A4: Special Issues in Energy, Environment and Climate Change

CYBER THEATS & ENERGY SECURITY

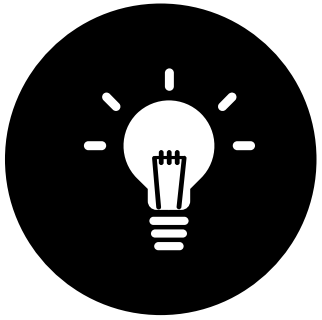
Andrew Liaropoulos
Associate Professor

17/10/2026



Structure

- ❑ **Introduction**
- ❑ **Cyberspace & Cybersecurity**
- ❑ **The digital transformation of the energy sector**
- ❑ **Cyber threats to the energy sector**
- ❑ **Enhancing cyber-resilience of the energy sector**
- ❑ **Conclusion**





Introduction

Questions:

- How do cyber threats affect the energy sector?
- How can we counter cyber threats to the energy sector?
- How can we enhance cyber-resilience in the energy sector?

Goal: Holistic understanding of the full spectrum of cyber threats to the energy sector and ways to counter such threats.

=> **Cybersecurity** has become a key component of ensuring overall **energy security** and thereby **national security.**



Cyberspace & Cybersecurity



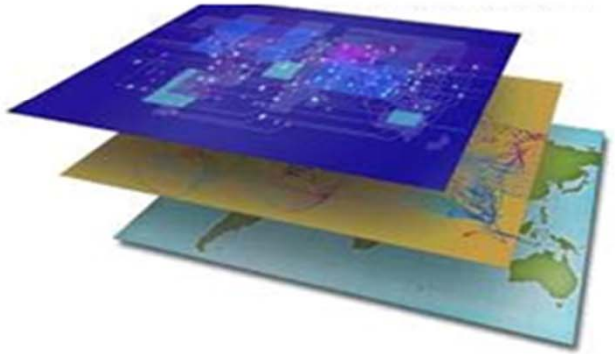
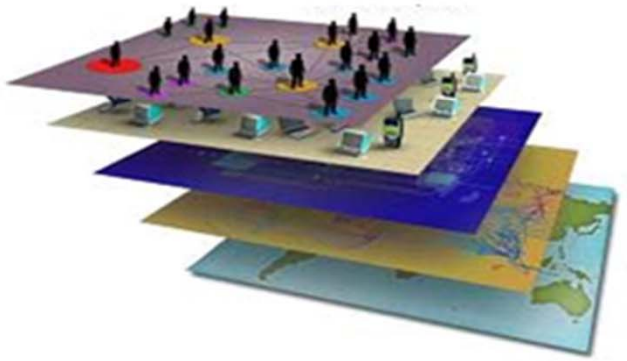
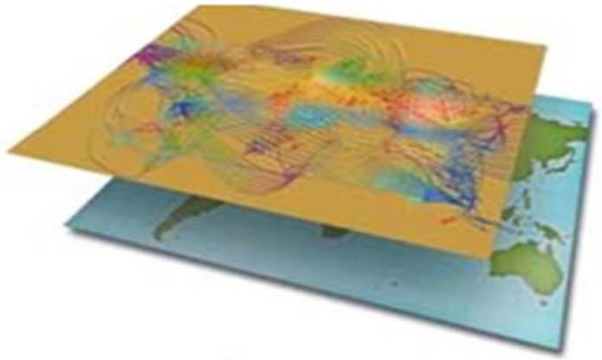
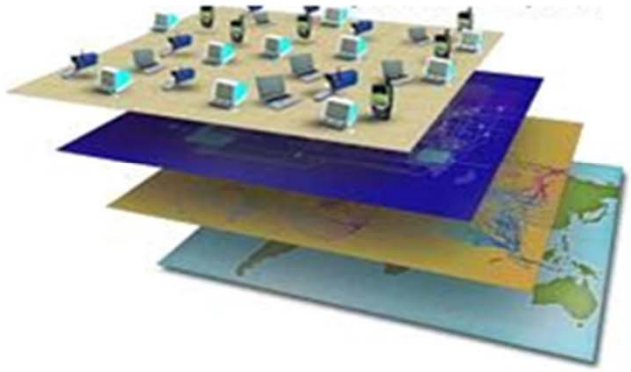
Cyberspace = cyber + space

Cyberspace consists of four dimensions:

- The **physical** dimension (hardware, computer systems, routers, fiber optics, etc.)
- The **software** dimension (computer program, software, code, algorithm, etc. the syntactic, the ‘language’ of cyberspace)
- The **data** dimension
- The **human** dimension (the end user)

Cyberspace is much more than the sum of its parts.

Cyberspace & Cybersecurity

Physical Layer	Logical Layer	Social Layer
Geographic Component 	*Logical Network Component* 	*Persona Component* 
Physical Network Component 		*Cyber Persona Component* 

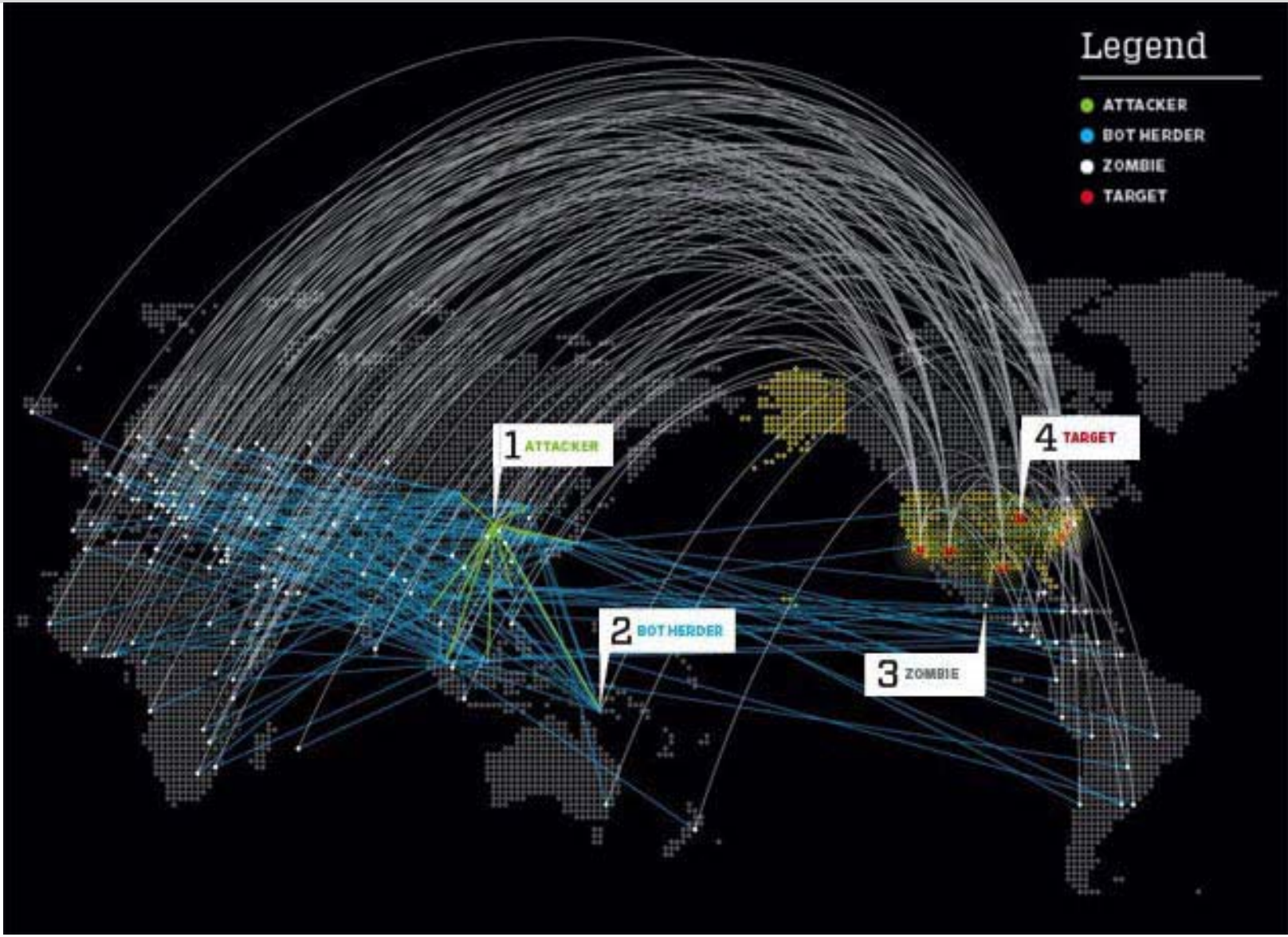
Cyberspace & Cybersecurity

- **The security problems:**
- cyberterrorism, cybercrime
- cyberespionage,
- cybersabotage, hacktivism
- ransomware, DDOS, etc…
- part of a hybrid operation
- part of a military operation

- **The attribution problem**
- Technical (cyber-forensics)
- Legal
- Political

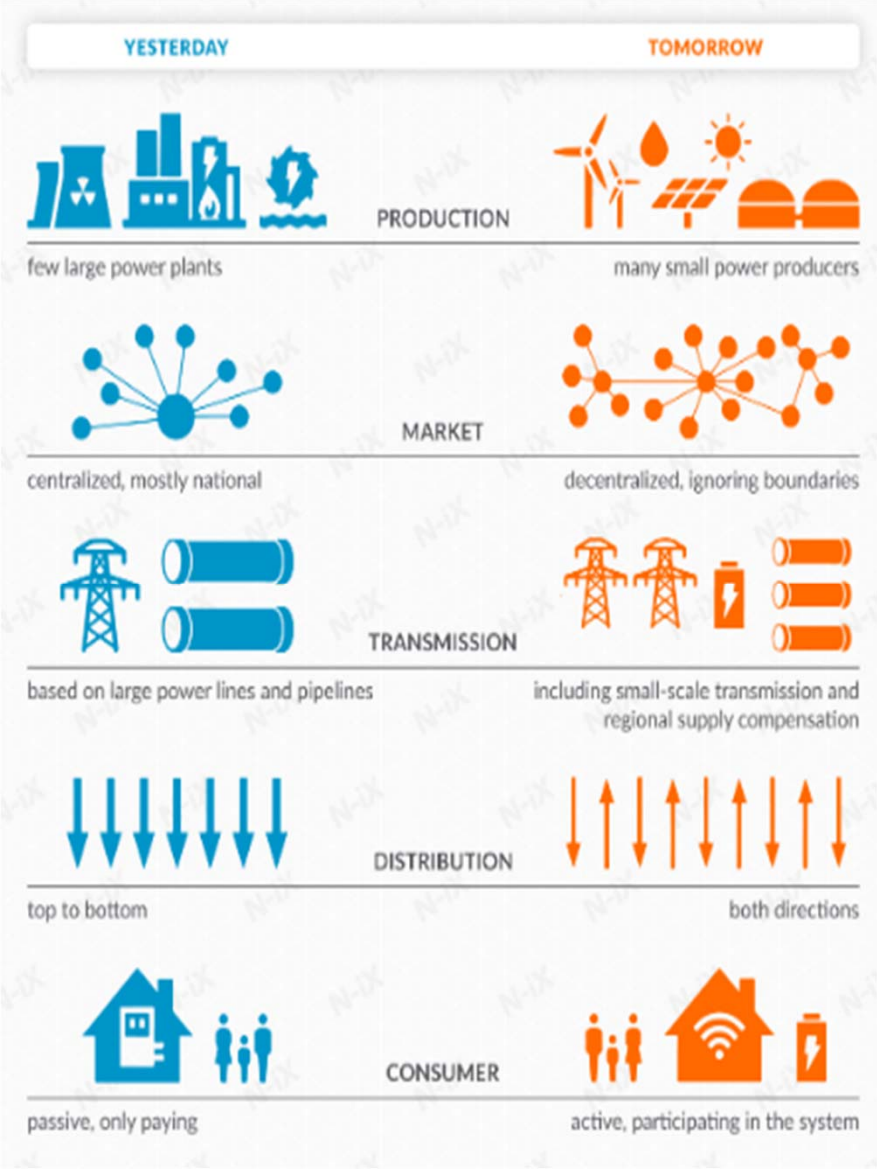
- **Cyber-deterrence**

- **Cyber-resilience**



The digital transformation of the energy sector

- Today's electricity system increasingly incorporates distributed generation, including rooftop solar panels, wind farms and battery storage.
- Transmission and distribution system operators require advanced digital technologies and platforms to coordinate power flows, connect these decentralised assets, and ensure overall grid stability.
- Additionally, the increasing deployment of smart meters and connected devices allows consumers to actively participate in the market. Smart meters provide real-time insights into consumption, enabling automated demand response and dynamic pricing mechanisms.
- For the power suppliers and retailers, AI-driven forecasting systems further optimize the balance by predicting demand patterns and adjusting supply accordingly, thus preventing overloads.



The digital transformation of the energy sector: risks & challenges

- Although digitalisation has numerous **advantages,** it also **introduces new challenges**. As more systems become interconnected and reliant on digital technologies, the number of potential access points for hostile actors increases.

- Modern power systems rely on complex networks of smart meters sensors and automated control systems, all of which can be exploited. Cybercriminals can **target weak points** in these networks to disrupt operations, steal data or manipulate energy flows.

- Another key challenge is the **dependency on real-time data and automation**. While it optimizes grid efficiency, it can also introduce risks if compromised. A cyberattack that manipulates data or disrupts automated controls could lead to widespread blackouts, equipment failures or financial losses.

- Additionally, **supply chain vulnerabilities** pose a growing threat. Energy infrastructure increasingly relies on external software providers, cloud services and imported hardware components. Should these **third-party systems become compromised,** attackers can gain access to critical grid operations.

Cyber threats to the energy sector

- **Phishing Attacks**: Cybercriminals often use phishing emails to trick employees into revealing sensitive information or installing malware on their systems.

- **Ransomware Attacks**: In these attacks, hackers encrypt a company's data and demand a ransom in exchange for the decryption key.

- **Supply Chain Attacks**: These attacks target third-party vendors with less secure networks to gain access to a larger company's systems.

- **Insider Threats**: Sometimes, the threat can come from within the organization, either from dissatisfied employees or those who unintentionally cause a security breach.

- **Advanced Persistent Threats (APTs):** APTs are **sophisticated cyber attacks** carried out by well-funded and organized adversaries, often with the support of nation-states. These attacks are characterized by their **persistent nature**, with threat actors employing sophisticated techniques to evade detection and maintain access to target networks over extended periods.

Cyber threats to the energy sector

- **Distributed Denial of Service (DDoS) Attacks:** DDoS attacks aim to disrupt the availability of services by overwhelming target systems with a flood of traffic. In the energy sector, DDoS attacks can disrupt operations, leading to financial losses. Threat actors may leverage botnets or compromised devices to orchestrate large-scale DDoS attacks against energy infrastructure.

- **Zero-Day Exploits:** Zero-day exploits refer to **previously unknown vulnerabilities** in software or hardware that have not been patched by vendors. Threat actors may exploit these vulnerabilities to gain unauthorized access to systems or execute malicious code, posing significant risks to the security of energy infrastructure. Effective vulnerability management and patching practices are essential for mitigating the risk posed by zero-day exploits.

- **Malware Targeting Industrial Control Systems (ICS):** Malware specifically designed to target ICS and supervisory control and data acquisition (SCADA) systems poses a significant threat to energy infrastructure. These malware variants, are capable of causing physical damage to critical assets, disrupting operations, and compromising safety systems.

Cyber threats to the energy sector

Figure 2: Distribution of Cyber Attacks by Type (2020–2024)

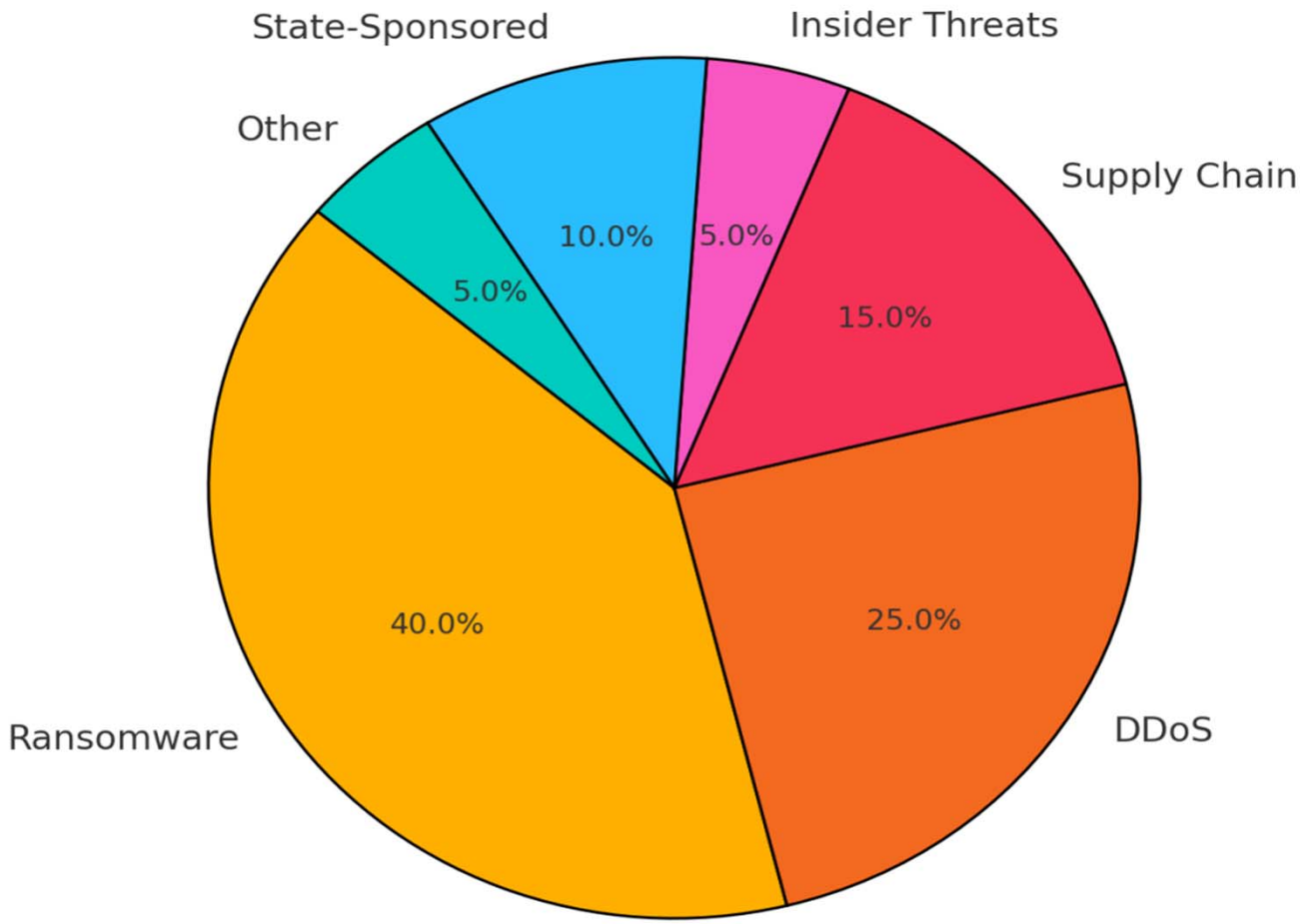
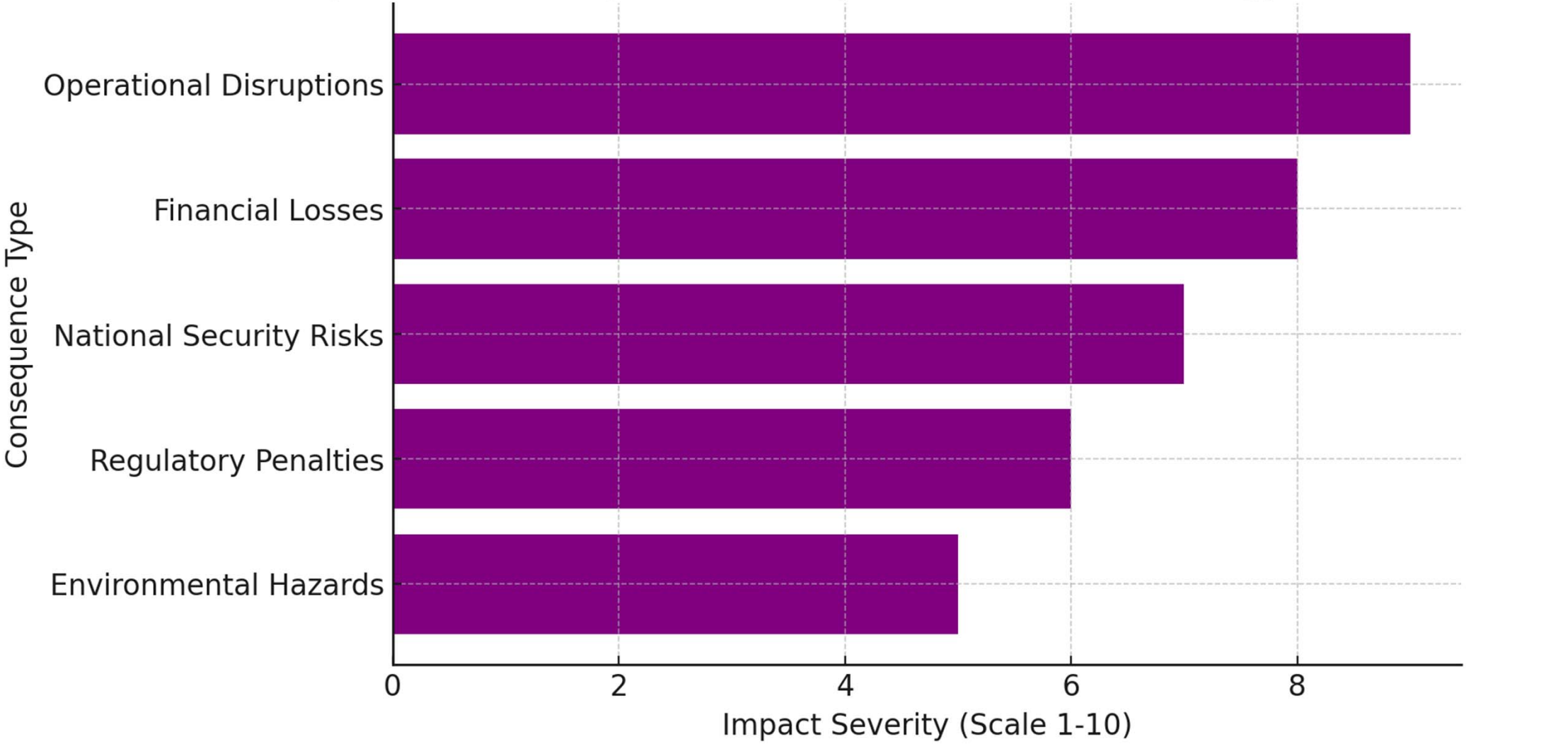


Figure 4: Consequences of Cyber Attacks on Energy Infrastructure



SolarWinds supply-chain compromise - 2020

Country: United States and international victims. **Type:** Software supply-chain compromise and cyberespionage. **Attribution:** Russian Foreign Intelligence Service (SVR), according to US government attribution

Discovered in December 2020, the SolarWinds incident involved attackers inserting malicious code, known as SUNBURST, into legitimate updates of SolarWinds' Orion network-management software. The compromised updates were distributed to thousands of customers, enabling the attackers to establish persistent access to selected government and private-sector networks. The US Department of Energy confirmed that it was affected, although its initial investigation found the compromise limited to business networks and reported no impact on mission-essential national security functions, including those of the National Nuclear Security Administration. The full operation was principally an espionage campaign rather than an attempt to disrupt energy production.

Implications: Economically, the incident generated extensive investigation and supply-chain security costs. From a security perspective, it exposed the strategic risks of trusted software dependencies and privileged network-management tools. Geopolitically, it intensified US-Russia cyber tensions and demonstrated how a state actor could exploit a widely distributed commercial product to gain intelligence access across government and critical infrastructure.

Colonial Pipeline ransomware attack - May 2021

Country: United States. **Type:** Ransomware and operational shutdown **Attribution:** DarkSide, a cybercriminal group operating from the Russian-speaking ecosystem

On 7 May 2021, Colonial Pipeline suffered a ransomware attack attributed by the FBI to the DarkSide group. Although the initial compromise affected the company's IT environment rather than directly disabling its operational technology, the company proactively shut down its pipeline system to contain the threat. The pipeline, which transports a substantial share of the fuel consumed on the US East Coast, remained offline for several days, contributing to fuel shortages, panic buying, and temporary price increases in affected areas. Colonial paid approximately $4.4 million in ransom, part of which the US Department of Justice later recovered.

Implications: Economically, the incident disrupted fuel distribution and demonstrated how a corporate IT compromise can create physical supply-chain consequences. From a national security perspective, it exposed the interdependence of digital systems and essential energy services. Geopolitically, it prompted renewed debate about ransomware actors operating from jurisdictions where enforcement cooperation is limited, and accelerated US efforts to strengthen critical-infrastructure cybersecurity and incident reporting.

Rompetrol / KMG International HIVE ransomware attack - March 2022

Country: Romania. **Type:** Ransomware and digital-service disruption. **Attribution:** HIVE ransomware group, according to contemporaneous cybersecurity reporting

On 6–7 March 2022, Rompetrol, part of KMG International, experienced a ransomware attack that disrupted much of its IT infrastructure. The company temporarily suspended its websites and the Fill&Go digital fueling service used by private customers and fleet operators. Rompetrol stated that its fuel stations continued operating and that the operational activity of the Petromidia refinery was not affected. The company progressively restored its IT services during March. Contemporary reporting attributed the incident to the HIVE ransomware group, which reportedly demanded a multimillion-dollar ransom.

Implications: Economically, the attack disrupted customer services and business processes and generated recovery costs, although no refinery shutdown or national fuel-supply interruption was reported. From a security perspective, the incident illustrates the vulnerability of digital platforms supporting downstream energy operations, even where industrial processes remain operational. Geopolitically, it highlights the exposure of energy infrastructure in south-eastern Europe to transnational cybercrime during a period of heightened regional insecurity following Russia's invasion of Ukraine; however, there is no established evidence that the attack was state-directed or connected to the war.

Industroyer2 Attack Against Ukraine's Power Grid - April 2022

Country: Ukraine. **Type:** OT/ICS-targeted malware, attempted grid disruption. **Attribution:** Sandworm (Russia-linked)

In April 2022, the Russian-linked Sandworm group attempted to disrupt electricity distribution in Ukraine using Industroyer2, a modified version of the malware previously deployed against Ukraine's power grid in 2016. The attackers targeted high-voltage substations and simultaneously deployed destructive wiper malware against IT infrastructure, potentially complicating recovery. The operation was detected and disrupted through cooperation between Ukraine's CERT-UA and ESET before the intended power outage could be achieved.

Implications: The incident demonstrated the strategic integration of cyber operations into conventional warfare, particularly their potential to undermine civilian infrastructure and complicate military and emergency responses. It also illustrated the continuing evolution of malware designed to manipulate industrial control systems directly, reinforcing the importance of OT-specific defensive capabilities and cyber-physical resilience.

Sandworm's Cyber-Induced Power Outage in Ukraine - October 2022

Country: Ukraine. **Type:** OT manipulation and destructive malware. **Attribution:** Sandworm (Russia-linked)

In October 2022, Sandworm successfully disrupted a Ukrainian electricity substation, causing an unplanned power outage. Unlike previous attacks relying on specialized ICS malware, the attackers used legitimate operational tools and commands already present in the target environment, an approach known as living off the land. The cyber operation coincided with Russian missile strikes against Ukrainian critical infrastructure and was followed by the deployment of CaddyWiper malware against the victim's IT systems.

Implications: This case provides particularly strong evidence of the convergence of cyber and kinetic operations within contemporary warfare. It illustrates how cyberattacks can contribute to infrastructure degradation without requiring sophisticated custom malware, while also complicating attribution, detection, and recovery. Geopolitically, it demonstrates the use of energy disruption as an instrument of coercion and strategic pressure against civilian populations.

Coordinated Cyberattacks Against Denmark's Energy Infrastructure - May 2023

Country: Denmark. **Type:** Network intrusion and potential OT compromise. **Attribution:** Contested; possible state involvement

In May 2023, a series of cyberattacks compromised 22 Danish energy companies, exploiting vulnerabilities in Zyxel firewalls and other network infrastructure. According to Denmark's SektorCERT, attackers gained access to industrial control systems at some organizations, prompting several operators to adopt isolated operating configurations (island mode) as a precaution. Although widespread energy disruption was avoided, the incident represented one of Denmark's most significant cybersecurity emergencies involving critical infrastructure.

Implications: The attacks exposed systemic vulnerabilities associated with common technologies deployed across multiple energy operators. They also demonstrated the risks posed by compromised perimeter devices and the importance of sector-wide threat intelligence sharing. From a geopolitical perspective, the incident heightened concerns over European energy security amid Russia's war against Ukraine, although direct Russian responsibility was not conclusively established.

Cyberattack Against Halliburton - August 2024

Country: United States. **Type:** Corporate IT compromise and data exfiltration. **Attribution:** Not conclusively established in the company's disclosure

In August 2024, Halliburton, one of the world's largest oilfield services companies, experienced a cyberattack that forced it to take certain information systems offline and temporarily restricted access to business applications supporting its operations and corporate functions. The company subsequently confirmed that unauthorized actors had accessed its systems and were believed to have extracted information. Although Halliburton continued providing services and the incident did not reportedly disrupt national energy supplies, it generated operational difficulties, recovery expenses, and potential legal and regulatory exposure.

Implications: The case demonstrates how cyberattacks against energy-sector service providers can generate economic and supply-chain risks even without directly compromising industrial control systems. It highlights the strategic importance of securing the broader energy ecosystem, including contractors, service providers, and interconnected digital platforms.

Coordinated Attacks Against Poland's Energy Infrastructure - December 2025

Country: Poland. **Type:** OT sabotage, destructive malware and remote-control disruption. **Attribution:** Subject to investigation

On 29 December 2025, coordinated destructive cyberattacks targeted more than 30 Polish wind and solar installations and combined heat and power facilities. Attackers damaged industrial automation devices, disrupted communications between renewable generation facilities and distribution operators, and attempted to destroy data using wiper malware. A subsequent investigation also identified an attack against another heating and power facility, where attackers exploited connectivity through a private mobile access network (APN), causing a temporary interruption of the cogeneration process. Electricity production at the targeted renewable facilities continued, and major disruptions to consumer heating supplies were avoided.

Implications: The incident demonstrated that distributed renewable energy infrastructure is increasingly exposed to coordinated cyber-physical sabotage. It highlighted vulnerabilities in remote-access arrangements, industrial device configurations, and the integration of decentralized generation into national grids. Strategically, the attacks underscored the vulnerability of energy infrastructure in NATO's eastern flank, especially during periods of heightened geopolitical tension and winter energy demand.

CYBER THREATS TO THE ENERGY SECTOR | EVIDENCE & IMPACT

A INCIDENT TRENDS

Energy sector share of reported incidents (ENISA NIS360)

10%
of reported CIRAS incidents in 2023 involved the energy sector
2023

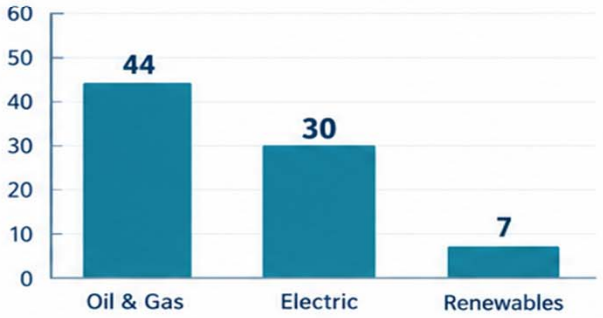
15%
of reported CIRAS incidents in 2024 involved the energy sector
2024

36%
of energy-sector incidents in 2023 were attributed to malicious activity
2023

Note: These figures refer to reported incidents through the EU's CIRAS system (NISD), not to all cyberattacks. Source: ENISA NIS360 2024.

B RANSOMWARE BY INDUSTRIAL SECTOR, 2024

Number of publicly reported ransomware incidents (Dragos, 2024)



1,693
ransomware incidents across **ALL** industrial sectors, +87% vs 2023

Note: The 1,693 figure covers all industrial sectors, not just the energy sector.

Source: Dragos 2025 OT Cybersecurity Year in Review.

C CONSEQUENCES

Operational impact (Dragos, 2024)

Some operational disruption — **75%**

Full shutdown — **25%**

Among Dragos incident-response ransomware cases in 2024; not sector-wide rates.

Common impacts

- Downtime
- Fuel supply disruption
- Recovery costs
- Data theft
- Public services disruption

D THREAT LANDSCAPE & STRATEGIC EFFECTS

Common attack types

- **Ransomware & extortion** — *Encryption, data theft, leak sites*
- **Phishing / credentials** — *Stolen accounts, initial access*
- **Supply-chain compromise** — *Trusted software or services*
- **OT/ICS manipulation** — *Process disruption, physical impact*
- **DDoS / hacktivism** — *Service unavailability, distraction*

Strategic effects

- **Energy security** — Risk to infrastructure and supply continuity
- **Economic resilience** — Financial losses, market and supply-chain disruption
- **Geopolitical coercion** — State-linked activity, conflict escalation

Sources: ENISA NIS360 2024; European Commission / ENISA Annual NISD Incidents Report 2024; Dragos 2025 OT Cybersecurity Year in Review.

Note: Figures are from different datasets and reporting periods and should not be combined.

EU’s regulatory response

Over the past decade, the EU has introduced several legislative and regulatory frameworks to enhance security across critical infrastructure such as electricity networks.

- **The NIS 2 Directive (2024):** The Network and Information Security Directive 2, aims to create a more robust and harmonised approach to cybersecurity across the EU. NIS 2 expands the scope of cybersecurity requirements to electricity, oil & gas networks. Its mandates include:
  - Greater coordination between EU Member States when responding to cyber threats.
  - Stronger risk management measures for energy operators.
  - Improved incident reporting to national authorities.



- **The Cyber Resilience Act (2024):** This Act sets new cybersecurity standards for hardware and software products, ensuring that all digital components used in energy systems meet strict security requirements. It applies to smart meter gateways.



EU’s regulatory response

- **The Network Code on Cybersecurity (2024):** This introduces cybersecurity rules tailored to electricity networks, focusing on:

- Grid protection measures to prevent unauthorised access.
- Incident response protocols to detect and contain cyber threats.
- Stronger security requirements for third-party vendors supplying IT and OT to energy companies.

- **The EU Preparedness Union Strategy (2025):** The strategy offers a comprehensive approach to preparedness, bringing different actors together, from the public and private sectors, civilian and military. Goals and actions presented by the strategy include:

- Stockpiling of energy equipment
- EU-wide preparedness exercises
- Cooperation with NATO
- Integrated risk and threat assessments



EU REGULATORY RESPONSE TO CYBER THREATS IN THE ENERGY SECTOR

A COMPREHENSIVE FRAMEWORK FOR RESILIENCE & COOPERATION

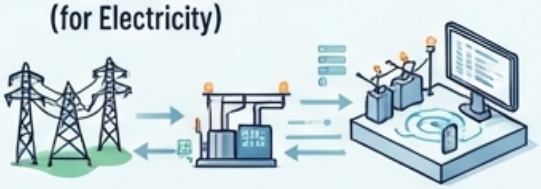
KEY LEGISLATION & DIRECTIVES

1.1 NIS 2 DIRECTIVE
(Network & Information Systems)



- Broader Scope (Energy Entities)
- Stricter Incident Reporting (e.g., 24h notifications)
- Enhanced Security Requirements (Supply Chain)
- Mandatory Management Responsibility

1.2 NETWORK CODE ON CYBERSECURITY
(for Electricity)



- Harmonized Rules for Cross-Border Flows
- Risk Assessment Methods
- Common Minimum Requirements
- Information Exchange

EU REGULATORY FRAMEWORK

STRATEGIC LAYERS OF PROTECTION

2.1 GOVERNANCE & COOPERATION



- ENISA's Role (Guidance, Training)
- CSIRTs Network (Incident Response)
- Cooperation Group (Strategic Alignment)



OPERATIONAL RESILIENCE

- Regular Stress Tests & Audits
- Information Sharing Platforms (e.g., ISACs)
- Crisis Management Exercises

EU REGULATORY FRAMEWORK

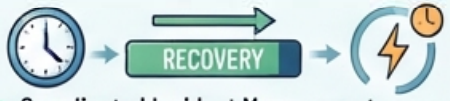
IMPACT & GOALS

3.1 ENHANCED PROTECTION



- Secure Critical OT/IT Systems
- Reduced Attack Surface
- Faster Threat Detection

3.2 FASTER RESPONSE & RECOVERY



- Coordinated Incident Management
- Effective Mitigation Strategies
- Minimal Operational Disruption

3.3 TRUST & STABILITY



- Cross-Border Energy Security
- Consumer Confidence
- Sustainable Digital Transformation

EUROPEAN UNION
ENISA
European Commission

Enhancing Cyber-resilience of the Energy Sector

- **Provide incentives to companies that invest in cybersecurity:** Offering grants or tax subsidies for cyber-security projects can encourage the energy sector to invest in research, training, and technology, making the cyber investment more financially viable for such organizations.

- **Assist companies to comply with cybersecurity regulations:** Regulatory bodies should make it easier for the energy sector to navigate compliance requirements and focus on building their cyber capabilities. This can be achieved through consolidation of legislation and regulation, also while emphasizing the move to a more risk-based approach.

- **Establish a collaborative and shared responsibility framework:** To safeguard the critical national infrastructure, various stakeholders including government entities, regulatory bodies, energy companies and other relevant parties, would need to engage in a coordinated effort to address cybersecurity challenges. By eliminating silos and enhancing communication by creating platforms for information sharing, the government can respond more effectively to the growing threat landscape.

- **Collaborate with national laboratories and universities for advanced cyber research:** Governments could provide national laboratories that would enable an organization to establish a digital twin of a particular critical system or even a wider ecosystem. This would allow for testing cyber architecture, configuration, and even change of a digital environment in a safe environment to stress test the cybersecurity.

Enhancing Cyber-resilience of the Energy Sector

- **Secure the supply chain:** Governments could assist in securing the supply chain of critical national infrastructure organizations by providing testing and certification of critical OT components.

- **Building future-ready cyber workforce:** Governments should provide an educational framework that will focus on the urgent needs to develop IT and OT talent to meet the growing demand. They should also consider options such as providing financial aid, scholarships or sponsorships for employees pursuing cybersecurity education to encourage skill development within the organization.

- **Establish guidelines and standards to address state-sponsored cyberattacks:** International collaboration can promote a more secure and stable energy infrastructure, by creating a framework for multilateralism that outlines appropriate responses, boundaries, and expectations when it comes to cyber activities affecting critical national infrastructure.

- **Contact regular exercises at the national / international level** (e.g. NATO, EU, ENISA, national CERTs)

* **Develop a (cyber)security culture at all levels !**



Conclusion

- **Digital transformation** and the rapid adoption of advanced technologies around the world is creating an even larger and more **complex attack surface** for adversaries to exploit. This is further exacerbated, as adversaries learn to leverage advanced digital technologies and sophisticated capabilities to exploit the industrial control systems in the energy sector.

- Moreover, **unstable geopolitical situations** have enabled the escalation of state-sponsored cyberattacks on critical infrastructure around the world. Despite the increasing cyber regulations and the addition of some resources and programs, cyberattacks are continuously rising.

- In conclusion, to combat increasing cyber threats while enabling energy companies to be creative and develop new energy sources, it is important to **build cyber resilience capabilities** in critical national infrastructure, using a more **proactive approach**, with advanced regulatory frameworks put in place by the government through increased collaboration with public and private sector organizations.



Questions