Texas Gas-Fired Power Plants Vulnerable to ICS Compromise Leading to Potential Regional Blackouts

30 April 2024

Edward "Ned" Pfeiffer - *Psychology & Data Analytics*
Lauren Stemler - *Master of Anticipatory Intelligence*
Sydney Perkins - *Master of Aerospace Engineering*

System: Texas Interconnection & Natural-Gas

The Texas Interconnection is one of the three major electricity grids in the United States, covering most of the state of Texas. It is operated by the Electric Reliability Council of Texas and is largely isolated from the Eastern and Western Interconnections that cover the rest of the country. This isolation means that Texas has limited ability to import or export electricity from neighboring states, relying primarily on its own generation resources. The Texas Interconnection serves over 26 million customers across the state and has a generating capacity of over 145,000 megawatts from various sources including natural gas, coal, nuclear, and renewables like wind and solar.

Natural gas-fired power plants play a crucial role in supplying electricity to the Texas Interconnection. These plants use natural gas as fuel to generate electricity through combustion turbines or combined-cycle systems. Texas has an abundance of natural gas resources, making it an attractive fuel source for power generation. Gas-fired plants are favored for their relatively low emissions compared to coal, their operational flexibility to quickly ramp up or down based on demand, and their ability to provide reliable baseload power. Currently, natural gas accounts for 42% of the total electricity generation in Texas, with numerous gas-fired plants scattered across the state contributing to the overall power supply.

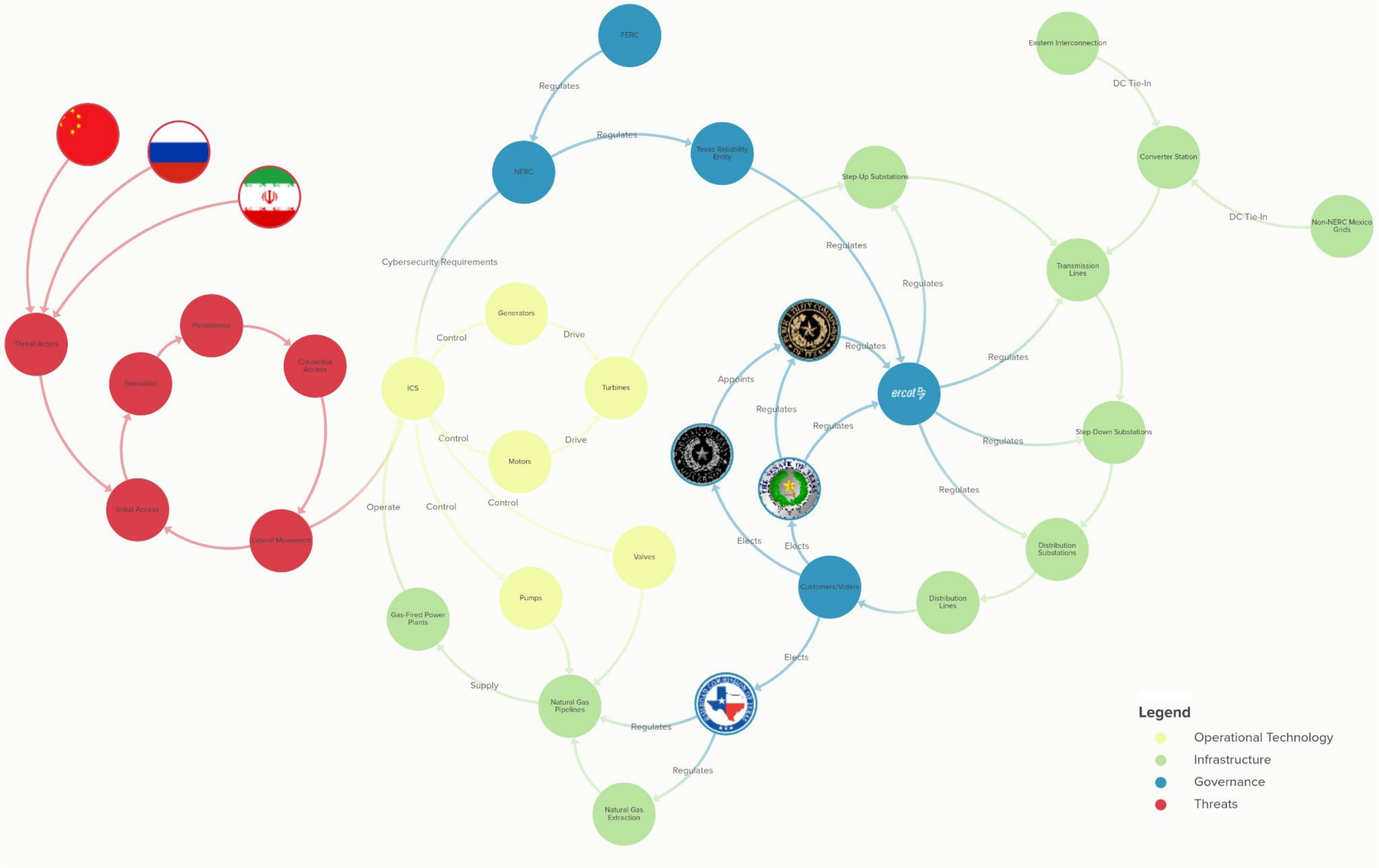

Figure 1. *A network diagram showing entry points for potential operational technology attacks on the Texas natural gas industry*

Threat: Industrial Control Systems & Cyberattacks

The nature of ICS compromise in critical infrastructure revolves around the intersection of advanced cyber capabilities and strategic intent. Threat actors, whether state-sponsored or sophisticated cyber criminal groups, target ICS due to their critical role in national security, public safety, and economic stability. The capability involves leveraging cybersecurity vulnerabilities, such as unpatched software, insecure remote access, and social engineering, to gain control or disrupt services. Intent varies from espionage, preparing the battlefield for potential conflict, to causing immediate disruption or damage.

The Iranian Islamic Revolutionary Guard Corps Cyber-Electronic Command has been involved in cyber operations against critical infrastructure, targeting programmable logic controllers and supervisory control and data acquisition systems. Additionally, Chinese based threat-actors such as Volt Typhoon are actively involved in sophisticated cyber espionage and disruption campaigns targeting critical infrastructure and ICS across various sectors. In the event of a geopolitical escalation such as a Chinese invasion of Taiwan or a conflict involving Iran, the Texas energy grid could become a target.

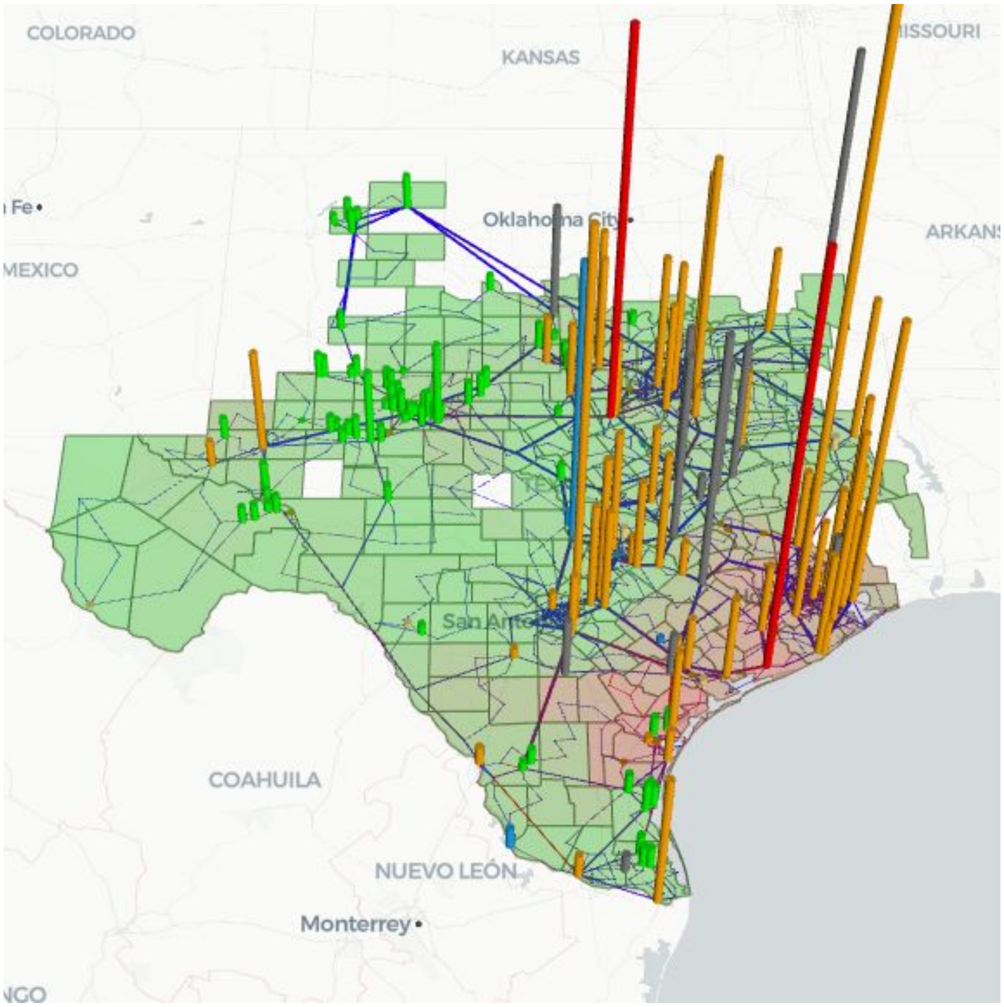

Figure 2. *A simulated cyberattack using Pacific Northwest National Lab's ExaGO, in which half of Texas' gas-fired power plants are disabled. Our simulations used synthetic data provided by researchers at Texas A&M University; no Critical Electric Infrastructure Information was used.*

This map provides a visualization of the impact of a sophisticated cyber attack against the Texas natural gas industry. This is a plausible scenario that Texas could experience if a significant pipeline was shut down or multiple power plants were disrupted. Each bar represents power plant generation capacity, and the colored regions of the map represent grid voltage, with the deep red regions experiencing blackouts. In this scenario, with half of Texas natural gas plants offline, the southeastern portion of the state would face extended power disruption, particularly densely populated areas in southeast Texas such as Houston, Galveston, and Corpus Christi.

Ned Pfeiffer, Lauren Stemler, Sydney Perkins

CAI 5200: Threats & Resilience

Resilience Assessment

The Four R's Resilience Framework provides a structured approach to assessing the resilience of Texas' gas-fired power plants by focusing on four key areas: resistance, retention, recovery, and resurgence. This framework allows for a thorough analysis of the grid's strengths and potential vulnerabilities. Each of the four categories receives a letter grade, offering an at-a-glance indication of the Texas grid project's resilience performance in these areas.

Resistance **B**

Complete prevention of the threat from accessing the system.

Doing Well

- Employee training and vetting are thorough, with comprehensive security awareness training and annual retraining. Network segmentation is effectively implemented to limit cyberattack spread.

Needs Improvement

- Supply chain security lacks a robust risk management plan for operational technology in the Bulk Electric System (BES). Audits require greater frequency and rigor to ensure compliance and identify areas for improvement.

Retention **B**

The system maintains core functionality during an attack.

Doing Well

- The grid has redundancy through multiple power plants, providing a buffer against smaller-scale attacks. Demand response and voluntary load response programs help reduce grid stress during critical periods, which can mitigate the impact of a cyberattack.

Needs Improvement

- Early detection is challenging due to sophisticated attackers like China's Volt Typhoon, who employ advanced techniques. Audits, while helpful, may not be rigorous enough, with some entities potentially self-certifying without meeting full requirements.

Recovery **B**

The system is prepared to restore its core functionality after an attack.

Doing Well

- Simulated attack scenarios test system resilience, allowing organizations to identify and address weaknesses. Data backups provide a reliable method to restore lost or compromised data, facilitating a quicker recovery after an attack.

Needs Improvement

- Audits should be conducted more frequently and with broader scopes to ensure compliance with cybersecurity standards and uncover potential vulnerabilities. This would improve the system's recovery capabilities and overall security.

Resurgence **A**

The system learns from the attack, leading to improvements and reinforcement.

Doing Well

- Thorough forensic analysis after a cyberattack uncovers the extent of damage and identifies vulnerabilities. It provides insights into how the attack occurred, enabling plants to implement targeted improvements and strengthen defenses against future threats.

Needs Improvement

- The gas-fired plants require quicker policy and regulatory updates to keep pace with evolving cyber threats. Infrastructure upgrades need more focus on modernizing operational technologies and strengthening cybersecurity frameworks for better detection and response.

Recommendations

In response to the catastrophic Texas grid failure during Winter Storm Uri and heightened threats of cyber attacks, there is an urgent need to bolster the state's electricity grid resilience through more frequent infrastructure audits and the integration of additional Direct Current (DC) grid tie-ins. These measures are essential to mitigate the risks of future disruptions, specifically cyberattacks from sophisticated nation-state actors.

Audits

Frequent and comprehensive audits are key to strengthening the Texas electricity grid security and resilience. Third-party cybersecurity firms should conduct biannual audits to evaluate the grid cyber security protocols, physical security, operational technology, and supply chain vulnerabilities. These audits aim to identify potential risks, such as supply chain attacks involving software and hardware from external vendors, and ensure the grid's overall security is up to standard. Though the financial and operational costs for these audits are significant, including additional manpower and training, the benefits far outweigh them. By focusing on high security standards and implementing corrective measures as needed, the grid will be better prepared to withstand various threats.

DC Tie-Ins

The integration of additional DC grid tie-ins is essential to boost the Texas grid's resilience and operational flexibility. With only limited connections to other interconnections, the grid needs more DC tie-ins to allow for electricity exchange with neighboring grids.

This increased connectivity offers a critical safety net during supply shortages, emergencies, or equipment failures. Plans are in place to build new DC ties, but they won't be operational until 2029. The estimated cost is between $1.5 billion and $2 billion, reflecting the construction and technology expenses. While costly, these new ties provide significant long-term benefits, including improved grid stability and a reduced risk of blackouts. Combining frequent audits with increased DC grid tie-ins creates a comprehensive strategy for addressing the Texas grid's vulnerabilities. These measures are crucial for ensuring the grid's resilience and reliability in the face of future threats and disruptions.

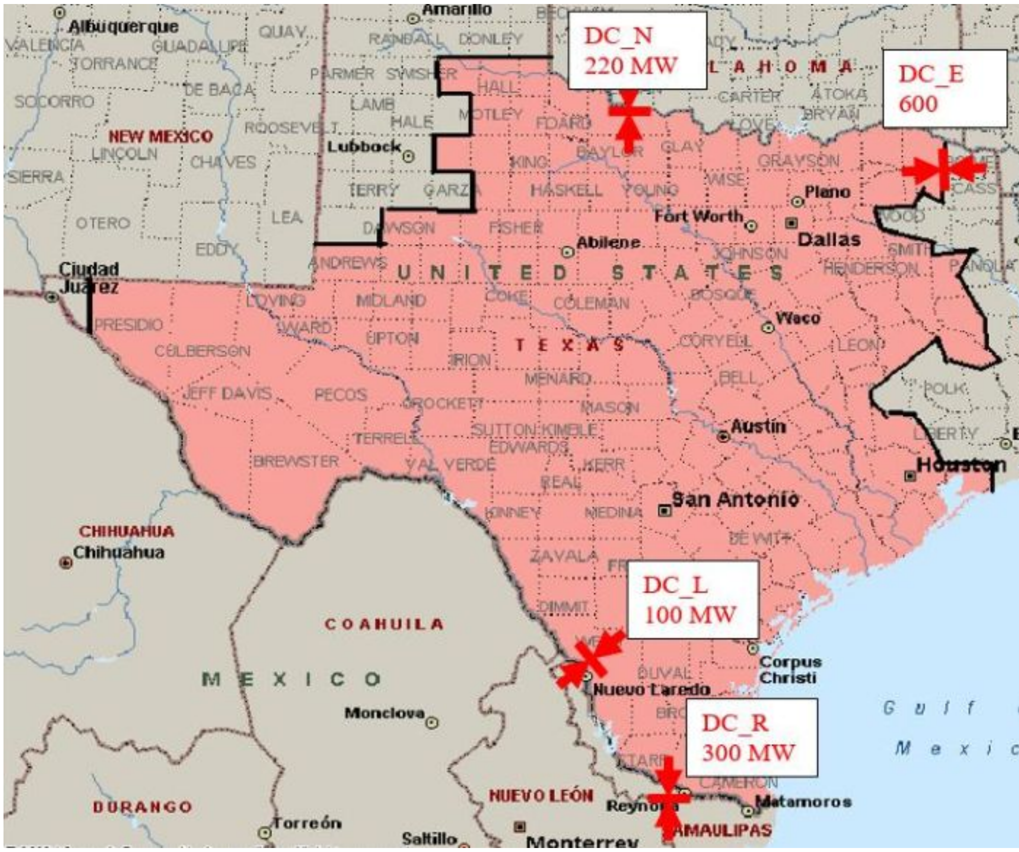

Figure 3. Map of DC Tie-Ins to the Texas Power Grid in 2020.

References

System Scope & Vulnerabilities

1. "Report: Chinese Hackers Targeted Texas Power Grid, Hawaii Water Utility, Other Critical Infrastructure." https://spectrumlocalnews.com/tx/south-texas-el-paso/news/2023/12/11/report--chinese-hackers-targeted-texas-power-grid--hawaii-water-utility--other-critical-infrastructure-.
2. "ERCOT - Texas Comptroller." Texas Comptroller of Public Accounts. Last modified 2023. https://comptroller.texas.gov/economy/economic-data/energy/2023/ercot.php#:~:text=The%20Texas%20Interconnection%20supplies%20electricity,254%20counties%20(Exhibit%201).
3. "Texas Bill Would Expand Power Grid's Capacity, Undercut Federal Oversight." Inside Climate News. Last modified March 22, 2024. https://insideclimatenews.org/news/22032024/texas-bill-power-capacity-regional-grid-federal-oversight/#:~:text=Isolated%20by%20Design,neighboring%20states%20and%20from%20Mexico.
4. "How Gas Turbine Power Plants Work." U.S. Department of Energy. Accessed April 19, 2024. https://www.energy.gov/fecm/how-gas-turbine-power-plants-work#:~:text=As%20hot%20combustion%20gas%20expands,a%20generator%20to%20produce%20electricity.
5. "Today in Energy." U.S. Energy Information Administration. Last modified March 24, 2023. https://www.eia.gov/todayinenergy/detail.php?id=61444#:~:text=Combined%20with%20increasing%20domestic%20supply,main%20reasons%20for%20their%20growth.
6. "Natural Gas Processing Plants." U.S. Energy Information Administration. Accessed April 19, 2024. https://atlas.eia.gov/datasets/natural-gas-processing-plants/.

Threat: Industrial Control Systems & Cyberattacks

1. Pierluigi Paganini, "US government imposed sanctions on six Iranian intel officials," *SecurityAffairs*, February 4, 2024, https://securityaffairs.com/158621/cyber-warfare-2/iranian-intel-officials-sanctions-critical-infrastructure.html.
2. Microsoft Threat Intelligence, "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," *Microsoft*, May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.
3. A.B. Birchfield, T. Xu, K.M. Gegner, K.S. Shetye, and T.J. Overbye, "Grid Structural Characteristics as Validation Criteria for Synthetic Networks," *IEEE Transactions on Power Systems, vol. 32*, no. 4, pp. 3258-3265, July 2017. https://doi.org/10.1109/TPWRS.2016.2616385.

Resilience Framework

1. NERC, "Security Guideline: Cyber Security Risk Management Lifecycle," NERC, December 6, 2022, https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Cyber_Security_Risk_Management_Lifecycle.pdf.
2. NERC, "Standard CIP–002–1 — Cyber Security — Critical Cyber Asset Identification," NERC, May 2, 2006, https://www.nerc.com/pa/Stand/Cyber%20Security%20Permanent/Cyber_Security_Standards_Board_Approval_02May06.pdf.
3. NERC, "Standard CIP–002–1 — Cyber Security — Critical Cyber Asset Identification."
4. CISA, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," CISA, February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.
5. NERC, "2023 E-ISAC END-OF-YEAR REPORT," NERC, 2023, https://www.nerc.com/pa/CI/ESISAC/Documents/2023%20E-ISAC%20End-of-Year%20Report.pdf.
6. Burger, Scott, et al. "The Economics of Demand Flexibility: How 'Flexiwatts' Create Quantifiable Value for Customers and the Grid." Energy Policy 114 (2018): 499-512. DOI: 10.1016/j.enpol.2017.12.044.
7. Wilcox, Lily. "Texas Interconnection SME Interview." Lauren Stemler and Ned Pfeiffer (Logan, UT), March 5, 2024.
8. "How to Use a Cyber-Attack Simulation to Reduce Your Security Risk." TitanHQ, https://www.titanhq.com/safetitan/how-to-use-a-cyber-attack-simulation-to-reduce-your-security-risk/.
9. 'The Importance of Data Backup for Cybersecurity.' Morgan Stanley, March 20, 2023. https://www.morganstanley.com/articles/data-backup-importance-cybersecurity."
10. Irwin, Luke. "What is a Cyber Security Audit and Why is it Important?" IT Governance Blog, 17 May 2022. https://www.itgovernance.co.uk/blog/what-is-a-cyber-security-audit-and-why-is-it-important.

Ned Pfeiffer, Lauren Stemler, Sydney Perkins

CAI 5200: Threats & Resilience

References Continued

Resilience Framework Cont.

11. Dhillon, Gurpreet. "What to Do Before and After a Cybersecurity Breach." American University. https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf.

12.. Harris, JD. "Why Cybersecurity Regulations and Oversight Are as Important as Safety Standards in the Modern Workplace." Forbes. January 30, 2023. https://www.forbes.com/sites/forbesbusinesscouncil/2023/01/30/why-cybersecurity-regulations-and-oversight-are-as-important-as-safety-standards-in-the-modern-workplace/?sh=206266415464.

13. Lenaerts-Bergmans, Bart. "Attack Vectors: What They Are and How They Are Exploited." CrowdStrike, April 13, 2023. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/attack-vector/.

Recommendations

1. Lenaerts, Bart. 2023. “What Is a Supply Chain Attack?” CrowdStrike. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/.
2. Korolov, Maria. 2021. “Supply chain attacks show why you should be wary of third-party providers.” CSO Online. https://www.csoonline.com/article/561323/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html.Erica Proffer, “Yes, there is a plan to connect Texas to the U.S. power grid. Sort of.” KVUE.com, January 4, 2024, https://www.kvue.com/article/news/investigations/defenders/connect-texas-power-grid-nationally-plan-ercot/269-2918ca91-8e6a-43d3-9fa1-ee2af138e487
3. Lily Wilcox, "Texas Interconnection SME Interview" By Ned Pfeiffer and Lauren Stemler, March 5, 2024.
4. U.S. Department of Energy. "Grid Modernization and the Smart Grid." DOE/GO-102016-4875. Washington, D.C.: U.S. Department of Energy, 2016.
5. Morgan, Granger. "The Grid: Understanding the Infrastructure That Powers Our Lives." Daedalus 146, no. 2 (Spring 2017): 8-17.
6. Rothwell, Geoffrey, and Tomas Gomez. "Electricity Economics: Regulation and Deregulation." IEEE Press & Wiley-Interscience, 2003.
7. Giuseppe Macri, "Symantec, FireEye, Others Join Together to Fight New Export Restrictions on Cybersecurity Tech," InsideSources, July 15, 2015, https://insidesources.com/symantec-fireeye-others-join-together-to-fight-new-export-restrictions-on-cybersecurity-tech/
8. Mark Golden, "New research consortium seeks to help optimize future grid," Stanford Doerr School of Sustainability, February 21, 2024, https://sustainability.stanford.edu/news/new-research-consortium-seeks-help-optimize-future-grid
9. North American Electric Reliability Corporation (NERC). "2020 Long-Term Reliability Assessment." Atlanta, GA: NERC, 2020.
10. Amin, S. Massoud, and Bruce F. Wollenberg. "Toward a Smart Grid: Power Delivery for the 21st Century." IEEE Power and Energy Magazine 3, no. 5 (September-October 2005): 34-41.