Key definitions, threat landscape and select cyber (hybrid) attacks in the energy sector

ERRA Workshop Cybersecurity of Energy Infrastructure

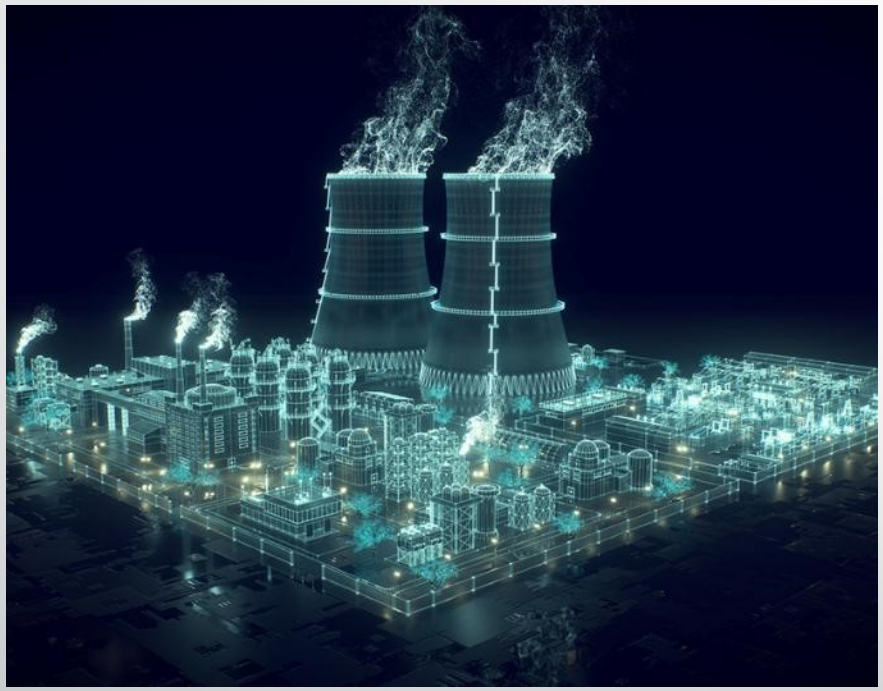
Perry Pederson

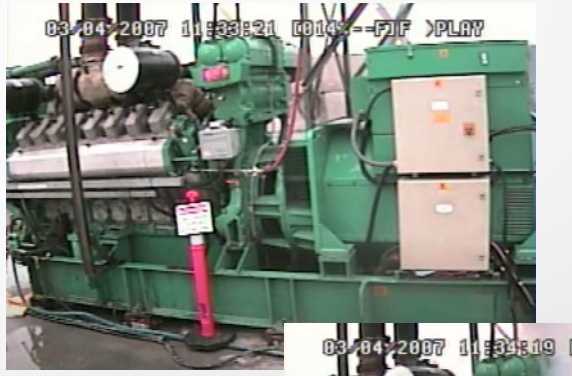
Nuclear Security IT Specialist

Introduction – Who am I?

- Currently with the IAEA
- Strategic thinker in R&D and cyber security
- Worked for US agencies: DoD, DHS, DOE, and NRC
- At the NRC helped shape regulatory framework for cyber security at nuclear power plants
- As the Director for the Control Systems Security Program at DHS, managed the **Aurora** project

Aurora Vulnerability





Aurora video (Youtube): Aurora)

https://www.muckrock.com/news/archives/2016/nov/14/aurora-generator-test-homeland-security/

Key Definitions

What is a Regulator?

- **Definition:**
  - A governing body or authority responsible for overseeing and enforcing rules, standards, and policies to ensure the safety, reliability, and resilience of essential systems and services.
- **What they do:**
  - The regulator works to mitigate risks, prevent disruptions, and safeguard public welfare by monitoring compliance, and coordinating emergency responses.

Definitions

- **Compliance:**
  - Compliance is a willing or required implementation of guidance.
- **Enforcement:**
  - Some frameworks of penalties or sanctions are for lack of compliance with the required guidance.

Definitions (cont.)

- **Safety:**
  - Ensuring that the power grid operates without causing harm to people, property, or the environment. This includes preventing accidents, managing hazardous materials, and maintaining safe working conditions.
- **Reliability:**
  - The ability of the power grid to consistently deliver electricity to consumers without interruptions. This involves maintaining a stable supply, managing demand, and quickly restoring service after outages.
- **Resilience:**
  - The capacity of the power grid to withstand and recover from disruptions, such as natural disasters, cyberattacks, or equipment failures. This includes planning for emergencies, implementing robust infrastructure, and adapting to changing conditions.

Best Practices

- **Definition:**
  - Established methods and procedures that are widely accepted as being the most effective and efficient in achieving desired outcomes.
- **Examples:**
  - ISA/IEC, ISO, IEEE and Vendor standards.
- In most cases these are not enforceable requirements, unless adopted by the regulator
- US NRC incorporated NIST SP 800-53 into their RG 5.71

Regulatory Basis

The overarching theme or goal of a regulatory framework can be several different things. Sometimes these themes can conflict. Examples include:

- **Safety:**
  - An example of safety-first regulation is employed by the US Nuclear Regulatory Commission.
- **Reliability:**
  - An example of reliability first regulation is employed by the North American Electric Grid via the NERC Reliability Standards.
- **Resilience:**
  - The ability of a critical sector to recover from a disruption. Various states and provinces in North America regulate resilience. These regulations are found in State and provincial government requirements.

Performance-Based Regulations

Emphasize outcomes and provide flexibility but can be challenging to measure and enforce.

Pros

- Flexibility
- Efficiency
- Incentives for Improvement

Cons

- Measurement Challenges
- Risk of Gaming the System
- Inconsistent Outcomes

Compliance-Based Regulations

Focus on adherence to specific rules, offering clarity and consistency but may limit innovation and efficiency.

Pros

- Clarity and Certainty
- Uniform Standards
- Easier Enforcement

Cons

- Lack of Flexibility
- Potential Inefficiency
- Stifles Innovation

You Control Your Fate

You can determine the regulatory environment you wish.

Things to consider

- Imposing best practices onto government or private sector companies providing critical services. This imposition will provide assurances of the suitability of the companies providing the services.
- Recognize that the regulated people do not always welcome you. You must present yourself as a positive influence on the reliability or safety of the services.
- Be careful what you wish for – personal anecdote

Recommendation

- Regulators should begin with a set of regulations based on best practices.
- After some experience monitoring compliance issues, then begin the journey toward required compliance and enforcement.
- Regardless of where you begin, the regulatory framework will continue to evolve.

Question for the Group

- Which framework would you recommend for your environment?
  - A voluntary best practices-based framework?
  - A performance-based framework?
  - A stronger compliance and enforcement-based regulatory framework?
- This question should be answered from the perspective of the country's culture in which the regulations will apply.

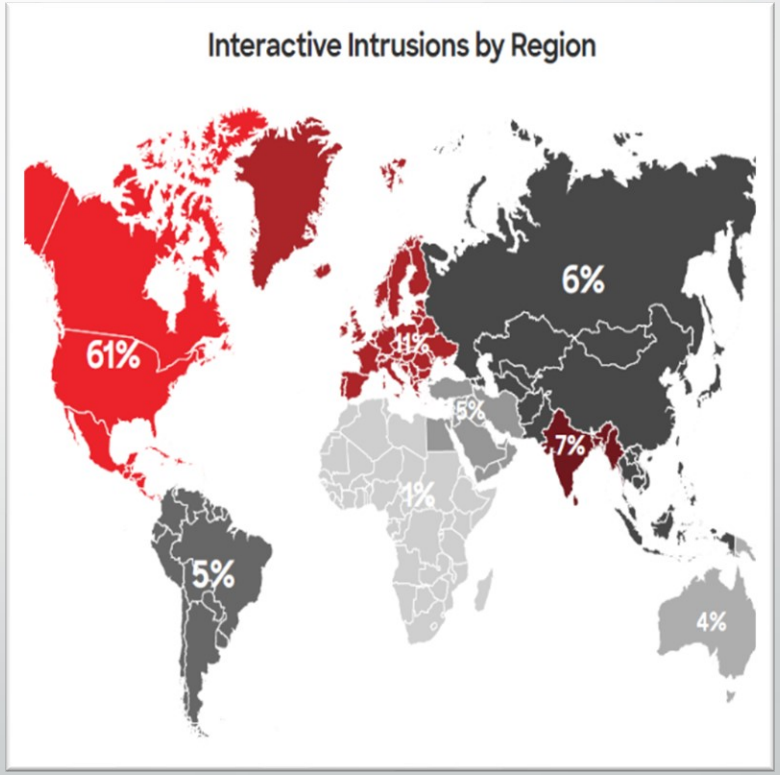
Discussion

- Consider what the US has done.
- The US developed these three regimes separately and now needs to deconflict them daily.
- Asset owners must comply with all three regimes.
- Additionally, the standards can be adopted the Asset Owners but are not enforceable unless they are part of the regulation.

Threat Landscape

Threat Landscape

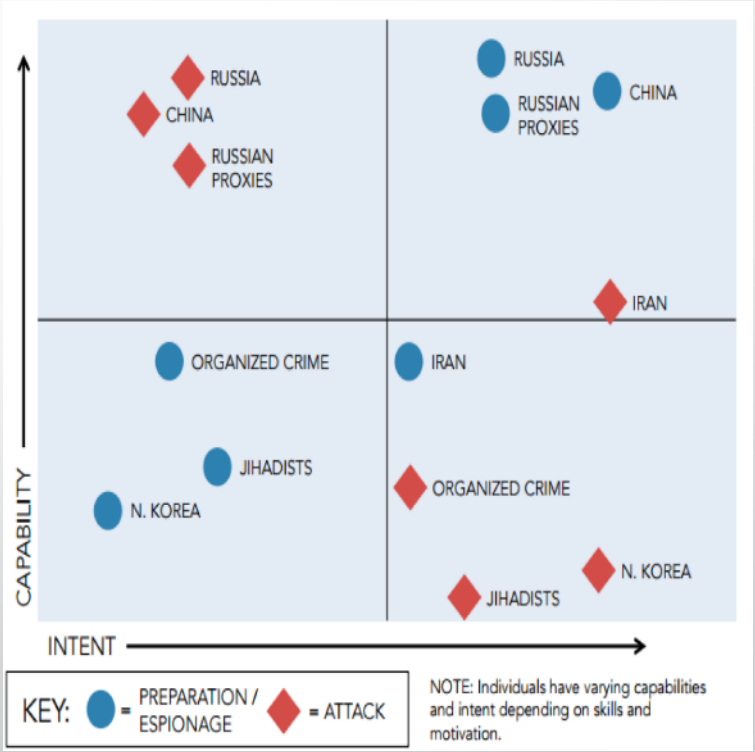
- **Adversaries are gaining speed:**
  - The average eCrime breakout time in 2023 was 62 minutes and once inside, 31 seconds to drop an initial discovery tool.
- **Interactive intrusions are accelerating:**
  - Hands-on-keyboard activity increased by 60% and three-quarters of attacks to gain initial access were malware-free.
- **Cloud is an evolving battleground:**
  - Cloud intrusions increased by 75% in 2023, and cloud-conscious cases spiked by 110%.
- **Data-theft extortion aids monetization:**
  - A 76% increase in the number of victims named on big game hunting (BGH) dedicated leak sites.



Source: Crowdstrike 2024 Global Threat Report

Threat Landscape

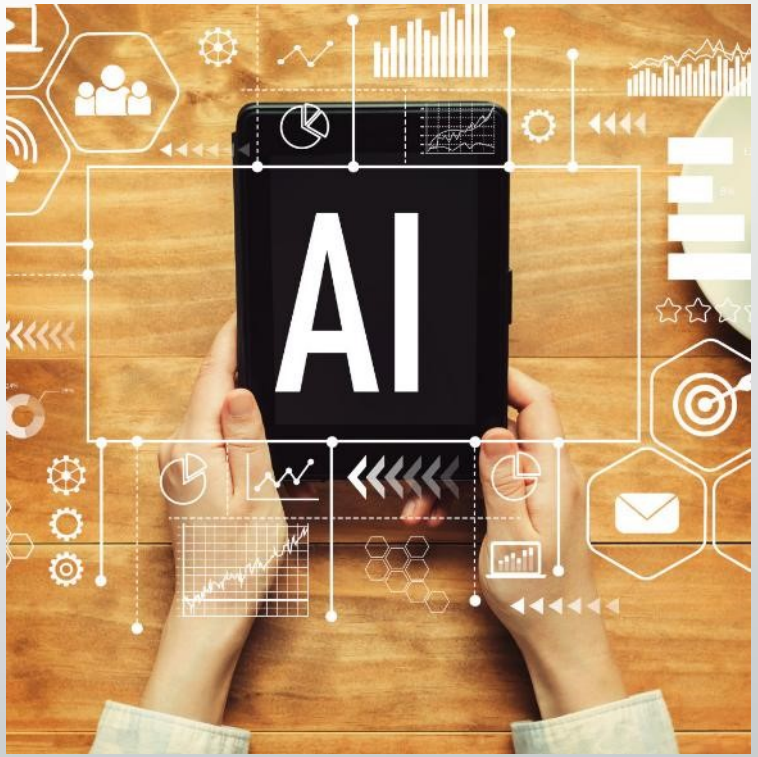
- Interoperable technologies will continue to expand the cyber attack landscape.
- State and non-state threat actors seek to exploit cyber vulnerabilities in the U.S. electrical grid.
- Utilities often lack full scope perspective of their cyber security posture.
- Some utilities require financial assistance to meet regulatory standards and for business security.
- The assortment of regulatory cyber security standards and guidelines produces varied methods of adoption.
- Utilities expect more qualitative, timely threat intelligence from information sharing programs.



Idaho National Lab report: [Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector]

Threat Landscape - AI

- We did not observe any original or persistent attempts by threat actors to use prompt attacks or other machine learning (ML)-focused threats.
- Threat actors are experimenting with Gemini to enable their operations, finding productivity gains but not yet developing novel capabilities.
- APT actors used Gemini to support several phases of the attack lifecycle, including researching potential infrastructure and free hosting providers, reconnaissance on target organizations, research into vulnerabilities, payload development, and assistance with malicious scripting and evasion techniques.
- IO actors used Gemini for research; content generation including developing personas and messaging; translation and localization; and to find ways to increase their reach.
- Gemini's safety and security measures restricted content that would enhance adversary capabilities as observed in this dataset.



Google report: Adversarial Misuse of Generative AI

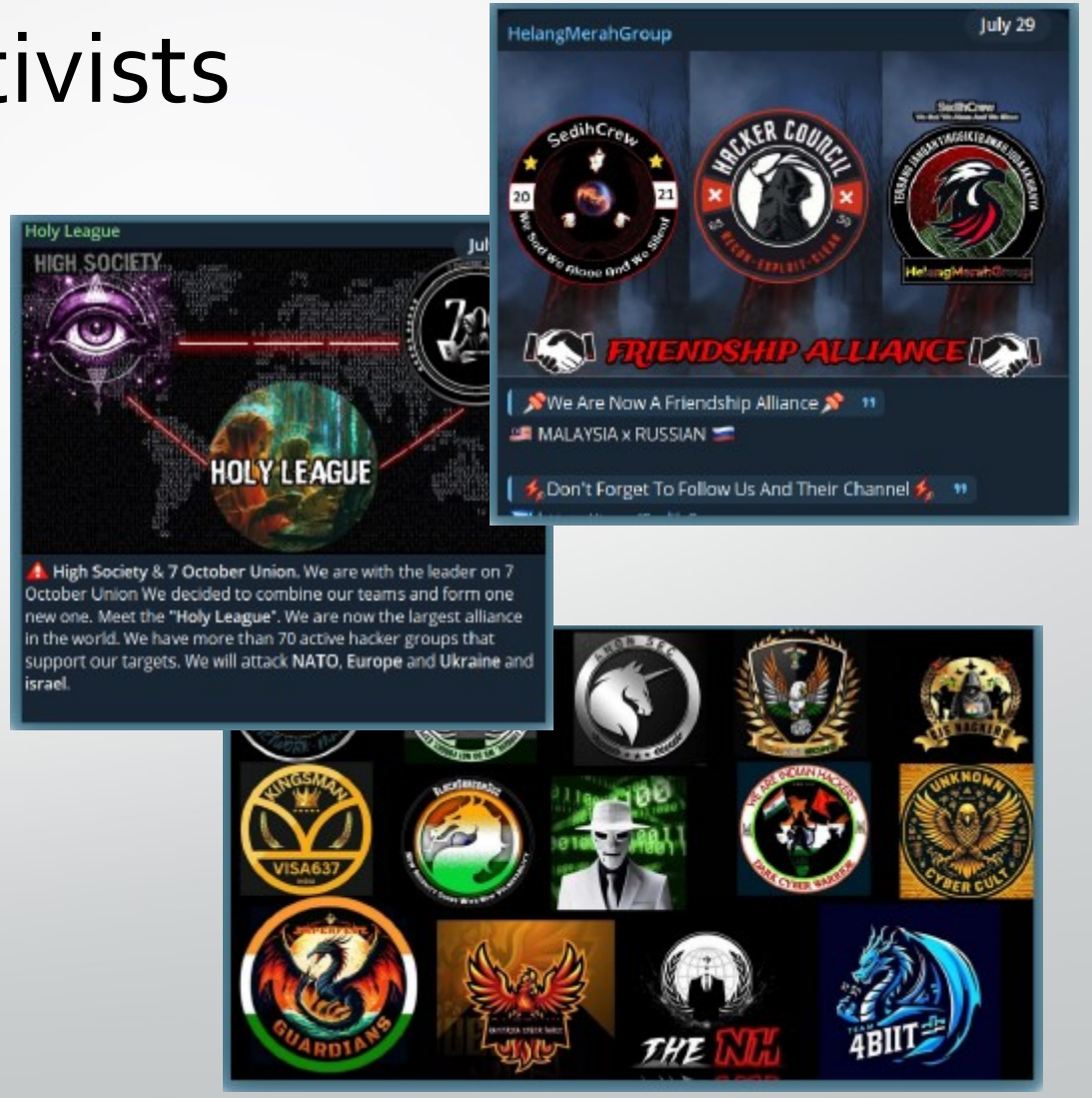
Threat Landscape - AI

- Examples of AI in Cybercrime
  - Phishing Attacks, Deepfakes, Automated Scanning, Malware Creation, Social Media Manipulation
- Novel AI Capability for Hackers
  - AI-driven autonomous hacking agents. These agents could operate independently to identify and exploit vulnerabilities without human intervention.
- Copilot prompt:
  - You are an AI savvy cybersecurity professional. Explain with examples how malicious hackers can use AI to enable or extend their capability. Can you think of an novel capability that malicious hackers could develop using AI?

Hacktivists

Hacktivists and their allies use various methods to harm the digital infrastructure of target countries.

- DDoS
- Doxing
- Ransomware
- Forming Alliances
- Selling Training Courses



Cyber Attacks

Ukraine

Three power distribution companies in Ukraine suffered consequences from a cyberattack on 23 December 2015

- Networks and systems were compromised months before using spear phishing
- BlackEnergy malware gathered intel on the IT and OT networks
- The attack lasted only 10 minutes
- Power outage for 230,000 customers

https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware

Ukraine

Prior to the attack, Ukraine had implemented several best practices:

- Nonobvious passwords were used
- A firewall with strict data flow restriction was in place
- Significant logging was performed
- Demonstrates the principle of “weakest link”

Ukraine

Actually, four power distribution companies in Ukraine experienced a cyberattack on 23 December 2015. However, only three suffered consequences.

The UA-ISAC had received YARA rules from DHS before the attack and sent them out.

Only one company ran the rule. That company discovered Black Energy and disconnected remote access while they worked to remove it.

Ukraine

IEC Foundational Requirement	Actions to stop or mitigate the attack
1: Identification, Authentication Control, and Access Control (AC)	Further restrict access from a non-trusted network
2: Use Control (UC)	More control of files in transit on the OT network, provide a means to terminate remote connection
3: System Integrity (SI)	Add malicious code protection (AV)
5: Restricted Data Flow (RDF)	Add authentication, detection, local control
6: Timely Response to Events (TRE)	Network monitoring
7: Resource Availability (RA)	Improve backups

Colonial Pipeline

The cyber attack occurred on May 7, 2021, when the pipeline's computerized equipment was targeted by a ransomware attack.

- A compromised password was used to gain access to the system.
- This attack led to the shutdown of the pipeline, which supplies about 45% of the fuel consumed on the U.S. East Coast.
- The company paid a ransom of 75 bitcoins (approximately $4.4 million USD at the time).
- A portion of the money was recovered.

Colonial Pipeline

IEC Foundational Requirement	Actions to stop or mitigate the attack
1: Identification, Authentication Control, and Access Control (AC)	MFA would have made it more difficult to gain access using compromised credentials
3: System Integrity (SI)	Regular updates and patching help maintain the integrity of the system
5: Restricted Data Flow (RDF)	Network segmentation limits the flow of data between different network segments
6: Timely Response to Events (TRE)	Training employees to recognize and respond to security threats promptly
7: Resource Availability (RA)	Maintaining regular backups ensures that critical data can be restored quickly

Conclusion

- The energy sector faces a complex and evolving threat landscape, with adversaries leveraging advanced technologies and exploiting vulnerabilities.
- Effective regulatory frameworks, whether performance-based or compliance-based, are crucial for ensuring the safety, reliability, and resilience of energy infrastructure.
- The sector must continuously adapt to emerging threats, implement best practices, and foster collaboration between regulators and asset owners to enhance cybersecurity posture.

Köszönöm

Van valakinek kérdése?