A4: Special Issues in Energy, Environment and Climate Change

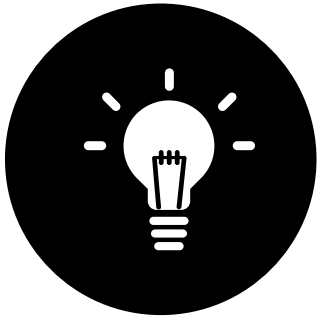
CYBER THEATS & ENERGY SECURITY

Andrew Liaropoulos
Associate Professor

29/11/2025

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**

Cyberspace & Cybersecurity

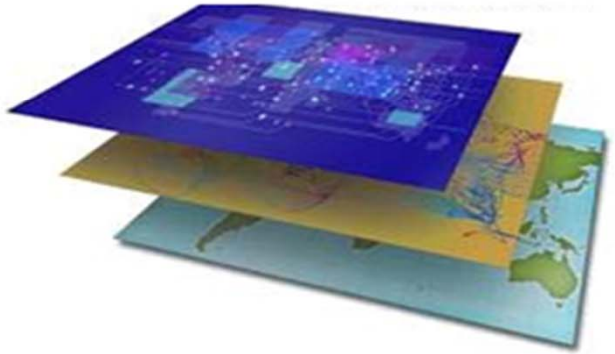
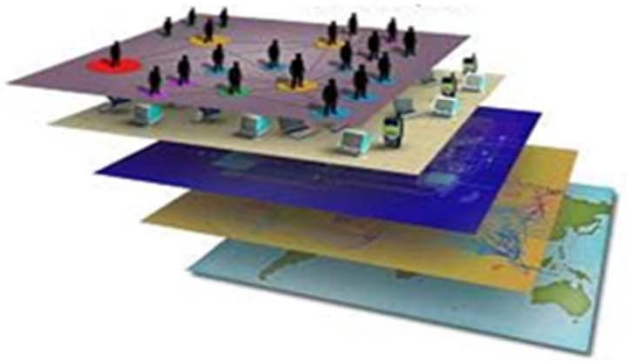
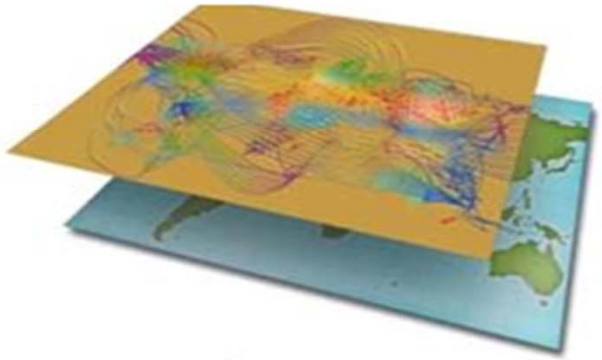
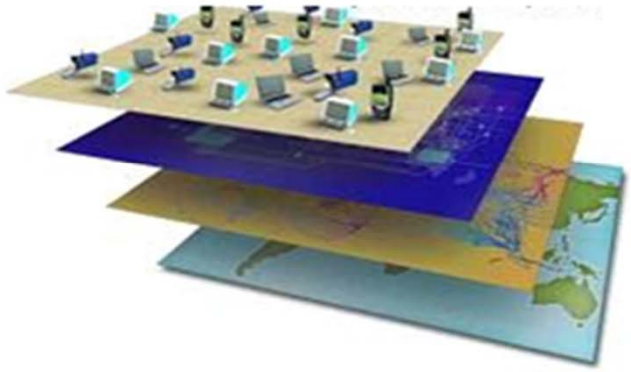
Cyberspace = cyber + space

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* 

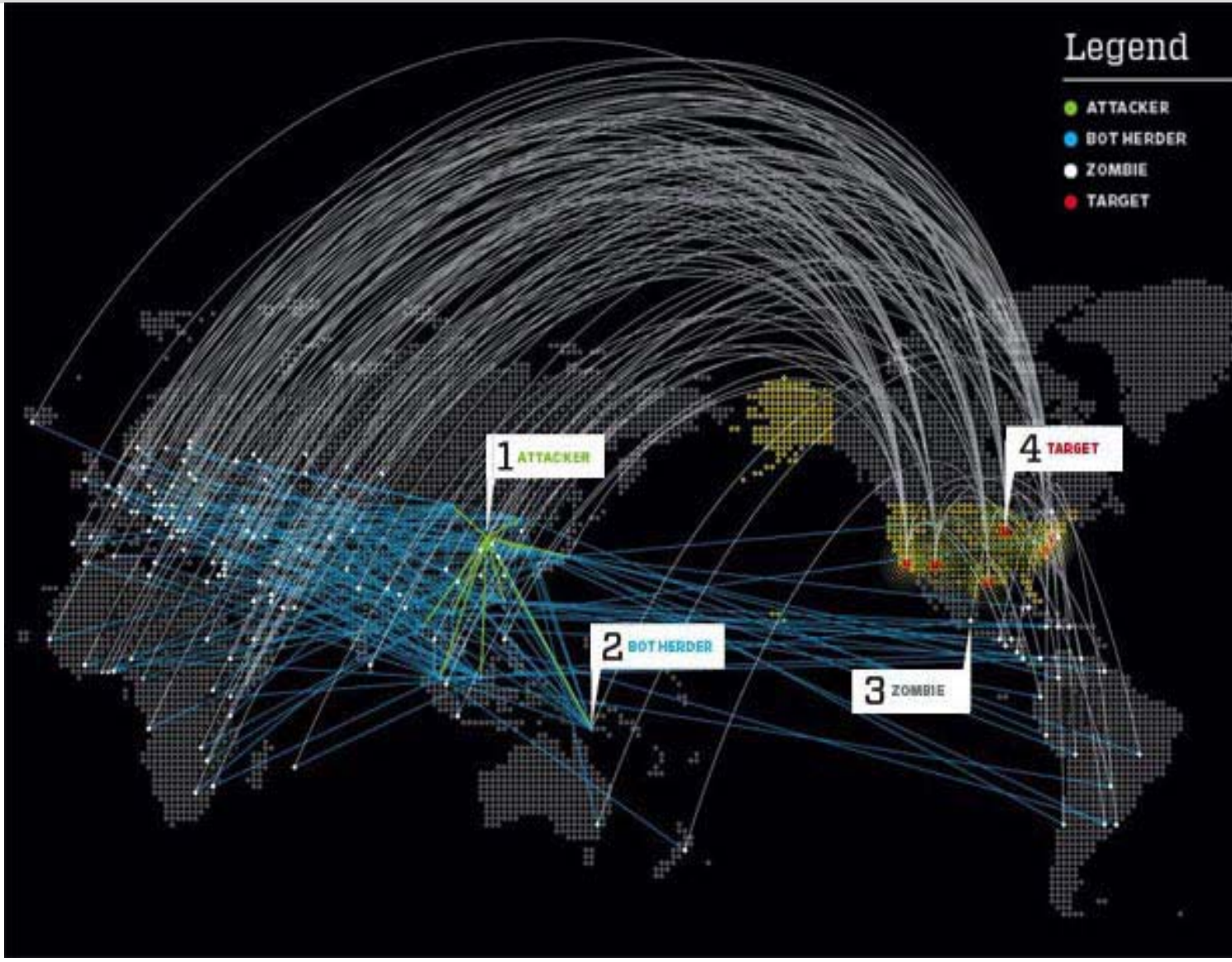
Cyberspace & Cybersecurity

- **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

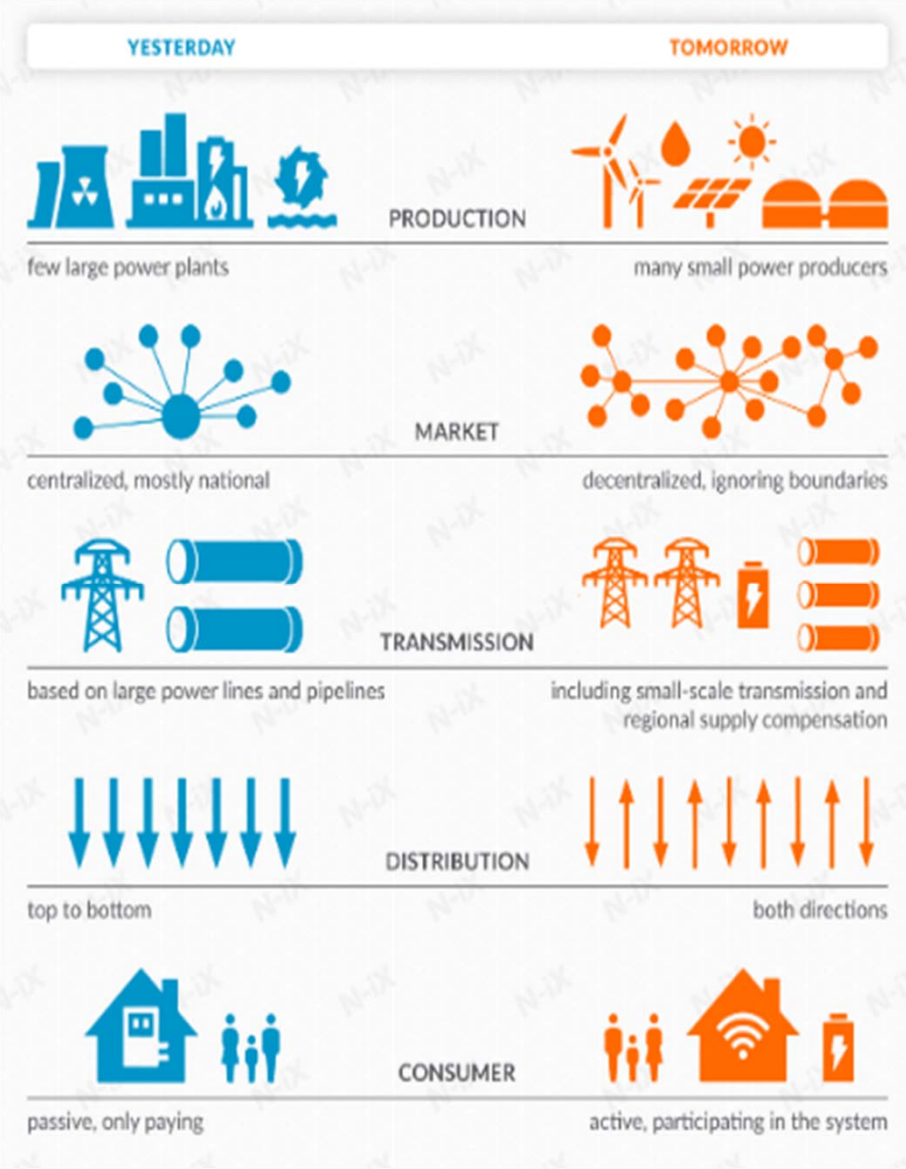
- **Cyber-deterrence**

- **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 optimise 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.

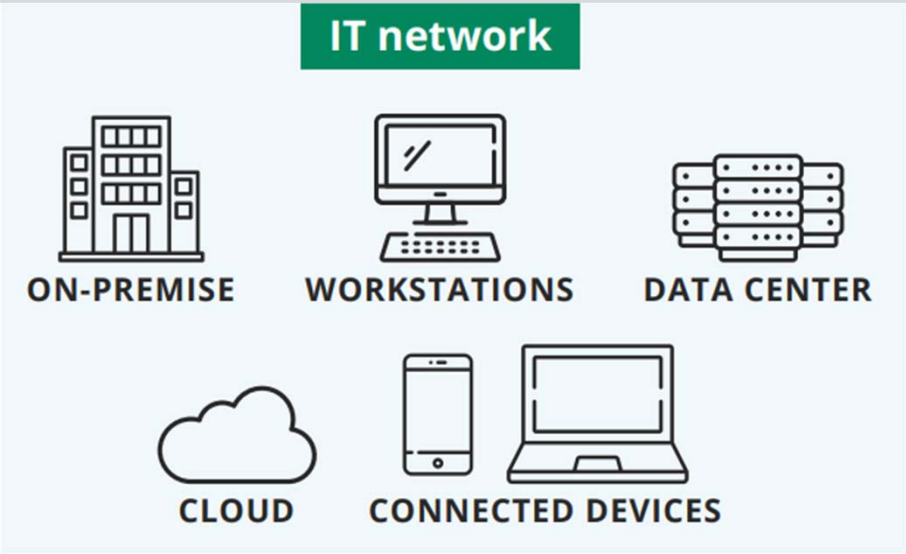
- Modern power systems rely on complex networks of smart meters sensors and automated control systems, all of which can be exploited. Cybercriminals can **target weak points** in these networks to disrupt operations, steal data or manipulate energy flows.

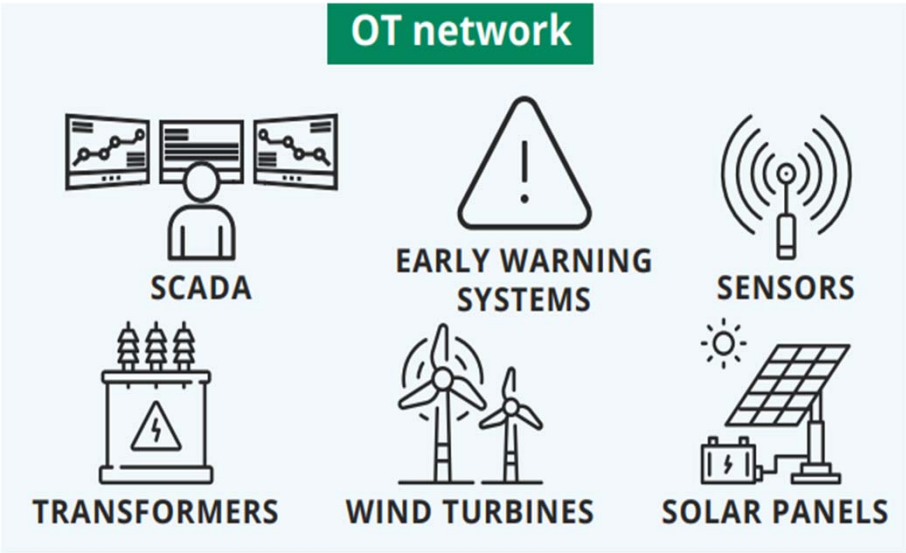
- Another key challenge is the **dependency on real-time data and automation**. While it optimises grid efficiency, it can also introduce risks if compromised. A cyberattack that manipulates data or disrupts automated controls could lead to widespread blackouts, equipment failures or financial losses.

- 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

- **Information Technology (IT)** combines technologies for networking, information processing, data centers, and cloud systems.
- **Operational technology (OT)** is the hardware and software that monitors and controls devices, processes, and infrastructure, and is used in industrial settings.
- OT devices control the physical world, while IT systems manage data and applications. IT is necessary for monitoring, managing, and securing core functions such as email, finance, human resources and other applications in the data center and cloud.
- OT is for connecting, monitoring, managing, and securing an organization's industrial operations. OT involves industrial control systems (ICS) and Supervisory control and data acquisition (SCADA).





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, such as **Stuxnet** are capable of causing physical damage to critical assets, disrupting operations, and compromising safety systems.

Cyber threats to the energy sector

Espionage

For the information

Espionage threat actors (often referred to as “Advanced Persistent Threats”, or APTs) typically seek to steal information which will provide an economic or political advantage to their benefactor. Attacks motivated by espionage usually originate from either industry competitors or state-sponsored threat actors. Often the benefactor is a nation state, and espionage activity aligned to state objectives will reflect geopolitics and real-world events.

Usually, the information sought out by espionage attackers is only found at specific organisations, meaning they repeatedly target the same organisation and their suppliers until they have completed their mission.

Sabotage

For the impact

Saboteurs seek to damage, destroy or otherwise subvert the integrity of data and systems. Sabotage attacks are not always deliberate and have been used to mask other malicious activity. Sabotage operations designed to be a diversion can still result in significant collateral damage.

Examples of attacks include wiping hard drives, causing SCADA systems to malfunction or altering trade data. As with espionage attacks, attacks from saboteurs tend to be influenced by real-world events, making the risk of attacks specific to geography and company actions in relation to political events/issues.

Cyber threats to the energy sector

Hacktivist

For the cause

Hacktivists conduct attacks to increase their public profile and raise awareness of their cause. This is typically done through the disruption of services such as denial of service (DoS) attacks, and website defacements. In many cases such attacks are random; they care little how this is done or who is affected, so long as their message is promoted.

In some cases, however, their victims are targeted, due to an organisation or individual's perceived actions or support of an issue. As with espionage, attacks from hacktivists are sometimes influenced by real-world events, meaning the risk of such attacks is subject to change.

Criminal

For the money

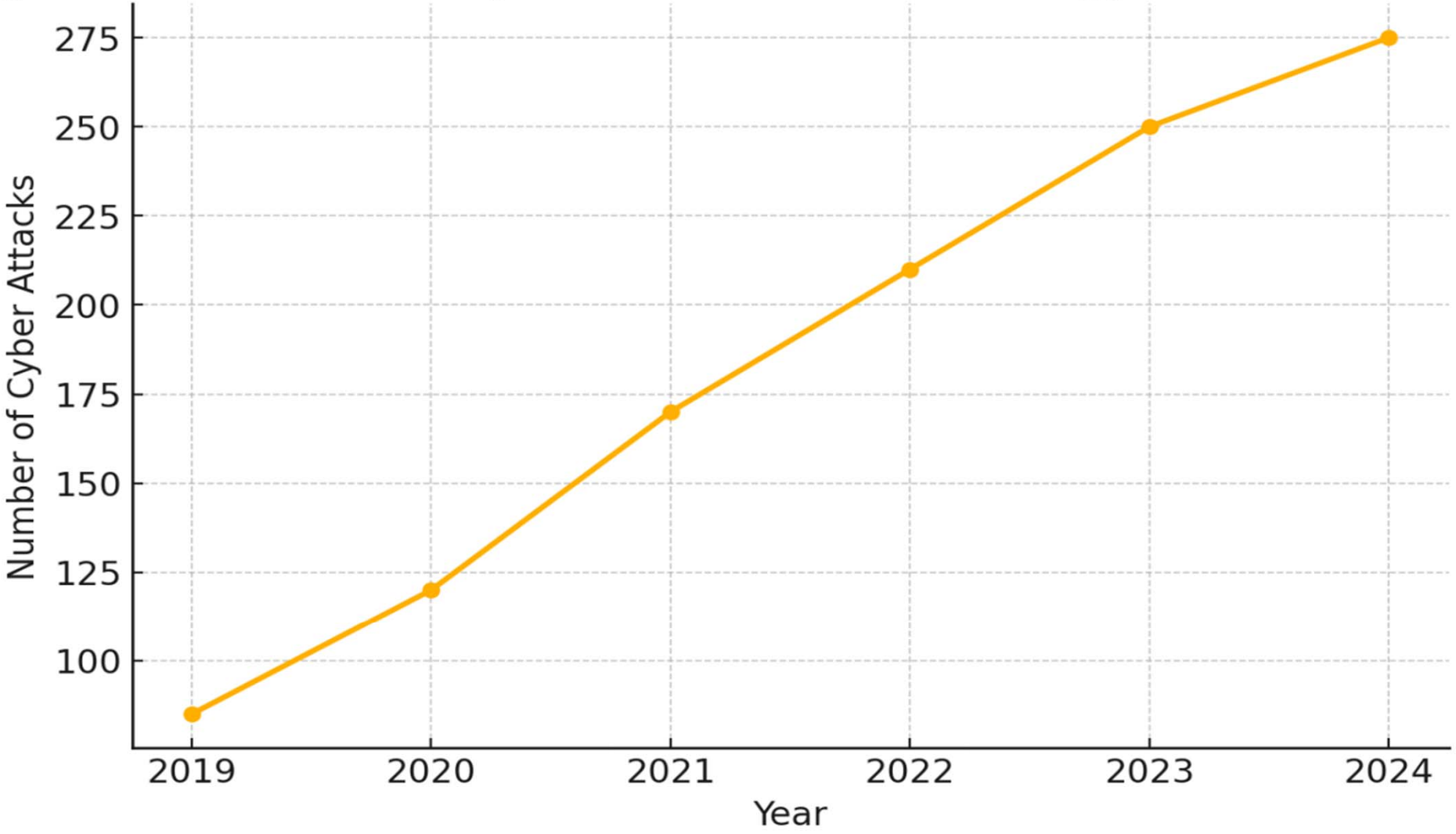
Cyber criminals can be indiscriminate in who they attack as they simply seek to monetise their activities. The range in sophistication of cyber criminals is vast, and displays a widely different set of Tactics, Techniques and Procedures (TTPs).

Cyber crime includes both direct 'cash out' schemes where an immediate financial gain is made, such as business email compromise, ATM hijacking or the theft of cryptocurrency wallets, as well as activity that seeks to monetise stolen data such harvesting payment card details or other personal information. Many cyber criminals are merely consumers of stolen data compromised by more sophisticated actors; this data is typically used to commit fraud or identity theft.

Ransomware has become a particularly prevalent cause for concern, affecting major private sector corporations through to charities and local government, and everything in-between.

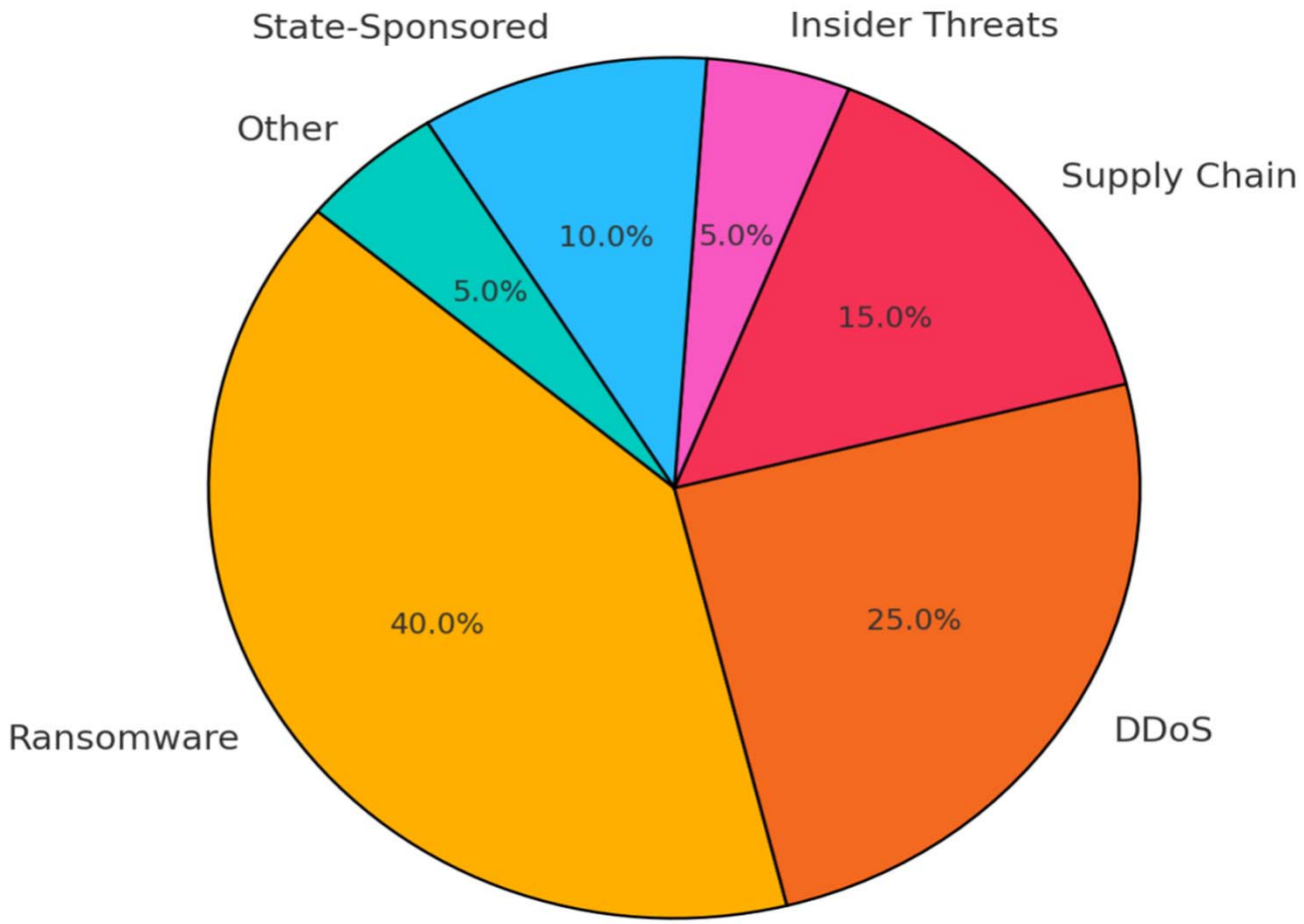
Cyber threats to the energy sector

Figure 1: Increase in Cyber Attacks on the Energy Sector (2019–2024)



Cyber threats to the energy sector

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



Cyber threats to the energy sector

Figure 3: Cyber Attacks on Energy – Regional Breakdown (2023)

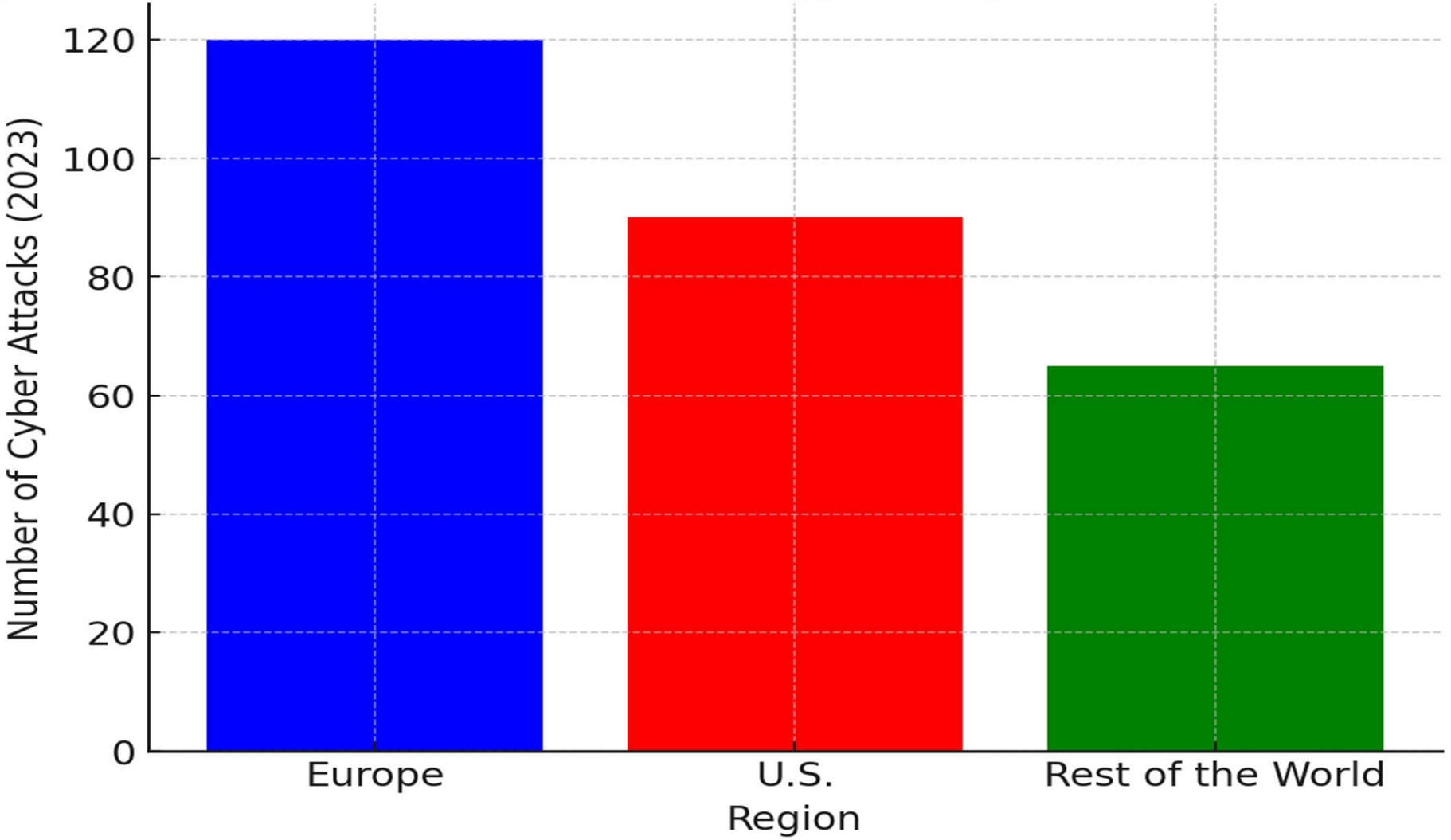
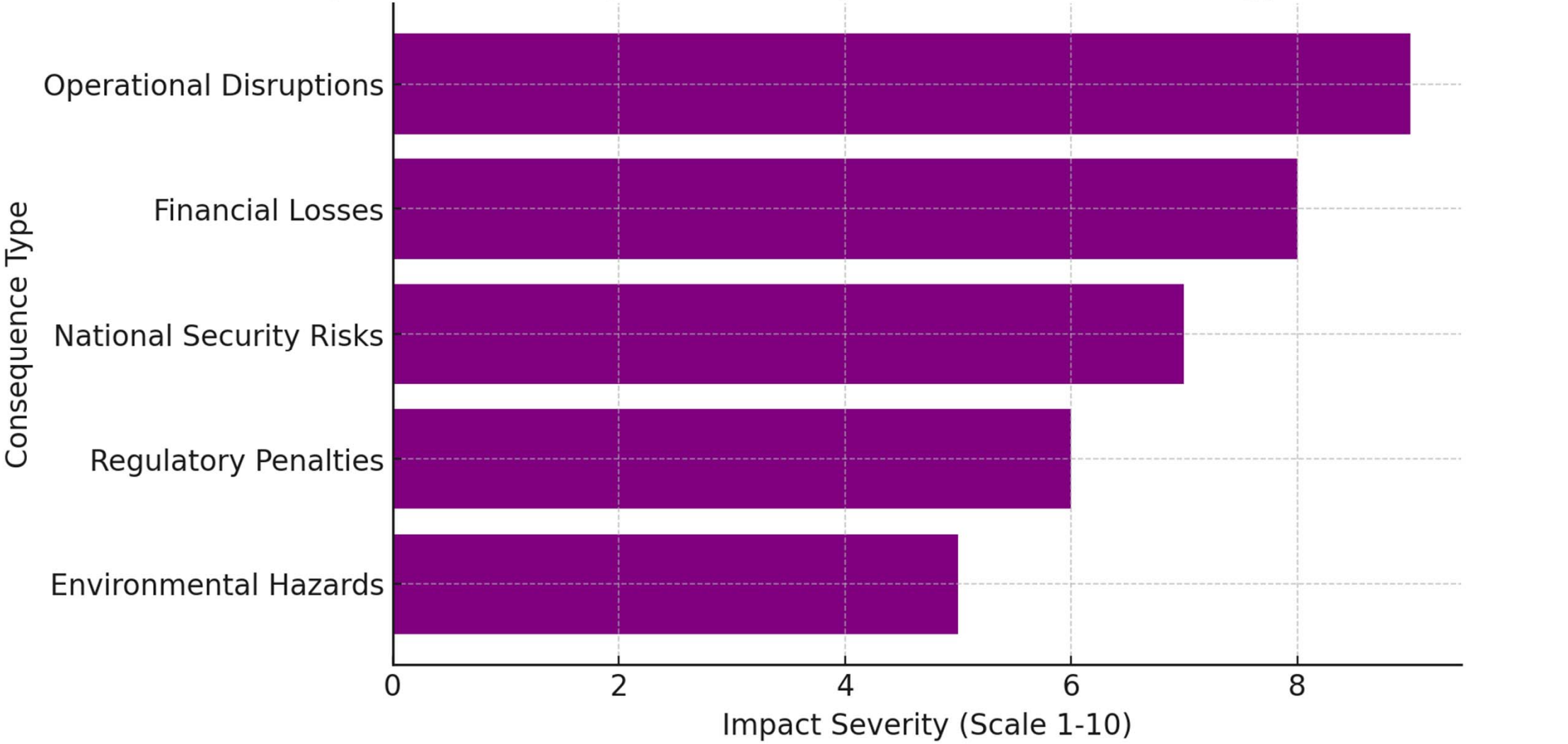
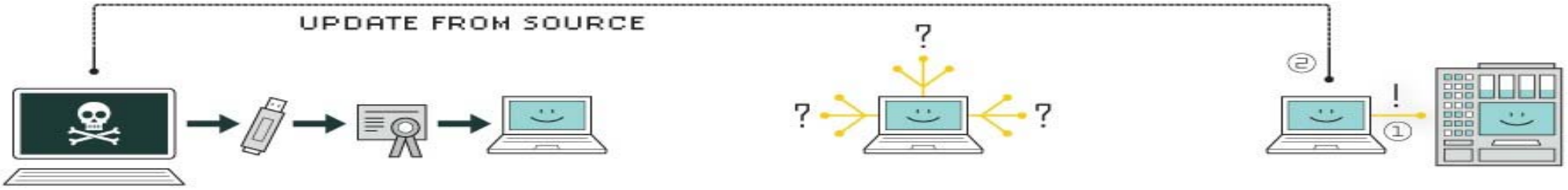


Figure 4: Consequences of Cyber Attacks on Energy Infrastructure



Cyber threats to the energy sector (Stuxnet 2008-2010)

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Cyber threats to the energy sector (Stuxnet 2008-2010)

Geopolitical Implications:

- Introduced cyber tools as strategic weapons against energy and nuclear infrastructure.
- Delayed Iran's nuclear program without direct military engagement (cyber being the preferable option).
- 'Forced' Iran to expand its own cyber capabilities, later used against Saudi Arabia, Israel, and the U.S.
- Raised global concerns about escalation thresholds for cyber warfare.
- Side effect: Collateral Damage caused by the worldwide spread of Stuxnet.

Cyber threats to the energy sector (Saudi Aramco 2012)

- In 2012, hackers wiped data from approximately 35.000 computers belonging to Saudi Aramco, one of the world's largest oil companies. Malware called **Shamoon** stole passwords, wiped data, and prevented computers from rebooting.
- Hackers calling themselves the **"Cutting Sword of Justice"** claimed responsibility for the incident, asserting they were retaliating against the al-Saud regime for what the group called widespread crimes against humanity. US intelligence sources have attributed the attack to Iran.
- Two weeks after the Aramco incident, the Qatari gas giant **RasGas** was also knocked offline by suspected state-sponsored attackers.
- The Saudi Aramco incident signaled Iran's growing cyber capabilities and Tehran's willingness to use them to promote its interests, particularly in the Middle East.

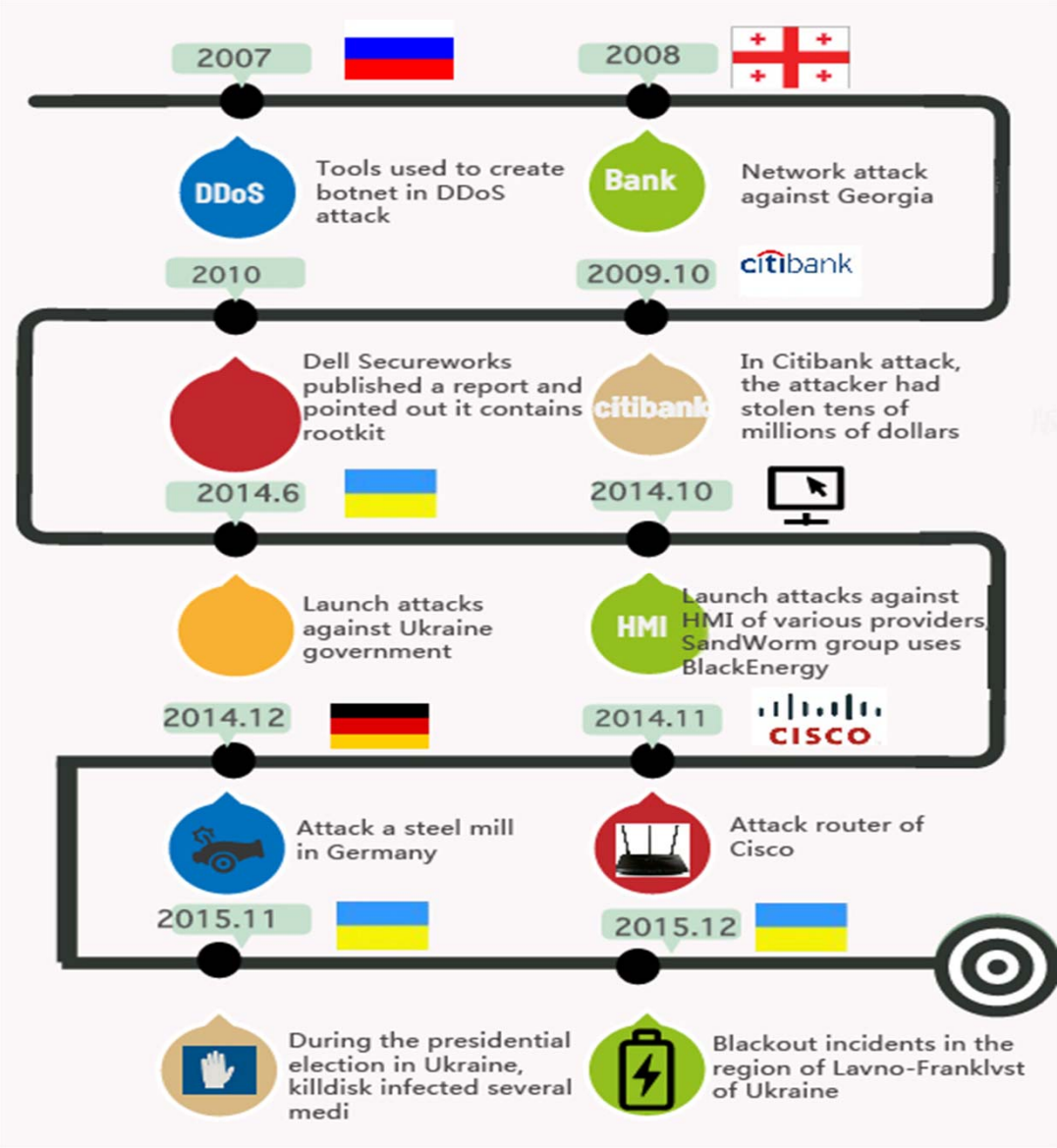
Cyber threats to the energy sector (Saudi Aramco 2012)

Geopolitical Implications:

- Seen as retaliation for Stuxnet and broader Iran-Saudi rivalry.
- Aimed to disrupt global oil markets and weaken a major U.S. ally.
- Triggered a cybersecurity race among Gulf states, with large investments in U.S. and European cybersecurity firms.
- Cyber warfare is being integrated into regional rivalries in the Middle East, especially around energy dominance.

Cyber threats to the energy sector (BlackEnergy 2015)

- On December 23, 2015, unknown cyber actors disrupted energy-grid operations causing blackouts for over 225,000 customers in Ukraine.
- The attackers used a malware tool, **BlackEnergy 3**, designed to enable unauthorized network access, then used valid user credentials to move across internal systems, and ultimately shut down electricity distribution using the utilities' native control systems.
- Attributed to Russia's GRU.



Cyber threats to the energy sector (BlackEnergy 2015)

***Motives:**

- The attackers may have intended to convey displeasure with a Ukrainian proposal to **nationalize assets owned by Russian oligarchs** with investments in Ukraine's energy sector.
- By disrupting operations in the energy sector, the threat actors may have sought to **reduce confidence in the Ukrainian government.** This would be consistent with Russia's IW doctrine, which seeks to sow discontent in a target country to induce political and economic collapse.
- Another possible objective may have been **in-kind retaliation** for perceived Ukrainian disruptions of electricity to Crimea. On November 21-22, 2015, Crimea lost power for more than 6 hours due to physical attacks on 4 pylons carrying transmission wires.

Cyber threats to the energy sector (BlackEnergy 2015)

Geopolitical Implications:

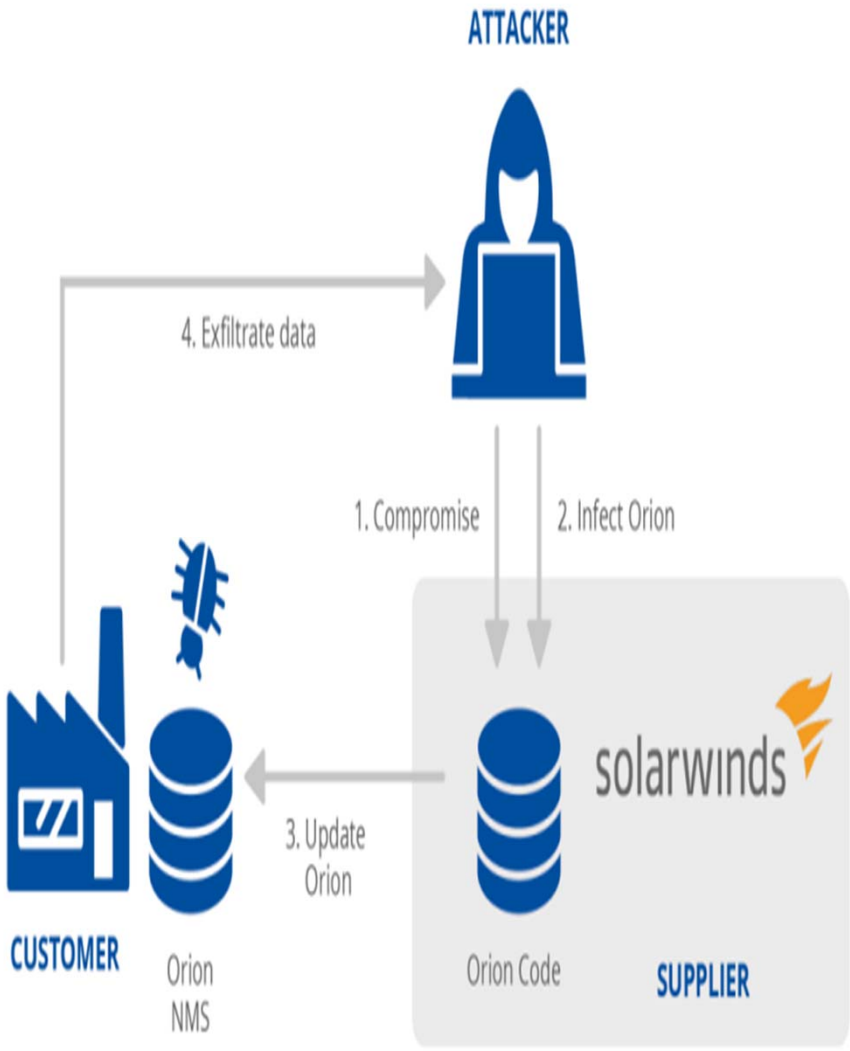
- Demonstrated that cyber-attacks could cause real-world blackouts.
- Used as a hybrid warfare tactic amidst Russia-Ukraine tensions.
- Signaled to NATO the vulnerability of European grids interconnected with Ukraine.
- Elevated debates about whether NATO's Article 5 collective defense could apply to cyber-attacks.
- Cyber-attacks on energy can be used to destabilize a state during military or political conflict.

Cyber threats to the energy sector (SolarWinds 2020)

- The SolarWinds company has over 300.000 customers worldwide.

- The SolarWinds cyberattack was a software supply chain attack involving the SolarWinds **Orion platform**, wherein a Russian nation-state adversary gained access to SolarWinds systems and deployed trojanized updates to the Orion software.

- This, in turn, allowed threat actors to install stealthy malware on SolarWinds customers' networks. The SolarWinds hack was disclosed by multiple cybersecurity companies in conjunction with the US Cybersecurity and Infrastructure Security Agency (CISA) in December 2020.



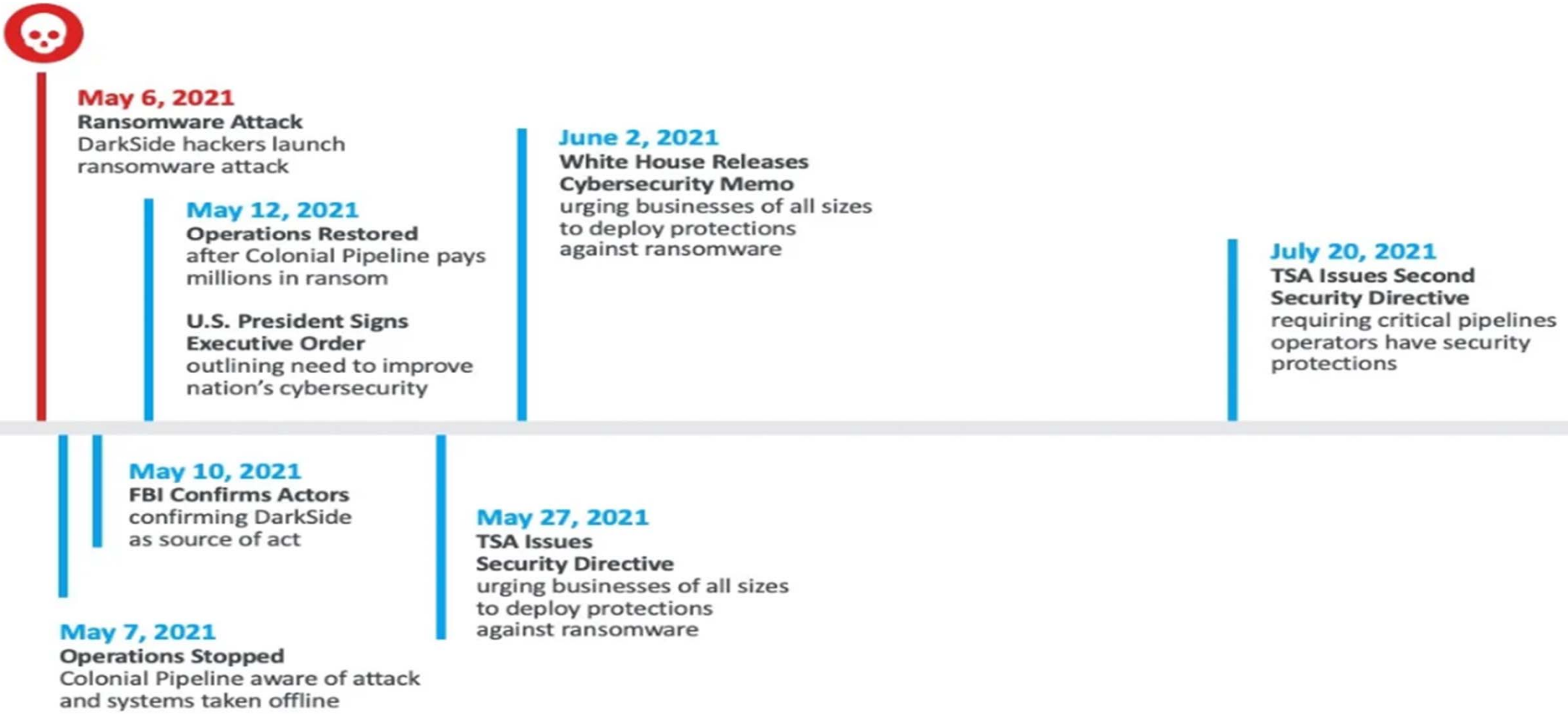
Cyber threats to the energy sector (SolarWinds 2020)

Geopolitical Implications:

- Supply-Chain Vulnerability as a Strategic Pressure Point: Demonstrated that adversaries can compromise energy-sector systems indirectly via software vendors.
- Exposed systemic risks: a single compromised platform affected thousands of networks, including energy regulators.
- The operation expanded Russia's intelligence visibility into U.S. critical infrastructure (including some energy systems).
- Gave Russia potential insights into grid vulnerabilities, emergency-response frameworks, and nuclear materials oversight (though not control systems).
- The U.S. framed the attack as a major national security breach, leading to sanctions and diplomatic expulsions.

Cyber threats to the energy sector (Colonial Pipelines 2021)

A ransomware attack by the group DarkSide forced the shutdown of a major U.S. fuel pipeline, causing fuel shortages on the East Coast.



Cyber threats to the energy sector (Colonial Pipelines 2021)

Geopolitical Implications:

- Exposed vulnerabilities in U.S. critical infrastructure.
- Prompted Washington to pressure Russia to take action against cyber-criminal groups operating from its territory.
- Led to new international agreements on ransomware (e.g., the Counter-Ransomware Initiative).

Cyber threats to the energy sector

- 2022 March: Ransomware HIVE hits Rompetrol, the largest gas station service provider in Romania for a $2 million ransom, causing huge impacts on the company's IT services.

- 2022 April: A cyberattack against German wind-energy company Deutsche Windtechnik in April prompted it to shut down remote-control systems for roughly 2,000 wind turbines for about a day.

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

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 companie,s 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.

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.

- **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.

- **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.

Enhancing Cyber-resilience of the Energy Sector

- **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