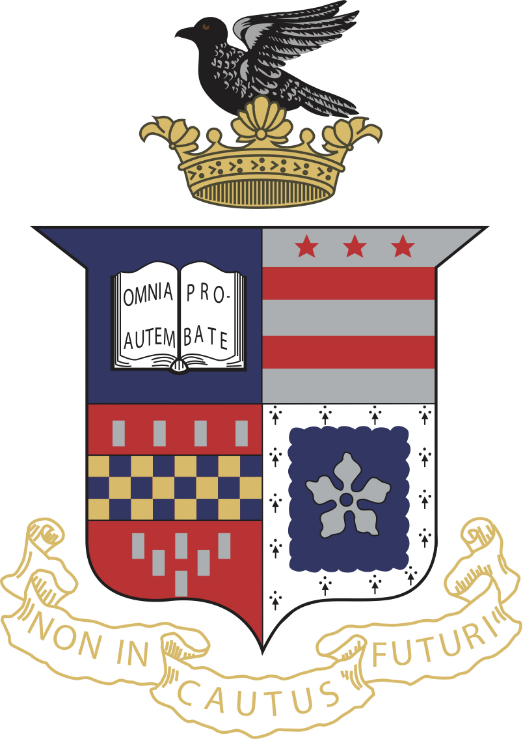
Lab 9: Attacking Critical United States Infrastructure:

Analyzing Threat and Defense Strategy



Will Hanna & Jimmy Horvath

CSCI 111: Introduction to Computer Science

November 15, 2024

*Background Research*

The Zero Days documentary highlights the effects of the Stuxnet virus on global digital infrastructure and international relations. For the first time, Stuxnet demonstrated that a piece of code, previously confined to the cyber realm, could cause physical destruction. This global issue prompted the United States to establish the U.S. Cyber Command, a branch of the National Security Agency, to address threats like Stuxnet and Iran's involvement, as well as future cyber challenges. Upon taking office in 2009, President Obama prioritized investing in digital infrastructure to counter growing concerns in the Middle East. Furthermore, the growth of coding and ability of nations to hide their activities have made it increasingly difficult to enforce international regulations. For instance, Iran developed a secret nuclear arsenal without UN approval. This shifted the global power dynamic, leveling the playing field between superpowers and smaller nations previously not considered large-scale threats.

James Burke’s documentary on the 1965 NYC blackout emphasizes society’s reliance on technology, even decades ago. A single automatic switch failure at a New York power station caused chaos throughout the northeastern U.S. While the technological advancements of the 1960s do not compare to those of the last half-century, the documentary reveals the vulnerability of critical infrastructure and the nation's inability to respond to large-scale disruptions.

A recurring theme in major societal interruptions in the U.S. is the malfunction of the Energy Sector. This critical infrastructure is uniquely intertwined with multiple industries, government operations, and daily civilian life. As such, the Energy Sector would be the most volatile and impactful target for an adversarial nation-state that is intent on harming the United States.

*Critical Infrastructure: Energy Sector*

For a nation-state adversary seeking to cause chaos in the United States, disrupting essential domestic operations would be the most effective strategy. In today’s technology-driven world, nearly all operations depend on the nation’s energy grid. As stated by the Cybersecurity and Infrastructure Security Agency (CISA), “without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function.” Presidential Policy Directive 21 designates the Energy Sector as uniquely critical, as it provides an “enabling function” across all critical infrastructure sectors.

The Energy Sector in the United States is made up of three interconnected segments: electricity, oil, and natural gas. Given that virtually all other critical infrastructure depends on electricity and fuel, an attack on this sector could trigger disruptions across the economy. More specifically, disrupting oil and natural gas pipelines would halt fuel distribution, affecting industries reliant on these supplies, such as manufacturing, transportation, and power generation. Given the U.S.'s dependence on these resources, such disruptions would have widespread consequences.

Second, targeting private companies that dominate the energy infrastructure could also cause chaos. Over 80% of the U.S. energy infrastructure is privately owned. While some argue that decentralized ownership promotes cybersecurity, the lack of a unified response mechanism can hinder effective action during crises. Additionally, private businesses may lack sufficient funding and training to defend against large-scale cyberattacks.

Within the “Energy Sector-Specific Plan” published by the Department of Homeland Security, “the Electricity Subsector identified several issues as the key risks and threats to its infrastructure and/or continuity of business in 2012 and 2013: Cyber and physical security threats; Natural disasters and extreme weather conditions; Workforce capability (“aging workforce”) and human errors; Equipment failure and aging infrastructure; Evolving environmental, economic, and reliability regulatory requirements; and Changes in the technical and operational environment, including changes in fuel supply” (DOHS). In order to have a meaningful impact and disrupt key infrastructure, the nation-state adversary needs to act in a way that is unexpected and leaves the Department of Homeland Security unprepared.

The best ways to disrupt the physical integrity of the Energy Sector revolves around a few key tactics: 1) Create malware that alters functionality of SCADA system, which has direct ties to the response times to potential hacks or energy security issues; 2) Industry plants within the private sector of the energy economy, preferably holding critical roles in the enterprises that have high ownership share of country’s energy grid; 3) Gain insightful information of companies through increased usage of ‘phishing’ emails; 4) Understand energy grid more comprehensibly to pinpoint key locations of access.

In February 2021, an extreme winter storm in Texas led to a massive electricity generation failure. 4.5 million homes lost power, 57 people died, and property damage totaled upwards of $195 billion. The energy outage persisted for longer than it should have due to Texas having an independent power grid from the rest of the United States but highlighted issues within the Energy Sector. This incident underscores the potential consequences of a large-scale Energy Sector disruption. A cyberattack on this infrastructure could result in widespread fatalities, safety concerns, and a loss of confidence in U.S. resilience and security.

*Mitigation Strategy Proposal*

Eric Chien of the Zero Days documentary highlights that no network is truly ever secure, using the Stuxnet virus as his chief example. While this may be true, it doesn't mean attacks can’t be defended against or at least mitigated. Especially given U.S. GDP accounted for twenty-five percent of global production, domestic infrastructure protection is as important for the homeland as it is for the rest of the world[[1]](#footnote-1). Thus, in late April, President Biden announced a National Security Memorandum (NSM) on critical infrastructure, launching a comprehensive effort to protect the U.S against all threats[[2]](#footnote-2). In analyzing the NSM and researching defense strategies across the web, therein lies two key modalities to bolster our safeguards. First, the U.S. must strengthen *cybersecurity* via regular assessments and intrusion detection systems (IDS). Second, reinforcing *physical security* such as increasing surveillance and physical access controls at key infrastructure sites is necessary. Overall, if we’re to strengthen our cybersecurity defense, we need to create a well-rounded protection against all types of threats.

Chiefly, bettering cybersecurity requires regular assessments. For practically any type of infrastructure, schedules are key for monitoring. This is due to the nature of most infrastructures, called SCADA systems. Short for Supervisory Control and Data Acquisition, a SCADA system, “uses computers, networked data communications, and graphical Human Machine Interfaces (HMIs) to manage and control industrial processes.”[[3]](#footnote-3) They collect and analyze real-time data from processes, record and log this data, and display it. Essentially, SCADA systems monitor levels of products in infrastructure, especially in energy. For example, Iranian SCADA systems monitoring their nuclear centrifuges were attacked by the United States and Israeli in 2010. Via the Stuxnet virus, the U.S. NSA and Israeli group 8200 targeted Siemens PLCs, computer software that facilitated the SCADA system, which monitored uranium-236 levels in the centrifuges. Additionally, these SCADA systems monitored the centrifuge spin speeds, as uranium-236 is a chaotic substance and must be controlled very particularly. So, SCADA systems were critical to the Iranian government, given nuclear power is a key electricity source.

The only reason Stuxnet was even discovered was that it spreads outside of the nuclear facility in Natanz. However, in the current day, the Iranians have ensured this attack won’t happen again by monitoring both their systems and the people who run them. After aware of the Stuxnet virus, Iran power plants have not been attacked again due to this particular planning.

Secondly, intrusion detection systems (IDS) are key to managing cybersecurity. An IDS matters to cybersecurity, given it monitors the traffic on a computer network to detect any suspicious activity and reports it. It analyzes the data flowing through the network, looking for signs of abnormal behavior. The IDS is able to observe this abnormal behavior because the humans predefine malware principles or patterns that the network can recognize.[[4]](#footnote-4) Then, when the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator. However, with the Stuxnet virus, the IDS was ineffective at deducing the threat. Stuxnet changed the PLCs’ programming, which was dangerous because PLCs give information to the computer controller that everything is working fine. However, in this case, the threat went unnoticed given it difficult to diagnose the problem. This resulted in malfunction and destruction of various centrifuges without a clue of what went wrong.

Thus, the Stuxnet example shows that network running with PLCs must be well defended. Perhaps more robust remote access control provides a solution to this complex problem. Especially for the Iranians, more complicated access controls would make getting into the PLC more difficult. This is even more pertinent, given none of the Natanz computers run on the internet.

While the priority should be to strengthen *cybersecurity*, reinforcing physical security should also be a tactic used to ensure there’s no intruder on the grounds of your infrastructure. The place to start is certainly access controls and video surveillance.[[5]](#footnote-5) This would limit or hopefully completely restrict uncredentialed personnel from entering the facility. Other strategies include installing alarm systems, training current employees on security standards, and doing background checks in hiring new employees.

Bibliography

“14 Major SCADA Hacks.” *DPS Telecom*, 6 Dec. 2024, www.dpstele.com/blog/major-scada-hacks.php.

*2015 Energy Sector-Specific Plan*, www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf. Accessed 9 Dec. 2024.

Bhutada, Govind. “The U.S. Share of the Global Economy over Time.” *Visual Capitalist*, 14 Jan. 2021, [www.visualcapitalist.com/u-s-share-of-global-economy-over-time/#google\_vignette](#google_vignette).

“Critical Infrastructure Sectors: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors. Accessed 9 Dec. 2024.

Group, Facility Protection. “12 Strategies for Enhancing Physical Security in Your Organization...” *Facility Protection Group |*, 30 Apr. 2024, facprogroup.com/12-strategies-for-enhancing-physical-security-in-your-organization/.

“Intrusion Detection System (IDS).” *GeeksforGeeks*, GeeksforGeeks, 18 June 2024, www.geeksforgeeks.org/intrusion-detection-system-ids/.

Muthukrishnan, Vidya. “SCADA System: What Is It? (Supervisory Control and Data Acquisition).” *Electrical4U*, 6 June 2024, www.electrical4u.com/scada-system/.

“National Security Memorandum on Critical Infrastructure Security and Resilience.” *The White House*, The United States Government, 30 Apr. 2024, www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

“SCADA System for Energy and Transportation: Emerson Us.” *SCADA System for Energy and Transportation | Emerson US*, www.emerson.com/en-us/automation/control-and-safety-systems/scada-systems/scada-systems-for-energy-transportation. Accessed 9 Dec. 2024.

“U.S. Energy Information Administration - EIA - Independent Statistics and Analysis.” *Oil Imports and Exports - U.S. Energy Information Administration (EIA)*, www.eia.gov/energyexplained/oil-and-petroleum-products/imports-and-exports.php. Accessed 9 Dec. 2024.

“What Is a SCADA System and How Does It Work?” *Embedded Industrial Computers for Edge & IoT*, www.onlogic.com/blog/what-is-a-scada-system-and-how-does-it-work/. Accessed 9 Dec. 2024.

1. Bhutada, Govind. “The U.S. Share of the Global Economy over Time.” *Visual Capitalist*, 14 Jan. 2021, [www.visualcapitalist.com/u-s-share-of-global-economy-over-time/#google\_vignette](#google_vignette). [↑](#footnote-ref-1)
2. “National Security Memorandum on Critical Infrastructure Security and Resilience.” *The White House*, The United States Government, 30 Apr. 2024, www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/. [↑](#footnote-ref-2)
3. Muthukrishnan, Vidya. “SCADA System: What Is It? (Supervisory Control and Data Acquisition).” *Electrical4U*, 6 June 2024, www.electrical4u.com/scada-system/. [↑](#footnote-ref-3)
4. “Intrusion Detection System (IDS).” *GeeksforGeeks*, GeeksforGeeks, 18 June 2024, www.geeksforgeeks.org/intrusion-detection-system-ids/. [↑](#footnote-ref-4)
5. Group, Facility Protection. “12 Strategies for Enhancing Physical Security in Your Organization...” *Facility Protection Group |*, 30 Apr. 2024, facprogroup.com/12-strategies-for-enhancing-physical-security-in-your-organization/. [↑](#footnote-ref-5)