

The viability of US cyber defense against
foreign adversaries and adaptive
cybersecurity through Public-Private
Partnership

By: Wilbert Bean III

ISSC499

3/17/25

Table of Contents.....	2
Forward.....	4
Abstract.....	4
Opening Material.....	6
Literature Review.....	8
US Cyber Defense through Offensive Strategies.....	8
Section 1: US Cyber Defensive Capabilities - Iranian Nuclear Enrichment Program	
Deterrence.....	8
Stuxnet Design Intelligence and Variants.....	9
Design Intelligence.....	9
Stuxnet's Variants.....	11
Stuxnet Attack Vectors and Cyber Kill Chain Analysis.....	14
Mitigating Suggestions.....	18
Nation State-Sponsored Adversarial Campaigns and Defensive Strategies.....	21
Section 2: Russian and North Korean Foreign Adversaries - Cyber Offensive Campaigns and the Defense of the US Critical Infrastructure.....	21
Cyber Attack on the Ukraine Power Grid Companies.....	22
Summary of Incidents.....	27
Mitigation Ideas.....	41
North Korean Offensive Campaign against the US Financial Systems Sector.....	43
Summary of Incidents.....	45
Important Learning Points.....	46
Mitigation Ideas.....	47
Adaptive Cybersecurity and Public-Private Partnerships.....	49
Section 3: The US Adaptive Cyber Security Strategy and Public-Private Partnership	
Efforts Strengthen National Defense.....	49
Critical Infrastructure Security and Resilience (CISR).....	52
Legislation, Acts and Presidential Actions.....	58
Federal Plans, Strategies and Guidance.....	61
Discussion.....	70
How does congress intend on securing the Internet to Ensure U.S. Cyber Defense over aging critical infrastructure?.....	71
Emerging Trends and Threats in Artificial Intelligence Cyber Offense and Defense.....	71
Impacts of Innovation and Policy on Societal Dimensions.....	72
Key impacts on privacy and trust.....	72
Recommendations and Suggestions.....	73

Operation Olympic Games & Stuxnet.....	73
Foreign Adversary Cyber Threat Mitigation.....	74
Russian Cyber Attack Remediation Recommendations:.....	74
North Korea/DPRK Cyber Attack Remediation Recommendations.....	75
Conclusion.....	76
References.....	78

Forward

This capstone paper represents the culmination of my senior seminar research, delving into the complex and ever-evolving landscape of United States cyber defense. As we navigate an era defined by sophisticated cyber threats, it is imperative to understand the strategic initiatives, technological advancements, and collaborative efforts that bolster our national security. This work examines pivotal moments in cyber warfare, from the groundbreaking development of Stuxnet to the disruptive attacks on critical infrastructure, highlighting the critical role of public-private partnerships in shaping a resilient cyber future. My aim is to provide a comprehensive analysis of the US's cyber defense capabilities, drawing on historical precedent and contemporary strategies to illuminate the path forward in an increasingly interconnected world.

Abstract

This capstone paper, authored by Wilbert Bean III, explores the United States' cyber defense capabilities through a multi-faceted analysis of historical and contemporary cyber warfare actions and strategic responses. It begins by examining Operation Olympic Games and the development of Stuxnet, highlighting the sophistication of US cyber weaponry and the strategic value of international partnerships, specifically with Israel, in countering nuclear proliferation. This section provides an in-depth look at the technical complexities of Stuxnet and its implications for industrial control system security. Subsequently, the paper analyzes adversarial cyber campaigns, focusing on Russia's attacks on the Ukrainian power grid and North Korea's

assaults on US financial systems, to extract critical lessons for regional and national cybersecurity. These case studies underscore the vulnerabilities of critical infrastructure and the need for robust defensive measures. Finally, the paper investigates the US's adaptive cyber defense strategy, emphasizing the pivotal role of public-private partnerships in safeguarding national interests. It clarifies the complex interplay of legislation, presidential actions, and federal plans that drive US cyber defense, demonstrating how collaborative efforts are essential in building a globally connected and resilient cyber defense framework. Through a comprehensive review of these critical areas, this capstone aims to demonstrate the US's proactive and evolving approach to cyber defense, positioning it as a global leader in cybersecurity resilience.

Opening Material

This capstone aims to demonstrate the US's Cyber defense capabilities, it will do this through the analysis of the novel cyber warfare action such the development of Stuxnet during Operation Olympic Games, it will review adversarial actions such as the Russian cyber offensive campaign on the Ukrainian power grid energy sector, and how cyber security adaptive strategies such as Public-Private Partnerships are shaping the future where US Cyber Defense is a global effort.

The first section of this paper will review the most comprehensive research from the US's Cyber defensive measures to mitigate the threat from the Iranian nuclear enrichment program capabilities. The operation called Olympic Games and the first cyber weapon of its kind, Stuxnet, demonstrate the sophistication of US cyber defense, as well as how the strategic partnership with Israel led to a successful attack on Iran's Nuclear Industrial Control Systems. Section one is organized to provide analytical reference into the design intelligence, the complexity of reproducing the cyber weapon by adversaries and mitigating practices for asset owners to protect against similar sophisticated cyber-physical attacks.

The second section of this paper will review research on foreign adversarial incidents such as the Russian initiated cyber-attack on the Ukrainian Power Grid energy sector that led to the loss of power availability, negatively impacting 225,000 Ukrainian citizens. In addition to that, it will cover a North Korean cyber offensive campaign against US Financial Systems. Section two is organized to provide an overview of lessons learned from the Regional Cyber

Security Community level. The subsections of section two analyze the summary of incidents that led to Russia's successful cyber-attack on Ukraine's power grid, summarizes important learning points and presents several mitigation ideas based on publicly available information on ICS incidents in Ukraine.

The third section of this paper will clarify and streamline the complex US cyber defense strategy, and public-private partnerships to safeguard the nation against future cyber-attacks with dire consequences. Section three is organized to provide a structured understanding of how the US adaptive cyber security strategy and Public-Private Partnerships are assisting in the nation's defense. The subsections of section three analyze Critical Infrastructure Security and Resilience, Legislation, Acts and Presidential Actions, and Federal Plans, Strategies, and Guidance. The subsections of section three frame the multifaceted efforts of US cyber-defense to clearly demonstrate the contemporary operations and roadmap to the future of national defense through partnerships expanding the globe.

Literature Review

US Cyber Defense through Offensive Strategies

Section 1: US Cyber Defensive Capabilities - Iranian Nuclear Enrichment Program Deterrence

This section analyzes Operation Olympic Games, a pivotal example of U.S. cyber defense employing offensive strategies, specifically leveraging geopolitical tensions to deploy malware to disable a foreign nation's critical infrastructure. Initiated in 2006 during the Bush administration orchestrated by the National Security Agency (NSA) and the Central Intelligence Agency (CIA), this operation targeted Iran's Natanz Nuclear Facility. This analysis draws upon Bruce Schneier's *to Kill a Centrifuge* and Mariusz A. Kamiński's Operation "Olympic Games" to examine the malware's ingenuity, propagation, and impact on SCADA systems, as well as the post variants, cyber kill chain analysis and mitigations. This section argues that Operation Olympic Games and Stuxnet resulting in the incapacitation of Iran's nuclear capabilities established a new paradigm for state-sponsored cyber warfare, highlighting the potential of U.S. Cyber Defense through the strategic use of intelligence collection, foreign partners, and offensive cyber operations.

The substantial damage Stuxnet malware inflicted upon the Natanz Nuclear Facility, damaging approximately 1,000 centrifuges, attributed to the U.S. and Israel demonstrated a paradigm for advanced cyber operations successfully disabling critical infrastructure, and

shifting international security norms. The threat of Iran's Nuclear Enrichment capabilities may have been neutralized but the accidental release of Stuxnet led to the reverse engineering of the malware and the development of new variants such as Duqu. Unlike Stuxnet, DuQu is an intelligence gathering tool, aiming to prepare the ground for attacks such as Stuxnet.

To maintain vigilance against adversaries who might adapt and evolve their tactics, Stuxnet's design intelligence and subsequent variants warrant continual analysis, as do understanding the cyber kill chain and continuous mitigation suggestions.

Stuxnet Design Intelligence and Variants

Design Intelligence

In this section topics such as the Stuxnet design intelligence, variants, and mitigating suggestions will be analyzed. Stuxnet remains the focus of studies today because its ingenuity remains highly relevant in today's cyber offensive landscape. According to Langner's to Kill a Centrifuge, Stuxnet's continues to baffle military strategies, computer security experts, political decision makers, and the public. Langner adds that being a cyber-physical attack, one must understand the physical part as well - the design features of the plant that was attacked, and of its process parameters. Stuxnet differs from cyber-attacks as we see them today, a cyber-physical attack involves three layers and their specific vulnerabilities. An example of those layers is displayed in Figure 1.

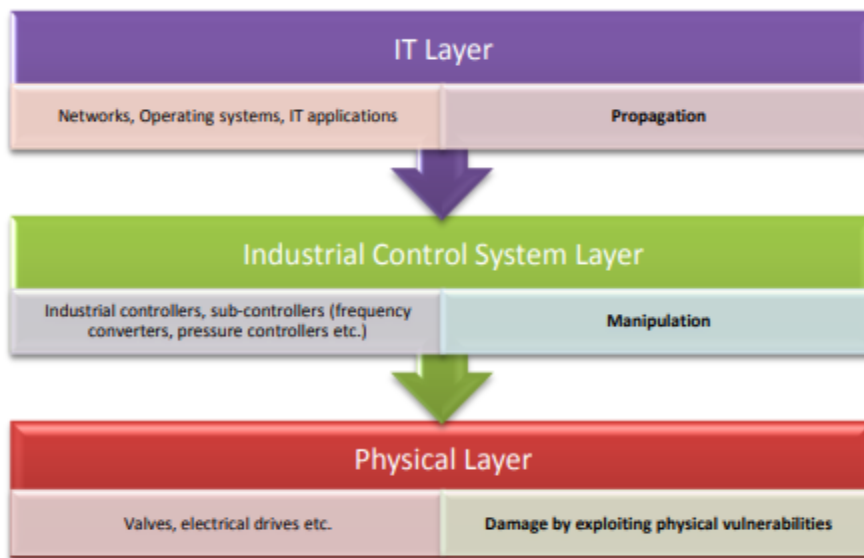


Figure 1: The three layers of a sophisticated cyber-physical attack

The IT layer, which is used to spread malware, the control system layer which is used to manipulate (but not disrupt) process control, and finally the physical layer where the actual damage is created (Langner et al., 2013). In the case of the cyber-attack against Natanz, the vulnerability on the physical layer was the fragility of the fast-spinning centrifuge rotors that were exploited by manipulations of process pressure and rotor speed (Langner et al., 2013). Stuxnet malware makes a textbook example of how interaction of these layers can be leveraged to create physical destruction by a cyber-attack (Langner et al., 2013). Visible through the various cyber-physical exploits is the silhouette of a methodology for attack engineering that can be taught in school and can be implemented in algorithms (Langner et al., 2013).

Langner says “while offensive forces will already have started to understand and work with this methodology, defensive forces did not - lulling themselves in the theory that Stuxnet

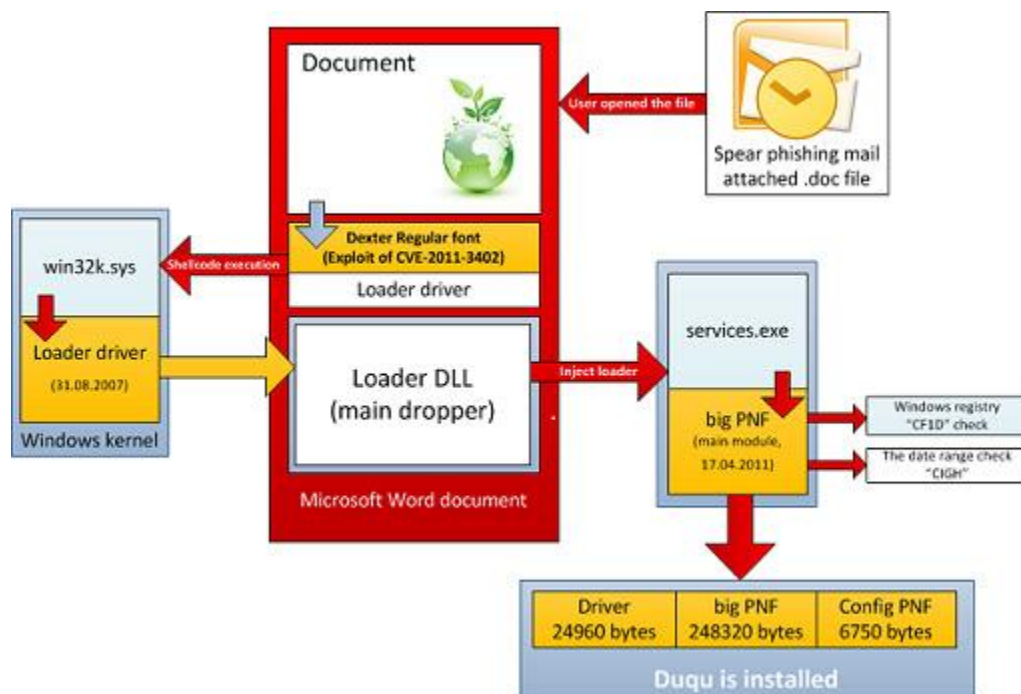
was so specifically crafted to hit just one singular target that is so different from common critical infrastructure installations.” That represents a major priority for defending against Stuxnet or Stuxnet-like malware. In the next section, the variants discovered in 2010 will be analyzed to understand how the Stuxnet variants have evolved, specifically discussing variants such as Duqu.

Stuxnet’s Variants

New variants of Stuxnet or Malware with Stuxnet-Like characteristics were stumbled upon by accident by a Belarusian Cyber Security Firm. The new variant that was not discovered until 2010 was much simpler and much less stealthy than its predecessor. It also attacked a completely different component: the Centrifuge Drive System (CDS) that controls rotor speeds (Langner et al., 2013). The attack routines for the overpressure attack were still contained in the payload, but no longer executed - a fact that must be viewed as deficient OPSEC. It provided us by far the best forensic evidence for identifying Stuxnet’s target, and without the new, easy-to-spot variant the earlier predecessor may never have been discovered (Langner et al., 2013). That also means that the most aggressive cyber-physical attack tactics would still be unknown to the public - unavailable for use in copycat attacks, and unusable as a deterrent display of cyber power (Langner et al., 2013).

Stuxnet was discovered, researched, and studied after the centrifuge destruction in Natanz, Iran. The significance of discovering variants of Stuxnet is that the malware remains hidden from conventional anti-virus and malware detection. Variants would make it significantly harder to discover because the anti-virus and malware software providers might not have the

signatures necessary for detection. Meanwhile, the discovery of a variant namely “Duqu” is highly important because until its discovery and study, the proliferation of Duqu has an unknown impact on systems as well as networks. Below is a diagram displaying the attack simulation of the Duqu malware:



The evolution of Stuxnet as well as Stuxnet-like malware all of a sudden became equipped with the latest and greatest MS Windows exploits and stolen digital certificates as the icing on the cake, allowing the malicious software to pose as legitimate driver software and thus not be rejected by newer versions of the Windows operating system (Langner et al., 2013). Langner further states “Obviously, organizations had joined the club that have a stash of zero-days to choose from and could pop up stolen certificates just like that. Whereas the development of the overpressure attack can be viewed as a process that could be limited to an in-group of top notch industrial control system security experts and coders who live in an exotic

ecosystem quite remote from IT security, the circle seems to have gotten much wider, with a new center of gravity in Maryland.”

The use of multiple zero-days came with a price. The new Stuxnet variant was much easier to identify as malicious software than its predecessor as it suddenly displayed very strange and very sophisticated behavior at the IT layer. In comparison, the dropper of the initial version looked pretty much like a legitimate or, worst case, pirated step 7 software project for Siemens controllers; the only strange thing was that a copyright notice and license terms were missing (Langner et al., 2013). The newer version, equipped with a wealth of exploits that hackers can only dream about, signaled even the least vigilant anti-virus researcher that this was something big, warranting a closer look (Langner et al., 2013). This happened in 2010 when a formerly not widely known Belarusian anti-virus company called VirusBlockAda practically stumbled over the malware and put it on the desk of the AV industry (Langner et al., 2013).

Stuxnet’s proliferation and reconnaissance success was in part due to the Operation Olympic Games. With actual physical intervention for recon adding major value to the success of the attack, Duqu differed greatly because it could perform its own reconnaissance without physical presence. This new malware attack vector shifted the offensive capabilities of threat actors in the landscape. In the next section of an analysis of Stuxnet attack vectors and cyber kill chain analysis.

Stuxnet Attack Vectors and Cyber Kill Chain Analysis

In this section a review of the Stuxnet attack vectors demonstrates the U.S. Cyber Defense capabilities to deter a threat from a hostile nation. Langner says “Everything has its roots, and the roots of Stuxnet are not in the IT domain but nuclear counter proliferation.” Sabotaging the Iranian nuclear program had been done before by supplying Iran with manipulated mechanical and electrical equipment (Langner et al., 2013). Stuxnet transformed that approach from analog to digital. Not drawing from the same brain pool that threw sand in Iran’s nuclear gear in the past would have been a stupid waste of resources as even the digital attacks required in-depth knowledge of the plant design and operation; knowledge that could not be obtained by simply analyzing network traffic and computer configurations at Natanz (Langner et al., 2013). Langner says “The post-Stuxnet cyber attack engineer looks at the plant and its control systems in a holistic way, trying to identify physical vulnerabilities and ways to reliably exploit such vulnerabilities by cyber manipulations.” The attack goal for Natanz was to exploit the physical vulnerability to overpressure the centrifuges or to manipulate rotor speeds, resulting in predictable damage. Below is the attack summary provided by Langner:

“Since centrifuge operating pressure at Natanz is controlled by the Cascade Protection System and rotor speed by the Centrifuge Drive System, these two systems became prime candidates for compromise. Only then started the cyber part of the attack engineers’ work. If they are able to determine cyber manipulations which reliably exploit a physical vulnerability, they have arrived at what I call a plant-level vulnerability, for which Stuxnet gives the perfect example. Getting there requires looking at cyber and physical systems in the context of the plant

and its physical processes; an approach waiting to be adopted in cyber defense.” Below is a diagram demonstrating the two different attacks implemented in Stuxnet.

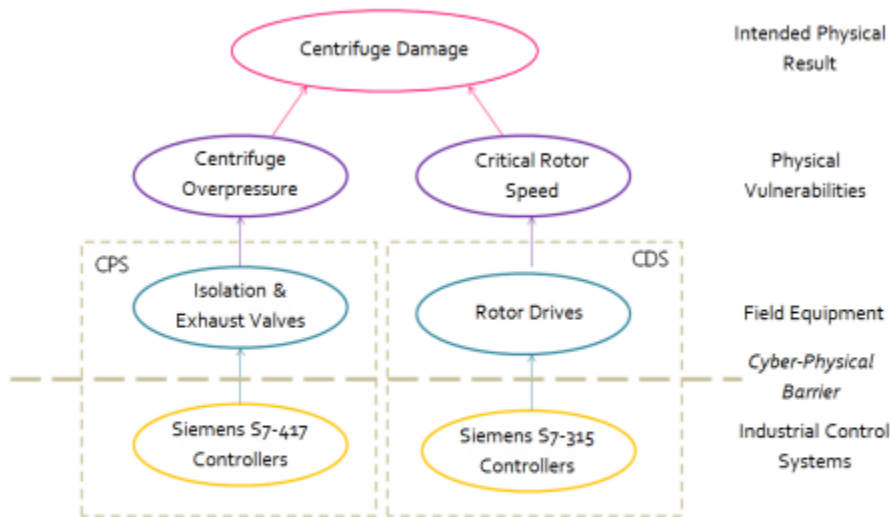


Figure 2: Synopsis of the two different attacks implemented in Stuxnet. Both use a manipulation of industrial control systems to achieve physical damage, exploiting different physical vulnerabilities of the equipment (centrifuge rotors) that basically lead to the same physical result

The sophistication of the malware is that it remained undetected as it targeted the centrifuge control systems and began delivering multiple payloads. Attack engineering is about reliably taking over control in order to exploit physical vulnerabilities (Langner et al., 2013). As Stuxnet began performing its own stress test of the system causing crashes and failures, this methodology displayed a different attack vector than information technology experts were familiar with. At the control system level, Stuxnet did not exploit any zero-day vulnerabilities, buffer overflows or other fancy geek stuff, but legitimate product features (Langner et al., 2013). In the industrial control system space, the worst vulnerabilities are not bugs, they are features (Langner et al., 2013). From the attackers point of view, exploiting flaws rather than bugs has a

significant advantage: They will not be fixed overnight by a vendor releasing a “patch”, and users rolling out the patch quickly (Langner et al., 2013). Instead, the attacker can be confident that those vulnerabilities are here to stay for years, even after successful exploits are out in the wild (Langner et al., 2013). Langner says “To be more specific, Stuxnet teaches potential cyber attackers how to inject malicious code on real time controllers, which may be done in the very same manner by hijacking a driver DLL or, in a more direct way, by directly talking to networked controllers without the need to compromise an engineer’s workstation. It teaches how to take over control from a legitimate program that remains running on a controller by placing malicious code at the very beginning of the main executive.” Below are screenshots displaying the data traffic between a Stuxnet-infected WINCC SCADA system and a controller and the attack entry point of an S7-315 controllers main executive.

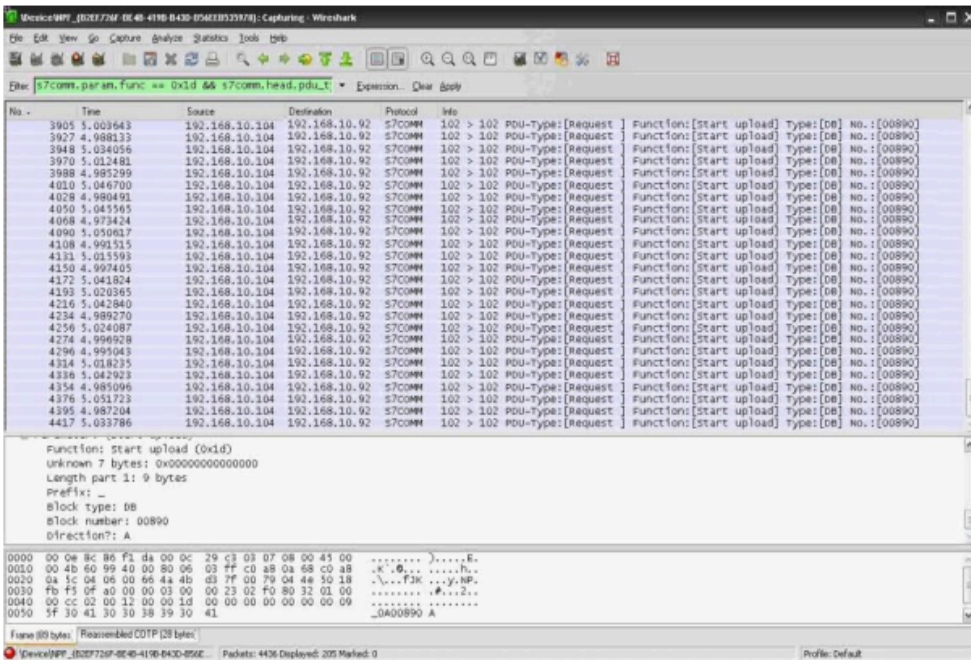


Figure 11: Data traffic between a Stuxnet-infected WinCC SCADA system and a controller, occurring periodically every five seconds, as captured in a properly equipped forensic lab. This traffic simply could not be missed or misinterpreted by ICS security experts; it points to a cyber attack at the controller's application layer

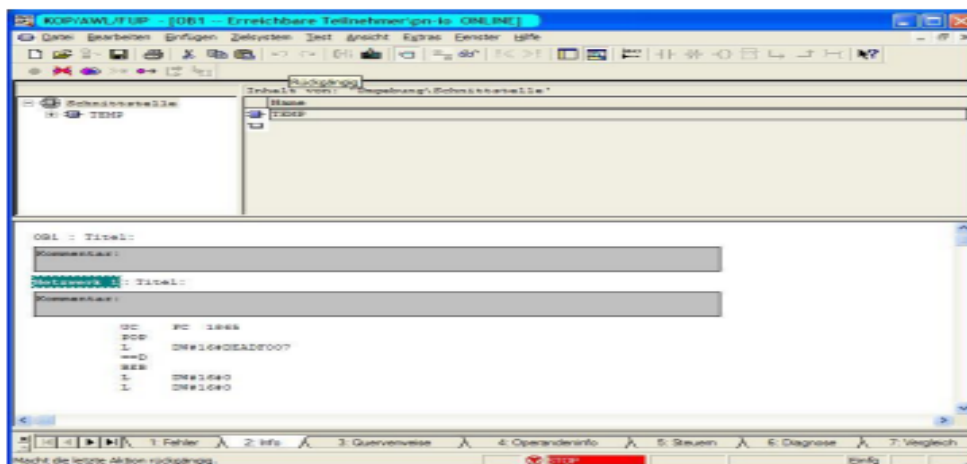


Figure 10: The attack entry point at the beginning of an infected S7-315 controller's main executive, shown in the engineering software. During attack execution, the BEB directive will disable any subsequent legitimate control logic. In comparison, the attack against the S7-417 is an order of magnitude more complex

The first screen capture points to a cyber attack at the controller's application level and the second screen capture demonstrates the disabling of subsequent legitimate control logic.

This sophisticatedly designed malware is still out there with a family of variants and capabilities that still make it a threat to certain industrial asset owners. The significance of Stuxnet is that it was in part a part of Operation Olympic Games, a physical intelligence gathering intervention and that the malware focused on SCADA controller systems, which information technology defenders could not detect through traditional methods. Let's review some of the mitigation strategies suggested by Ralph Langner of The Langner Group.

Mitigating Suggestions

In this section an overview of mitigating strategies suggested from the Langner research group. This section will review if technical security controls can block Stuxnet-Like attacks, and is Active Defense Against Cyber-Physical Attacks Sufficient. Anti-virus software will have issues recognizing the newer Stuxnet-like attack vectors majorly due to its ability to identify and block known malware that is listed in the AV Solutions signature database. Let's move onto determining if technical security controls block Stuxnet-Like Attacks.

Cybersecurity solutions that claim to protect critical infrastructure against Stuxnet-like attacks are mostly unsubstantiated marketing vapor, according to Langner. Langner also says "Anti-virus software doesn't help against a Stuxnet-like attack for a simple reason. It is based on identifying and blocking known malware that is listed in the AV solution's signature database.

Unfortunately there will be no signature for custom-built malware that doesn't display any strange behavior on average computer systems." Malware designed like Stuxnet is pretty indistinguishable from a legitimate application software package and thereby flying below the radar of anti-virus technology(Langner et al., 2013). According to Langner, even the next version with the rotor speed attack, loaded with zero day exploits, travelled at least a year in the wild until discovered by the antivirus industry. In conclusion Langner adds " the most elegant way is to solve the problem by not changing much other than applying technical point solutions. As has been pointed out in the Langner Group research, it can be demonstrated that such solutions don't do much good except for those who sell them. Stuxnet has presented cyber defense as a task that cannot be mastered by simply relying on conventional infosec wisdom." Drawing upon Langner's analysis it is evident that technical security controls cannot block Stuxnet-like attacks. Next an analysis of the viability of active defense against cyber-physical attacks is sufficient.

Active defense against sophisticated cyber-physical attacks in the wake of Stuxnet has been based on two assumptions. First, that such attacks would require nation-state resources, a clear conception as has been pointed out above. Secondly, speculations about adversaries' motivations, and how such motivations can be anticipated or even controlled, were interpreted to suggest that substantial passive defense is not necessary. The minority (including this author) believes that basing national security on theories about adversaries' motivations and wishful thinking on how to control them is a risky gamble. It advocates working towards effective passive defense "just in case", making substantial cyber-physical attacks against critical infrastructure if not impossible, much more difficult, and certainly difficult enough to put them

out of reach for non-state actors. Such a goal that is realistically achievable for those willing to accept the challenge presented by Stuxnet to start over and find and implement new and creative defensive solutions that render cyber weapons pretty much useless. Such solutions conflict with the objectives of cyber warriors not only abroad but also at home. It therefore has to be automatically welcomed by our own offensive cyber forces. This conflict of interest can presently not be resolved technologically but only politically. It has often been stated that cyber offense has an advantage over cyber defense. While it can be debated that is true in technical terms in the domain of industrial control system security, it certainly does apply in a political context. Cyber Offense is well-funded and implemented straightforward within the military chain of command. At the same time, cyber defense of critical national infrastructure is expected to be implemented voluntarily by a dispersed private sector that feels little desire to address matters of national security by ill-coordinated risk management exercises that negatively affect the bottom line.

Studying Operation Olympic Games and the Stuxnet malware provides a stark reality of what the U.S. Cyber Defense apparatus is capable of. Together Olympic Games and Stuxnet provided key factors that led to the success of the mission, intelligence gathering and customized malware to fit the Natanz nuclear facility. The collaboration between the U.S. and Israel's intelligence agencies provided the necessary information for the cyber offensive forces to create the delivery system with two payloads that were intelligently engineered to destroy the centrifuges. In the next section two case studies on major cyber threat groups targeting the

U.S. and allies from Russia and North Korea will be examined to provide visibility into the defense against foreign adversaries..

Nation State-Sponsored Adversarial Campaigns and Defensive Strategies

Section 2: Russian and North Korean Foreign Adversaries - Cyber Offensive Campaigns and the Defense of the US Critical Infrastructure

This section will introduce the structure for the subsequent subsections as well as introduce primary topics being analyzed. In the digital world we live in today adversarial countries with advanced cyber operations are continually evolving their cyber offensive campaigns which pose a significant challenge to the U.S. Cyber Defense Apparatus to keep pace. The primary topics discussed throughout the subsequent sections will examine identified state-sponsored cyber operations groups known as advanced persistent threat groups or APTs, novel cyber-attack incidents against critical infrastructure and mitigation strategies developed by the United States and partner nations.

The research drawn upon in these sections originates from accredited cyber organizations such as the SANS Industrial Control System - Computer Emergency Response Team (ICS-CERT), Electricity Information Sharing and Analysis Center(E-ISAC), U.S. Department of State, U.S. Department of the Treasury, U.S. Department of Homeland Security, and the U.S. Department of Justice. Reports from these agencies as well as organizations indicate that nations with aggressive intentions toward the U.S., such as North Korea/Democratic People's Republic

of Korea (DPRK) have matured and are fully capable of achieving a variety of strategic objectives against diverse targets, including a wider target set in the United States and South Korea.

The U.S. The Global Supply chain relies on the cyber solidarity of its partners such as Ukraine, who suffered a Russian advanced persistent threat (APT) cyber attack on energy grid companies leading to power outages impacting 225,000 people in the targeted regions. The following subsections will analyze significant nation-state adversaries such as Russia's Advanced Persistent Threat (APT) group, APT28 (Fancy Bear) who deployed the BlackEnergy3 Malware against the Ukrainian energy companies which temporarily disconnected three power distribution companies leaving 225,000 people without power for several hours. The analysis will expand into the North Korean APT, APT38(Lazarus Group) who deployed the WannaCry 2.0 Ransomware that damaged massive amounts of computer hardware globally and the theft of \$81 million dollars from Bangladesh Bank in 2016. The next section will introduce as well as examine the Russian APT28 Fancy Bear attack on the Ukraine Power Grid Energy Sector.

Cyber Attack on the Ukraine Power Grid Companies

Imagine the bustling routines of 225,000 people and what activities that might entail over an eight hour day. A vast amount of ideas and assumptions might come to mind. Now imagine what would happen if the same 225,000 people experienced an eight hour energy black out. In this section an analysis of the cyber-attack on the Ukrainian power grid will be examined to understand how it was possible to perform a cyber-attack on the power companies. The

sub-section will analyze in-depth the incidents and mitigation strategies. The majority of the information for this case study was drawn upon from the SANS Industrial Control System (ICS) Team and the Electricity Information Sharing and Analysis Center (E-ISAC). These companies were directly involved in the investigation and mitigation strategy development processes. Additional context will be provided for understanding what a blackout impacting 222,5000 people would be categorized as in terms of power outages from the E-ISAC. The E-ISAC emphasizes that power outages should be measured in scale, number of customers and amount of electricity infrastructure involved and duration to full restoration (Lee et al., 2016).

According to the E-ISAC's "Analysis of the Cyber Attack on the Ukrainian Power Grid" on December 23, 2015 the Ukrainian Kyvioblenergo, a regional electricity distribution company, reported service outages to customers (Lee et al., 2016). The outages were due to a third party's illegal entry into the company's computer and SCADA systems: Starting at approximately 3:35 p.m. local time, seven 110 kV and twenty-three 34 kV substations were disconnected for three hours (Lee et al., 2016). If a similar incident happened in a densely populated area in the U.S. such as Philadelphia, the disconnection of seven 110 kV and twenty-three 34 kV substations for three hours would likely result in widespread power outages across the city and potentially extend into surrounding suburban areas, impacting millions of residents and businesses. The exact impact would depend on the specific substations affected and the areas they serve. The calculation for impact radius considered the service radius of each substation and the area covered by each substation. 110 kV substations typically serve larger areas. A common estimate for the service radius of a 110 kV substation is around five to ten miles. A 34 kV substation generally serves smaller areas. A common estimate for the service radius of a 34 kV substation

in around one to three miles. The formula used to calculate the Area covered by each substation is displayed below:

The area covered by a substation can be approximated using the formula for the area of a circle:

$$\text{Area} = \pi \times r^2$$

where r is the service radius.

For 110 kV Substations:

- **Radius (r):** 5 to 10 miles
- **Area:** $\pi \times r^2$

For a 5-mile radius:

$$\text{Area} = \pi \times 5^2 = 25\pi \approx 78.54 \text{ square miles}$$

For a 10-mile radius:

$$\text{Area} = \pi \times 10^2 = 100\pi \approx 314.16 \text{ square miles}$$

For 34 kV Substations:

- **Radius (r):** 1 to 3 miles
- **Area:** $\pi \times r^2$

For a 1-mile radius:

$$\text{Area} = \pi \times 1^2 = \pi \approx 3.14 \text{ square miles}$$

For a 3-mile radius:

$$\text{Area} = \pi \times 3^2 = 9\pi \approx 28.27 \text{ square miles}$$

Next an estimation of the total impacted area was performed and produced the results below:

For 110 kV Substations:

- **Number of Substations:** 7
- **Area per Substation:** 78.54 to 314.16 square miles
- **Total Area (assuming minimal overlap):** $7 \times 78.54 \approx 550$ square miles to $7 \times 314.16 \approx 2200$ square miles

For 34 kV Substations:

- **Number of Substations:** 23
- **Area per Substation:** 3.14 to 28.27 square miles
- **Total Area (assuming minimal overlap):** $23 \times 3.14 \approx 72$ square miles to $23 \times 28.27 \approx 650$ square miles

This estimation considered the number of substations and their respective service areas.

However, since substation areas have overlap for coverage purposes, the total impacted area will be less than the sum of individual areas.

Next, the total impacted area would be the sum of the areas covered by the 110 kV and 34kV substations, considering some overlap.

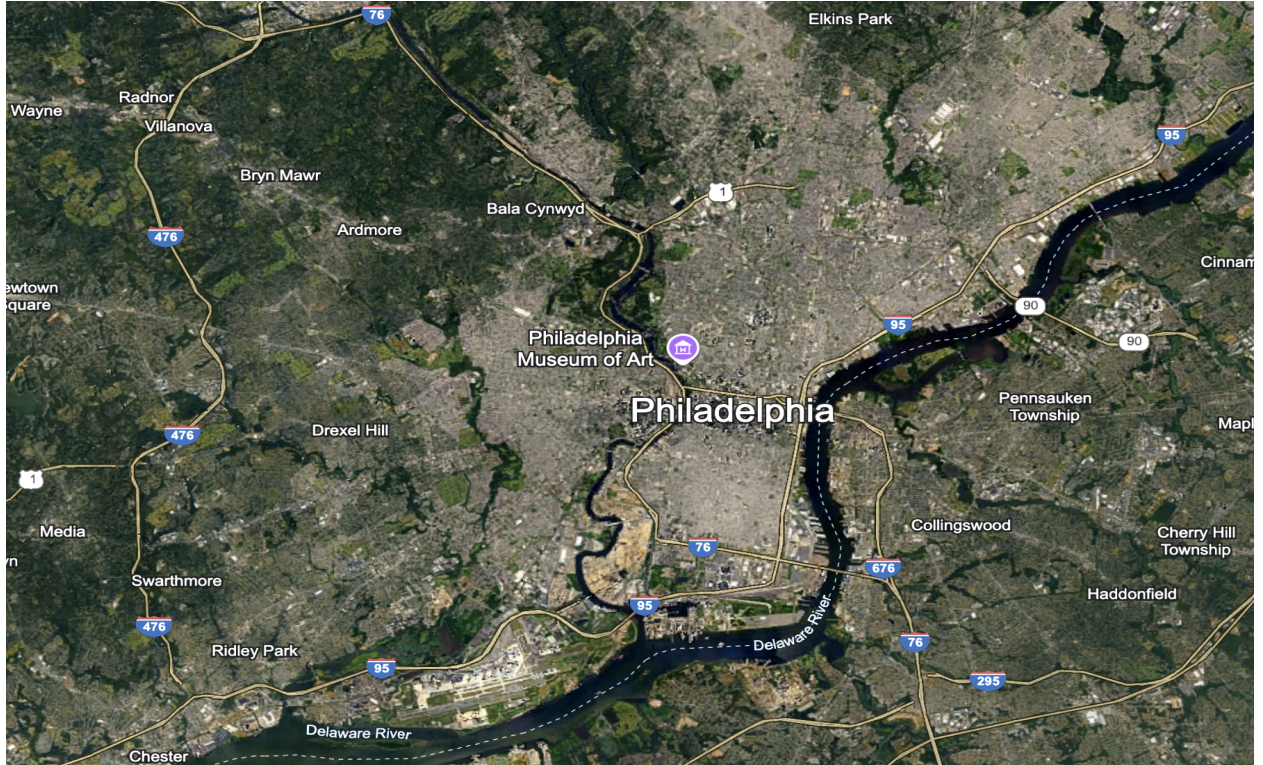
- **Total Impacted Area:** $550 + 72 \approx 622$ square miles to $2200 + 650 \approx 2850$ square miles

Next, based on the calculated impacted area, cities and regions that would be likely be affected are depicted below:

- **Philadelphia:** Approximately 142 square miles
- **Surrounding Suburbs:** Areas within a 5 to 10-mile radius of Philadelphia, including parts of Delaware County, Montgomery County, Bucks County, and Camden, NJ.

Summary of Calculations:

- **Service Radius:**
 - 110 kV: 5 to 10 miles
 - 34 kV: 1 to 3 miles
- **Area per Substation:**
 - 110 kV: 78.54 to 314.16 square miles
 - 34 kV: 3.14 to 28.27 square miles
- **Total Impacted Area:**
 - 110 kV: 550 to 2200 square miles
 - 34 kV: 72 to 650 square miles
 - Combined: 622 to 2850 square miles



Now that an image of the impact radius has been established, the continued coverage of the Ukrainian attack will resume. The event was reported and elaborated on by the Ukrainian news media, who conducted interviews and determined that a foreign attacker remotely controlled the SCADA distribution management system (Lee et al., 2016). Shortly after the attack, Ukrainian government officials claimed the outages were caused by a cyber attack, and that Russian security services were responsible for the incidents (Lee et al., 2016). Following these claims, investigators in Ukraine, as well as private companies and the U.S. government, performed analysis and offered assistance to determine the root cause of the outage (Lee et al., 2016). Both the E-ISAC and SANS ICS team was involved in various efforts and analyses in relation to this case since December 25, 2015, working with trusted members and organizations in the community (Lee et al., 2016). The joint report drawn upon in this case study called “Analysis of the Cyber Attack on the Ukrainian Power Grid,” consolidates the open source information, clarifying important details surrounding the attack, offering lessons learned, and recommending approaches to help the ICS community repel similar attacks.

The next section provides in-depth analysis of the strategy utilized and summarizes key factors leading to the disabled power companies and supporting facilities.

Summary of Incidents

This section examines the incident of the Russian attributed cyber attack on the Ukrainian Power Companies. Included within the examination is the analysis of the attacks utilizing structured approaches to understand the diagrams for electric systems, SCADA Hijacking

Techniques, Technical Components, The Cyber Kill Chain Analysis, and Purdue Model

Mapping. Definitions of the aforementioned analytical points are:

- **Supervisory Control and Data Acquisition (SCADA):** Is a type of industrial control system (ICS) used to monitor and control infrastructure and facility-based processes (CSRC Content Editor, n.d.). I.e. A common SCADA process example is monitoring and controlling a water treatment plant, where the system collects real-time data from sensors, pumps, and valves, allowing operators to adjust parameters like water flow and chemical dosages to ensure water quality and efficiency.
- **SCADA Hijacking or SCADA attack:** Unauthorized access into a SCADA system in order to cause harm (PCMag, n.d.). I.e. In the previous section the U.S. Cyber Defense against Iran's nuclear program through Operation Olympic Games, demonstrated Stuxnet's destructive impact on centrifuges.
- **Technical Components:**
 - **Black Energy Malware :** Modular malware used for initial access and persistence.
 - **KillDisk Component:** Destructive module for data wiping and system disruption.
 - **Exploitation of SCADA Systems:** Targeted control of substations and grid operations.
 - **Phishing and Social Engineering:** Initial intrusion vector via malicious attachments.

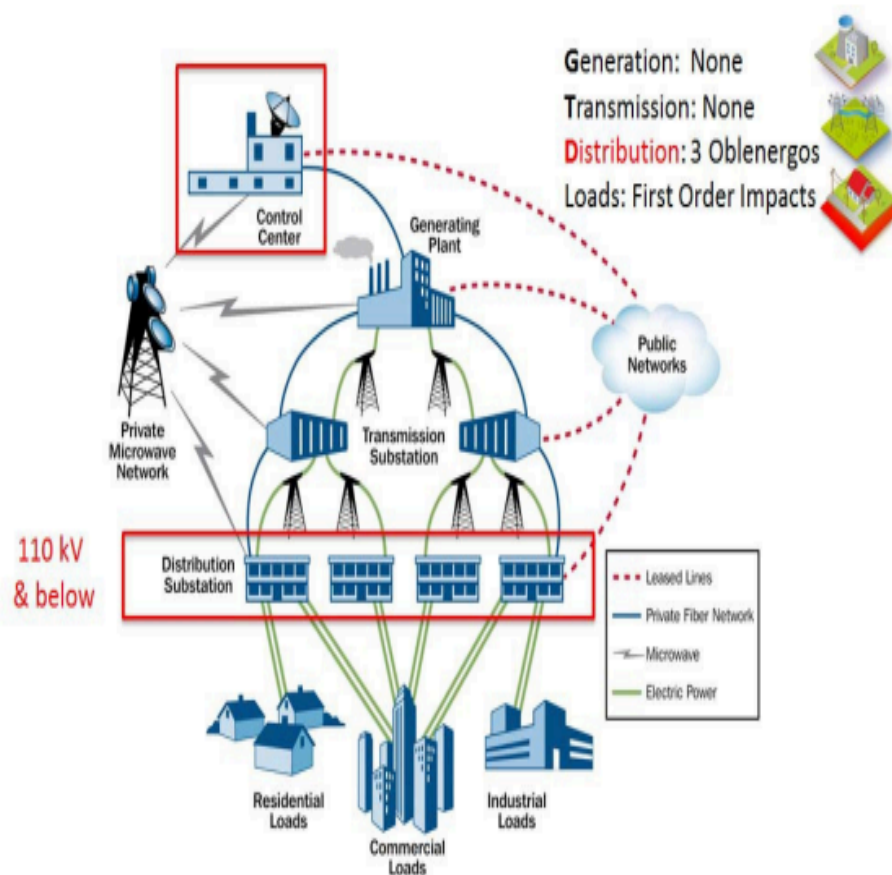
- **Lateral Movement and Privilege Escalation:** WMI, Pass-the-Hash, and weak credentials for spreading within the network.
- **Command and Control (C2) Infrastructure:** Remote servers used to coordinate the attack and exfiltrate data.
- **Destructive Payloads:** Data wiping, scheduled tasks, and manipulation of HMIs.
- **Key Takeaways**
 - The attack demonstrated the convergence of IT and OT vulnerabilities.
 - It highlighted the need for increased cybersecurity measures.
 - The use of destructive malware like KillDisk showed that cyberattacks could have physical, real-time consequences.
- **The Cyber Kill Chain:** Outlines the stages of a cyberattack from its inception to its ultimate goal, typically data exfiltration or system compromise.
 - The Steps of the cybersecurity kill chain process are: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control (C2) & Actions on Objectives (*Cyber Kill Chain: Definition & Examples | DarkTrace, n.d.*).
- **The Purdue Model Mapping:** The Purdue Model, also known as the Purdue Enterprise Reference Architecture (PERA), is a hierarchical framework for organizing industrial control systems (ICS) and their networks, used to segment

and secure OT (Operational Technology) environments from IT (Information Technology) networks (Stouffer et al., 2015).

Now that the analytical points have been defined the examination of the Russian attributed attack on Ukrainian Power Companies will resume. Based on the Department of Homeland Security report, three different distribution energy companies were temporarily disabled due to cyber-attacks from Russian APT28, resulting in several outages impacting an estimated 225,000 people. Included in the impact radius of disabled industrial power facilities were seven 110 kv substations and twenty-three 35 kv substations. The overall downtime was several hours before services were fully restored. A key point to recognize about this specific incident is that this attack was the first publicly acknowledged incident to result in power outages. As future attacks may occur, it is important to scope the impacts of the incident (Lee et al., 2016).

As mentioned earlier and stated within the E-ISAC report, power outages should be measured in scale (number of customers and amount of electricity infrastructure involved) and in duration to full restoration. The Ukrainian incidents affected up to 225,000 customers in three different distribution-level service territories and lasted for several hours. These incidents should be rated on a macro scale as low in terms of power system impacts as the outage affected a very small number of overall power consumers in Ukraine and the duration was limited. In contrast, it is likely that the impacted companies rate these incidents as high or critical to the reliability of their systems and business operations.

The diagram below taken from the E-ISAC analysis report displays an overview of an electric system. This visual aid disseminates the complex infrastructure of an Electric System. Next a review of the attacker techniques and procedures will be analyzed.

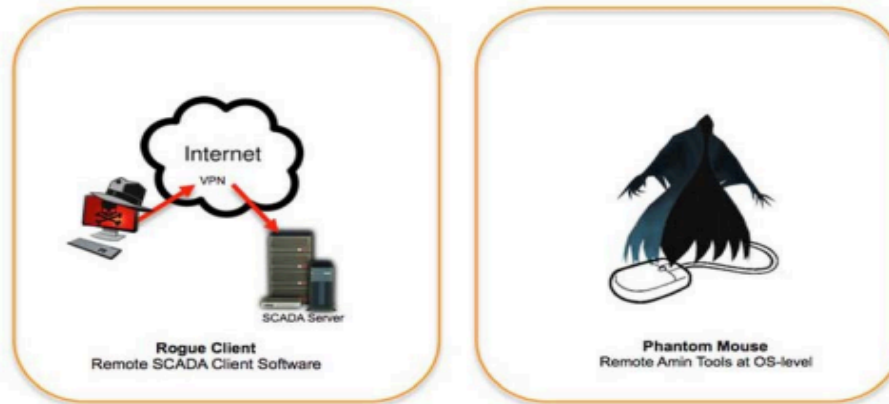


Source: Modification to the DHS Energy Sector-Specific Plan 2010

Figure 1: Electric System Overview

It is noted that attribution of this attack isn't necessary to learn from this attack and to consider mitigation strategies. According to Lee, the motive and sophistication of this power grid attack is consistent with a highly structured and resourced actor. This actor was co-adaptive and demonstrated varying tactics and techniques to match the defenses and environment of the three impacted targets (Lee et al., 2016). Upon analyzing these actors an examination of capabilities provided insight into the technical components utilized to conduct the attack. The attackers demonstrated a variety of capabilities, including spear phishing emails, variants of the Black Energy 3 malware, and the manipulation of Microsoft Office documents that contained the malware to gain a foothold into the Information Technology (IT) networks of the electricity companies (Lee et al., 2016). They demonstrated the capability to gain a foothold and harvest credentials and information to gain access to the ICS network (Lee et al., 2016). Additionally, the attackers showed expertise, not only in network connected infrastructure; such as Uninterruptible Power Supplies (UPSs), but also in operating the ICSs through supervisory control system; such as the Human Machine Interface (HMI), as shown in the figure below (Lee et al., 2016).

SCADA Hijacking Techniques



The attackers develop two SCADA Hijack approaches (one custom and one agnostic) and successfully used them across different types of SCADA/DMS implementations at three companies

Figure 2: Control & Operate: SCADA Hijacking Techniques

Finally, the adversaries demonstrated the capability and willingness to target field devices at substations, write custom malicious firmware, and render the devices, such as serial-to-ethernet converters, inoperable and unrecoverable (Lee et al., 2016). According to Lee, the strongest capability of the attackers was not in their choice of tools or in their expertise, but in their capability to perform long-term reconnaissance operations required to learn the environment and execute a highly synchronized, multistage, multisite attack (Lee et al., 2016). In the figure below a diagram displays the technical components used by the attackers. For examples and definitions of the technical components reference the technical components listed in the previous section.



Figure 3: Ukraine Attack Consolidated Technical Components

Next a review of existing opportunities for the Russian adversary will be analyzed. Multiple opportunities existed for the adversary to execute its attack (Lee et al., 2016). External to the oblenergos and prior to the attack, there was a variety of open-source information available; including a detailed list of types of infrastructure such as Remote Terminal Unit (RTU) vendors and versions posted online by ICS vendors (Lee et al., 2016). The VPNs into the ICS from the business network appear to lack two-factor authentication and the firewall allowed the adversary to remote admin out of the environment by utilizing a remote access capability native to the systems (Lee et al., 2016). Based on the details provided in the DHS report, the adversary used a consistent attack approach on all three impacted targets. The adversary also used consistent tactics to impact field controllable elements and irreparably damage field devices (Lee et al., 2016). Opportunity-based considerations for selecting a specific target may focus on an

attacker's confidence and ability to cause an ICS effect. Some examples provided by E-ISAC's are:

- Targets with common systems and configurations
- Multiple systems with common centralized control points
- ICS impact duration estimates (long term or short term)
- Existing capabilities required to achieve desired results
- Risk level of performing the operation and being discovered
- Achieved access and ability to move and act within the environment

Next a review of the ICS Cyber Kill Chain Mapping to examine the steps the adversary followed to perform the attack. The ICS Cyber Kill Chain was published by SANS in 2015 by Michael Assante and Robert M. Lee as an adaptation of the traditional cyber kill chain developed by Lockheed Martin analysts as it applied to ICS (Lee et al., 2016). The attack on the Ukrainian power grid followed the ICS Cyber Kill Chain completely throughout Stage 1 and Stage 2 (Lee et al., 2016). The attack gained access to each level of the ICS, as shown in the figures below, with the Cyber Kill Chain plotted alongside a segmentation/hierarchy model (Lee et al., 2016).

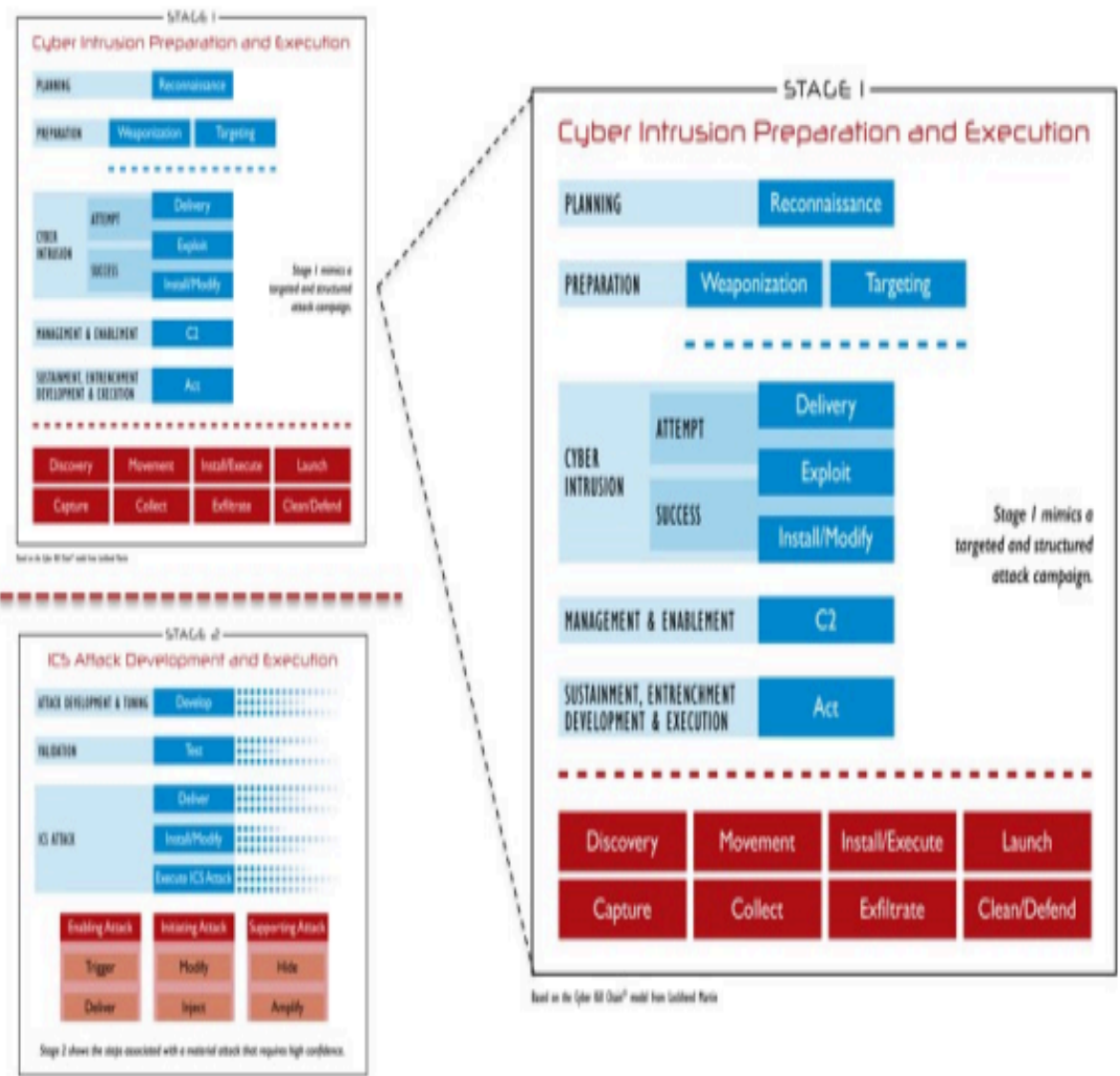


Figure 4: The ICS Cyber Kill Chain with Stage 1 Highlighted

Drawing upon the details from the Cyber Kill Chain Stages from the E-ISACs report will provide insight into the structured approach the adversaries utilized to complete each stage:

Completing Stage 1 entails a successful cyber intrusion or breach into an ICS system, but is not characterized as an ICS attack. Completion of Stage 2 completed the ICS Kill Chain, resulting in a successful cyber attack that led to an impact on the operations of the ICS.

The next discussion includes a brief analysis of each stage of the Cyber Kill Chain along with the Purdue Model Mapping.

ICS Cyber Kill Chain Mapping - Stage 1

- The first step in stage 1 is Reconnaissance
 - There were no reports of observed reconnaissance having taken place prior to targeting the energy companies.
 - An analysis of the three impacted organizations shows they were particularly interesting targets due to the levels of automation in their distribution system; enabling the remote opening of breakers in a number of substations
- The Second step is Weaponization and/or targeting
 - Targeting would normally take place when no weaponization is needed such as directly accessing internet connected devices. In this attack, it does not appear that targeting of specific infrastructure was necessary to gain access.
 - The adversaries weaponized Microsoft Office documents by embedding BlackEnergy 3 within the documents.

- During the cyber intrusion stage of Delivery, Exploit, and Install, the malicious Office documents were delivered, via email to individuals in the administrative or IT network of the electricity companies.

ICS Cyber Kill Chain Mapping Stage 2

In most cases, the Develop stage occurs in the adversary's networks, thereby limiting any available forensic information, but the attack that follows this stage can reveal a lot about the adversarial process. In the Attack Development and Tuning Stage of Stage 2, the attackers executed the Develop step in at least two ways (Lee et al., 2016).

First, they learned how to interact with the three distinct DMS environments using the native control present in the system and operator screens. Second, and more importantly they developed malicious firmware for the serial-to-ethernet devices (Lee et al., 2016). E-ISAC and the SANS ICS team assess with high confidence that, during the Validation Stage of Stage 2 the adversary did Test their capabilities prior to their deployment (Lee et al., 2016). During the ICS Attack Stage, the adversaries used native software to Deliver themselves into the environment for direct interaction with the ICS Components. They achieved this using existing remote administration tools on the operator workstations. The threat actors also continued to use the VPN access into the IT Environment (Lee et al., 2016). In the final preparation for the attack, the adversaries completed the Install/Modify stage by installing malicious software identified as a modified or customized KillDisk across the environment. Finally, to complete the ICS Cyber Kill Chain and to Execute the ICS Attack, the adversaries used the HMIs in the SCADA environment to open the breaks. A short bulleted summary and diagram for the Cyber Kill Chain with the Purdue Model are presented below.

- Supporting attacks
 - Schedule disconnects for UPS System
 - Telephonic floods against at least one oblenenergog's customer support line
- Primary attack
 - SCADA hijack with malicious operation to open breakers
- Amplifying attacks
 - KillDisk wiping of workstations, servers, and an HMI card inside of an RTU
 - Firmware attacks against Serial-to-Ethernet devices at substations

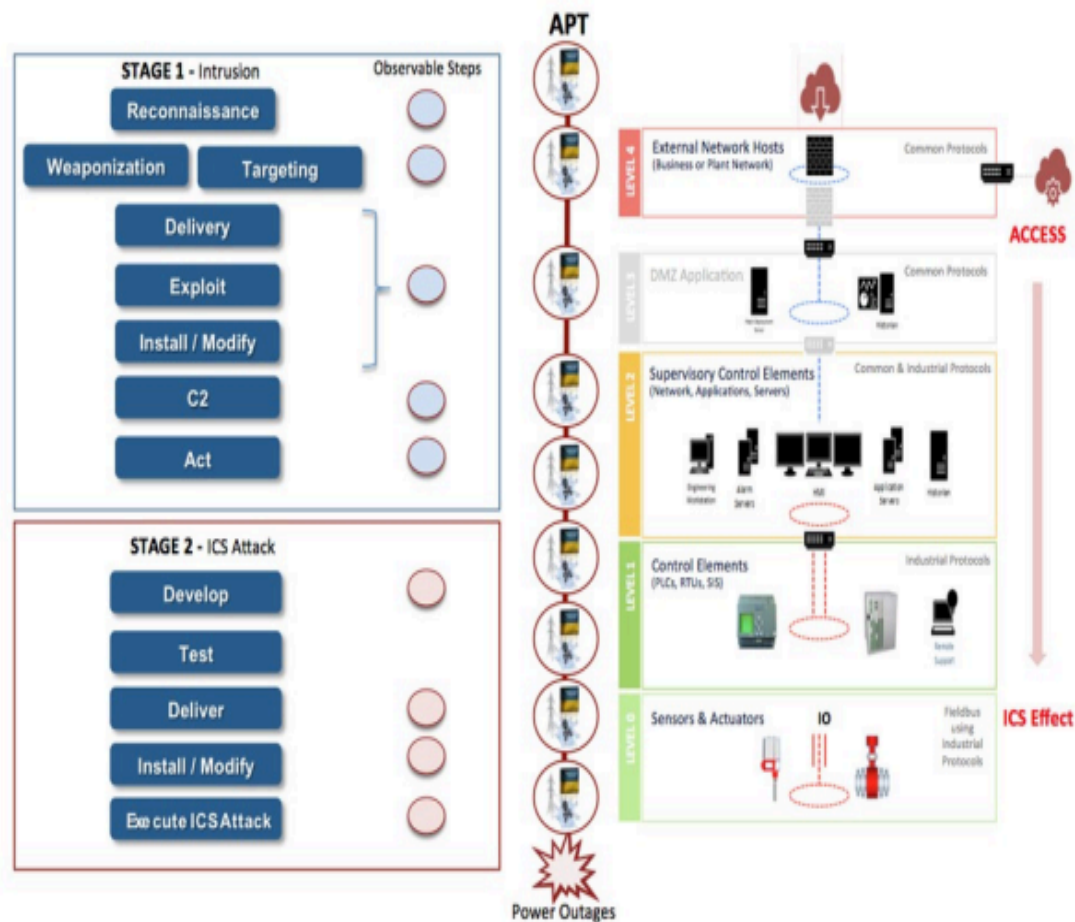


Figure 5: Ukraine Cyber Attack ICS Cyber Kill Chain and Purdue Model Mapping²²

In conclusion, information analyzed presents a clear view of the level of sophistication of the Russian Nation State-Sponsored Cyber Threat Groups. In the next section an analysis of the mitigating ideas as well as the examination of defensive lessons learned, passive and active defenses will be reviewed to demonstrate the knowledge gained for both the Ukraine and US Cyber Defense apparatus.

Mitigation Ideas

In this section an examination of defensive lessons learned, passive and active defenses as well as mitigating suggestions will be analyzed. Lee from the SANS ICS-CERT Team says “We reviewed the mitigation strategies provided through the DHS ICS-CERT Alert and considered how an adversary may alter the next attack based on the mitigation taken by a target; we support many of the mitigation recommendations provided to date. However, it is likely that the adversary will modify attack approaches in follow-on campaigns and these mitigation strategies may not be sufficient.” Below is a figure displaying the mitigations that represent the recommendations for Architecture, Passive Defense, and Active Defense methodologies along the Sliding Scale of Cyber Security.

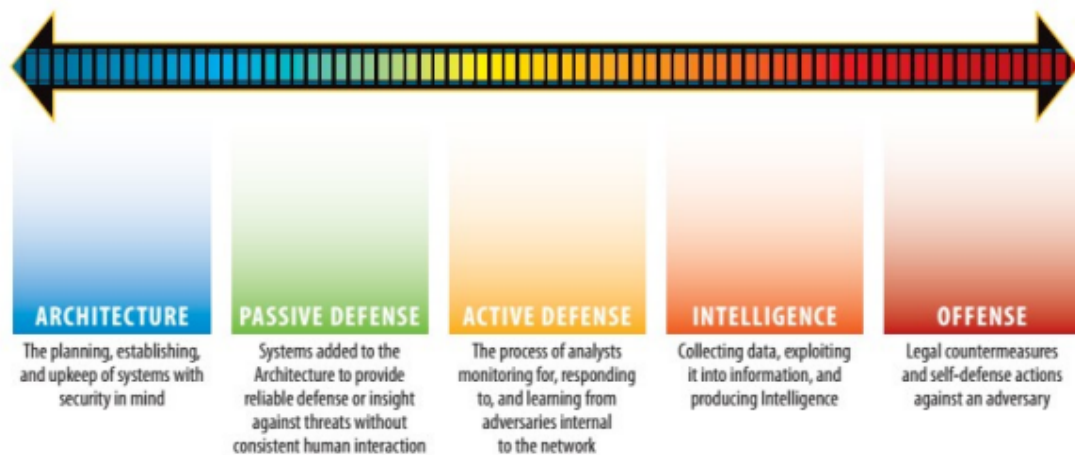


Figure 9: The Sliding Scale of Cyber Security

To expand upon the recommendations from the E-ISAC report, a list with details is provided below:

Architecture

- Properly segment networks from each other
- Ensure logging is enabled on devices that support it, including both It and Operational Technology (OT) assets.
- Ensure that network architecture, such as switches, are managed and have the ability to capture data from the environment to support Passive and Active Defense mechanisms.

Passive Defense

- Application whitelisting can help limit adversary initial infection vectors and should be used when not too invasive to the ICSs.
- DMZs and properly tuned firewalls between network segments will give visibility into the environment and allow defenders the time required to identify intrusions.
- Establish a central logging and data aggregation point to allow forensic evidence to be collected and made available to defenders.

Active Defense

- Train defenders to hunt for odd communications leaving the networked environment such as new IP communications.
- Perform network security monitoring to continuously search through the networked environment for abnormalities.
- Plan and train to incident response plans that incorporate both the IT and OT network personnel.

That summarizes the Russian Cyber Offensive Campaign against the Ukrainian Critical Infrastructure Power Grid. This campaign showcased two Industrial Control/SCADA impacting

malwares as well as a new threat to Energy Sectors across the globe. The U.S. and Ukrainian Cyber Defense apparatus have collaborated to investigate, understand and develop defensive capabilities against the known attack vectors. In the next section an analysis of the U.S. Cyber Defense against the North Korean Cyber Offensive Campaign targeting the financial systems sector.

North Korean Offensive Campaign against the US Financial Systems Sector

This section examines the Democratic People's Republic of Korea's(DPRK)/North Korean cyber offensive campaign against the U.S. and its allies' financial systems sector. In addition it will analyze key components such as a summary of incidents, important learning points, and mitigation suggestions from cyber defense professionals. The research drawn-upon to support the findings for this section come from the Cybersecurity Infrastructure Security Agency (CISA) as well as federal agencies including but not limited to the U.S. Department of Homeland Security, The Department of Justice, The Department of State, and The Department of Treasury. For over a decade of cyber warfare with North Korea the U.S. along with its allies have developed detailed profiles of its adversarial capabilities. These profiles detail cyber threat types, strategies, classification i.e. nation-sponsored, extremist group or hacker group as a way of life.

The Democratic People's Republic of Korea's (DPRK) malicious cyber activities threaten the U.S. and broader international community in particular, pose a significant threat to the integrity and stability of the international financial system. These cyber attacks are attributed to pressure from robust U.S. and UN sanctions, and the DPRK has increasingly relied on illicit

activities including cyber crime to generate revenue for its weapons of mass destruction and ballistic missiles program. The DPRK has the capability to conduct disruptive or destructive cyber activities affecting the U.S. critical infrastructure expanding beyond the Financial Systems Sector.

Those cyber offensive capabilities are but not limited to, to steal from financial institutions, and has demonstrated a pattern of disruptive and harmful cyber activity that is wholly inconsistent with the growing international consensus on what constitutes responsible state behavior in cyberspace. The US Cyber Defense apparatus has developed measures to defend against the Democratic People's Republic of Korea (DPRK) Cyber Threat. North Korea's Cyber defense program is ranked the highest if not in the top tier of cyber offensive capable global superpowers.

The U.S. works closely with like-minded countries to focus attention on and condemn the DPRK's disruptive, destructive, or otherwise destabilizing behavior in cyberspace. For example, in December 2017, Australia, Canada, New Zealand, the U.S., and the United Kingdom publicly attributed the WannaCry 2.0 ransomware attack to the DPRK and denounced the DPRK's harmful and irresponsible cyber activity. The North Korean Cyber offensive program differs from other nation state-advanced persistent threat (APT) groups such as Iranian APT33 (Refined Kitten) who focus their efforts on disrupting supply chains for Oil and Aviation sectors. The North Korean APT 38 (Lazarus Group) focuses on financial sector compromising efforts. It is vital for the international community, network defenders, and the public to stay vigilant and to work together to mitigate the cyber threat posed by North Korea. In the next section a summary of incidents will be examined to gain insight into the DPRK's cyber activities.

Summary of Incidents

In this subsection historical cyber attacks include the heist of a Bangladesh bank, the WannaCry 2.0 Ransomware Campaign and modern day persistent campaigns. Many DPRK cyber actors are subordinate to UN and US designated entities such as the reconnaissance bureau (*Guidance on the North Korean Cyber Threat* | CISA, 2020). DPRK state-sponsored cyber actors primarily consist of hackers, cryptologists, and software developers who conduct espionage, cyber-enabled theft targeting financial institutions and digital exchanges, and politically-motivated operations against foreign media companies (*Guidance on the North Korean Cyber Threat* | CISA, 2020). Cyber Offensive campaigns have the adaptability to pivot once an attack vector is no longer available for exploitation. The U.S. Cyber Defense apparatus draws knowledge from these historical and contemporary incidents alike to establish necessary defensive baselines to protect the nation as well as share information with its partners with the goal of reducing the campaigns effectiveness.

Collectively the DPRK and its state-sponsored threat groups develop and deploy a wide range of malware tools around the world to enable these activities and have grown increasingly sophisticated (*Guidance on the North Korean Cyber Threat* | CISA, 2020). According to the CISA, *Guidance on the North Korean Cyber Threat*, common tactics to raise revenue illicitly by DPRK state-sponsored cyber actors include, but are not limited to:

- **Cyber Enabled Financial Theft:** The UN Security Council 1718 Committee Panel of Experts' 2019 mid-term report (2019 POE mid-term report) states that the DPRK is increasingly able to generate revenue notwithstanding UN Security Council sanctions by

using malicious cyber activities to steal from financial institutions through increasingly sophisticated tactics.

- **Extortion Campaigns:** DPRK cyber actors have also conducted extortion campaigns against third-country entities by compromising an entity's network and threatening to shut it down unless the entity pays a ransom.
- **Cryptojacking:** The 2019 POE mid-term report states that the POE is also investigating the DPRK's use of "cryptojacking," a scheme to compromise a victim machine and steal its computing resources to mine digital currency. The POE has identified several incidents in which computers infected with crypto-jacking malware sent the mined assets - much of it anonymity-enhanced digital currency (sometimes also referred to as "privacy coins") - to servers located in the DPRK, including at KIM II Sung University Pyongyang.

These activities highlight the DPRK's use of cyber-enabled means to generate revenue while mitigating the impact of sanctions and show that any country can be exposed to and exploited by the DPRK. In the next section an analysis of the WannaCry 2.0 Ransomware will provide the necessary learning to prevent repeat attacks with the devastating impact that ransomware inflicted upon its targets.

Important Learning Points

Historically, a key factor to cybercrime was the anonymity of the criminals and the lack of evidence to prove the suspected person of interest carried out the said crime. Awareness,

technical information sharing and models for collaboration are aiding Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT) and Counter-Proliferation Financing.

In Sept. 6 2018 a complaint alleging Park Jin Hyok, a North Korean citizen, for his involvement in a conspiracy to conduct multiple destructive cyber attacks around the world resulting in damage to massive amounts of computer hardware and the extensive loss of data and money (*#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities* | CISA, 2023). The conspiracy's malicious activities include the creation of the malware used in the 2017 WannaCry 2.0 global Ransomware attack. The announcement from the U.S. Justice Department serves in some ways as a pyrrhic victory demonstrating the combined efforts of the DOJ and FBI's unceasing commitment to unmasking and stopping malicious actors and countries behind the world's cyber attacks. Information sharing between the DOJ (Department of Justice), DHS (Department of Homeland Security) and Private Cyber Security are becoming the cyber defensive bulwark against foreign adversaries. However due to the efforts within the Public-Private Partnership national defense is actively being fortified with the goal of reducing the success of said offensive campaigns.

Mitigation Ideas

Through the guidance of the Department of State, The Department of the Treasury, The Department of Homeland Security, and the Department of Justice measures to counter the DPRK (The Democratic People's Republic of Korea) Cyber threat will be covered in this section. Those departments strongly urge governments, industry, civil society, and individuals to take all relevant actions below to protect themselves and counter the DPRK cyber threat (*Guidance on*

the North Korean Cyber Threat | CISA, 2020). Below are suggestions provided by the collaborative groups, agencies, and allied nations:

- Raise Awareness of the DPRK Cyber Threat
- Share Technical Information of the DPRK Cyber Threat
- Implement and Promote Cybersecurity Best Practices
- Notify Law Enforcement
- Strengthen AML/ CFT / CPF Compliance

CISA North Korea State-Sponsored Cyber Threat: Advisories

- July 25, 2024 North Korean Cyber group conducts espionage campaign
- February 9, 2023 Stop Ransomware: Ransomware Attacks on Critical Infrastructure Fund
DPRK Malicious Cyber Activities
- July 6, 2022 Joint FBI-CISA-Treasury CSA: Trader Traitor: North Korea
State-Sponsored APT Targets Blockchain

Overviewing the Democratic People's Republic of Korea's cyber offensive campaign demonstrates the efforts of the U.S. Cyber Defense apparatus to reduce the threat surface and campaign effectiveness. The next section examines and analyzes how the U.S. Cyber Defense has achieved adaptive cybersecurity as well as expanded it through Public-Private Partnerships.

Adaptive Cybersecurity and Public-Private Partnerships

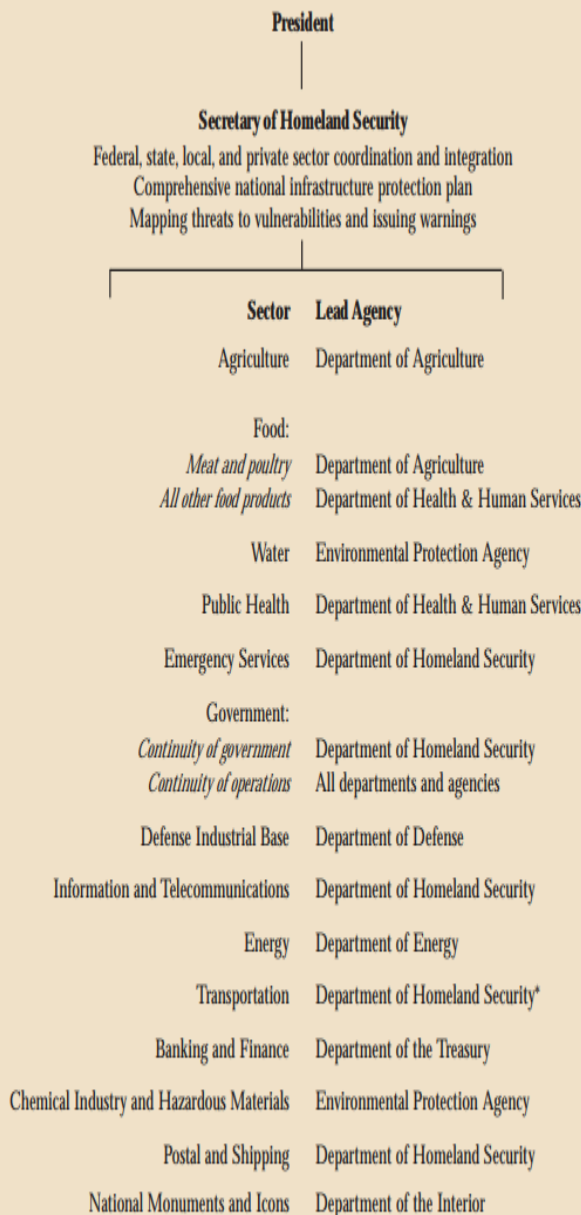
Section 3: The US Adaptive Cyber Security Strategy and Public-Private Partnership Efforts Strengthen National Defense

This section will analyze Critical Infrastructure Security and Resilience (CISR), Legislation, Acts and Presidential Actions, and Federal Plans, Strategies and Guidance. This section draws upon research from the U.S. Department of Homeland Security in partnership with the National Coordination Office for Space-Based Positioning Navigation and Timing, Building a Resilient Ecosystem from the U.S. Department of National Intelligence, the U.S. Department of Homeland Security Plan: Fiscal Years 2023-2027, Memorandum's from Alejandro N. Mayorkas, The National Physical Protection of Critical Infrastructures and Key Assets, Homeland Security and Critical Infrastructure Protection by Baggett and Simpkins. There are 16 sectors of Critical Infrastructure within the U.S. comprising essential services for millions of citizens. Providing protection for those assets has evolved into a national effort.

The U.S. Cyber Defense apparatus has recognized the many challenges of protecting assets identified as critical, aligning risk management at all levels of critical infrastructure, and protecting the nation as a whole-of-nation effort. Recognizing these challenges set the federal agencies, policy makers, and presidents to the task of strategically addressing these issues by creating a comprehensive framework of executive orders, legislation and federal plans. A few of the components of the framework are the National Infrastructure Protection Plan (NIPP) of 2013, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, and Executive Order 13636: Improving Critical Infrastructure Cybersecurity which directs a coordinated

national effort between public and private asset owners. Below is a figure of the U.S. Critical Infrastructure organization as well as protecting federal agencies and the challenge of protection utilizing quantitative data.

FEDERAL GOVERNMENT ORGANIZATION TO PROTECT CRITICAL INFRASTRUCTURE AND KEY ASSETS



* Under the *Homeland Security Act of 2002*, the Transportation Security Administration, responsible for securing our Nation's transportation systems, will become part of the Department of Homeland Security. The new Department will coordinate closely with the Department of Transportation, which will remain responsible for transportation safety.

THE PROTECTION CHALLENGE

Agriculture and Food	1,912,000 farms; 87,000 food-processing plants
Water	1,800 federal reservoirs; 1,600 municipal waste water facilities
Public Health	5,800 registered hospitals
Emergency Services	87,000 U.S. localities
Defense Industrial Base	250,000 firms in 215 distinct industries
Telecommunications	2 billion miles of cable
Energy	
<i>Electricity</i>	2,800 power plants
<i>Oil and Natural Gas</i>	300,000 producing sites
Transportation	
<i>Aviation</i>	5,000 public airports
<i>Passenger Rail and Railroads</i>	120,000 miles of major railroads
<i>Highways, Trucking, and Busing</i>	590,000 highway bridges
<i>Pipelines</i>	2 million miles of pipelines
<i>Maritime</i>	300 inland/coastal ports
<i>Mass Transit</i>	500 major urban public transit operators
Banking and Finance	26,600 FDIC insured institutions
Chemical Industry and Hazardous Materials	66,000 chemical plants
Postal and Shipping	137 million delivery sites
Key Assets	
<i>National Monuments and Icons</i>	5,800 historic buildings
<i>Nuclear Power Plants</i>	104 commercial nuclear power plants
<i>Dams</i>	80,000 dams
<i>Government Facilities</i>	3,000 government owned/operated facilities
<i>Commercial Assets</i>	460 skyscrapers

*These are approximate figures.

The next section analyzes the growth of the U.S. Critical Infrastructure Protection (CIP) to Critical Infrastructure Security and Resilience (CISR).

Critical Infrastructure Security and Resilience (CISR)

This section will provide a comprehensive overview of what Critical Infrastructure Security and Resilience (CISR) is, whom it impacts, and where it is today as it pertains to the U.S. Cyber Defense efforts. The term “infrastructure,” as defined by the Oxford Dictionary, is the “basic physical and organizational structures and facilities (e.g., buildings, roads, and power supplies) needed for the operation of a society or enterprise (Collins & Baggett, 2009).” Prior to the 1990s, understanding of U.S. infrastructure primarily followed this definition, which referred to the U.S. public works system comprising roadways, bridges, water and sewer systems, airports, sea ports, and public buildings (Collins & Baggett, 2009). Following the bombings of the World Trade Center (New York, New York) in 1993 and the Alfred Murrah Federal Building (Oklahoma City, Oklahoma) in 1995, an increased interest in the nation’s infrastructure became evident and discussions went beyond the concern regarding the adequacy of these systems to a focus on how better to protect them (Collins & Baggett, 2009). Therefore, concepts surrounding infrastructure were broadened to include the threat of international and domestic terrorism (Collins & Baggett, 2009).

In many ways these events became the precursor for the adaptive cybersecurity strategy. On July 15, 1996, President William Clinton signed Executive Order (EO) 13010: Critical Infrastructure Protection, which established the President’s Commission on Critical Infrastructure Protection (PCCIP) and expanded the definition of infrastructure to include:

A framework of interdependent networks and systems comprising, identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole (Collins & Baggett, 2009).

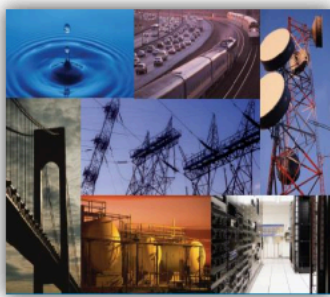
In the time we live today, Critical Infrastructure Security and Resilience (CISR) has become the industry recognized phrase for critical infrastructure protection. Previously, efforts were folded under the critical infrastructure protection (CIP) phrase and primarily focused on physical protection (Collins & Baggett, 2009). In this era of technological innovation and dynamic global volatility, the security and resilience of our critical infrastructure are of paramount importance. Energy grids, water and wastewater systems, transportation networks, healthcare facilities, communication networks, and other essential systems are vital for public safety, economic security, and national security (Collins & Baggett, 2009)

In the next section an overview of what Critical Infrastructure Security and Resilience(CISR) is, will be analyzed to establish a working understanding through the progression of this section.

In the Figure below you will see a snapshot and description of what the U.S. Critical Infrastructure is and how it is organized.

United States Critical Infrastructure

Critical Infrastructure includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both physical and cyber space, and governance constructs that involve multi-level authorities, responsibilities, and regulations.



16 Critical Infrastructure Sectors in the U.S.

- | | | |
|---------------------------|--------------------------------|---|
| • Chemical | • Emergency Services | • Information Technology |
| • Commercial Facilities | • Energy | • Nuclear Reactors, Materials and Waste |
| • Communications | • Financial Services | • Transportation Systems |
| • Critical Manufacturing | • Food & Agriculture | • Water & Wastewater Systems |
| • Dams | • Government Facilities | |
| • Defense Industrial Base | • Healthcare and Public Health | |

Critical Infrastructure Defined: "Assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."

The increasing interconnectivity of critical infrastructure systems and reliance upon global technologies and supply chains make these systems susceptible to a myriad of threats (Collins & Baggett, 2009). Recent threat assessments, including the 2024 Homeland Threat Assessment, identify potentially disruptive cyberattacks, physical sabotage, climate change, and geopolitical tensions among the greatest risks that we face. As those of us responsible for the security and resilience of the U.S. critical infrastructure navigate this increasingly complex risk landscape, we must collectively address emergent risks and an uncertain future while remaining

vigilant against long standing threats like terrorism, cyber espionage, and targeted violence. To demonstrate the adaptive strategies that led to the cybersecurity adaptive strategy an overview of the national infrastructure protection plan (NIPP) will be analyzed. NIPP 2013 defines security and resilience as follows:

Security: Reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or man made disasters.

Resilience: The ability to prepare for and adapt to changing conditions, withstand and recover rapidly from disruptions.

Therefore Critical Infrastructure Security Resilience (CISR) encompasses the key activities of reducing risks, preparing and adapting to-changing risk conditions, and rapidly recovering from all-hazards (Collins & Baggett, 2009). Presidential Policy Directive 21 (PPD-21) provides the following definition of all-hazards:

All-Hazards: Means a threat or an incident, natural or man-made, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. The lexicon shift from Critical Infrastructure Protection(CIP) to Critical Infrastructure Security Resilience(CISR) outlined seven focus areas:

1. Recognition
2. Natural Disaster Recovery
3. Definition Phase
4. Public-Private Cooperation
5. Federalism
6. Resilience

7. Risk-informed Decision Making

This led to the foundation of cybersecurity and critical infrastructure security resilience. Although a singular focus on physical protection was adequate thirty years ago, this approach is no longer sufficient (Collins & Baggett, 2009). Critical Infrastructure is now a system of systems in which practically everything is connected to or linked through cyberspace. According to Collins & Baggett “The cyber physical convergence has not only increased efficiencies and reduced costs but has also altered risks to critical infrastructure in every sector.” The convergence has also impacted dependency and interdependency as connected critical infrastructure is increasingly on multiple information systems that rely on each other for operations, including those operations independent of human direction.

Below is the Risk Management Framework from the Department of Homeland Security (DHS) detailing elements of Critical Infrastructure, the process chain for risk management, and the information sharing flows. In the figure below you will also find benefits to partners, varying risk tolerances, costs and benefits, as well as information sharing being an integrated core component of risk management. Establishing this risk management framework and sharing it as an opt-in mechanism with partners provides a holistic approach to adaptive cybersecurity security (Collins & Baggett, 2009). The magnitude of complexity involved with risk management stems from the diversities within the Critical Infrastructure Security and Resilience participant’s own risk management models. However the risk management framework provided by the department of homeland security provides an avenue to align within a singular risk management framework where information sharing is the core component.

The figure below demonstrates the expansion of Critical Infrastructure Security and Resilience to international partners as they participate in the global supply chain and could represent a significant risk factor. It highlights what Resilience is within the context, summarizes Presidential Policy Directive 21 (PPD-21) which allows State and federal agencies to work with foreign governments within the scope of best practices, lessons learned, and the promotion of CISR.

International Partners in Critical Infrastructure Security and Resilience

- Resilience – stakeholders, interdependencies, and risk environment change over time and conditions. Continually seek to build upon:
 - relationships with foreign infrastructure
 - streamlined supply chains
- PPD-21 provides for State Department, DHS and others:
 - Engage with foreign governments and organizations
 - Exchange best practices and lessons learned
 - Promote security and resilience of critical infrastructure
- Bilateral work with Public Safety Canada
- Multilateral work through:
 - Partnership with Canada, UK, Australia, New Zealand
 - Asia Pacific Economic Cooperation (APEC) economies
 - European Union – US – Canada Experts meeting
 - North Atlantic Treaty Organization (NATO) - Industrial Resources Communication Services Group (IRCSG)

 **Homeland Security**

Presidential Policy Directive 21 | June 17, 2011

The next section examines the legislative acts and presidential orders that established the legal framework to maintain a structured approach to CISR.

Legislation, Acts and Presidential Actions

In this section a timeline of key Presidential Directives, Executive Orders and Acts will be presented to demonstrate the authorization of as well as maintenance and management for critical infrastructure security resilience (CISR). Below is a figure discussing the Presidential Policy Directive 21 and Executive Order 13636, which represent a major building block of the adaptive cyber security strategy.

National Policies

President Barack Obama signed two policies related to critical infrastructure security and resilience in February 2013:

Presidential Policy Directive 21:
Critical Infrastructure Security and
Resilience

Executive Order 13636:
Improving Critical Infrastructure
Cybersecurity

"The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure that are vital to public confidence and the Nation's safety, prosperity, and well-being."

– Presidential Policy
Directive (PPD) 21



**Homeland
Security**

In this section a framework of Presidents as well as their orders provided the legislative framework for CISR today. The information utilized for this section was drawn-upon from Collins & Baggett's "Homeland Security and Critical Infrastructure Protection."

President William J. Clinton

- Presidential Decision Directive 39: Counter Terrorism (June 21, 1995)
 - Fundamentally declared war on terrorists, which is evident in the first phrases of the unclassified version.
 - Subsequent to the first phrases, PPD 39 assigned specific cabinet members the responsibility to protect personnel and facilities under their jurisdiction from terrorism.
- EO 13010: Critical Infrastructure Protection (CIP)(July 15, 1996)
- PDD 62: Combating terrorism (May 22, 1998)
- PDD 63: Critical Infrastructure Protection (May 22, 1998)

President George Bush

- EO 13228: Established the Office of Homeland Security and the Homeland Security Council (October 8, 2001)
- EO 1323: Critical Infrastructure Protection in the Information Age (October 16, 2001)
- USA Patriot Act (October 26, 2001)
- Aviation and Transportation Security Act (November 19, 2001)
- Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (June 12, 2002)
- Homeland Security Act (November 25, 2002)

- Maritime Transportation Security Act (November 25, 2002)
- HSPD 7: Critical Infrastructure Identification, Prioritization, and protection (December 17, 2003)
- Project Bioshield Act of 2004 (July 21, 2004)
- Intelligence Reform and Terrorism Prevention Act (December 17, 2004)
- Post-Katrina Emergency Management Reform Act (October 4, 2006)

President Barack Obama


- PSD 1: Organization of the National Security Council System (February 13, 2009)
- PPD 8: National Preparedness (March 30, 2011)
- EO 13636: Improving Critical Infrastructure Cyber Security (February 12, 2013)
- EO 13650: Improving Chemical Facility Safety and Security (August 1, 2013)
- EO 13691: Promoting Private Sector Cyber Security Information Sharing (February 13, 2015)
- PPD 21: Critical Infrastructure Security and Resilience (February 12, 2013)

This list/framework represents the adaptive nature of the U.S. Critical Infrastructure CyberSecurity Strategy. The next section will examine the Federal Plans, Strategies and Guiding factors that demonstrate the Public-Private Partnership enhancing effect on the cybersecurity adaptive strategy.


Federal Plans, Strategies and Guidance

This section analyzes federal plans, strategies and guidance which further explains the distribution of the U.S. Adaptive Cybersecurity Strategy across the nation including Public-Private Partnership Models. The national effort to strengthen critical infrastructure security and resilience depends on the ability of public and private critical infrastructure security and resilience (CISR) or have related missions. The plans, strategies, and guidance follow asynchronously to the evolution pattern of Critical Infrastructure Security and Resilience (CISR) legislation, acts and presidential actions discussed in the previous sections. Let's expand on the National Infrastructure Protection Plan (NIPP)


National Infrastructure Protection Plan - 2013



NIPP 2013
Partnering for Critical Infrastructure
Security and Resilience

 Homeland
Security

Courtesy of DHS

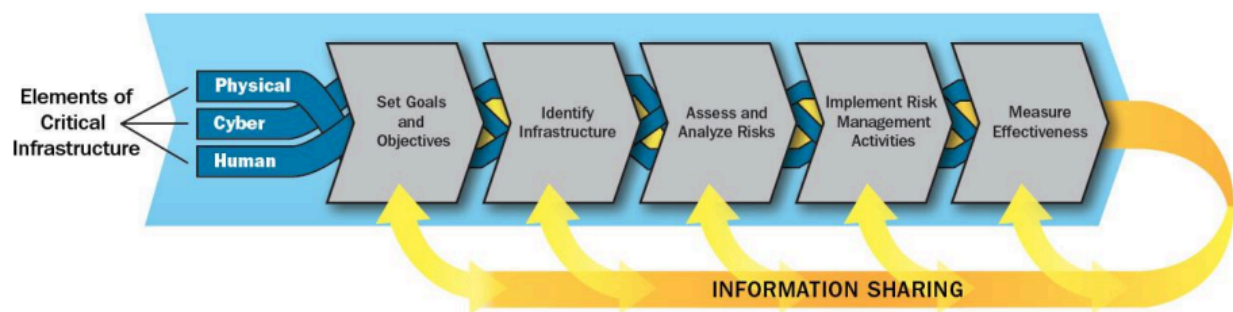
 **Homeland
Security**

- Provides strategic guidance for the national effort to enhance security and resilience through critical infrastructure community collaboration:
 - Applies a risk management focus
 - Promotes collective action through partnerships
 - Outlines authorities, roles and responsibilities
- Guides DHS programs and activities and those of:
 - Federal departments and agencies
 - State, local, tribal, and territorial governments
 - Regional organizations and partnerships
 - Critical infrastructure owners and operators
 - Other critical infrastructure stakeholders (e.g., academia, non-profit organizations)
- Vision: A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.

Presented by: Name | Date: 17-2-2019 | 8

When examining CISR plans, strategies and guidance, the most appropriate document to begin with is the NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. NIPP 2013 is based on the model described in presidential decision directive 63: Critical infrastructure protection (Collins & Baggett, 2009). So, what is NIPP 2013? NIPP 2013 is guidance for the national effort to manage risk to the nation's critical infrastructure (Collins & Baggett, 2009).

Risk Management Framework



Critical Infrastructure Risk Management Framework

- Partners benefit from access to knowledge and capabilities that would otherwise be unavailable to them
- Risk tolerances and priorities will vary
- Costs and benefits considered during decision making
- Information sharing integrated as core component of risk management



**Homeland
Security**

9

According to Collins & Baggett, the objective of this integrated approach is to:

- Identify, defer, detect, disrupt, and prepare for threats and hazards to the national critical infrastructure.

- Reduce vulnerabilities of critical assets, systems, and networks.
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

NIPP 2013 addresses EO 13636 and PPD 8 and is based on the following fundamental components:

- Strong Public-Private Partnerships to foster relationships and facilitate coordination within and across critical infrastructure sectors.
- Robust multi-directional information sharing to enhance the ability to assess risks, make prudent security investments, and take protective action.
- Risk Management framework establishing processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or security risk.

NIPP 2013 supersedes the previous version but recognizes the progress made to date in CISR efforts. Further, NIPP 2013 addresses the changing risk and threat profile of the U.S. Critical Infrastructure as well as the need to integrate the cyber, physical, and human elements of CISR within operational and policy environments. To accomplish this, NIPP 2013 accounts for varying risk management perspectives across public and private Critical Infrastructure but also identifies alignment of interest and additional synergies that can be leveraged to make critical infrastructure more secure and resilient (Collins & Baggett, 2009). There are seven important points that demonstrate the evolution from NIPP 2009 to 2013:

1. Evaluation of security and resilience as the primary aim of critical infrastructure homeland planning efforts.
2. Updates critical infrastructure risk management framework and aligns with national preparedness system.
3. Focus on prioritizing critical infrastructure jointly with public-private sectors.
4. Integration of cyber-physical security and resilience into an enterprise approach to risk management.
5. Actions critical infrastructure security and resilience efforts require international collaboration.
6. Supports execution of the national preparedness goal of both the national and community levels.
7. Organized a planned approach based on each sector's priorities in collaboration with critical infrastructure partners, to make progress toward security and resilience.

Next an overview of the NIPP2013 vision, mission, and goals will be conducted to demystify the path forward. The mission is to focus on the core tenets related to risk management and partnerships. Using the NIPP 2013 RMF encourages all infrastructure partners at all levels and in all sectors to identify critical functions and resources in a nation unity effort, whole of nation approach to support CISR.

The partnership structure is as follows:

- Critical Infrastructure Cross-Sector Council

- Government Coordinating Councils
- Federal Senior Leadership Council
- State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)
- Regional Consortium Coordinating Council (RC3)
- Information Sharing Organization

Many Stakeholders, Many Strengths



Homeland Security

Presenter's Name June 17, 2010

Core Tenets

1. Risk should be identified and managed to evolve effective allocation of security and resilience.
2. Understanding and addressing risks from cross-sector dependencies and interdependencies.
3. Gaining knowledge of infrastructure risk through required information sharing.
4. The partnership approach to Critical Infrastructure Resilience and Security (CISR) recognizes the diverse critical infrastructure community.
5. Regional and SLTT Partnerships address gaps and act to improve CISR.
6. Infrastructure critical to the US transcends borders requiring mutual and cooperative assistance.
7. Security and resilience should be considered during the design of assets, systems, and networks.

Additional Federal Frameworks, Plans, Strategies, and Reports

The national plan for information system protection

- The National Plan for Information System Protection (NPISP) is considered the first major element of the current comprehensive cyber security effort within critical infrastructure security and resilience.
- The NPISP assessed the cyber vulnerabilities of US critical infrastructures.
- This assessment resulted in the NPISP defining three broad cyber security objectives:
 - Prepare and Prevent
 - Detect and Respond

- Build strong foundations

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (February 2003) reaffirms the National Policy on CISR, as a nation we remain committed to protecting our critical infrastructure and key assets from acts of terrorism that would:

- Impair the federal government's ability to perform essential national and homeland security to ensure public health and safety.
- Undermines state and local government capacities to maintain order and to deliver minimum essential public services.
- Damage the private sector's capability to ensure the orderly functioning of the economy and the delivery of essential services.
- Undermine the public morale and confidence in our national economic and political institutions.

National Strategy to Secure Cyberspace (February 2003)

This strategy provides a framework for protecting cyberspace, which is essential to the U.S. economy, security, and way of life as it is considered the nervous system of the country. The overall strategic objective of the strategy included preventing cyber attacks against the U.S.'s critical infrastructure; reducing national vulnerability to cyber attacks; and minimizing damage and recovery time from cyber attacks that do occur. The strategy also defined the government's role in securing cyberspace. Below figures of the most recent strategic objective, goals, and performance management models are displayed to provide the recent focus of the Federal Government.

The current 2025 strategic objectives and goals.

Fig. 2. Homeland Security Missions and Objectives

Strategic Goals	Strategic Objectives
Mission 1: Counter Terrorism and Prevent Threats	1.1 Collect, Analyze, and Share Actionable Intelligence and Information
	1.2 Prevent and Disrupt Terrorist and Nation State Threats
	1.3 Protect Leaders and Designated Individuals, Facilities, and Events
	1.4 Identify and Counter Emerging and Chemical, Biological, Radiological, and Nuclear Threats
Mission 2: Secure and Manage Our Borders	2.1 Secure and Manage Air, Land, and Maritime Borders
	2.2 Expedite Lawful Trade and Travel
	2.3 Counter Transnational Criminal Organizations and Other Illicit Actors
Mission 3: Administer the Nation's Immigration System	3.1 Administer the Immigration System
	3.2 Enforce U.S. Immigration Laws
Mission 4: Secure Cyberspace and Critical Infrastructure	4.1 Support the Cybersecurity of Federal Civilian Networks
	4.2 Strengthen the Security and Resilience of Critical Infrastructure
	4.3 Assess and Counter Evolving Cyber and Emerging Technology Risks
	4.4 Combat Cybercrime
Mission 5: Build a Resilient Nation and Respond to Incidents	5.1 Coordinate Federal Response to Incidents
	5.2 Strengthen National Resilience
	5.3 Support Equitable Community Recovery
	5.4 Enhance Training and Readiness of First Responders
Mission 6: Combat Crimes of Exploitation and Protect Victims	6.1 Enhance Prevention through Public Education and Prevention
	6.2 Identify, Protect and Support Victims
	6.3 Detect, Apprehend, and Disrupt Perpetrators
Enable Mission Success by Strengthening the Enterprise	E.1 Mature Organizational Governance
	E.2 Champion the Workforce
	E.3 Harness Data and Technology to Advance Mission Delivery

The performance management framework of the 2025 federal objectives and goals.

Fig. 3. DHS Performance Management



The explanation of the evolution of critical infrastructure protection (CIP) to critical infrastructure resilience and security (CISR), supportive legislation, federal plans and partnerships provides the necessary transparency into how the U.S. Cyber Defense apparatus is building defense against foreign adversaries.

Discussion

In congress today, justification for securing the internet is a highly important conversation to the U.S. Cyber Defense apparatus. Historically the creators and innovators of the internet wanted a no hands approach as it pertains to governments attempting to regulate the internet. One of the many reasons justifications are being made is that the government can no longer remain idle as the internet continues to threaten national security as it pertains to industrial architectures. Referencing the first two major points of this paper, US Cyber Defense through offensive strategy and Adversaries as well as defensive strategies against them, demonstrate what the public-private partnership, international partnerships and military cyber command has been able to achieve. In the overview of the adaptive cyber security strategy and public-private partnerships section, demonstrated how the U.S. and its ecosystems of industry, policies, international and domestic relations have converged to combat a dangerous threat to national security.

Aging Critical infrastructure has been put under the scope due to the advent of technological advancements in artificial intelligence, quantum compute, and the unforeseen threats hidden within the minutiae of capability to protect against personal privacy. In this section the topics of securing the internet to ensure cyber defense over aging critical infrastructure to ensure the U.S. Cyber Defense capabilities, emerging threats of Artificial Intelligence for both Cyber Defense as well as Cyber Offense, and how these critically important points are changing societal dimensions of the U.S,

How does congress intend on securing the Internet to Ensure U.S. Cyber Defense over aging critical infrastructure?

In an effort to bolster the U.S. Cyber defense against foreign adversaries and the internet must be secured. To secure the internet and protect U.S. aging critical infrastructure, Congress primarily aims to incentivize private sector cybersecurity improvements through legislation, foster collaboration between government and industry, invest in cybersecurity workforce development, and enact regulations to standardize security practices across critical infrastructure sectors, often working through agencies like CISA (Cybersecurity and Infrastructure Security Agency) (*Committee Advances “Cyber PIVOTT Act,” Adopts 119th Congress Oversight Plan – Committee on Homeland Security, 2025*).

Emerging Trends and Threats in Artificial Intelligence Cyber Offense and Defense

Cyber attackers are increasingly using artificial intelligence (AI) to create adaptive, scalable threats such as advanced malware and automated phishing attempts (*Emerging Threats to Critical Infrastructure: AI Driven Cybersecurity Trends for 2025 | Capitol Technology University, n.d.*). With an estimated 40% of all cyberattacks now being AIO-driven, AI is helping cyber criminals develop more believable spam and infiltrative malware (*Emerging Threats to Critical Infrastructure: AI Driven Cybersecurity Trends for 2025 | Capitol Technology University, n.d.*).

Impacts of Innovation and Policy on Societal Dimensions

A vital component to the success of holistic solidarity between the people and public-private initiatives, is trust. There are many controversies surrounding privacy and trust when it comes to national security being taken past the perimeters publicly communicated. Government policies aimed at securing the internet and developing AI offense/defense capabilities can significantly impact social dimensions like privacy and trust, often creating a complex balancing act between security needs and individual security purposes can erode public trust and privacy concerns, while inadequate security measures can lead to vulnerabilities that threaten personal information and safety.(Van Rijmenam Csp, 2024)

Key impacts on privacy and trust:

- Increased surveillance
- Algorithmic bias
- Lack of transparency
- Erosion of anonymity

The next section summarizes the recommendations and suggestions provided in the previous sections for maintaining as well as expanding the U.S. Cyber Defense Apparatus.

Recommendations and Suggestions

Industrial Control System and aging infrastructure based malware engineering is a growing threat. Below are suggestions and recommendations drawn upon from industry experts explaining how the U.S. can establish a defense against these steadily evolving threats. Additionally a review of foreign adversaries defensive measures will be analyzed and suggestions drawn upon from industry experts. Lastly, a correlation between legislation, federal strategies, and public private partnerships suggest what needs are being prioritized to safeguard the future. Starting with Operation Olympic Games and Stuxnet, key points as well as suggestions will be drawn upon to provide a canvas of what can be done in the time we live in today. These suggestions provide transparency into the directions of efforts being made and that could be made to safeguard the U.S. critical infrastructure as well as its citizens.

Operation Olympic Games & Stuxnet

According to Ralph Langner a suggested resolution to industrial malware defense would be most effective through a complete overhaul of the industrial technology and infrastructure. Below is a reference to Ralph Langner's professional suggestion.

Such a goal that is realistically achievable for those willing to accept the challenge presented by Stuxnet to start over and find and implement new and creative defensive solutions that render cyber weapons pretty much useless. Such solutions conflict with the objectives of cyber warriors not only abroad but also at home. It therefore has to be automatically welcomed by our own offensive cyber forces. This

conflict of interest can presently not be resolved technologically but only politically. It has often been stated that cyber offense has an advantage over cyber defense. While it can be debated that is true in technical terms in the domain of industrial control system security, it certainly does apply in a political context.

Foreign Adversary Cyber Threat Mitigation

Russian Cyber Attack Remediation Recommendations:

Architecture

- Properly segment networks from each other
- Ensure logging is enabled on devices that support it, including both It and Operational Technology (OT) assets.
- Ensure that network architecture, such as switches, are managed and have the ability to capture data from the environment to support Passive and Active Defense mechanisms.

Passive Defense

- Application whitelisting can help limit adversary initial infection vectors and should be used when not too invasive to the ICSs.
- DMZs and properly tuned firewalls between network segments will give visibility into the environment and allow defenders the time required to identify intrusions.
- Establish a central logging and data aggregation point to allow forensic evidence to be collected and made available to defenders.

Active Defense

- Train defenders to hunt for odd communications leaving the networked environment such as new IP communications.
- Perform network security monitoring to continuously search through the networked environment for abnormalities.
- Plan and train to incident response plans that incorporate both the IT and OT network personnel.

North Korea/DPRK Cyber Attack Remediation Recommendations

Below are suggestions provided by the collaborative groups, agencies, and allied nations:

- Raise Awareness of the DPRK Cyber Threat
- Share Technical Information of the DPRK Cyber Threat
- Implement and Promote Cybersecurity Best Practices
- Notify Law Enforcement
- Strengthen AML/ CFT / CPF Compliance

CISA North Korea State-Sponsored Cyber Threat: Advisories

- July 25, 2024 North Korean Cyber group conducts espionage campaign
- February 9, 2023 Stop Ransomware: Ransomware Attacks on Critical Infrastructure Fund
DPRK Malicious Cyber Activities
- July 6, 2022 Joint FBI-CISA-Treasury CSA: Trader Traitor: North Korea
State-Sponsored APT Targets Blockchain

In this section an overview of recommendations and suggestions were covered. This demonstrates the capability of the U.S. Cyber Defense capabilities. The next section wraps and concludes this paper.

Conclusion

Since the advent of Operation Olympic Games and Stuxnet the world of cyberspace has evolved in many ways both good as well as bad. The U.S. Cyber Defense Apparatus surely has a significant challenge when it comes to defending national critical infrastructure. However, as demonstrated through the research and supporting evidence the United States has appropriately identified and risen to the challenge of protecting its assets from foreign adversaries. The solution isn't a single trajectory but multiple dimensions of persistence. The apparent and realistic efforts of the Critical Infrastructure Community, Public-Private Partnerships, and Allied Nations create the necessary defensive bulwark to prevent massively destructive cyber attacks.

However, that doesn't mean adversaries aren't successfully attacking critical infrastructure and critical global supply chains. The growth and demand for capable cyber defenders as well as technology such as AI is paramount to the U.S. Cyber Defense. Below suggested themes from Ralph Langner will be overviewed for defenders to provide important takeaways that could help bolster cyber defense. Theme 1: In a prolonged attack campaign, there are likely numerous opportunities to detect and defend the targeted system. The two-stage ICS cyber kill chain helps note that in an ICS environment, there is an increased window for the detection and identification of the most concerning attack types. Theme 2: There is likely a significant amount of unobservable adversarial testing performed prior to introducing the attack

into the environment. Many capabilities were demonstrated throughout this paper, and provide specific lessons learned for defenders to take action on. Theme 3: Information sharing is key in the identification of a coordinated attack and directing appropriate response actions. In the US and other countries with established information sharing mechanisms, such as ISACs (Information Sharing and Analysis Centers), the focus should be on maintaining and improving the information provided by asset owners and operators. This increased data sharing will enhance situation awareness within the sector, which will in turn lead to earlier attack detection and facilitate incident response. That concludes this paper and from the findings of the research prove that the U.S. has proven its capability to defend itself against massively damaging cyber attacks but still faces challenges protecting critical infrastructure sectors due to the diversity as well as the complexity of the critical infrastructure industry as a whole.

References

1. Kamiński, M. (2020). Operation “Olympic Games.” Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran’s nuclear programme. *Security and Defence Quarterly*, 29(2), 63–71.
<https://doi.org/10.35467/sdq/121974>
2. CYBERSECURITY: NEXT STEPS TO PROTECT OUR CRITICAL INFRASTRUCTURE. (n.d.).
<https://www.govinfo.gov/content/pkg/CHRG-111shrg57888/html/CHRG-111shrg57888.htm>
3. Cybersecurity Act of 2010, S. 773, 111th Cong. (2010). Congress.gov. Retrieved from <https://www.congress.gov/bill/111th-congress/senate-bill/773>
4. Andress, Jason, and Steve Winterfeld. The Basics of Cyber Warfare : Understanding the Fundamentals of Cyber Warfare in Theory and Practice, Elsevier Science & Technology Books, 2012. ProQuest Ebook Central,
<https://ebookcentral.proquest.com/lib/apus/detail.action?docID=1073026>.
5. Lee, R. M. (2025, February 12). The Industrial Control System Cyber Kill Chain | SANS Institute. <https://www.sans.org/white-papers/36297/>
6. Livingstone, D. (2024, January 16). Cyber security at civil nuclear facilities: Understanding the risks. Chatham House – International Affairs Think Tank.
<https://www.chathamhouse.org/archive/cyber-security-civil-nuclear-facilities-understanding-risks>

7. Langner, R., The Langner Group, & Schneier, B. (2013). To kill a centrifuge. The Langner Group.
<https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>
8. Lee, R. M. & Dragos, Inc. (2018). THE INDUSTRIAL CYBER THREAT LANDSCAPE. In COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE.
<https://www.energy.senate.gov/services/files/5F40E0A2-B836-40EA-ACC6-9BF3B43A1B8F>
9. Collins, P. A., & Baggett, R. K. (2009). Homeland Security and Critical Infrastructure Protection. Praeger Security International.
10. U.S. Department of Homeland Security, National Coordination Office for Space-Based Positioning, Navigation and Timing, International Committee on Global Navigation Satellite Systems, & Dragseth, J. (2014). *Critical infrastructure security and resilience*. <https://www.gps.gov/multimedia/presentations/2014/11/ICG/dhs.pdf>
11. *Fact sheet: Executive Order on Cybersecurity / Presidential Policy Directive on Critical Infrastructure Security and Resilience | Homeland Security*. (2013, February 13). U.S. Department of Homeland Security.
<https://www.dhs.gov/archive/news/2013/02/13/fact-sheet-executive-order-cybersecurity-presidential-policy-directive-critical>
12. The White House. (2003). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.
https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

13. U.S. Department of Homeland Security, & Mayorkas, A. N. (2024). *Strategic Guidance and National Priorities for U.S. Critical Infrastructure security and resilience (2024-2025)*.
https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-critical-infrastructure-security-resilience.pdf
14. https://www.dhs.gov/sites/default/files/2024-11/24_1119_plec_dhs-strategic-plan-fy23-27.pdf
15. Department of National Intelligence (DNI). PROTECTING CRITICAL SUPPLY CHAINS. In *Unknown*.
<https://www.dni.gov/files/NCSC/documents/supplychain/Building-a-Resilient-Ecosystem.pdf>
16. *North Korea State-Sponsored Cyber Threat: Advisories* | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA.
<https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/north-korea/publications>
17. *North Korean Regime-Backed Programmer Charged With Conspiracy to*. (2025, February 6).
<https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>
18. *North Korea Cyber Threat Overview and Advisories* | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA.

- <https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea>
19. *Emerging Threats to Critical Infrastructure: AI Driven Cybersecurity Trends for 2025*
| Capitol Technology University. (n.d.). Capitol Technology University.
<https://www.captechu.edu/blog/ai-driven-cybersecurity-trends-2025>
20. *Committee advances “Cyber PIVOTT Act,” Adopts 119th Congress Oversight Plan – Committee on Homeland Security.* (2025, February 26).
<https://homeland.house.gov/2025/02/26/committee-advances-cyber-pivott-act-adopts-119th-congress-oversight-plan/>
21. *Revolutionizing Public Services: The role of AI in Government Efficiency* | LinkedIn.
(2024, July 24). <https://www.linkedin.com/pulse/ai-government-strivemindz-de9nc/>
22. Van Rijmenam Csp, M. (2024, September 25). *Privacy in the age of AI: Risks, challenges and solutions.* Dr Mark Van Rijmenam, CSP | Strategic Futurist Speaker.
<https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/>