement of ICT manufacturers and service providers in Coordinated Vulnerability Disclosure is insufficient.
- **ICT providers** are best placed to address cyber risks in their own products, services, and processes.
- Expand the scope to introduce **risk management obligations** upon ICT providers that offer products of services for the critical functions of regulated entities.

Conclusive Thoughts

- ✓ **The EECC**'s limited, yet important innovations have yet to be put to the test due to slow implementation.
- ✓ **Regulatory fragmentation** affecting the telecom sector calls for greater consistency and harmonisation.
- ✓ **NIS2** offers an opportunity for a coherent framework, but its rules need improving to increase in effectiveness.
- ✓ **The key role of the ICT supply chain** in determining the resilience of digital infrastructure should be properly addressed.

etno

European Telecommunications
Network Operators' Association

info@etno.eu
Tel: +32 (0)2 219 3242

www.etno.eu