For Distribution to NAIMI Workshop Participants Only

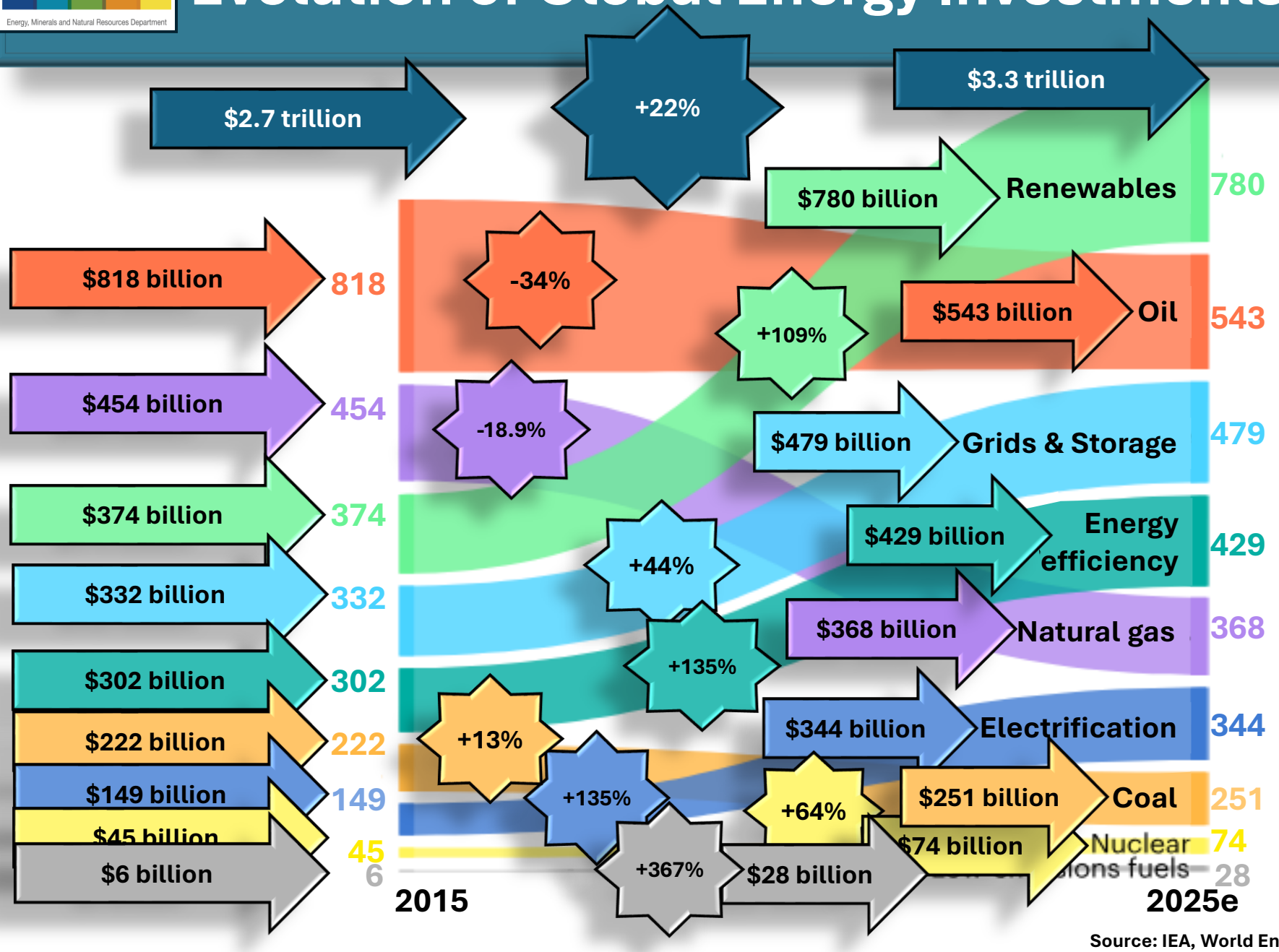
Cybersecurity and the Energy Sector

Melanie Kenderdine

November 14, 2025

Los Alamos, New Mexico

Evolution of Global Energy Investments, 2015-2025e* (billion USD)



% total 2025e

$1.6 trillion investment in these three energy subsectors in 2025

Natura	11%
Renewables	24%
Grids/Storage	14%
Energy Efficiency	13%
Coal	8%
Electrification	10%
Nuclear	2%
Low Emissions Fuels	0.8%

Source: IEA, World Energy Investment 2025

*percentages rounded

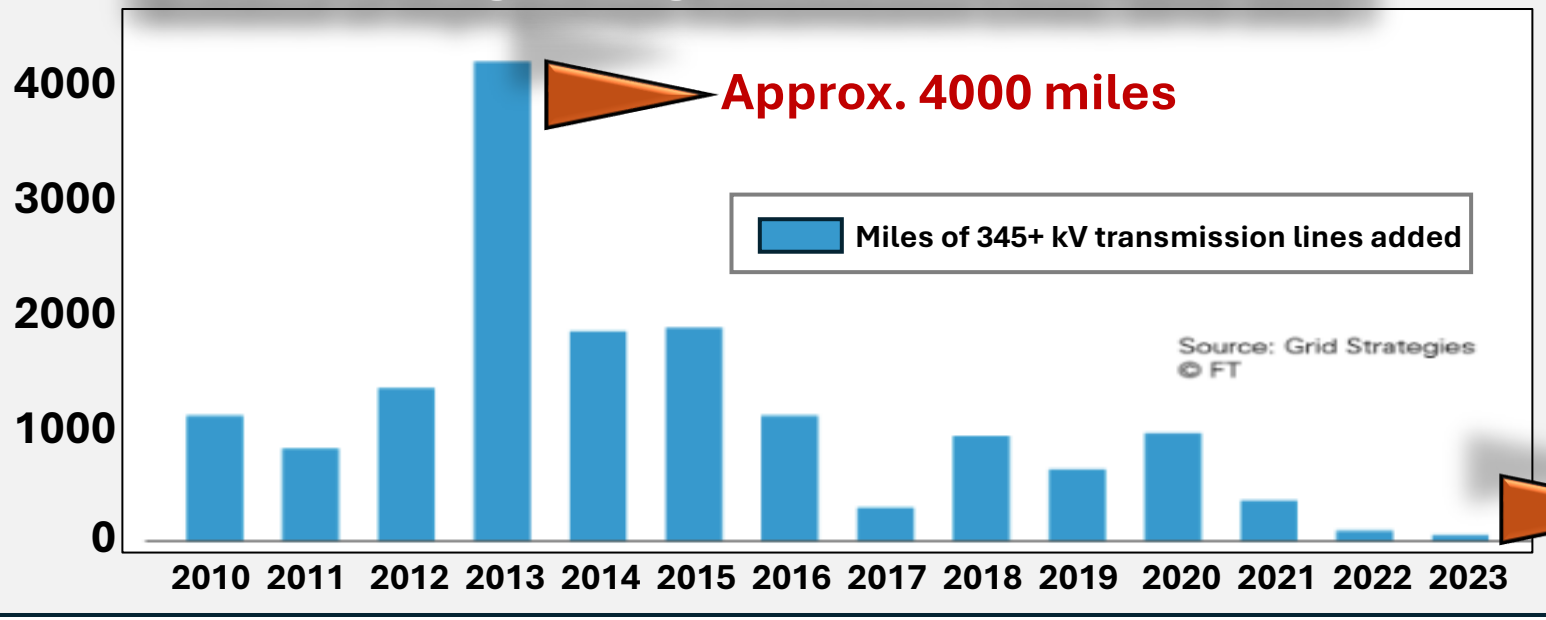
Load Growth, Emerging Sectors/Transmission Line Buildout

Load Growth in Emerging Sectors

Demand Driver	Current Capacity	Increase by 2030	
Data Centers	*~ 19 GW*	*+ 16 GW*	+84%
Onshoring & Industrial Electrification	*~ 118GW*	*+ 36 GW*	+30%
Transportation Electrification	*~ 7 GW*	*+ 8 GW*	+114%
Building Electrification	*~ 50 GW*	*+ 7 GW*	+14%
Cryptocurrency Mining	*~ 10-17 GW*	*+ 8-15 GW*	+80-88%

Increased electricity demand for data centers by 2030 is only 19.5% of total demand increases

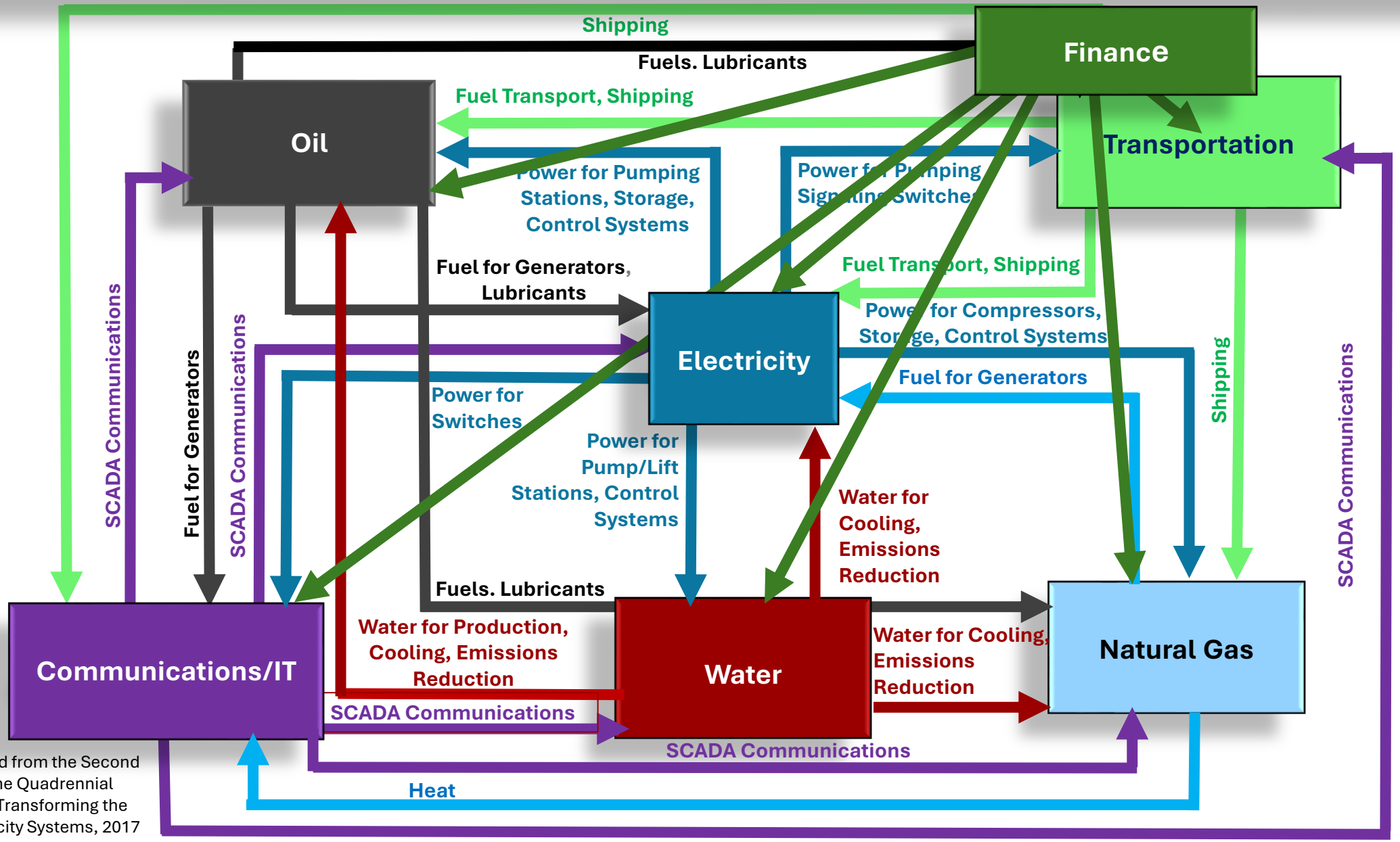
Buildout of High-Voltage Transmission Lines, 2010-2023



By 2030, electricity demand for these five sectors alone could equal 23% of the US' 2023 nameplate generating capacity

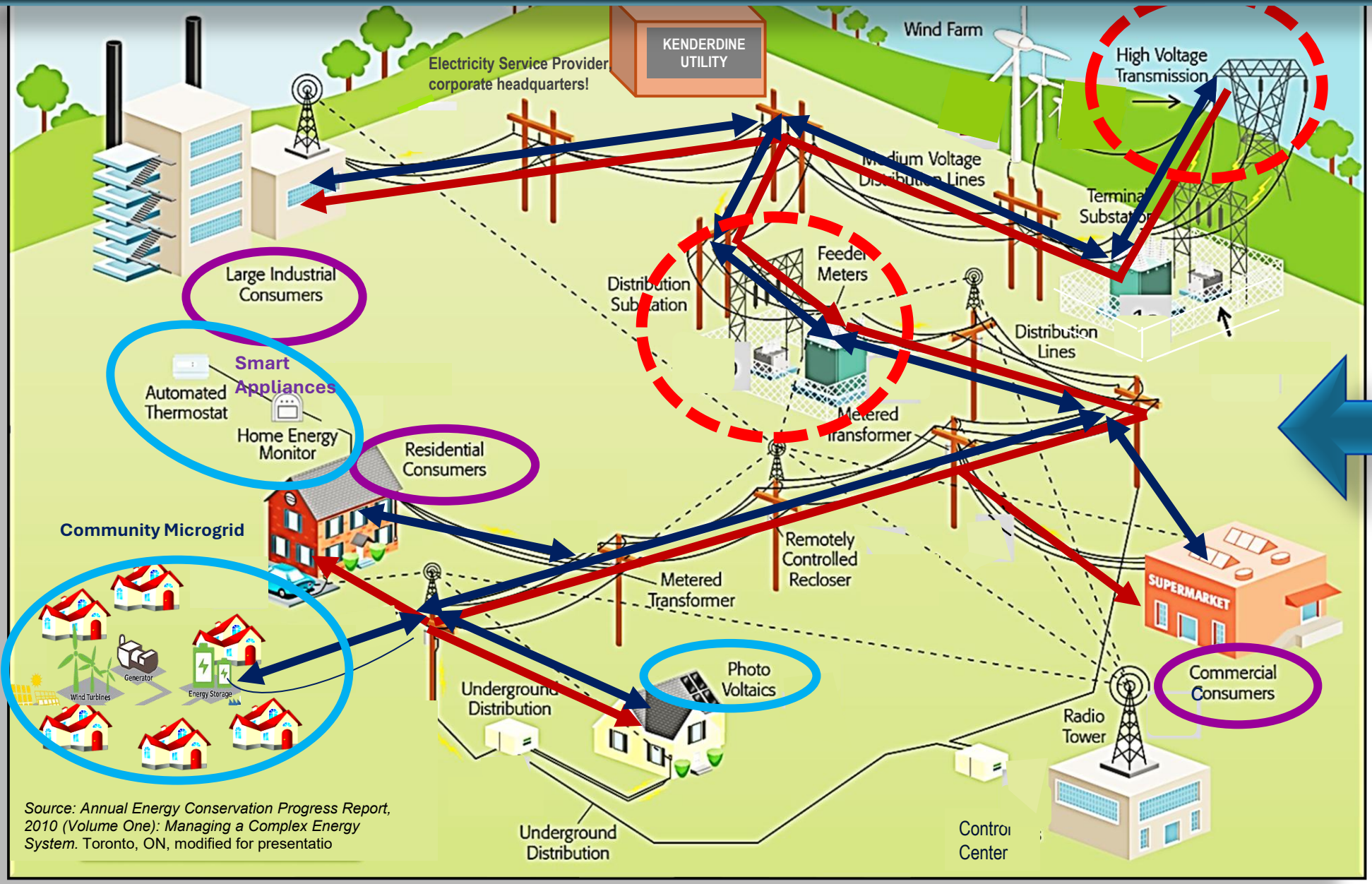
Approx. 100 miles

Electricity and Lifeline Network Interdependencies



Source: Modified from the Second Installment of the Quadrennial Energy Review, Transforming the Nation's Electricity Systems, 2017

Two Way Electricity Flows and Grid Security



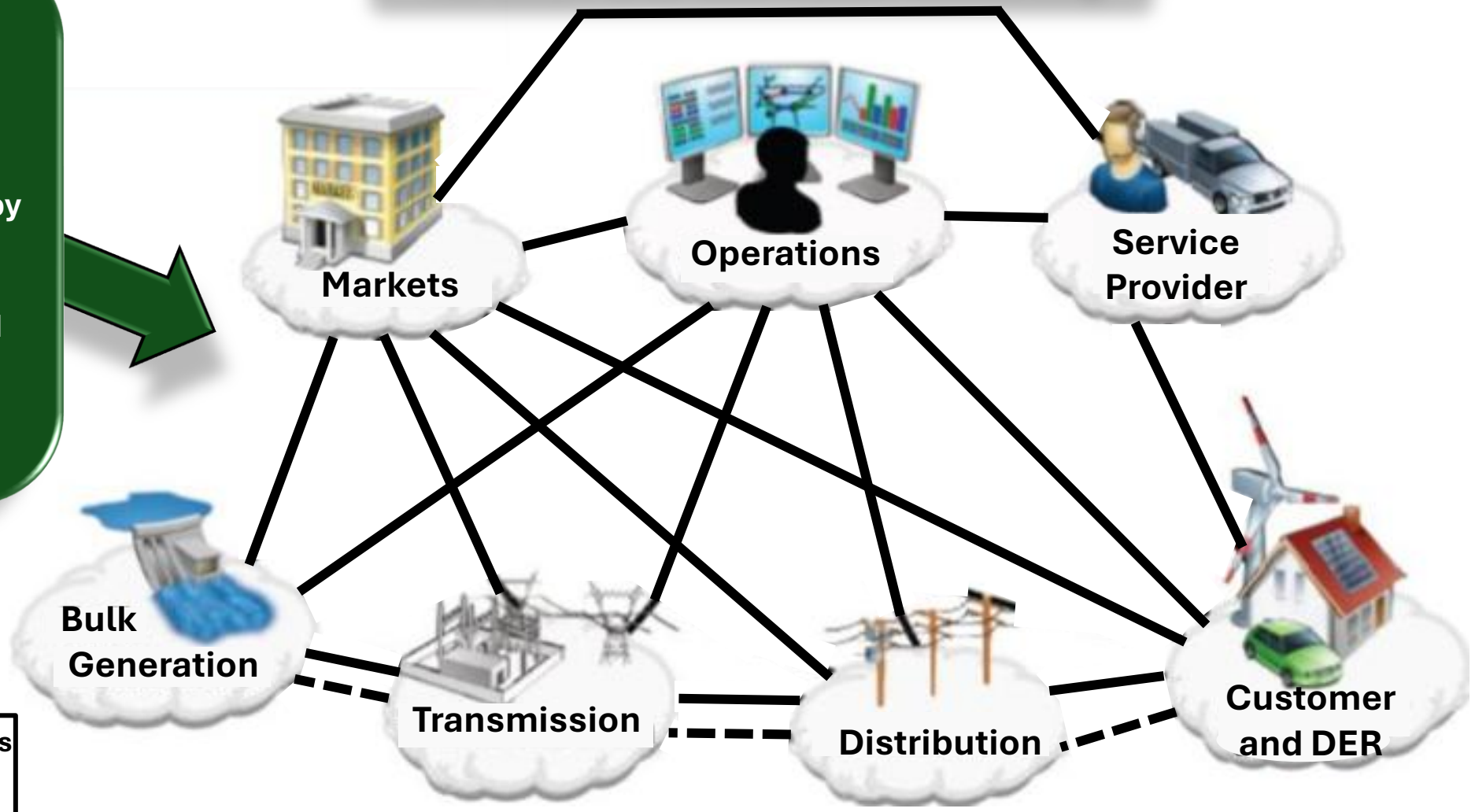
Source: Annual Energy Conservation Progress Report, 2010 (Volume One): Managing a Complex Energy System. Toronto, ON, modified for presentatio

"…emerging advancements in … smart grid technologies, cloud computing services, grid-cyber vulnerability & assessments, and distributed energy resources represent significant cybersecurity threats to the continuity of delivered power. " (Sandia National Laboratory)

The Smart Grid, Information Networking: Increased Vulnerabilities

"...the smart grid's heavy reliance on information networking exposes it to vulnerabilities inherent in communication systems. Potential network intrusions by adversaries can have severe consequences, including customer data breaches and cascading failures like widespread blackouts and infrastructure destruction."

The Smart Grid: Information Networking



https://eepower.com/tech-insights/smart-and-secure-digital-twin-unmasks-grid-cyber-risks/

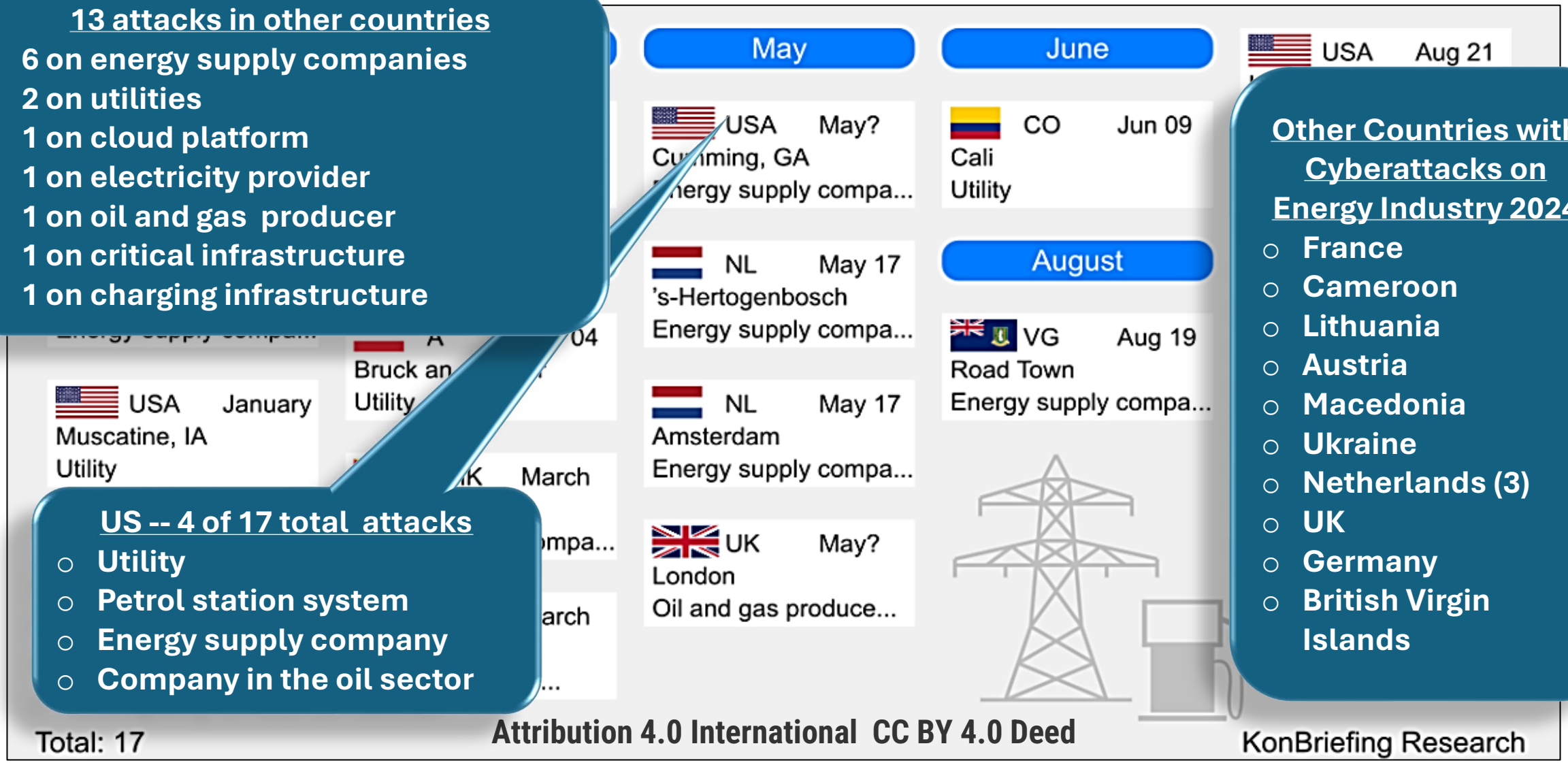
Cyberattacks on the Energy Industry 2024

13 attacks in other countries

- 6 on energy supply companies
- 2 on utilities
- 1 on cloud platform
- 1 on electricity provider
- 1 on oil and gas producer
- 1 on critical infrastructure
- 1 on charging infrastructure

US -- 4 of 17 total attacks

- Utility
- Petrol station system
- Energy supply company
- Company in the oil sector



Other Countries with Cyberattacks on Energy Industry 2024

- France
- Cameroon
- Lithuania
- Austria
- Macedonia
- Ukraine
- Netherlands (3)
- UK
- Germany
- British Virgin Islands

Types of Cyber Attacks

CYBER ATTACK TYPES

An attack targeting an enterprises' use of cyberspace for the purpose of disrupting, disabling, or maliciously controlling a computing environmental/infrastructure, or destroying the integrity of the data or stealing controlled information

SOCIAL ENGINEERING

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes

DENIAL OF SERVICE

Overloading a system through continual resource usage that prevents legitimate use. Distributed Denial of Service attacks often use "botnets" or "Zombies" to scale an attack

PENETRATION ATTACKS

The use of legitimate publicly available resources on the internet to check for servers, open ports, and other information that may allow unintended access to into the system

MALWARE

A computer program that is covertly placed onto a computer or electronic device with the internet to compromise the confidentiality, integrity or availability of data applications or operating systems

VIRUSES AND WORMS

Introduction of self-propagating or inflated malware into a system through methods such as malicious email attachments, USBs, etc., that seeks to monitor, access, delete or alter data for nefarious use

TROJANS

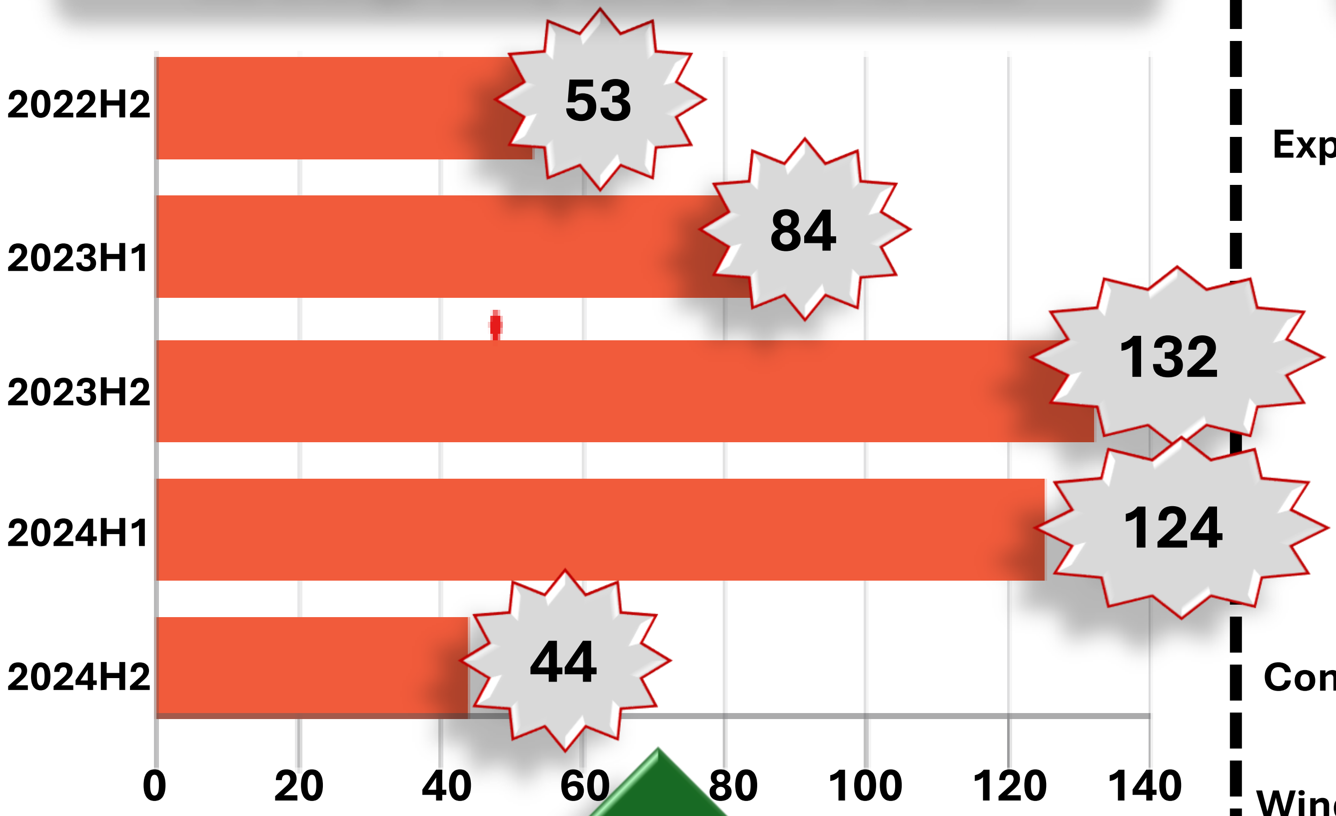
Malware that allows "back door" access into a system. This allows an attacker to have a longer reconnaissance through continual check-ins

RANSOMWARE

Maliciously locking up data or systems and demanding payment of a fee (ransom) or other concessions to unlock the data or systems

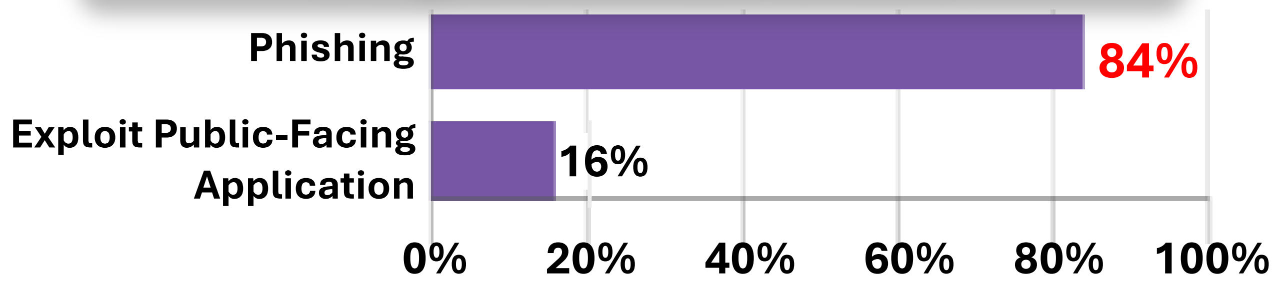
Ransomware Attacks on Energy/Utility Sector: Access/ Execution Techniques

Number of ransomware attacks waged against the energy/utility sector since H2 2022

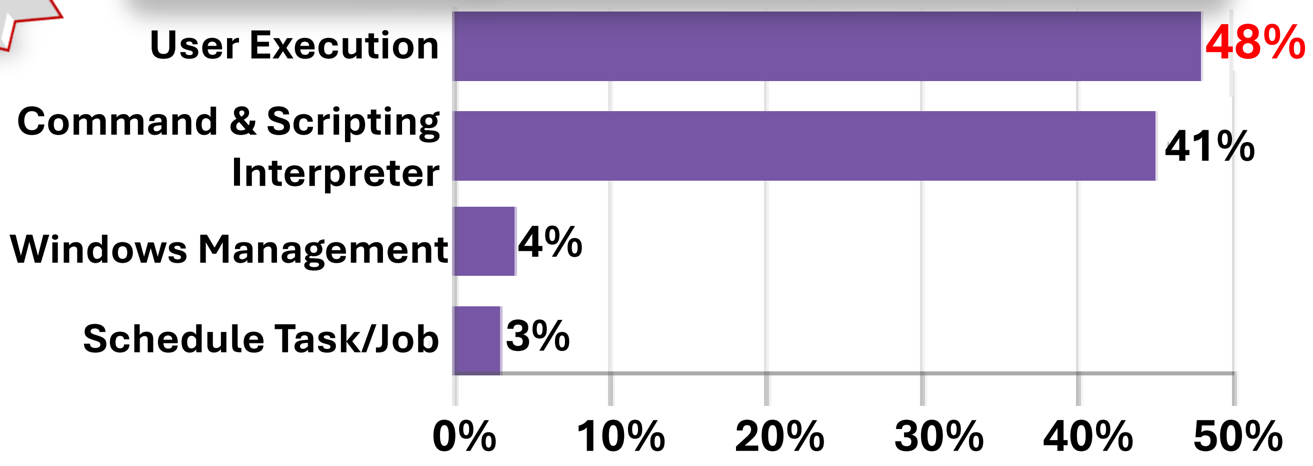


"The number of ransomware attacks…for the energy and utilities sector was significantly higher in H2 2023 and H1 2024 – an 80% increase in ransomware activity…than the same time period one year prior."

Initial Access Techniques Used by Attackers of Energy and Utilities Providers



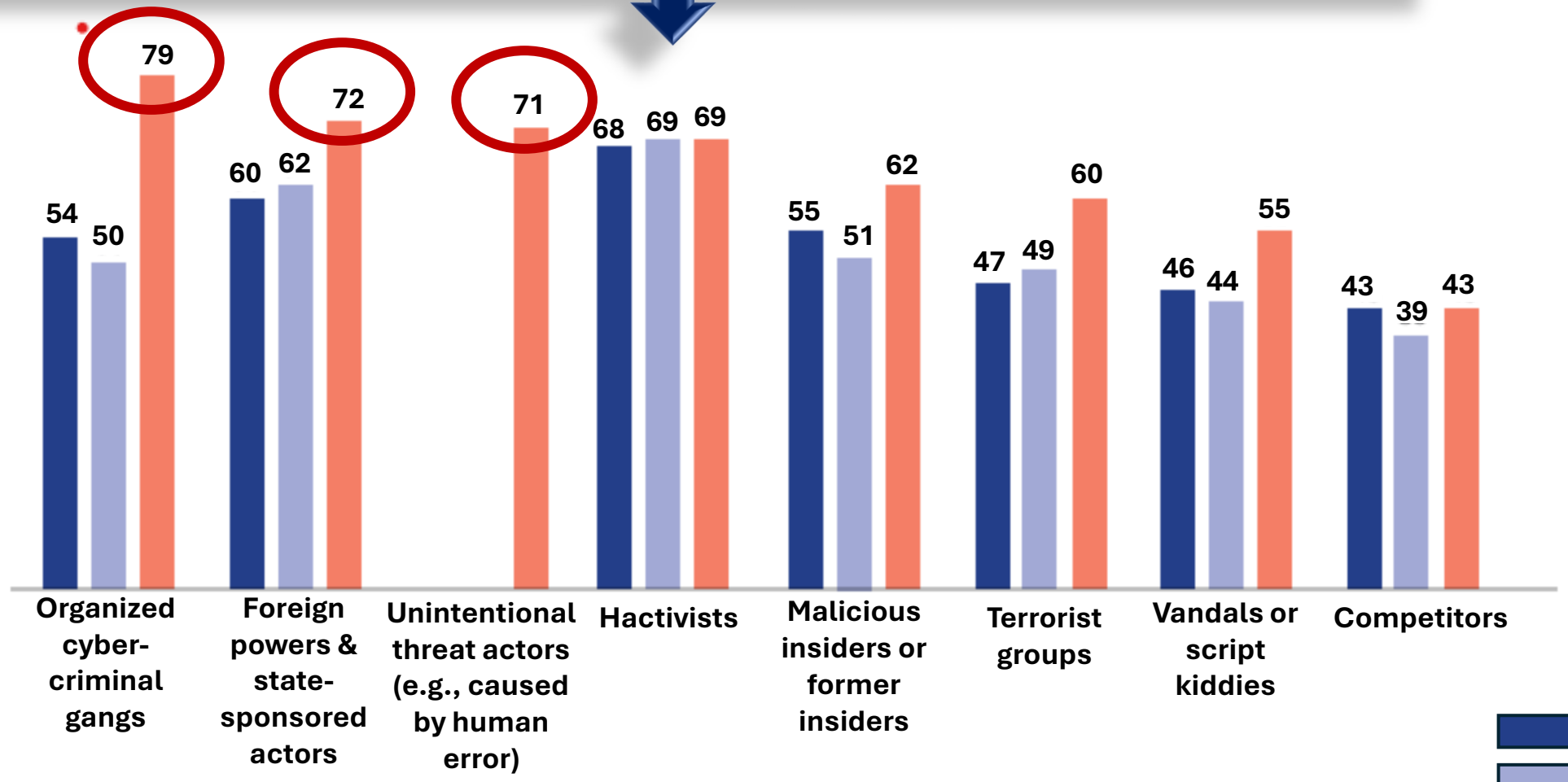
Execution Techniques Used by Attackers of Energy and Utilities Providers



…hubfs/Web/Library/Documents_pdf/2025_Trustwave_Energy_Utilities_Risk_Radar_Report.pdf

Industry Concerns About Cyber-threats are Growing

Q. Are you concerned about these threat actors attacking your business?*

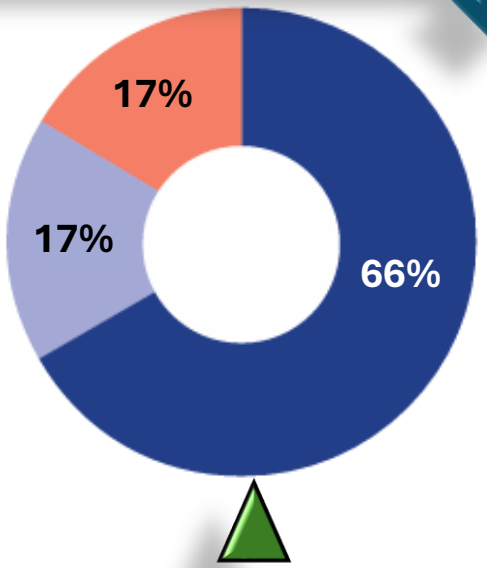


* Numbers are percentages

Source: ENERGY CYBER PRIORITY 2025 Addressing evolving risks, enabling transformation

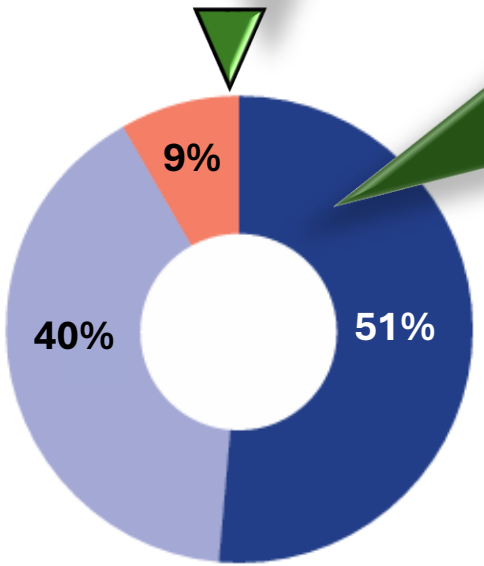
Industry Uncertainties About Cyber-threats

Q. To what extent do you agree with the following statement?



The use of generative AI in phishing is making it harder for us to judge which e mails are real and which are not

Senior management in my organization underestimate how quickly the cyber threat is evolving and becoming more sophisticated



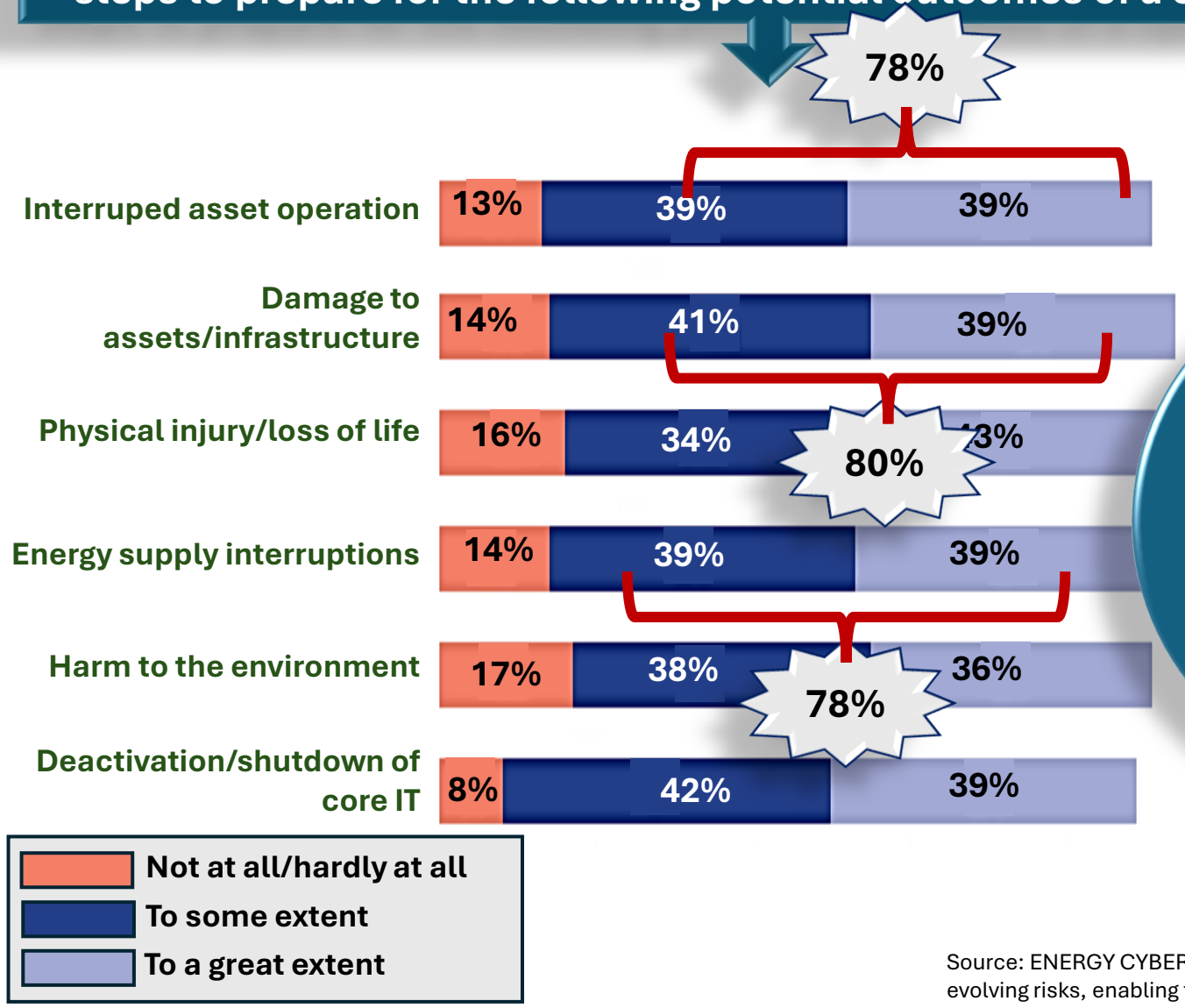
Agree (strongly/slightly)
Disagree (strongly/slightly)
Don't know

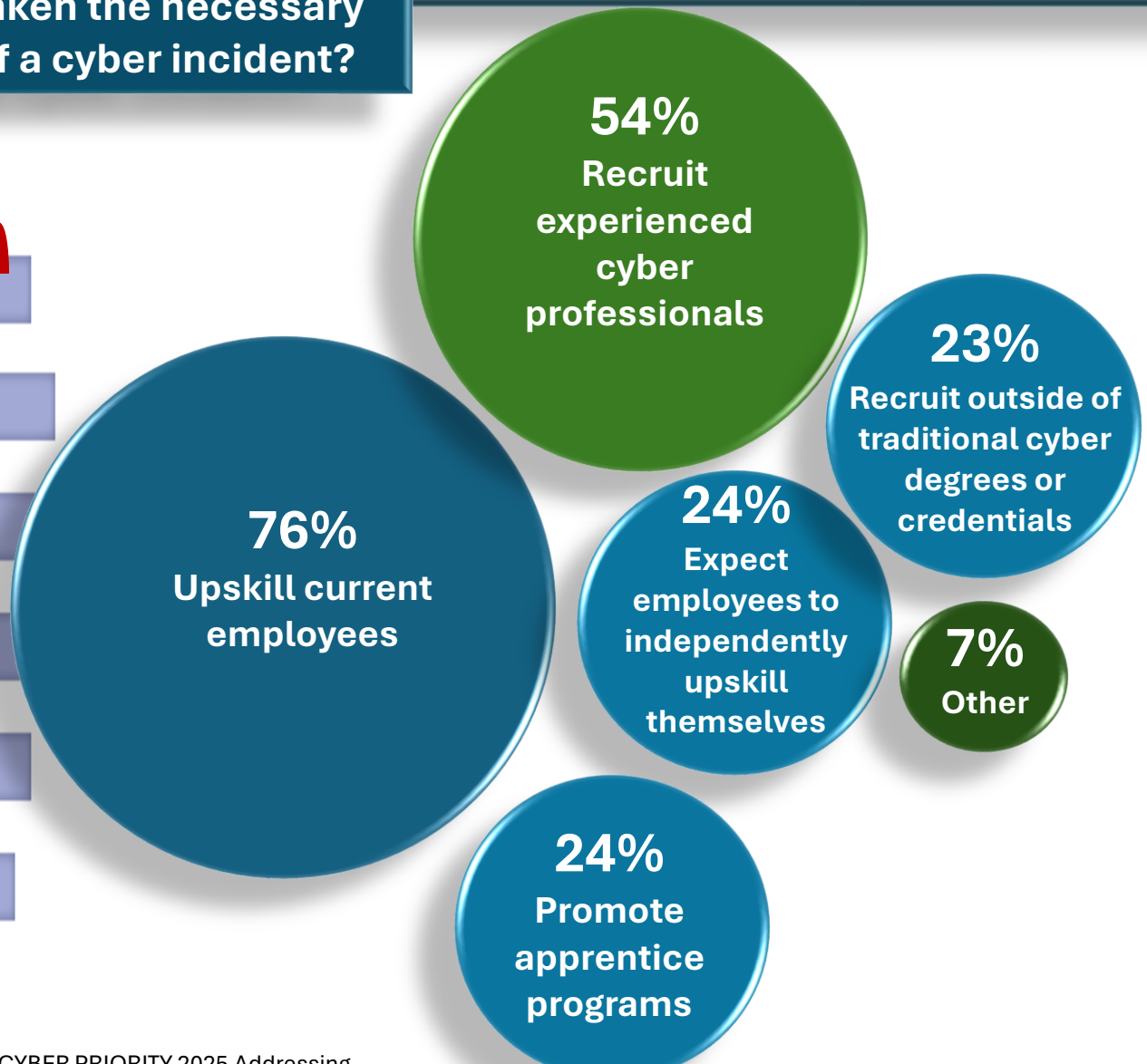
"According to the [IEA], the average number of weekly attacks on utilities has more than doubled in the last few years alone. High-profile attacks have compromised critical energy systems worldwide, while the US National Security Agency (NSA) issued a rare urgent warning to energy operators in 2024, warning them of a rise in pro-Russia hacktivist activity."

Source: ENERGY CYBER PRIORITY 2025 Addressing evolving risks, enabling transformation

Views on Cyber-Issue Management and How Organizations are Addressing the Cyber-skills Gap

Q. To what extent would you say your organization has taken the necessary steps to prepare for the following potential outcomes of a cyber incident?





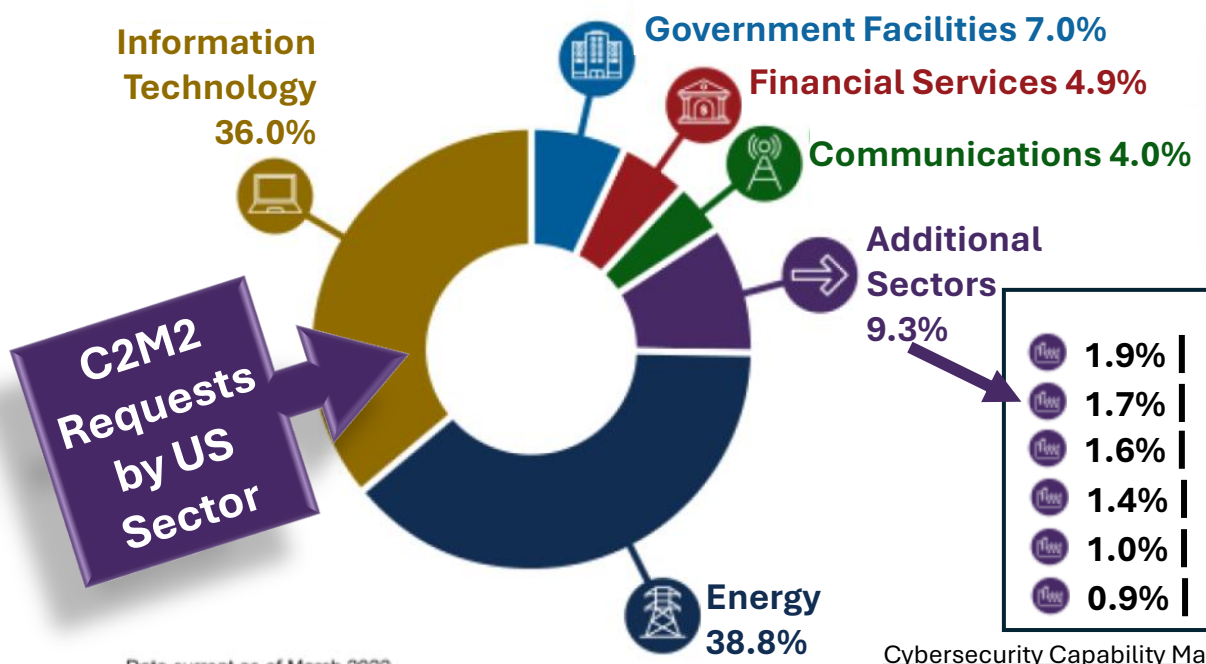
Source: ENERGY CYBER PRIORITY 2025 Addressing evolving risks, enabling transformation

Source: WEF_Global_Cybersecurity_Outlook_2025.pdf

C2M2: DOE Tool for Evaluating Cyber Capabilities and Investment Optimization

DOE's Cybersecurity Capability Maturity Model (C2M2) is a free tool to help organizations evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments. C2M2 goals include:

- **Enhance cyber posture**
- **Consistently measure cyber capabilities**
- **Share knowledge**
- **Prioritize actions and investments**



US energy organizations have been using the C2M2 to evaluate and improve their cybersecurity capabilities for more than a decade. Since 2012, DOE has responded to more than 2,400 requests for the C2M2 BDF-based tool from owners and operators in US critical infrastructure sectors…

1.9%	Critical Manufacturing	0.6%	Transportation Systems
1.7%	Government	0.1%	Emergency Services
1.6%	Health Care & Public Health	1.6%	Health Care & Public Health
1.4%	Defense Industrial Base	0.1%	Nuclear Reactors, Materials, Waste
1.0%	Water and Wastewater Systems	0.1%	Foods and Agriculture
0.9%	Chemical		

Cybersecurity Capability Maturity Model (C2M2) | Department of Energy

Cyber-security Resources for the Electricity Sector

- **American Public Power Association's Public Power Cybersecurity Scorecard**: an online self-assessment tool for municipal utilities to evaluate their cybersecurity programs and overall posture.

- **National Rural Electric Cooperative Association's Rural Cooperative Cybersecurity Capabilities Program Cybersecurity Self-Assessment**: designed to assist cooperatives understand their cybersecurity posture and provides tools and resources focused on improving the cybersecurity capabilities of cooperatives. The program also provides opportunities for collaboration, education, and training.

- **National Association of Regulatory Utility Commissioners' Cybersecurity Manual**: a comprehensive suite of cybersecurity tools to help public utility commissions gather and evaluate information from utilities about their cybersecurity risk management and preparedness.

- **Edison Electric Institute's Electricity Subsector Coordinating Council**: a coordinating entity between federal agencies and investor-owned utilities to bolster defense against cyber and physical security threats.

Critical Cybersecurity Issues the Energy Sector Needs to Address

Ransomware Threats: Attacks targeting energy and utility providers have surged, making it clear that a robust cybersecurity strategy is essential for combating this persistent threat and minimizing its impact.

IT/OT Convergence: While integrating IT and OT systems has unlocked greater efficiencies, it has also exposed critical infrastructure to new risks. A unified cybersecurity approach across both domains is now more important than ever.

Regulatory Compliance: With stringent and evolving cybersecurity regulations in place, staying compliant is not just about avoiding penalties – it's also about reducing vulnerabilities and safeguarding the integrity of critical infrastructure.

Aging Infrastructure: The sector's reliance on outdated technologies creates significant security gaps. To stay ahead of modern threats, companies must invest in upgrading systems and enhance collaboration between IT and OT systems.

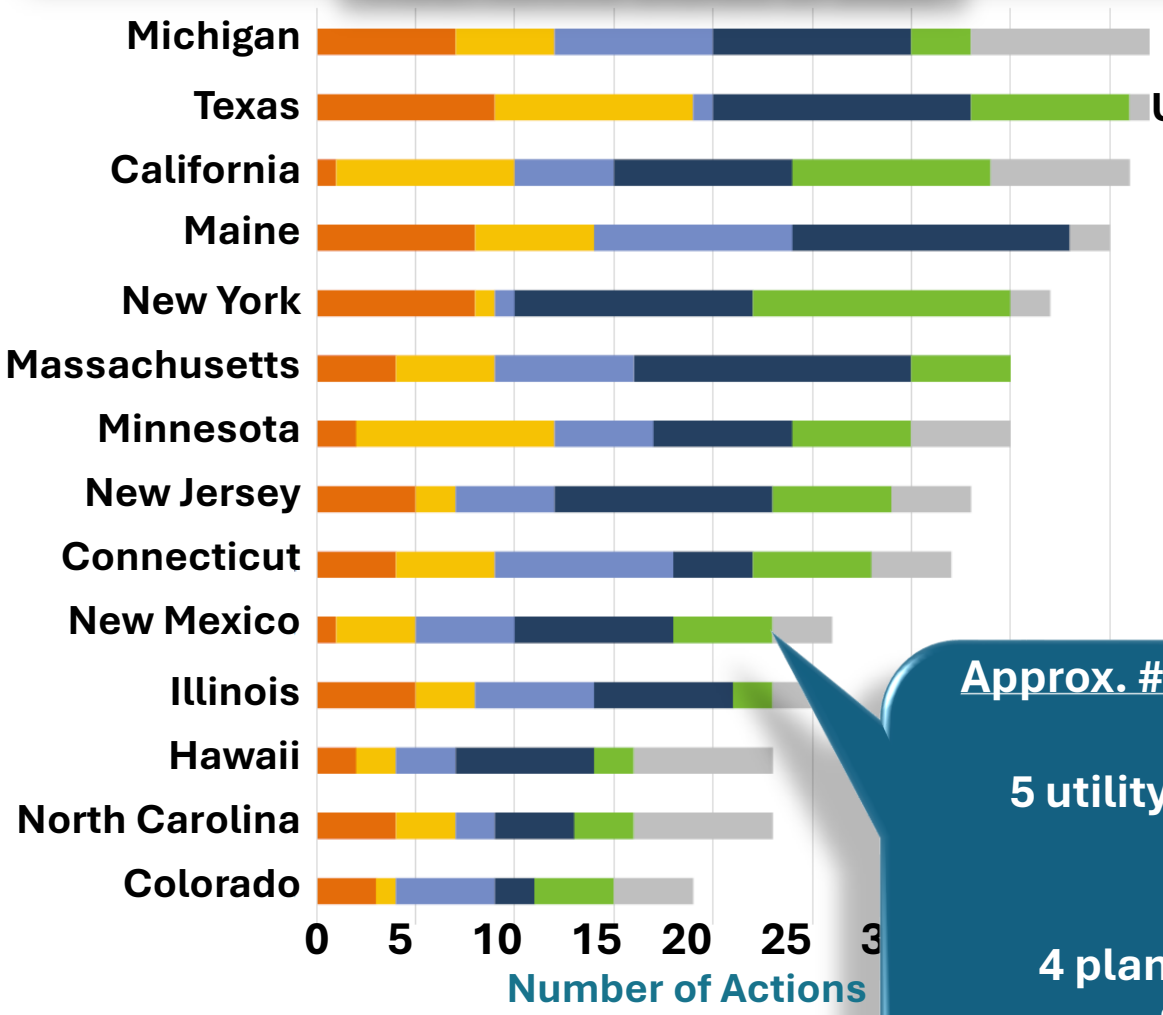
Geopolitical Significance: The energy sector's strategic importance makes it a prime target for state-sponsored cyberattacks. Providers must be ready to defend against highly sophisticated threats that are as much about national security as they are about financial gain.

By addressing these key areas, energy and utility providers can better prepare for the evolving cyber threat landscape. Strengthening defenses, investing in new technologies, and maintaining a proactive security strategy will help ensure the continued reliability and safety of operation, even in the face of growing risks.

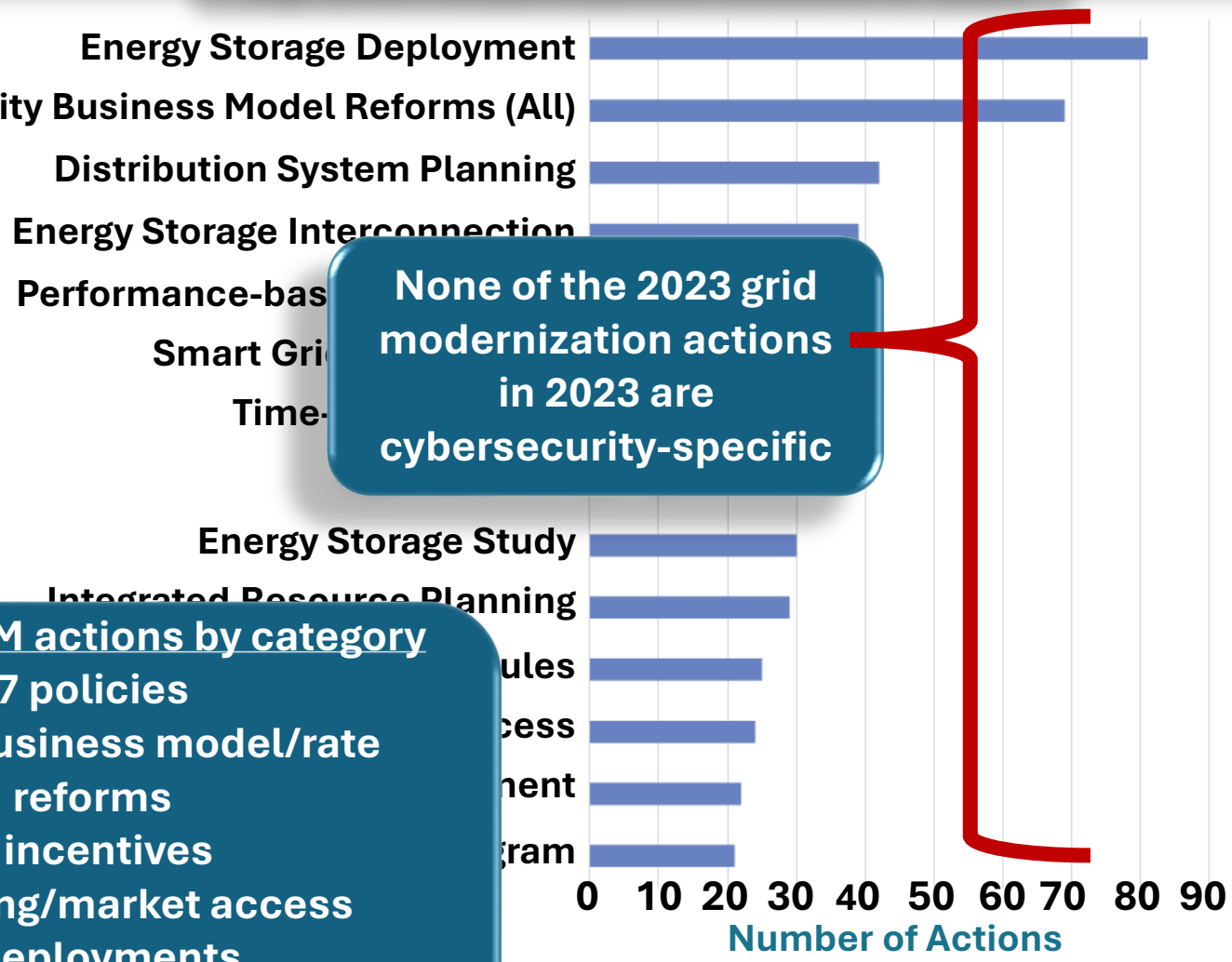
chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/2025_Trustwave_Energy_Utilities_Risk_Radar_Report.pdf

State Actions on Grid Modernization, 2023

Most Active States of 2023



Top Grid Modernization Actions of 2023



None of the 2023 grid modernization actions in 2023 are cybersecurity-specific

Approx. # NM actions by category

7 policies
5 utility business model/rate reforms
5 incentives
4 planning/market access
3 deployments
1 study/investigation

Source: 50 States of Grid Modernization: Q42023 Report and 2023 Annual Review, NC Clean Energy Technology Center

G-7/EU Energy Security Principles: Modernized Definition of Energy Security

Collective Action of G-7/EU Allies to…

- **Develop flexible, transparent and competitive energy markets**, including gas markets
- **Modernize infrastructure to improve energy system resilience.** Promoting supply and demand policies will help withstand systemic shocks.
- **Diversify energy fuels, sources and routes** and encouraging the **development of indigenous sources of energy.**
- **Reduce greenhouse gas emissions** and accelerate the transition to a low carbon economy, **key contributors to enduring energy security.**
- **Enhance energy efficiency** in demand and supply, and demand response
- **Deploy clean and sustainable energy technologies** and promoting ongoing **investment in research and innovation**.
- **Maintain emergency response systems**, including reserves and fuel substitution for importing countries, **are in place** to manage major energy disruptions.
- **Address and constantly update responses to cyber security threats to energy production and distribution systems.**
- **Protect supply chains for key metals and minerals, establish domestic options/alternatives.**

Adapted from Joint Statement, Rome G7 Initiative for Energy Security, May, 2014

Illustrative Assessment of AI Potential for Accelerating Progress Against Selected Energy Technology Challenges

Technology challenge	Solution space complexity	Structured data availability	Pre-deployment verification	Integration and scaling
Synthetic fuels – Catalysts with high efficiency, selectivity and stability	High	High	High	Medium
Hydrogen electrolysis – Low-cost, highly efficient and durable electrolyser catalysts	High	High	High	Medium
Carbon capture, utilization and storage – Stable CO2 capture materials with high affinity and low energy penalty	High	Medium	High	Medium
Electric vehicles – Novel battery chemistries using cheap materials (e.g., sodium-ion, solid-state	High	Medium	High	Medium
High-temperature heat storage – Stable phase change materials with high conductivity and latent heat	High	Low	High	Medium
Desalination – Productive, stable and energy efficient reverse osmosis membranes	High	Medium	High	Low
Advanced biofuels – Improved performance of enzymes and yeasts for 2nd/3rd generation biofuels	High	High	Medium	Low
Solar photovoltaics – Efficient, stable, scalable perovskite cells without critical mineral inputs	High	Low	High	Medium
High-temperature heat pumps – Identification of working fluids that phase change at high temperatures	Medium	Low	High	Medium
Long duration energy storage – Cheaper, efficient re-dox flow or other long-duration batteries	High	Low	Medium	Medium
Decarbonized cement – Cement production from calcium silicate raw materials	Medium	Low	Medium	Medium
Plastics recycling – Energy-efficient upgrading of pyrolysis oils	Medium	Medium	Low	Medium
Effective nuclear fusion – Fusion reaction controlled	High	Low	Low	Low

High
Medium
Low

https://iea.blob.core.windows.net/assets/601eaec9-ba91-4623-819b-4ded331ec9e8/EnergyandAI.pdf

CETS: The Energy Trilemma and High-level Goals