

Cybersecurity in a Digital Europe: Implementing NIS2 in the Energy Sector

Aspen Institute Romania Roundtable

Brussels, June 2nd, 2025

About the Event

This roundtable event has been organized by the **Aspen Institute Romania (AIR)**, under the aegis of the **Aspen Institute Romania Brussels Office & European Hub**, the **European Center for Economic Security, Technology and Resilience (ECESTR)** powered by AIR, and the **Aspen Energy & Sustainability Program**. The event benefitted from the crucial support of the **Romanian National Cyber Security Directorate (DNSC)**, the **Romanian Energy Center (CRE)** and **ENEVO Group**. This by invitation only, under Chatham House rules event, brought together European and Romanian policymakers, regulatory authorities, cybersecurity experts, and industry representatives to discuss the **strategic, operational, and legal implications of NIS2** — and how Romania can position itself as a **proactive and resilient actor** in the European cybersecurity ecosystem.

The digital transformation of Europe is accelerating, but so are the cyber threats facing its public and private sectors. The **NIS2 Directive**, adopted by the European Union, marks a significant step in strengthening the resilience and security of essential and important entities across Member States — introducing **stricter supervision, enforcement, and risk management requirements**. As Member States navigate the complexities of NIS2 implementation, **key challenges** emerge: coordination among competent authorities, capacity-building in critical sectors, cross-border cooperation, and aligning national strategies with EU-wide frameworks.

The event has focused on the **energy sector** — a cornerstone of critical infrastructure, but increasingly vulnerable to cyberattacks — from SCADA systems in electricity grids to remote control of gas and oil infrastructure. The NIS2 Directive classifies a wide range of energy actors as essential entities, including electricity, gas, oil, district heating, hydrogen providers, and cross-border operators. Transposition of NIS2 presents both a **compliance challenge** and an **opportunity to embed cybersecurity as a core pillar of the energy transition**.

About the Aspen Institute Romania Brussels Office & European Hub

The **Aspen Institute Romania Brussels Office & European Hub** aims to contribute significantly to **promoting a non-partisan dialogue platform** and to strengthening collaboration on critical challenges faced by Europe and its partners. Building upon the successful establishment of the Aspen Institute Romania Office in Chisinau, Republic of Moldova, two years ago, the Aspen Institute Romania Brussels Office & European Hub reflects the commitment to fostering transatlantic dialogue and bolstering a **forward thinking platform** which nourishes **deeper cooperation perspectives**. Brussels, as a central hub for European policymaking and international affairs, presents an invaluable environment for advancing our mission of promoting a **values-based leadership and a more just and more democratic society**.

Nowadays, in the context of a seriously challenged transatlantic relation, this office will only increase its role as a **strategic focal point and a highly recognized international arena for political and economic development**. Engaging its communities in developing a structural presence closer to the heart of European policy making will prove beneficial for Aspen Institute Romania and the entire **Aspen International Network**, contributing to a neutral dialogue platform among decision-making institutions, international organizations, private sector, civil society, and academia, by promoting and advancing fundamental debates on deciding policies and strategies. This continuous presence will significantly enhance our capacity to convene leaders, spark dialogue, and **drive positive change at a crucial juncture for Europe and the wider world**.



Event Report

Cyber Security for the energy sector is a unique opportunity to show strong leadership and tighten collaboration between public administration and the energy sector. In order to ensure the general public is protected and energy security is provided, immediate action is needed and the public opinion needs to be informed to **support fiscal stimuli to deliver safe, reliable and sustainable operational excellence.**

1. Strategic Leadership & Collaboration

Key take-aways: Frame cybersecurity as an executive priority that unites regulators, utilities, and industry bodies. Foster joint threat reporting, shared incident responses, and public dialogue to secure fiscal support and cohesive policies.

- Cybersecurity must be positioned as a **leadership opportunity and a cross-sectoral responsibility.** **Enhanced cooperation between public authorities and energy operators** is essential to safeguard both public interest and energy security. Informed public discourse and **supportive fiscal policies** can enable critical investments to ensure safe, reliable, and resilient energy systems.
- Cybersecurity is inherently **collaborative.** Even competitors must engage in **shared learning, transparent reporting, and mutual assistance.** Leadership, training, and an honest reassessment of current OT security programs are urgently needed.
- Industry associations are stepping up to provide technical guidance and disseminate **cost-effective best practices.** However, **public procurement** remains a significant bottleneck. Streamlining procedures to enable timely adoption of cybersecurity solutions is imperative.
- Price is the most important KPI in public procurement, however **safety of data and cybersecurity preparedness should also be part of the KPI importance scale.**
- Major initiatives such as the European Green Deal **have yet to adequately incorporate OT cybersecurity as a funded priority.** This blind spot must be addressed to ensure the energy transition does not come at the cost of resilience.

2. Escalating Threats & Regulatory Accountability

Key take-aways: With attacks tripling in four years, energy firms must adopt a proactive, risk-based security posture. NIS2's stricter liability rules—and the upcoming Cyber Resilience Act—demand continuous risk assessment and certified device integrity.

- Cyber incidents targeting the energy sector have tripled over the past four years, rising from approximately 500 to over 1,500. This **escalating threat** highlights the urgency for proactive risk management and the implementation of effective security controls.
- Under NIS2, energy entities fall under a regime of **stricter accountability and regulatory oversight.** Legal liability for cybersecurity failures has become a reality for those in scope. The



directive mandates a cultural shift—from **compliance-led approaches to a proactive, risk-informed mindset.**

- The EU is advancing the **Cyber Resilience Act** to address these challenges. This legislation aims to certify the cyber trustworthiness of digital products made in the EU, reinforcing consumer and infrastructure protection. In parallel, DG CONNECT and DG ENER have issued **guidance to mitigate supply chain risks.**
- **Cyber threats are no longer theoretical** — they are a daily operational reality. State-aligned and criminal actors have demonstrated the capability to disrupt energy systems as part of broader geopolitical strategies. Moreover, also on a geopolitical scale, the energy sector is a systemic target of the biggest threats due to its critical infrastructure.
- NIS2 is a critical step—but not the full picture. **Local energy regulators** play a decisive role in financial flows and priorities. Bridging national and EU-level regulations is key to a coherent cybersecurity strategy.

3. Integrated Digital-OT Governance

Key take-aways: Overcome visibility gaps by mapping digital assets to physical operations. Build unified IT/OT frameworks that incorporate AI responsibly, deploy routine supply-chain inspections, and monitor emerging AI-driven threats.

- Energy infrastructure comprises **deeply interconnected digital and operational systems.** Visibility into digital assets, and understanding their cross-dependencies with physical processes, remains a major challenge. This complexity necessitates robust governance and an integrated approach to cybersecurity.
- Cybersecurity should not be viewed solely as a technical challenge, but rather as an **enabler of organisational transformation.** Legacy mindsets and underinvestment remain barriers, especially as **emerging technologies like AI amplify both opportunities and risks.**
- Artificial Intelligence has contributed to the rapid proliferation of sophisticated cyber threats, including **AI-generated malware.** However, basic cybersecurity practices are often still lacking, largely due to inadequate investment. Cyber resilience cannot be built on outdated foundations.
- Critical vulnerabilities have been identified in the **supply chain of digital energy control systems** — including undisclosed mobile communication modules embedded in devices. Without a systematic cyber-inspection regime, these devices pose significant systemic risk.
- The rise of **private prosumers** introduces new risks to **grid stability,** especially as they operate outside traditional regulatory frameworks. Similarly, home energy control systems require basic cyber hygiene education, akin to previous public awareness campaigns on safe internet use.



4. Resilience-First Investment & Culture

Key take-aways: Shift security from a cost center to a strategic asset by embedding cyber requirements in procurement and budgeting. Develop national crisis playbooks, run cross-border exercises, and prioritize workforce training and daily cyber-hygiene as the first line of defense.

- Cybersecurity investments should not be framed only in terms of cost avoidance. They must be integrated into the broader context of **digital transformation, operational resilience, and strategic risk management**. The business case needs to reflect long-term value and risk reduction. In addition, in the medium to long term, these costs will be lower than actually fixing the problems after a cyber attack.
- Cybersecurity should be seen as a **strategic asset**, not an expense. A **resilience-first approach** — prioritizing preparedness, detection, and recovery — delivers better outcomes than narrowly pursuing regulatory compliance alone.
- While many utilities allocate up to 15% of capital for annual investments, cybersecurity typically receives only a small fraction. **Regulatory incentives**—such as requiring NIS2 compliance for public tenders—could be a pragmatic lever to drive better funding alignment.
- Major initiatives such as the European Green Deal **have yet to adequately incorporate OT cybersecurity as a funded priority**. This blind spot must be addressed to ensure the energy transition does not come at the cost of resilience.
- We need to develop and rehearse operational playbooks for national-level cyber crises in the energy sector. These should map out response pathways, stakeholder responsibilities, and escalation mechanisms.
- **Effective cyber defence at national level** requires both **European and NATO-level coordination**. Cross-border exercises, shared threat intelligence, and joint response mechanisms are essential to collective security.
- The **EU Cyber Solidarity Act** will bolster the Union’s ability to prevent, detect, and respond to major incidents. It introduces a cybersecurity reserve of private incident response providers deployable upon Member State request—strengthening Europe’s **unified defence posture**.
- From boards to technicians, people remain the first line of defence. Investing in **skills development**, promoting **honest industry dialogue**, and **reinforcing daily cyber hygiene practices** are non-negotiable pillars of a secure energy future.



Call to Action

The cybersecurity of our energy sector is not just a technical challenge—it's a **matter of national security and public safety**. We suggest treating cybersecurity as a **strategic investment** in our energy future rather than a necessary cost. The peace of mind that comes from robust cyber defenses benefits everyone: operators, regulators, and the public alike.

Success will require **unprecedented cooperation across traditional boundaries, sustained investment** in both technology and human capabilities, and a **shared commitment** to treating cybersecurity as the team sport it truly is. The threat actors are already operating as part of our daily reality—our response must be equally coordinated and persistent.

Next Steps

We recommend:

1. Establishing a **working group** to prioritize these suggestions and develop detailed implementation timelines. Regular progress reviews and industry-wide sharing of lessons learned will be essential to building the resilient energy sector our society depends on.
2. *(pending financing)* Organizing **Strategic Decision-Making Exercises**: High-level (CEOs & decision-makers) simulations in case of cyberattacks, via a specialized platform, which will provide a strong foundation for building cybersecurity maturity. These thought-provoking scenario-based simulations and discussions provide aim to create fictitious “regulated chaos” and to be able to efficiently test participants’ decision-making capabilities & options in a safe training environment.
3. Organizing a **Romania Energy Day** in the margins of the next **Eurelectric Power Summit** *(tentative dates 3-4 June 2026)* to showcase Romania's pivotal role in Europe's energy transition and highlight the country's significant contributions to regional energy security. Romania offers a unique energy portfolio combining substantial renewable capacity, nuclear expertise, and strategic position as a regional energy hub connecting Southeast Europe with EU markets.

Supporting documentation

Below are 12 key documents (with links) prepared by EU institutions, especially the European Commission, relevant to cybersecurity, NIS2, digitalisation in the energy sector, and regional security—including the new Black Sea strategy and the latest cyber crisis management framework:

- 1. NIS2 Directive: new rules on cybersecurity of network and information systems**
<https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
The core EU law establishing stricter cybersecurity requirements for essential and important entities, including the energy sector, with expanded scope, risk management, and incident reporting obligations.
- 2. EU Cybersecurity Strategy for the Digital Decade**
<https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>
The EU's overarching strategy for strengthening cyber resilience, technological sovereignty, and operational capacity across all sectors.
- 3. EU Strategic Approach to the Black Sea Region (2024/2025)**
https://www.eeas.europa.eu/eeas/black-sea_en
The latest EU strategy for the Black Sea, focusing on security, connectivity, and resilience of critical infrastructure amid heightened geopolitical tensions.
- 4. EU Blueprint for Cyber Crisis Management (2025)**
<https://cadeproject.org/updates/council-of-the-eu-adopts-updated-cyber-crisis-management-blueprint/>
The updated EU-wide framework for coordinated response to large-scale cyber incidents, defining roles, escalation procedures, and cross-border cooperation for crisis management.
- 5. Cyber Solidarity Act**
<https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>
A new regulation (in force since February 2025) that creates a European Cybersecurity Alert System, an EU Cybersecurity Reserve, and a Cyber Emergency Mechanism to strengthen preparedness, detection, and response to major cyber incidents.
- 6. Cyber Resilience Act**
<https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>
Sets mandatory cybersecurity requirements for products with digital elements (hardware and software), ensuring security throughout their lifecycle and introducing CE marking for compliant products. In force since December 2024.
- 7. Delegated Regulation (EU) 2024/1366: Network Code on Cybersecurity for the Electricity Sector**
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1366>
Sector-specific rules for cybersecurity in cross-border electricity flows and grid operators, supporting NIS2 implementation in the energy sector.



- 8. Digital Europe Programme (2021–2027)**
<https://digital-strategy.ec.europa.eu/en/activities/digital-programme>
The EU's main funding programme for digital transformation, including investments in cybersecurity, artificial intelligence, and digital skills.
- 9. Council Conclusions on the Future of Cybersecurity: Implement and Protect Together (May 2024)**
<https://data.consilium.europa.eu/doc/document/ST-9592-2024-INIT/en/pdf>
Sets out strategic priorities for EU cybersecurity policy, calling for enhanced cooperation, capacity building, and a revised strategy.
- 10. 2024 EU Risk Assessment Report: Cybersecurity in Telecommunications & Electricity Sectors**
<https://www.enisa.europa.eu/publications/sectoral-cybersecurity-risk-assessment-2024>
A comprehensive risk assessment by ENISA and the European Commission, focusing on cyber threats and vulnerabilities in telecom and electricity sectors.
- 11. Cyber Security in the Energy Sector – EECSP Expert Group Report**
https://energy.ec.europa.eu/publications/cyber-security-energy-sector_en
Expert analysis and recommendations for strengthening cybersecurity in the EU energy sector, addressing policy, technical, and operational challenges.
- 12. Commission Communication: Shaping Europe's Digital Future**
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0067>
Outlines the EU's digital transformation goals, including secure digital infrastructure, data, and innovation, with cybersecurity as a key pillar.
- 13. Key Actions for Digitalising Energy (European Commission)**
https://energy.ec.europa.eu/topics/markets-and-consumers/digitalising-energy_en
Overview of EU initiatives to digitalise the energy system, including cybersecurity measures for smart grids and critical infrastructure.
- 14. Open Calls for Proposals under the Digital Europe Programme**
<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital>
The official portal for current funding opportunities and priorities in digital and cybersecurity projects managed by the European Commission.