Ref. Ares(2025)2193540 - 18/03/2025

BoR (25) 36

Summary of the BEREC Stakeholder Workshop on Network Resilience

—

19 November 2024

13 March 2025

Contents

1. Introduction and aim of the Workshop

In 2024 the BEREC Cybersecurity Working Group (CS WG) was tasked to identify the most relevant cybersecurity and resilience issues and challenges that need to be addressed in an external workshop in order to discover good practices and experiences worth sharing. For that purpose, in April, the CS WG conducted a survey requesting network operators to provide information on a number of questions related to resilience, the use of satellite systems, and protection of submarine cables, multivendor strategies and security approaches taken by the operators. This survey helped to identify some of the most relevant issues and challenges. After the analysis of the responses the CS WG decided to organize two external workshops, first one - in 2024 focused on resilience and a second one - in 2025 with focus on challenges related to technological advancements.

On 19 November 2024 the BEREC CS WG held the first workshop in the envisaged set of the planned two workshops - Stakeholder Workshop on Network Resilience.

The overall purpose of this workshop was to raise awareness of the current resilience and security related challenges among NRAs, operators and other stakeholders by bringing them together to exchange experiences and best practices. The lessons and insights learned from the workshop are presented in this summary report.

2. Opening of the workshop

The Co-Chairs of the BEREC Cybersecurity Working Group, **Katja Kmet Vrčko** (AKOS/Slovenia) and **Zdravko Jukić** (HAKOM/Croatia) welcomed all participants and opened the workshop by explaining the structure and house rules of the workshop before introducing the keynote speaker of the workshop, Mr **Hrafnkell V. Gíslason**, Managing Director of Electronic Communications Office of Iceland (ECOI).

In his keynote speech, Mr Gíslason underscored the critical need for resilient communication networks amidst increasing societal reliance on digital infrastructure, convergence to systems like 5G, geopolitical tensions, and natural phenomena related disasters. He presented a spectrum of cyber and physical threats challenging network stability and the essential role of National Regulatory Authorities (NRAs) in overseeing resilience, despite current regulatory limitations. Mr Gíslason highlighted the problem related to funding of resilience enhancements and the question of a “market failure”. He concluded by advocating for a harmonized European effort, guided by BEREC, to improve understanding and practices around cybersecurity and network resilience.

After the keynote speech, the workshop proceeded with the two panels:

The first panel, The National Perspectives on Resilience and Coordination, covered three country case studies from Iceland, Norway and the United Kingdom, while the second panel, "Solutions for Resilience", presented solutions from operators (A1 Slovenija, Vodafone Group and ASTRID Blue Light Mobile) as well as from the European Emergency Number Association (EENA).

Following the panels, representatives of the European Union Agency for Cybersecurity (**ENISA**), **Dr Georgia Bafoutsou,** Cybersecurity Officer and **Dr Marnix Dekker**, ENISA Head of sector for the NIS Directive, gave an overview of ENISA's work related to the building up of the cybersecurity and resilience in the EU's telecom sector.

3. Panel 1: The National Perspectives on Resilience and Coordination

3.1. Resilient and robust networks in Iceland

The first to speak on the panel was Mr Njörður Tómasson, Network Specialist and Project Manager at the Icelandic national regulatory authority **ECOI**. Mr Tómasson presented ECOI’s project to develop a strategy for building **resilient and robust networks in Iceland** that includes goals and measurable targets for the next decade (2024 - 2034). Mr Tómasson firstly illustrated the consequences of network interruptions of fixed and mobile networks, by presenting some recent cases of fiber cables being cut or power outages that led to significant blackouts in different parts of the country. He stressed that its strategy is intended to prevent or minimise the impact of such incidents in the future.

In order to achieve its goal of guaranteeing resilient and reliable networks, ECOI has laid out a set of **measures and requirements** which include ensuring physical separation between fiber paths, having multiple Points of Presence (POPs) in larger communities, increasing the number of nationwide autonomous transmission networks, and providing at least two independent broadband connections to households and businesses. These measures at national level are to be complemented by specific measures to ensure **international connectivity** through a minimum of four submarine cables and satellite connections for critical infrastructure and emergency restoration.

All these measures are designed to:

- Prevent total outages and ensure uninterrupted service if one network fails.
- Enhance reliability and resilience by minimizing risks of single points of failure.
- Increase redundancy and failover capabilities by providing backup systems to maintain connectivity.
- Provide continuous service by guaranteeing uptime for all users, including critical infrastructure.

This comprehensive approach aims to create a robust network infrastructure that improves resilience of Iceland’s connectivity against all types of failures or disruptions.

For all these measures and requirements, ECOI takes into account the **level of urbanisation**, which means that requirements for larger towns or cities are higher than for small rural communities. i.e. more separate fiber paths, POPs or autonomous transmission networks.

Key messages:

ECOI's strategy for enhancing Iceland's network infrastructure resilience over the next decade is to focus on reliability through redundancy, physical separation of fiber paths, multiple POPs, autonomous networks, and ensuring dual broadband connections and international connectivity with submarine cables and satellite links.

3.2. Diversified challenges call for diversified responses

The second presentation in the Panel on „National Perspectives on Resilience and Coordination“ was held by Mr Johan Foldøy, Chief Engineer in the Security department of the Norwegian Communications Authority (**Nkom**).

Under the title “**Diversified Challenges Call for Diversified Responses**” Mr Foldøy started by presenting a collection of specific incidents and challenges in the last few years.

Two incidents concerned subsea cables, namely a damaged scientific cable as part of a system to monitor the chemical condition of the deep sea and a damaged optical cable carrying traffic from an island called Svalbard to the Norwegian mainland including traffic from numerous antennas at Svalsat, the world’s largest satellite ground station. These incidents were investigated and the reports were published. While fishing boats were reported as being in the area at the relevant time, the investigations led to no conclusions as to who/what caused the incidents.

Another recent incident concerned damage to a fiber cable just before the beginning of an important stress test during which organizations and companies from all over the world were planning to test the response of their systems to so-called “jamming” attacks. The investigation of this incident outside easily accessible areas led to no definitive conclusions.

Mr Foldøy then laid out Nkom’s work on **regional risk and vulnerability analyses**. In 2019, Nkom started to map infrastructure that is important for both national and regional communications. Travelling through the regions – from the north to the south of Norway – Nkom employees inspected the infrastructure in order to identify weaknesses and vulnerabilities.

Mr Foldøy emphasized that the changes in the security policy situation and climate challenges underline the need for a secure and robust digital infrastructure. He presented Nkom’s proposed **Security Plan 2025-2030** setting out a catalogue of important goals for the next five years, addressing cybersecurity as well as resilience aspects. These include measures to strengthen the resilience of mobile networks by increasing battery backup and ensuring redundant transmission to targeted base station locations, to increase cooperation between power companies and electronic communications sector, to strengthen redundancy and autonomy of the transmission networks, to increase capacity against ever-increasing data- and cybercrime / attacks and to enhancing preparedness.

Finally, Mr Foldøy concluded with a summary of the main **present and future challenges** for the electronic communications sector:

- dependencies and concentration in value and supply chains,
- security of marine fiber cables,
- extreme weather,
- sabotage and cyber-attacks,
- change management in general.

In the **Questions and Answers** section, Mr Foldøy addressed the challenges in facing extreme weather conditions, such as regional flooding. Both forecasting and early warning systems play a key role in applying most appropriate mitigation measures. While it is important to roll out backup solutions and equipment quickly in these cases, the safety of the involved personnel must always be considered.

When asked what he wanted to highlight as focal points for increased resilience Mr Foldøy underlined the importance of the core part of networks (i.e. transport networks) and of redundancies.

Key messages:

Mr. Foldøy highlighted the importance of robust digital infrastructure in Norway, addressing challenges from damaged cables to cyber threats. Nkom's regional analyses led to the proposal for a Security Plan prioritizing mobile network resilience, power back up, redundancy, and preparedness against cybercrime and extreme weather. Key challenges include supply chain dependencies, cable security and adapting to changes. The importance of core network parts and of general redundancies was emphasized.

3.3. Network Resilience in the UK

Ms Gina Baikenycz, the Principal Technology Advisor for Network Resilience from the United Kingdom’s Office of Communications (Ofcom), held the final presentation in the first panel.

Ms Baikenycz provided the workshop participants with a concise overview of Ofcom’s recently published Resilience Guidance and the role Ofcom plays in monitoring network resilience.

She first laid out the **regulatory framework in the UK –** with primary legislation providing overarching obligations for telecommunications operators to take appropriate and proportional measures to manage their **security risks and resilience risks** and secondary legislation setting out measures that are more detailed. Additionally, the UK government published statutory guidance, the Telecommunications Security Code of Practice. Together with a procedural guidance laying out Ofcom's monitoring and enforcement activities and incident reporting processes for industry, this framework focuses mainly on cybersecurity. Since communications providers also have a legal obligation to identify, prepare for and reduce the risk of anything that compromises the availability, performance or functionality of their network or service, Ofcom published an updated Resilience Guidance in September 2024 after public consultation[1].

The new **Resilience Guidance** provides greater clarity and detail on how operators and providers of public electronic communications networks and services can comply with their resilience- related duties resulting from the legislation.

The measures in the guidance reflect the changing nature of resilience risk, society's increased reliance on connectivity, lessons learnt from outages in and beyond the UK as well as Ofcom's experience with incident reporting and incident investigations over the past years. The Guidance focuses on addressing risks related to service availability, dealing with risks resulting from weather events, hardware failures and internal process failures. The Guidance is structured into three main areas: network infrastructure domains, logical plans and services, process tools and training.

Specific measures detailed in the guidance address include, among others:

- the training of staff,
- ensuring that networks are designed to avoid or reduce single points of failure impacting a significant number of customers
- ensuring built-in automatic failover functionality for key infrastructure points,
- power backups,
- management of supply chains
- maintaining clear lines of responsibility
- building of infrastructure resilient to physical damage
- thorough testing of new software

[1] Network and Service Resilience Guidance for Communication Providers, 6 September 2024, https://www.ofcom.org.uk/internet-based-services/network-security/resilience-guidance/.

The Resilience Guidance is prepared to serve as a practical reference for industry on how UK telecoms providers are expected to reduce the risk and impact of network or service outages. Ofcom intends to use the guidance (1) in information gathering and monitoring of network and service resilience when engaging with communications providers and the wider industry and (2) as a starting point for considering compliance as part of any enforcement activities in relation to resilience issues.

Ms Baikenycz then proceeded to give an update on **Ofcom's approach to power resilience in mobile access networks**. With an increasing reliance on mobile services it is becoming more important that mobile networks are resilient.

One key risk stems from the dependence on the connection to UK main electrical power. For this reason, Ofcom published a **call for input** to prompt a discussion on what power backup mobile network operators can and should provide for their networks and services. The call for input inquired what services should be provided during an outage as well as what users' needs are during an outage and finally what steps are needed to address these needs. Ofcom has received feedback that shows a great deal of interest in the topic of mobile network resilience. It also highlighted the **need for better cross-sectoral coordination and information sharing** (in particular between energy and telecommunications sector) when striving for resilience.

To conclude, Ms Baikenycz underlined that Ofcom's work to address this issue is ongoing: Information from network operators as well as international best practices have been collected and analyzed. Established best practices have been included in Ofcom's Resilience Guidance. Ofcom will continue to closely collaborate and coordinate with the energy sector (both industry and regulatory authority) in order to improve resilience in cases of power outages.

Key messages:

Ofcom's updated Network and Services Resilience Guidance for UK network operators focuses on non-cybersecurity, service availability, and resilience against various risks. Ofcom emphasizes the need for industry compliance, staff training, robust infrastructure, and cross-sectoral coordination, particularly with respect to mobile network power resilience in response to power outages.

4. Panel 2: Solutions for Resilience

4.1. Resilience of critical infrastructure – in the aftermath of catastrophic floods in Slovenia in August 2023

The Slovenian mobile operator A1 Slovenija (herein: A1) was represented by two speakers Ms Špela Dekleva and Mr Luka Šušteršič, who covered on one hand the **legislative and**

regulatory background and **technical aspects of the crisis management** during the 2023 floods.

Legislative and Regulatory Background

In the aftermath of the catastrophic 2023 flooding in Slovenia, in order to improve critical infrastructure resilience, A1 suggested reviewing the existing national legislation (which involves three different legal/operational regimes with three different state administrations in charge). The Electronic communication sector is amongst the most important pillars of critical infrastructure. Operators are therefore required to deal with many different challenges during different national crises. In such situations, reaction time and cooperation of all stakeholders under the lead of one competent authority, which coordinates the activities is crucial for fastest restoration of services. General (legal) obligations put on the operators in such situations must be reasonable and proportionate (e.g. mobile roaming obligation).

In summary, A1 suggests that single legislative environment that covers all relevant stakeholders' cooperation would work best for crisis management.

Telecommunications Crisis Management during the 2023 Floods

Between 4 and 5 August 2023 Slovenia experienced enormous electronic communication networks outages due to flooding across the entire country. The power and transport infrastructure including electronic communications (especially RAN, but fixed as well) was severely damaged. The impact to the A1 network resulted in significant network outage across almost entire Slovene regions.

The immediate actions taken by A1 were as follows:

- activation of A1.SLO Crisis Team;
- focus on internal and external communications;
- cooperation with civil protection, police and army;
- recovery of power supplies;
- transport to inaccessible areas and
- close cooperation among the operators.

The focus was fast reactivation of the service. By Monday August 7, over half of the affected sites were restored, except for locations in the northern part of Slovenia due to the inaccessibility of the terrain by road and limited possibility to transfer very heavy loads (such as generators) by helicopters. To continue providing services to the subscribers in those areas, regionally limited roaming was recognised as the best solution. Within one day, A1 together with Telekom Slovenija successfully developed, tested and deployed a technical solution and delivered services to the subscribers in the affected areas. The lessons learnt by

A1 included a need for clear KPIs for public warnings, a need for internal and external communication protocols and availability of transportable power generators. In addition, the need for redundancy measures to mitigate risks of fibre cuts and backup microwave transmission paths was noticed. The operator learned that there are limitations to the capacities of a roaming service and to a free data service for subscribers during a crisis.

Key messages:

Because of the 2023 Slovenian floods, all operators faced a major network outage. Significant number of A1 sites were affected. Prompt crisis management included activating a specialized team, prioritizing communications and collaborating with State's emergency services to restore power and physical access. While services were restored on over half of the sites relatively swiftly, inhabitants (A1 customers) in another part of the country received them later via quickly established roaming with another operator. Challenges faced and highlighted by A1 were the need for established clear crisis communication protocols, availability of transportable power generators and redundancy contingency plans. Enabling regional roaming and offering free subscriber data during crises to maintain service continuity proved beneficial in providing access to services.

4.2. Vodafone's Technology Resilience Programme

Vodafone representative, Mr **Ettore Genta**, provided a detailed analysis of Vodafone's strategy for strengthening the resilience of its networks in the face of increasingly complex risks, including natural disasters and cyber-attacks. This strategy is guided by a clear technology resilience policy that defines risk scenarios, scope and service level objectives aligned to the company's risk assessment.

The importance of resilience due to the scale of Vodafone's global technological footprint was emphasized in the presentation. In the presentation, they showed some insights from the past incidents, such as a 2011 fire in Rotterdam, which highlighted the importance of robust disaster recovery measures. This was the input for the **Technology Resilience Programme**, which has evolved since to cover all aspects of the network, including fixed-line services, mobile platforms, and TV services. The resilience measures are now integrated into network design. Defense plan is based on three pillars: **Prevention**, **Reaction**, **Governance**. Emergency Power and Fibre redundancy for **Prevention** and Distributed Network setup, highly meshed backhaul network and On Site Intervention (Truck-based Disaster Recovery solution to intervene where Examples included geo-redundancy) for **Reaction**. 10 technical recommendations like constant risk assessments, recovery plans, and resilience testing and internal policies form the **Governance** pillar. Third-party collaboration to ensure that recovery operations run smoothly is very important. Vodafone's representative also stressed the **value of preparedness during "peace times,"** enabling teams to act swiftly in times of a crises.

An example of the programme's effectiveness was a fire incident in Italy, where traffic was seamlessly rerouted to alternate sites, ensuring that 95% of customers experienced no service disruption. Specialized vehicles and equipment, such as mobile protection units and recovery vans, play a crucial role in addressing failures in challenging environments.

Lastly, Mr Genta presented Vodafone's "**Instant Network**" initiative, which supports remote communities and disaster-stricken areas by providing connectivity. This programme, run by trained volunteers, ensures access to education and communication in underserved regions and during emergencies. It was used recently in Valencia during the tragic floods in October.

The presentation concluded by highlighting Vodafone's commitment to connecting communities and maintaining essential communication services through a systematic and innovative approach to resilience. This strategy combines advanced technologies, detailed governance principles, and dedicated human resources to mitigate the impact of disasters effectively.

Key messages:

Vodafone has implemented a comprehensive Technology Resilience Programme to enhance network robustness against risks like natural disasters and cyber-attacks. The policy outlines risk scenarios and objectives, emphasizing proactive measures integrated into network design for resilience, such as geo-redundancy and detailed recovery plans. Effective risk assessment, change management, and collaboration are crucial. Additionally, Vodafone's "Instant Network" initiative provides vital connectivity to remote and disaster-affected areas by supporting and maintaining communication services through innovative and systematic resilience strategies.

4.3. Network resilience for emergency communications

The European Emergency Numbers Association (EENA), represented by Ms **Cristina Lumbreras**, EENA Technical Director, is an NGO focused on public safety and emergency communications. EENA promotes the 112 emergency number and promotes the improvement of emergency services such as advanced mobile location, eCall, public warning systems and network resilience amongst others. It collaborates with various stakeholders in the field.

The request for emergency assistance is often the result from a crisis when accessibility to emergency services must be guaranteed. This implies that resilience of the telecom network is of the utmost importance as enables access to emergency services.

However, telecom networks and emergency services face significant challenges. Disruptions due to **Climate Change** (extreme weather events, such as floods and storms), **Geopolitical Threats** (cyberattacks and supply chain disruptions), **Technological Transitions** that shift legacy systems to IP networks and bring new vulnerabilities. Shutting down legacy networks will influence network redundancy and by extension also the emergency services.

Real-Life Incidents Highlighting the Need for Network Resilience

EENA supported its stance by referencing two major incidents where the emergency services outage was caused by the widespread network disruption. One occurred in Australia, the other in the UK. Both cases revealed that inadequate network design and management led to failures that affected countless people relying on emergency services.

These incidents emphasize the need for:

Robust Network Design: Ensuring that all network components, particularly those specific to emergency services, are resilient and redundant, **Component Verification:** Regular testing and validation of all network components to ensure they function correctly in emergencies;

Efficient Procedures and Training: Establishing well-defined protocols and training personnel to execute them swiftly and accurately during crises and **Stakeholder Communication:** Prompt notification to all relevant parties helps manage expectations and facilitates coordinated responses to network issues.

Opportunities to Enhance Resilience in Emergency Networks

EENA highlights several opportunities to strengthen telecom networks to ensure they meet the demands of emergency services:

1. **Power Resilience** Extended power back up is vital during emergencies (e.g. energy solutions, comprising of renewable power sources, battery backup and independent power sources),
2. **Emerging Technologies** The new technologies (e.g.5G and 6G) offer promising solutions whereby the satellite communication can provide vital backups when terrestrial networks fail or are overwhelmed.
3. **Traffic Prioritization** Emergency services must have prioritized access to networks during resource shortages.
4. **Better Network Design** Eliminating single points of failure through various means, primarily by adding redundancies and failover mechanisms, spreading key components across a larger geographic area.
5. **Business Continuity Plans** The importance of business continuity plans where the need to prioritize emergency services to maintain service levels during disruptions and ensure the continued availability of emergency communications is included.

In conclusion, EENA stressed that resilient networks are not a luxury but a necessity. Emergency services are only as reliable as the infrastructure supporting them.

Key messages:

EENA emphasized the importance of resilient telecom networks for reliable emergency services, highlighting the challenges from climate change, geopolitical threats, and technological transitions. EENA cited incidents in Australia and the UK as examples of network failures affecting emergency response. It advocates for robust design, regular testing, efficient procedures, and stakeholder communication to enhance network resilience. Opportunities like power resilience, emerging technologies, traffic prioritization, and business continuity plans are crucial. Ensuring robust and redundant networks is essential for the effectiveness of emergency services.

4.4. Blue Light Mobile

ASTRID serves as the operator of Belgium's national network for emergency and security services, which includes the **TETRA-based radio communications network**, a dedicated POCSAG paging system, **Blue Light Mobile** (a Mobile Virtual Network Operator or MVNO solution), emergency centers, and a training facility. Mr. Jo Dewaele elaborated on these developments and features during a workshop presentation, highlighting ASTRID's continuous efforts to enhance communication solutions for emergency and security services in Belgium.

The TETRA network was conceived to support both voice and data communications. However, given the technological limitations of the time, particularly those aligned with **2G capabilities**, its data functionality was significantly constrained by today's standards. When the development of TETRA wideband technologies stalled, ASTRID sought commercial solutions to meet growing data demands, leading to the introduction of Blue Light Mobile.

In 2014, the 1st generation of BLM was launched. This was a data-only solution with fast data communications, priority access on Proximus network and national data roaming capability. In 2017, the 2nd generation of BLM added voice communication, priority voice, pre-emption (for a maximum of 6000 users) and access class barring (ACB) on the Proximus network and international roaming. In 2022, the 3rd generation was launched following a public procurement renewal and it added 5G on Proximus network and pre-emption for all users on the Proximus network.

With the auction of 700MHz frequency bands stringent Public Protection and Disaster Relief (PPDR) requirements are **imposed** on the participants. These include a **national roaming** (with Belgian IMSI and Belgian MSISDN) on all public (700 MHz) MNOs with **priority access**, **pre-emption and ACB**. In 2025 these additional features will be included in the Astrid solution.

There are currently 12.000 BLM cards in use with the following benefits:

- access to all MNO networks with a single SIM card,
- priority access and better data performance on Proximus network,

- pre-emption on the Proximus network,
- ACB protection in case of crisis and saturation of networks.

Priority access and pre-emption will not just be available on Proximus network, but on all MNO networks in Belgium. ACB will be activated in cases of saturation, even outside of crisis situations, as also foreseen in 5G spectrum rules. Evolutions are taking place towards mission-critical data and voice, with a focus on incorporating **broadband data capabilities** into the ecosystem. The initial goal was to develop a single, unified solution that would integrate all necessary capabilities for a Mission Critical ecosystem, including group discussions, push-to-talk (PTT), video and data, fast call setup, and robust terminals with Direct Mode Operation (DMO). This unified solution aimed to provide high availability, confidentiality, and reliability, meeting the stringent requirements of emergency and security services. However, while significant progress has been made, the **current state of the regulatory, commercial, and technological ecosystem** has made it challenging to achieve this full convergence into a single solution. As a result, ASTRID has adopted a **dual-track approach** to address the evolving needs:

- **Safety critical track** with a light MVNO model. Blue Light Mobile enhanced with a focus on flexibility with features such as national roaming, QPP, BYOD flexibility, voice telco VAS, but with limitations in security, sovereignty and continuity of service
- **Mission critical track** with a hybrid solution combining a dedicated network (MCRAN) with partnerships through Mobile Network Operators (MOCN), enabling broadband data alongside mission-critical functionalities like seamless handovers, robust security, confidentiality, and integrated mission-critical applications, albeit with less flexibility for devices and applications.

Mission critical network resilience requires power continuity and autonomy, connectivity continuity and ICT service continuity and sovereignty that goes beyond the standard requirements of public MNOs.

Key messages:

ASTRID operates Belgium's national network for emergency and security services, offering TETRA radio communications, paging, and Blue Light Mobile (BLM). BLM has evolved to include broadband data, voice, 5G, and pre-emption capabilities, ensuring priority access across all MNO networks.

The future service addresses mission-critical needs through a dual-track approach: a Safety Critical Track for flexibility and a Mission Critical Track for robust security, resilience, and sovereignty. ASTRID's solutions integrate advanced features like national roaming, ACB, and QoS, aligning with PPDR requirements from the 700 MHz auction.

Future plans focus on enhancing network resilience and security to meet the evolving needs of emergency services, emphasizing collaboration between operators and regulators to strengthen European network resilience efforts.

5. ENISA's work to build up cybersecurity and resilience in the EU's telecom sector

ENISA, the European Union Agency for Cybersecurity, represented by Mr Marnix Dekker and Ms Georgia Bafoutsou, highlighted the importance of increasing the resilience of critical sectors, focusing on cybersecurity and the NIS2 directive, outlined ENISA's role and activities in this area.

First, they presented ENISA’s role in implementing the cybersecurity regulation and outlined the main operational collaborations and tasks performed by ENISA. They also summarized the EU policies regarding cybersecurity, explaining where ENISA has a leading role and who are the main stakeholders.

In the presentation, there was an overview of the main cyber threats for the European Union, such as DDos attacks, ransomware attacks, supply chain attacks, industrial and state espionage, and Russia’s war of aggression against Ukraine, foreign interference, and supply chain risks, emerging threats of IoT and AI and future issues on Quantum computing.

They explained the main goal of the NIS2 directive and outlined the steps to achieve a high common level of cybersecurity across the European Union. ENISA illustrated the collaboration with different expert groups and telecommunication authorities that are part of the NIS Cooperation group, including ECASEC, the BEREC Cybersecurity Working Group, and other stakeholders. They shared information on some of their current projects, in particular related to the security of subsea cables, NIS 2 Directive implementation and informed about the main activities in the upcoming months.

Some of the main challenges identified by ENISA are:

- How to create a culture of trust, better reporting about non-outages and incidents at suppliers, 3rd party service providers?
- How to protect the larger most critical operators, especially in a crisis, disaster or black swan events?
- How to support the smaller companies in the sector or supply chain, with more security that is basic?

6. Main messages

Resilient communication networks are essential for the stability of society and the economy, particularly in times of crisis. Ensuring continuity of services requires strategic, operational, and technical measures to mitigate threats.

Resilience must be embedded in telecom infrastructure, recognizing that communities depend on connectivity for daily activities and emergency responses. To maximize service availability, networks must address vulnerabilities such as single points of failure by implementing multiple failover solutions, enhancing power backup systems, securing backhaul connectivity, and enabling national roaming. Prioritizing emergency services within these frameworks is fundamental. Regular preparedness drills and collaboration among stakeholders contribute to strengthening overall network reliability.

A national approach to resilience planning should consider digital infrastructure robustness, power backup, redundancy, and supply chain dependencies. Adaptation to extreme weather conditions and cyber threats requires clear security strategies and comprehensive frameworks. Ensuring that telecommunications can withstand and recover from disasters calls for continuous improvements in crisis management, legislative updates, and investments in power resilience.

Emergency services rely heavily on resilient networks, making it crucial to maintain high levels of reliability amid challenges posed by climate change, geopolitical risks, and technological transitions. Future initiatives will focus on reinforcing cybersecurity policies, enhancing digital product certification, and implementing sector-wide resilience activities to better protect critical services from evolving threats. By prioritizing these efforts, communication infrastructure can remain a reliable foundation for both public safety and economic stability.

Annex 1 Agenda of the BEREC Stakeholder Workshop on Network Resilience

AGENDA

BEREC Stakeholder Workshop on Network Resilience

19 November 2024

	Start of Workshop
14:00	Welcome and introduction by the **Co-Chairs of the BEREC Cybersecurity Working Group,** **Katja KMET VRČKO** (AKOS/Slovenia) and **Zdravko JUKIĆ** (HAKOM/Croatia)
14:05	**Keynote speech**: **Hrafnkell V. Gíslason**, Managing Director Electronic Communications Office of Iceland (**ECOI**)
14:15	**Panel 1: The National Perspectives on Resilience and Coordination** Introduction by the moderator: **Adriana Georgescu,** Security Expert (ANCOM/Romania)
14:20	**Resiliant and robust networks in Iceland** **Njörður Tómasson**, Network Specialist and Project Manager Electronic Communications Office of Iceland (**ECOI**)
14:35	**Diversified challenges call for diversified responses** **Johan Foldoy**, Head Engineer Norwegian Communications Authority (**Nkom**), Norway
14:50	**Network Resilience in the UK** **Gina Baikenycz**, Principal Technology Advisor Network Resilience Office of Communications (**Ofcom**), United Kingdom
15:05	Panel discussion and Q&A

16:00	**Panel 2: Solutions for Resilience** Introduction by the moderator
16:05	**Resilience of critical infrastructure – in the aftermath of catastrophic floods in Slovenija in August 2023** **Špela Dekleva**, Regulatory Expert and **Luka Šušteršič**, CSN, IT Infrastructure and TV services Director **A1 Slovenija d.d.**
16:20	**Vodafone's Technology Resilience Programme** **Ettore Genta**, Energy & Policy manager Network Strategy and Architecture, **Vodafone group**
16:35	**Network resilience for emergency communication**s **Cristina Lumbreras**, Technical Director European Emergency Number Association (**EENA**)
16:50	**Blue Light Mobile** **Jo Dewaele**, Marketing Strategy Team Leader **ASTRID** Communication for security, Belgium
17:05	Panel discussion and Q&A
17:25	**ENISA's work to build up cybersecurity and resilience in the EU's telecom sector** **Dr Georgia Bafoutsou,** Cybersecurity Officer and **Dr Marnix Dekker**, ENISA Head of sector for the NIS Directive European Union Agency for Cybersecurity (**ENISA**)
17:40	**Closing remarks and outlook to the next BEREC CS WG Stakeholder Workshop**
17:45	**End of Workshop**