BEREC
Body of European Regulators for Electronic Communications

BoR (25) 82

Summary of the BEREC sessions at ENISA Telecom and Digital Infrastructure Security Forum 2025

20 March 2025

5 June 2025

Contents

1. Introduction and aim of the Forum

In 2024 the BEREC Cybersecurity Working Group (CS WG) was tasked to identify the most relevant cybersecurity and resilience issues and challenges related to new technological developments 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.

The second workshop was part of the ENISA Telecom and Digital Infrastructure Forum 2025 that was jointly organised for the first time by BEREC and ENISA. This report summarises the key takeaways of those presentations held at the conference, which explore how new and advanced technologies are used to enhance the protection of electronic communication networks.

The event brought together leading experts in the field of cybersecurity and network security. The workshop was planned in the BEREC's 2025 Work Programme, specifically under item 1.8: External workshop on the technological advances as security opportunities and challenges for network resilience.

The sessions featured in this report provide insights from a wide range of experts who are actively working to improve the resilience and security of telecommunications infrastructure in an increasingly digital and connected environment, on lessons learned, current practices and innovative tools and methodologies.

2. Stakeholder presentations organised/coordinated by BEREC

2.1. Massive Cyber Attack against A1 - lessons learned- Wolfgang Schwabl, CISO, A1 Telekom Austria

Mr Wolfgang Schwabl presented an interesting case of a cyber attack on the A1 network. A1 became aware of a cyber attack on 12 December 2019 and made a voluntary notification to the CSIRT in Austria. Then the A1 cybersecurity team started an assessment of the situation and initiated the process to establish how extensive the attack was, what effect would it have on their business, was any information stolen, was the attack limited to their network in Austria or were their operations in other countries also affected. The team also

began the process to assess who their attacker was and how an attacker could have breached their defenses.

They discovered that one external server lacked adequate protection, it did not have two-factor authentication, and the hackers gained access by using a password.

To protect customers and services, the team disconnected critical infrastructure network elements from the infected office systems temporarily, allowing the network to operate independently. Access to these network elements was possible by individual separate authentication only. Logging and auditing of all lookup and transactions with customer care applications was initiated and the monitoring of the access to databases was started. It was essential to be able to distinguish between legitimate and illegitimate traffic on these systems.

In order to securely plan a recovery from this attack A1 could not risk using any network devices or storage that might be infected. The A1 team used private devices and other secure external services such as FabaSoft Cloud, a new tenant on Microsoft 365, Signal for mobile devices and S/MIME encrypted user certificates to handle internal communications while planning their defense and recovery.

A1 took measures to strengthen their defenses as they improved their monitoring systems. Data Leakage Protection (DLP) tools enabled the observation and monitoring of the hacker's activities on their network. Defender ATP[1] and Azure ATP were used. Logfiles were forwarded to Splunk, and scanning was intensified. Red and Blue Team testing was carried out.

Finally, following an additional delay caused by COVID, it was time to put measures into action and remove the malware from A1 systems.

Key messages:

The E-Day initiative highlights a significant cybersecurity overhaul, focusing on strengthening password protocols, implementing two-factor authentication, and cleansing systems of malware. A key action was notifying employees of new passwords via SMS, alongside deploying fresh system installations and improved threat detection capabilities. From these efforts, several critical lessons emerged. Strong, complex passwords combined with MFA are essential. Regular forced password changes may reduce security if users resort to insecure practices like writing them down. Allowing special characters, including spaces, increases password strength. Crucially, passwords must never be transmitted in clear text—encryption is vital. The importance of corporate password management tools is emphasized. Keeping systems patched, deploying DLP and SIEM tools, and monitoring network traffic are all necessary for proactive defense, also using whitelisting rather than blacklisting is recommended for more effective threat control.

[1] Microsoft Defender ATP is an enterprise-grade security platform designed to protect endpoints against advanced threats. It offers features such as real-time protection, endpoint detection and response (EDR), threat analytics, automated investigation and remediation, and cloud-based security powered by AI.

2.2. From Shadows to Insights: Using Deception Technology to Stay Ahead of Cyber Threat Matej Rabzelj, Cyber Systems

Mr Matej Rabzelj, a cybersecurity researcher from the Faculty of Electrical Engineering at the University of Ljubljana, delivered a presentation on the application of cyber deception technologies, with a particular focus on network honeypots and honeynets for threat detection and cyber threat intelligence.

The presentation addressed the growing landscape of cyber threats and introduced CyberLab—a geo-distributed, highly interactive honeypot platform developed at the Laboratory for Telecommunications and licensed by Cyber Systems. CyberLab supports rapid deployment of diverse honeypot services that emulate management protocols (e.g., Telnet, SSH), HTTP-based services (e.g., cloud APIs, web applications), and IoT devices. The platform enables containerized provisioning of honeypot nodes across a range of networks, facilitating real-time attack data collection and centralized analysis.

The presenter showcased actionable insights derived from CyberLab deployments across three key sectors: academic institutions, public cloud service providers, and domestic critical infrastructure networks. The research included automated bot detection on HTTP and SSH traffic, behavioral differentiation between legitimate users and attackers based on web requests, and in-depth recording of Telnet and SSH session data—including command sequences and execution timings. This analysis enabled the identification of network scanners, malware distribution campaigns, and preliminary detection of botnet activity.

The talk concluded with statistical findings from the honeynet deployments and an overview of the platform's development. Special attention was given to custom-built analysis and visualization tools, including interactive dashboards for attack graph traversal and full session replay capabilities. Participants were invited to provide feedback on the presented solution and to consider its applicability within their own organizations.

Key messages:

This part of the session emphasizes the role of cyber deception in enhancing both defensive strategies and intelligence capabilities in the modern threat landscape. It introduces technologies like honeypots, honeynets, and honeytokens, which, powered by AI-driven analytics, detect insider and external threats in real time. These tools help identify breaches, analyze hackers' methods, and uncover emerging threats, providing valuable insights for improving cybersecurity preparedness. The key message from Matej Rabzelj's presentation highlights the CyberLab platform, a geo-distributed honeypot system designed to detect cyber threats. It emulates management protocols, HTTP services, and IoT devices to gather data on attacks. The research demonstrated actionable insights such as bot detection, malware campaigns, and network scanner identification, supported by interactive visualization tools. By combining these technologies, organizations can stay ahead of cybercriminals, improving both internal protection and external threat intelligence.

2.3. Cyber Conflict Simulator (CCS) - Professor Stjepan Groš, Faculty of Electrical Engineering and Computing Zagreb - Goran Polonji, Utilis, Zagreb

Professor Stjepan Groš from the Faculty of Electrical Engineering and Computing at the University of Zagreb, along with Mr. Goran Polonji from Utilis, presented the Cyber Conflict Simulator (CCS) — an advanced, tactical-level training and simulation platform that introduces a new approach to cyber exercises. CCS is the result of a three-year joint R&D project between the University of Zagreb's Faculty of Electrical Engineering and Computing and the SME Utilis d.o.o.

Unlike traditional tabletop exercises, which focus on decision-making but lack realism and complexity, CCS offers highly realistic simulations to support decision-makers. It allows for the modeling of one or multiple organizations to a desired level of detail and scope. Since it does not focus on technical specifics, setting up an exercise is relatively straightforward. Tactical attack and defense actions are then conducted within these models, enabling decision-makers to train and refine their responses to real-world cyber incidents.

Complementary to cyber ranges, CCS accelerates the simulation of incidents that would typically unfold over months, allowing them to be processed in a single day. The platform supports training, incident response procedure testing, what-if analyses, procedure development, and more.

Designed for both the civil and military sectors, CCS provides decision-makers with a risk-free, accelerated environment to test and refine their incident response strategies. By mirroring the IT and business systems that trainees use in their daily work, the platform enhances situational awareness and strengthens cybersecurity readiness.

Key messages:

The Cyber Conflict Simulator (CCS) is an innovative tactical-level simulation platform developed through a three-year R&D collaboration between the University of Zagreb's Faculty of Electrical Engineering and Computing and Utilis d.o.o. It introduces a new approach to cyber exercises, providing realistic, complex simulations that go beyond traditional tabletop exercises, which often lack real-world complexity. CCS allows one or more organizations to be modeled in great detail, enabling decision-makers to engage in tactical attack and defense actions, refining their responses to cyber incidents.

The platform is designed to support both civil and military sectors, offering a risk-free environment for training, testing incident response procedures, and conducting what-if analyses. Its ease of setup, without requiring deep technical details, makes it accessible and versatile. By simulating incidents that would normally span months in a single day, CCS accelerates decision-making training and enhances preparedness. This capability, coupled with realistic IT and business system modeling, enables organizations to improve cybersecurity readiness through hands-on experience. CCS serves as a complementary tool

to cyber ranges, ensuring comprehensive, effective cybersecurity training and procedure development.

2.4. Defending the digital future by harnessing novel technologies in critical networks - Mikko Karikytö - VP, Chief Product Security Officer, Ericsson

The presentation began by Mr Karikytö emphasizing the significant role nation-states sponsored actors' play in cyber-attacks, with most threat actors originating from specific regions. There are no reports hear about threat actors from Swedish or Finnish Nexus APTs, but China nexus and Russia nexus players are discussed in length.

Artificial Intelligence (AI) has a crucial role in enhancing telecoms security, for instance in threat modeling, provided that high-quality data is utilized. However, it is essential to ensure that privacy is respected when implementing AI solutions. AI should be seen as a complementary tool, rather than a replacement for existing effective methods, as the saying goes, "a good old trick is better than a bag full of new ones." Not everything we can solve with AI.

The advancements in detecting security threats, such as identifying false base stations where AI plays a crucial role, have motivated and encouraged Ericsson to further develop AI-powered cybersecurity capabilities and investigate in general other uses of AI for security. Currently, the company has 5,000 to 6,000 personnel (approximately 5% to 6% of its total employees) dedicated to security roles. Ericsson's cybersecurity training program is structured into four levels, with all employees required to complete Level 1. Employees who reach Level 4 are considered fully qualified cybersecurity practitioners.

The well-known statistic that there are 100,000 unfilled cybersecurity jobs in the EU highlights the need for the development of security defence and AI to work together to address this gap.

To establish trust in AI, it is essential to integrate it holistically into cybersecurity systems, using accredited and signed-off software[2]. The importance of AI in cybersecurity is evident, as failing to utilize it would result in missing potential cyber threats. Moreover, preventing insider threats is vital, and this can be achieved by knowing staff members and ensuring they receive the appropriate level of training. In terms of 5G standalone deployment, Europe is lagging behind, with India having deployed more standalone (SA) 5G networks during last year over a period of eight months than what exists in the entire Europe.

The US and China are currently leading in 5G deployment, with China commercially deploying 5G Advanced. At the same time, half of the EU member states have not yet implemented the 5G toolbox as recommended by the 2nd EU 5G Toolbox and Communication from the European Commission (June 2023).

[2] https://www.ericsson.com/en/reports-and-papers/further-insights/ai-ml-in-telecom-network-security

Key messages:

The rapid digitalization of society, fueled by advancements in mobile connectivity, AI, and cloud technologies, are expanding the cyber threat landscape. To ensure service continuity, integrity and user trust, a resilient, secure and trusted network infrastructure is essential. The future of mobile technology hinges on adopting Zero Trust Architecture (ZTA), AI and quantum resilient encryption.

2.5. Harnessing AI for Next Gen Threat Detection & Response - Zeina Zakhour - EVIDEN, an ATOS company

In this presentation the impact of AI in the telecommunications sector, in particular its capabilities for security solution AIsaac of EVIDEN was presented.

Ms Zeina Zakhour started by presenting the increasing cybersecurity challenges the telecommunications sector faces. Due to its expanding role beyond traditional services, the sector poses a larger attack surface while at the same time the accumulation of sensitive user data makes the telecommunications industry an attractive target for cyber-attacks. Additionally the complexity of modern telecommunications networks, coupled with supply chain risks and the integration of numerous IoT devices, makes security more challenging. Consequently, the telecommunications sector has become the third largest target for cyberattacks in the digital landscape.

While telecommunications providers already utilize AI for example for network control, there is a need to strategically implement it to address security blind spots. Traditional security mechanisms fail to cover 84% of specific known cyber-attack and intrusion techniques, creating a significant gap that AI may help to close. Enterprises can leverage AI to enhance detection and response capabilities, accelerating decision-making processes.

There are two major ways to utilize AI for detection. The first is anomaly-based detection, where the approach identifies deviations from normal behavior to detect unusual activities that may indicate a threat. The second is hypothesis-based detection, which involves forming assumptions about potential malicious activity and testing these hypotheses through investigation.

In practice, AI can be used to uncover hidden connections within data and leverage deep learning to predict future attacks. Ms Zakhour proceeded to explain the detection and response capabilities of the AI security solution "AIsaac" by EVIDEN. The system employs a multi-vector approach to secure telecommunications networks across all nodes, using modern technologies for detecting and responding to threats. Some examples of the detection capabilities include the detection of rogue base stations, voice and SMS fraud detection, SS7 authentication bypass attack detection, downgrade attacks, real-time radio jamming detection, and supply chain trust. The AI solution "AIsaac" demonstrates that AI-powered systems offer significant advantages in securing telecommunications networks. These advantages include the rapid synthesis of large amounts of data, enabling real-time threat analysis, automated threat detection and response, and early detection with proactive defense even against

unknown threats. AI may also be utilized in other fields in the future, such as leveraging AI to counter emerging quantum computing threats, using AI for energy efficiency in network operations, and implementing self-healing networks through AI.

Overall, the telecommunications sector must ensure the security of the AI systems themselves when deploying AI in telecommunications networks.

Key messages:

In today's rapidly evolving cyber threat landscape, traditional security methods are no longer sufficient. Cybercriminals are utilizing AI, automation, and advanced evasion tactics, leaving security teams struggling to identify real threats from false alarms. However, AI is transforming cybersecurity by enabling faster detection, reducing false positives, predicting attacks, and automating responses. The integration of AI empowers security teams to stay ahead of adversaries, minimize attack dwell time, and respond with greater precision. This proactive approach not only strengthens defenses but also allows organizations to anticipate threats rather than simply react to them. As the telecommunications industry increasingly incorporates AI into network security, it becomes clear that AI-driven resilience is crucial in addressing the challenges posed by sophisticated cyber threats. The symbiosis between AI and network security is now a present reality, offering a powerful tool to safeguard communication infrastructure in an era of escalating cyber risks.

3. BEREC summary conclusion from the Forum

The BEREC sessions of the ENISA Telecom and Digital Infrastructure Security Forum 2025, jointly organized by BEREC and ENISA for the first time focused on cybersecurity challenges and technological advancements in electronic communication networks. Key presentation included a detailed case study of a massive cyberattack on A1 Telekom Austria, highlighting the importance of strong passwords, multi-factor authentication, and proactive monitoring to enhance network resilience. Next highlight was the use of cyber deception technologies, such as honeypots, to detect and analyze cyber threats in real time and for improving threat intelligence. The forum also introduced the Cyber Conflict Simulator, a tactical training platform that accelerates realistic cyber incident simulations for better decision-making and preparedness. The role of AI was also presented, with AI-powered systems offering key advantages in securing telecommunications networks through early detection, real-time threat analysis, and proactive defense against unknown threats.

BEREC recognises several advantages of co-organising the Forum together with ENISA Our common target audience are all our most important stakeholders - operators, equipment suppliers, cybersecurity experts, academia, regulatory authorities and other public entities. The joint event offered the possibility to observe and analyse the cybersecurity challenges from two slightly different but complementing perspectives – a more technical one was supported by ENISA and more market oriented by BEREC.