Spring 5-5-2016

U.S. Critical Infrastructure Cybersecurity: An Analysis of Threats, Methods, and Policy-Past, Present, and Future

Justan Phillip Dustan
University of South Carolina - Columbia

U.S. Critical Infrastructure Cybersecurity: An Analysis of Threats, Methods, and Policy–Past, Present, and Future

By

Jacob P. Dustan

Submitted in Partial Fulfillment
of the Requirements for
Graduation with Honors from the
South Carolina Honors College

May, 2016

Approved:

Mr. Daniel Ostergaard
Director of Thesis

Dr. Juliana Iarossi
Second Reader

Steve Lynn, Dean
For South Carolina Honors College

Table of Contents

Thesis Summary

This thesis was conceived to provide an overview of the state of critical infrastructure cybersecurity in the United States to better understand where we were, where we are, and where we are going in the face of international terrorism and hostile, rogue nations. The paper consists of three primary sections: why we are facing critical infrastructure cyber threats, what we have done and need to do in the future to protect against attacks, and appendices with explanations of various forms of malicious actors and threats within the field. It is written with the nontechnical reader in mind, offering explanations of technical terms in the appendices. This thesis also addresses major events, related policy, evolving practices, and theory for future improvement within the field.

Findings

Through extensive research it became apparent that the U.S. lags behind other nations in terms of cybersecurity policy and defensive practices. We suffer crippling attacks due to both the sheer volume of assaults on all forms of businesses and government networks and the lack of resilience within critical infrastructure networks. As the Internet of Things evolved legacy systems were brought online without putting proper safeguards in place, leaving sensitive equipment and facilities vulnerable to cyberattacks. As a result, our critical infrastructure systems are outdated and dangerously exposed. Antiquated, bloated policy compounds the problem by limiting the scope of active cyber defense.

Conclusions

Research contributed to the development of The Red Queen Theory, which borrows directly from its biological cousin, The Red Queen Hypothesis. Both effectively state that the only way to stay abreast of competition is to run as fast as possible–and to surpass them one must redouble their efforts further. This paper sets forth the assertion that in order to regain former cyber supremacy both the federal government and private sector must invest in active cyber defense, artificial intelligence programs, and training; improve resiliency through redundant network architecture and backups; drastically reform aging cybersecurity policies; and accept that the rules of engagement in cyberspace are effectively nonexistent.

For the Bristlecone Snag

A home transformed by the lightning
the balanced alcoves smother
this insatiable earth of a planet, Earth.
They attacked it with mechanical horns
because they love you, love, in fire and wind.
You say, what is the time waiting for in its spring?
I tell you it is waiting for your branch that flows,
because you are a sweet-smelling diamond architecture
that does not know why it grows.

(Scholl, 2011)

Introduction

June 23rd, 2008 was unique in many ways, but the most notable was also the most unknown. At 4:40 am the offices of Iranian engineering firm Foolad Technic stood empty, the soft whirring of servers in the background providing a gentle lullaby for sleeping desktop computers and dark monitors. LEDs blinked softly while hard drives spun in smooth circles within their metal casings. The network was quiet, save for a small trickle of data that did not belong. Unknown to Foolad, this trickle would eventually flow into every company computer, downloading packages and modules that would later cross from digital to physical, doing what no other computer program had before. It would jump across open air, embed itself in a hostile nation's nuclear enrichment centrifuge control system, and slowly but steadily dismantle their dreams of nuclear proliferation. This silent saboteur was later named Stuxnet and determined to be the world's first advanced cyber weapon. (Zetter, An Unprecedented Look at Stuxnet, the World's First Digital Weapon, 2014)

Our world has changed drastically since the first sighting of weaponized malware in the wild. We have grown accustomed to hearing of digital heists costing companies hundreds of millions of dollars, watched as foreign governments attacked public corporations in retaliation for their exercising the right to free speech, and are pretty safe in assuming our medical records are floating around on the dark web somewhere. Without a doubt, our world is more wired–and vulnerable–than ever before. (Wasik, 2013) Barbie dolls learn a child's name and respond to questions using artificial intelligence, personal digital assistants like Siri and Cortana now track your most visited locations along with traffic and weather patterns to better suggest accurate departure times, and hyperlocal sensors can notify you within minutes of an impending sudden downpour. Such modern conveniences and marvels are seemingly innocuous and helpful,

however the possibility of their perversion is both disturbing and potentially life-threatening. (Lohr, 2015)

These seemingly small digital advances are indicative of a trend over the past ten years as more industrial and government sectors have come online. As we connect heavy industry, transportation, energy production, public health and safety, and many other major–oft unseen–parts of our daily lives we encounter a paradox. With enhanced intelligence and efficiency comes an Achilles heel–the previously unforeseen capability of adversaries to dismantle or destroy the very fiber of our national infrastructure with a few swift keystrokes.

The Internet of Things (IoT), as this increasing connectivity has been deemed, extends beyond Wi-Fi-enabled thermostats and smartphone-controlled coffee makers. It has increasingly permeated the foundation of the developed world's industrial sectors, creating networks of billions of sensors and equipment that can can be monitored and controlled from anywhere in the world. These industries are also often considered part of a nation's critical infrastructure–sectors, both public and private, that are deemed so crucial to the functioning of that nation that their debilitation would be considered disastrous for both national wellbeing and security (Bumiller & Shanker, 2012). Herein lies the challenge, for these sectors are considered vital yet are increasingly vulnerable to cyberattack and often owned by the private sector (Lewis, 2015). Therefore, we as a nation must ask ourselves who is actually responsible for protecting these installations, both in the physical and digital realms. Do we mandate companies invest in security using their own funds? Does the government bear responsibility for providing this security–and if so, how much? And finally, how do we ensure national security in a realm that, "has been identified as the fifth domain of warfare [by the U.S. Department of Defense]," (Flowers &

Zeadally, 2014) where the rules of combat are still being written and anyone with a high-speed internet connection can become an insurgent?

These questions don't have simple, and frankly we as a nation are still trying to determine the best course of action. The digital realm is quickly evolving, and policy simply cannot keep up. We are currently lagging behind, but government and private sectors are now coming together in a conceited effort to modernize and fortify our critical infrastructure before it is too late. (Chayes, 2015) However, the challenge we face lies with resilience and deterrence rather than simply defense, a difficult strategic shift that may prove difficult given current industry norms, outdated government policy, and increasingly voracious and sophisticated attacks.

Setting the Stage for a Firestorm

Every period of human development has had its own particular type of human conflict---its own variety of problem that, apparently, could be settled only by force. And each time, frustratingly enough, force never really settled the problem. Instead, it persisted through a series of conflicts, then vanished of itself---what's the expression---ah, yes, 'not with a bang, but a whimper,' as the economic and social environment changed. And then, new problems, and a new series of wars.

–Isaac Asimov, I, Robot (Asimov, 1950)

Worlds Collide

Proposed by Thomas Freedman in his book The World is Flat, The Triple Convergence consisted of three major waves that effectively "flattened" the world through increased access to the web and related digital platforms. These inundations of technology and connectivity enabled billions who were formerly locked out of the developing world to gain access to information and tools once reserved solely for the most technologically advanced nations (Friedman, 2005).

The first convergence was based on the development of new, collaborative digital platforms that span the globe and connect using advanced networking technology. According to Friedman, "This platform enables individuals, groups, companies, and universities anywhere in the world to collaborate-for the purposes of innovation, production, education, research, entertainment, and, alas, war-making-like no creative platform ever before" (Friedman, 2005). It is, in itself, transcendent of the physical world, never sleeps, disregards geography, and breaks down barriers among cultures and peoples. However, as Friedman notes early in his postulation, humankind has a nasty habit of perverting tools for gain in unscrupulous ways, and as a result we

must now view the platform cautiously, for with these great gains now comes grave danger. As he notes, "I don't mean we are all becoming equal. What I do mean is that more people in more places now have the power to access the flat world platform-to connect, compete, collaborate, and, unfortunately, destroy-than ever before." (Friedman, 2005) We must view this first great convergence as a significant leap forward for mankind but not without certain perils.

The second convergence was based on horizontalization–the connecting of business around the world via advanced computing processes. Globalization 2.0 and 3.0, the former fostered primarily by mainframe computing and the latter by personal computing and the microprocessor, "flipped the playing field from largely top-down to more side to side" (Friedman, 2005). By readjusting the business landscape, this second convergence saw the rise of unified global businesses capable of responding internationally in real-time, "naturally foster[ing] and demand[ing] new business practices, which were less about command and control and more about connecting and collaborating horizontally" (Friedman, 2005). Without the constraints of geopolitical boundaries and physical distance, these new, more agile and collaborative companies could blossom. This framework for rapid growth and development suddenly became the norm, ushering in a new era of expedited globalization.

The third and final convergence was effectively an explosion of connectivity in the developing world. With the rise of unified business processes in the West, the fall of the Soviet Union, the (relative) opening of China, and widespread internet connectivity came drastic increases in the world's population of daily internet users. By opening up the platform to the East, "three billion people who had been locked out of the field suddenly found themselves liberated to plug and play with everybody else" (Friedman, 2005). Practically overnight, the global marketplace flooded with inexpensive talent from developing nations, people around the

world were able to collaborate and communicate over high-speed fiber optic lines in real-time, and the amount of global malware and internet crime skyrocketed (IBM, 2011).

Friedman published the The World is Flat in 2005, just prior to the massive expansion in mobile internet use brought about by decreasing component prices and expanding global cellular connectivity. He suggested but could not have totally foreseen the astounding growth in data creation and use around the world, the wild popularity and expansion of social media, or the proliferation of the Internet of Things. Cellular technology has effectively increased access to the point that almost anyone, in some cases for less than a dollar a month (IBM, 2011), can connect to others using a mobile handset. The rise of these platforms has been astounding, however their ubiquity is also their weakness, for universal access means both good and bad sit on a level playing field. We are witnessing the development of a nascent digital Wild West, and while we may think of the technology as rapidly maturing, it has a long way to go before we truly understand the ramifications of universal global connectivity.

The Rise of Industrial Intelligence

Although Moore's Law–that computing power will roughly double every two years–is nearing its end (Waldrop, 2016), since the 1970s we have witnessed a near-exponential trend towards increasing computing power and the evolution of formerly "dumb" (analog/disconnected) devices into "smart" (digital/internet-enabled) appliances with the IoT. Arrays of sensors form supermassive networks that generate massive volumes of operating logs by the millisecond, offering treasure troves of easily-accessible data to better understand and optimize processes from robotic BMW X-series manufacturing to life-saving ICU respirators and international air traffic control systems (Wasik, 2013). Big Data, as this overwhelming amount of

continually generated information is called, has become the norm in the modern business world, illustrating an ever increasing level of interconnectedness and, unfortunately, vulnerability.

IoT networks are truly astounding in that they go beyond WiFi-enabled thermostats and are capable of analyzing millions of data points almost instantaneously, giving rise to real-time interpretation and pattern recognition of supermassive quantaties of detailed information that would normally be incomprehensible to the human brain. These networks therefore, "become tools for understanding complexity and responding to it swiftly… and some of them even work largely without human intervention" (Chui, Löffler, & Roberts, 2010). By autonomously watching, interpreting, and learning, these systems can simplify processes for human operators or save lives, dependent on the application, and have become crucial to understanding complexity in the modern world.

These systems, "are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet," (Chui, Löffler, & Roberts, 2010) and are therefore inherently operating in the emerging digital Wild West. Some are modern and were properly designed for web connectivity, however many more are antiquated and have been belatedly updated as networking became a necessity. These legacy systems were generally designed to float in a vacuum behind what security experts call an air gap–a space between two systems that contains no digital connections and requires an operator to physically carry data on removable media (such as a USB thumb drive) from one network to the other. This security measure was semi-intentional because, while it was beneficial for the system's integrity, there generally wasn't a need to connect this early digital equipment to the web prior to Moore's Law taking effect and drastically driving down computing costs. (Wasik, 2013)

Supervisory Control And Data Acquisition (SCADA) systems–the connected industrial control terminals responsible for daily operations of power plants, water treatment facilities, etc.–were never intended to connect to the nascent web. Most believed they were completely protected because, according to prevailing logic, you can't hack what you can't see. Since the 1990s however, all types of industrial management systems have been brought online in droves and are now subsequently vulnerable due to outdated technology and a lack of proper digital safeguards. They are now visible on the network, potentially propping open a door leading straight into the heart of a critical infrastructure facility. (The Economist, 2010)

Critical Infrastructure Vulnerability

Animals don't behave like men,' he said. 'If they have to fight, they fight; and if they have to kill they kill. But they don't sit down and set their wits to work to devise ways of spoiling other creatures' lives and hurting them. They have dignity and animality.

–Strawberry, Watership Down (Adams, 1972)

The Internet of Things' Proliferation

The IoT proses tremendous challenges for critical infrastructure cybersecurity because formerly disconnected systems are now coming online in droves and dependent on this newfound connectivity for both efficient and safe operation. Its pervasiveness is both a boon to industrial productivity and potentially crippling should the network be compromised, a powerful double-edged sword that can cut in either direction depending on the wielder's intent. However, while government and private critical infrastructure operators are just beginning to take threats associated with the IoT seriously, as discussed in a New York Times interview with members of General Electric's management, "'today's reality', observed Paul Rogers, chief executive of Wurldtech and G.E.'s general manager for industrial cybersecurity, 'is that much of the world's heavy industry is already online and it is vulnerable'" (Lohr, 2015).

These ubiquitous systems–connected sensors, computer-controlled motors, SCADA terminals, telecommunications equipment, etc.–are vulnerable to the attacks explained in Appendix D, posing a serious threat to critical infrastructure integrity. We must remember that those little internet-enabled devices are actually fully-fledged computers, each susceptible to the

same types of malware that so easily infect our laptops, desktops, servers, and mobile devices. And while new industrial monitoring networks promise incredible gains,

> The optimism is tempered by an increasing recognition of the security risk inherent in combining online and physical resources and cultures in industry. Unless the security challenges can be managed, experts agree, the march toward the industrial Internet will be slowed and the payoff will be much smaller. (Lohr, 2015)

Companies like G.E. are taking the initiative to protect their connected equipment by acquiring industrial cybersecurity startups, such as Wurldtech, because they anticipate tremendous demand for their services as attacks targeting IoT networks rise. Again, according to the New York Times, "Wurldtech's corporate parent alone represents a huge market. G.E. says it monitors the data flowing from 10 million sensors on $1 trillion worth of equipment every day." (Lohr, 2015) Their automated industrial management systems, such as RailConnect360, rely heavily on cloud computing and countless distributed sensors throughout a facility to manage thousands of moving parts, monitor efficiency and productivity, and limit errors (General Electric, 2016). They are the epitome of the industrial IoT, however their complexity may also serve as a future pitfall should integrated security not catch up with product development.

Various incidents have already occurred involving critical infrastructure IoT compromises on smaller scales and significant vulnerabilities recently discovered. One of the earliest incidents involved the 2008 case of a Polish teen who hacked into the tram system in his hometown of Lodz and caused four derailments, injuring a dozen people (Squatriglia, 2008). According to the local police, "He treated it like any other schoolboy might a giant train set… He clearly did not think about the consequences of his actions" (Leyden, 2008). The boy apparently studied the local rail system for several months and then built a transmitter from a television

remote to control the trams as they moved about the city, writing the best junctions for controlling the vehicles down in a notebook at school (Leyden, 2008).

Eight years later a similar issue resurfaced in a much more widespread manner. In 2016 Spanish security researcher Jose Carlos Norte published a blog post discussing his discovery that many government vehicle tracking systems, called telematics gateway units (TGUs), were unprotected against hijacking (Norte, 2016). These devices monitor basic functions of the vehicle through the CAN bus, a system that connects vital parts of the automobile together so that they can work in tandem (Corrigan, 2008). One model, the C4Max, sold by the French firm Mobile Devices, shipped without password protection, leaving the vehicle and operators completely exposed to interference from the internet. By accessing one vehicle's TGU he was able to scan for all vehicles using that specific transmitter on the network, potentially enabling someone with more malicious intent to bring an entire fleet of government vehicles to a literal standstill (Greenberg, 2016).

Norte's work was likely inspired by that of Charlie Miller and Chris Valasek, who famously hacked into a Jeep Cherokee in 2015 using the vehicle's cellular internet connection to cut the engine power, breaks, and electric power steering. Their discovery was a much-needed reminder that anything connected to the internet is susceptible to attack, bringing into question the safety of self-driving cars and connected automotive amenities, such as OnStar and mobile hotspots (Drozhzhin, 2015). Much like the critical infrastructure sector, automotive manufacturers are beginning to understand the dangers associated with these technologies and the challenges posed by protecting passengers from both physical and digital threats on the road.

Increasing Attack Volume & Sophistication

Per the U.S. Government Accounting Office, cyberattacks on critical infrastructure and federal systems increased 782% between 2006 and 2012 (Flowers & Zeadally, 2014). Similarly, according to Dell Security, "the number of attacks against industrial control systems more than doubled to 675,186 in January 2014 from 163,228 in January 2013," (Perlroth, 2015) and although these figures are now outdated, they indicate the beginning of a dangerous trend–that our critical infrastructure is now under ever increasing siege by digital adversaries. In an interview with the New York Times, Michael V. Hayden, former head of the National Security Agency, had the following to say about the current state of cyber threats facing U.S. critical infrastructure, "Despite all the talks of a cyber-Pearl Harbor, I am not really worried about a state competitor like China doing catastrophic damage to infrastructure… It's the attack from renegade, lower-tier nation-states that have nothing to lose" (Perlroth, 2015). These smaller, loose-cannon states, such as North Korea and Iran, have already launched sophisticated assaults against U.S. companies and foreign governments, and it is relatively safe to assume that key systems have already been infiltrated by dormant malware–much like enemy sleeper cells–that could be activated quickly to cause damage during wartime. (Schutgens & van Beek, 2015)

However, unlike traditional attacks on critical infrastructure–such as missile strikes or arson–cyberattacks are difficult to discover until after the fact and nearly impossible to trace, leaving defenders scrambling to contain the damage and investigators in the dark. Furthermore, Mr. Hayden additionally commented that, "not only do we not have the mitigation, we don't even have any type of adequate forensics to know this is happening, and whether it was intentional or unintentional," (Perlroth, 2015) implying we are woefully underprepared for these sorts of advanced, targeted assaults against key hubs of our critical infrastructure networks.

Indifference Is Not an Option

Mr. Hayden ended the interview with the New York Times by answering their final question as follows, "Will there be a cyber-Pearl Harbor? Most likely… Will we know it's cyber? Most likely not" (Perlroth, 2015). Admittedly chilling, the thought of a rogue nation-state bringing down or corrupting critical nodes in our national infrastructure likely provokes thoughts of widespread blackouts, poisoned drinking water supplies, and Netflix outages. The following three incidents serve as harbingers of what is likely to come, and although some contest the validity of the Soviet pipeline logic bomb, Thomas Reed, former Air Force Secretary, details the incident in his recently published memoirs.

In June, 1982 a massive fireball in Siberia triggered U.S. early warning systems above the USSR designed to detect nuclear weapons tests and launches. The blast was caused by a critical system malfunction in a major gas pipeline after its software unexpectedly sent operating pressures skyrocketing and jammed key valves, "produc[ing] pressures far beyond those acceptable to pipeline joints and welds" (The Economist, 2010). Although the issue appeared on the surface to be simply a malfunction, it was in reality a crude cyber weapon called a logic bomb. The code within the system effectively triggered a digital meltdown to cause, "the most monumental non-nuclear explosion and fire ever seen from space," (The Economist, 2010)– fireworks courtesy of the U.S. Central Intelligence Agency. They had placed the crude cyber munition in a Canadian pipeline computer developer's source code because they knew the USSR was planning to pilfer the product for use in a new facility. Subsequently, the logic bomb was unknowingly but graciously accepted and embedded in the pipeline, later causing catastrophic real-world damage and ushering in the new age of cyberwarfare.

Although not nearly as violent–yet potentially more disruptive to a national economy–in 2011 a chilling hacking operation infiltrated the NASDAQ's computer system, illustrating the need for increased cybersecurity within the financial sector. The attackers injected NASDAQ's servers with malware that was very similar to samples the NSA identified as being developed by the Federal Security Service of the Russian Federation, their government's main spy agency. (Riley, 2014) Federal investigators and the company tread gingerly for months, hoping that the malware would lie dormant. Luckily, it had not penetrated select critical systems responsible for transferring large sums of money among client companies, however its placement in the network would have allowed its activation to cripple many key servers and terminals, bringing the company and potentially the U.S. financial system to their knees–at least temporarily. According to Businessweek, "It was more than spyware: Although the tool could be used to steal data, it also had a function designed to create widespread disruption within a computer network. The NSA believed it might be capable of wiping out the entire exchange" (Riley, 2014). Thankfully, the Russian government was "just" stealing data about network architecture and banking system design to update their own exchange, however for several months the U.S. financial service industry's collective breath caught in its chest.

While the NASDAQ hack brought the threat of significant cybercrime and need for bolstered cybersecurity home for many, according to Bloomberg Businessweek,

> For some U.S. officials, however, the lessons of the incident are far more chilling. The U.S. national security apparatus may be dominant in the physical world, but it's far less prepared in the virtual one. The rules of cyberwarfare are still being written, and it may be that the deployment of attack code is an act of war as destructive as the disabling of any real infrastructure. And it's an act of war that can be hard to trace: Almost four years

> after the initial Nasdaq intrusion, U.S. officials are still sorting out what happened. Although American military is an excellent deterrent, it doesn't work if you don't know whom to use it on. (Riley, 2014)

We as a nation must take heed of the warning signs ahead on the digital horizon, for cybersecurity is both a question of national security and business continuity, and it is only going to get far, far worse rapidly. House Intelligence Committee Chairman Mike Rodgers commented in the same article,

> If anybody in the federal government tells you that they've got this figured out in terms of how to respond to an aggressive cyberattack, then tell me their names, because they shouldn't be there… The problem is that whatever we do, the response to it won't come back at the government, it'll come back at the 85 percent of networks in America that are in the private sector. And they are already having a difficult time keeping up. (Riley, 2014)

In other words, it is time to pay attention. We as a nation are falling behind in the cyber arms race due to slow government action and disconnects with the private sector, leaving critical infrastructure susceptible to dangerous digital compromises.

Several years after the NASDAQ hack, another jarring and far more physically impactful attack occurred on the Ukrainian power grid in 2015. Unknown attackers logged in remotely to poorly protected SCADA terminals at three power distribution centers, completely locking operators out of their management consoles and leaving them to watch helplessly as the network went dark. More than 230,000 residents were left without power, including the centers themselves. Subsequently, operators had to manually override the system and roll back to antiquated analog technology, but at least they were able to restore power quickly. The same

could not be said for most modern critical infrastructure management systems in developed nations today. A total loss of power and disabling of production facilities' emergency backup systems would cause extended blackouts and very likely permanent damage. (Zetter, Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, 2016)

Cybersecurity: Past, Present, Future

Over the last 33 years, U.S. cyber policy and operations have evolved drastically. From original military mainframes to vital communications satellites and the PRISM surveillance program, we have always worked to maintain technological superiority but are steadily falling behind. Until recently, cybersecurity was mostly an afterthought, leaving crucial networks vulnerable, protected only by luck. The cyber domain was formerly left to clandestine departments such as DARPA, SPAWAR, and the NSA (Flowers & Zeadally, 2014). However, in the past decade we as a nation have begun to incorporate it into every facet of government out of dire necessity. The following sections follow these developments by examining policy, motivations, and defense methodology.

Past (1983 to 2013)

A strange game. The only winning move is not to play. How about a nice game of chess?

–Joshua (NORAD Supercomputer), "WarGames" (Lasker & Parkes, 1983)

Your Turn, Joshua

Hollywood was the first to illustrate the danger of cyber vulnerabilities to the general public and federal government. They foretold of attacks against U.S. critical infrastructure in the 1983 movie "Wargames", which involved a teenage boy hacking into a top-secret nuclear command system in the Pentagon and playing what he perceived to be a game with the WPOR (War Operations Plan Response) supercomputer–which in reality nearly started World War III

using NORAD's (North American Aerospace Defense Command) nuclear missile arsenal (Kaplan, 2016). President Ronald Reagan saw the movie upon its release and walked into a Joint Chiefs of Staff meeting the following morning to ask the question, "Could something like this really happen? Could someone break into our most sensitive computers?" (Kaplan, 2016). General John W. Vessey Jr., then chairman of the Joint Chiefs, "said he would look into it" (Kaplan, 2016). One week later, his response was, "Mr. President, the problem is much worse than you think" (Kaplan, 2016). And thus began the U.S. government's policy of cyber defense.

Unfortunately, President Reagan was not the only one inspired by the movie. Shortly after its premier a group of teen hackers, nicknamed the 414s, attempted to and succeeded in hacking into the Los Alamos Nuclear Laboratory, Sloan-Kettering, and Security Pacific Bank (CNN, 2016). The boys were eventually caught by the FBI, however their exploits and later presentations to Congress encouraged further development of government cybersecurity programs and related policy.

Y2K's Jolt to the System

The Y2K (Year 2000) bug was a computer glitch caused by a commonly used piece of shorthand in computer code, which TIME Magazine explained as the following in their special 1999 issue on the potential disaster:

> The bug at the center of the Year 2000 mess is fairly simple. In what's proving to be a ludicrously shortsighted shortcut, many system programmers set aside only two digits to denote the year in dates, as in 06/15/98 rather than 06/15/1998. Trouble is, when the computer's clock strikes 2000, the math can get screwy. Date-based equations like 98 –

> 97 = 1 become 00 – 97 = -97. That can prompt some computers to do the wrong thing and stop others from doing anything at all. (Rothman, 2014)

Although no major destruction or chaos ensued as a result of the dawning of the new millennium, we don't really know if the silent outcome was due to the estimated $100 Billion (approximately $143 Billion in today's dollars) spent on software patches, system updates, and new hardware in the U.S. alone–or if the systems were actually fine in the first place (Ackerman, 2014). That said, the incident brought about a heightened national consciousness regarding the dangers associated with technological failures, prompting increased interest and investment in cybersecurity. During this time we began to see the emergence of unified network-level security systems and the Security Information and Event Management (SIEM) market (Ackerman, 2014), which attempts to approach network security holistically by monitoring multiple data sources from one centralized vantage point (Rouse, 2014).

> Prior to the early 2000s, malware infections were relatively simple, easy to detect, and more preventable than today's complex Trojans and Zero-Day exploits (Schutgens & van Beek, 2015). Cybersecurity was primarily concerned with building (fire)walls to keep intruders out of sensitive areas of networks, which usually sufficed. However, since then the emergence of a myriad of exploit varieties coupled with social engineering and physical crime has forced security to take on a more comprehensive, multidisciplinary role within organizations. (F-Secure, 2015)

Legislative Highlights

The "WarGames" revelation and 414s' destructive shenanigans jolted Washington into the digital age, at least for a brief time. These two incidents eventually resulted in the signing of NSDD-145, a National Security Decision Directive detailing "National Policy on Telecommunications and Automated Information System Security" and acknowledging both that government networks were susceptible to attack and that more investment was needed to protect these vital systems against unseen foes. The directive outlined steps the federal government needed to take to protect sensitive networks, mandated improved collaboration among departments, and established a national committee–The National Telecommunications and Information Systems Security Committee (NTISSC)–to oversee nascent cyber defense implementation (The White House, 1984).

Policy regarding critical infrastructure protection was updated under President Bill Clinton with Executive Order 13010, which established the President's Commission on Critical Infrastructure Protection. This mandate focused primarily on physical security but laid groundwork for today's Department of Homeland Security and critical infrastructure cyber protection policy. It aimed to establish cooperation and coordination among various federal departments and agencies to protect systems, "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States" (Clinton, 1996). Just as we realized the dangers of crucial hubs in national networks going down due to traditional physical threats then, we are beginning to realize those same consequences associated with cyberattacks today.

Shortly after the attacks of 9/11, President George W. Bush signed into effect the Homeland Security Act of 2002, which established the U.S. Department of Homeland Security

(DHS) as a standalone agency and brought various disparate agencies under one umbrella organization. The new department was then primarily tasked with protecting against terrorist attacks and miscellaneous manmade and natural crises, specifically focusing on critical infrastructure protection (Bush, 2003). According to Ted G. Lewis, author of Critical Infrastructure Protection in Homeland Security, there was no clear-cut path forward, no obvious track to follow–it was all new at the time (Lewis, 2015). We as a nation had always protected our military installations and select vital industries, but it was not until the late 90s and early 2000s that we began thinking about protecting the actual infrastructure supporting the day-to-day operations of our nation as a whole. Compounding the endeavor's complexity was the reality that 85% of this vital framework was owned by the private sector, posing its own set of challenges and headaches. (U.S. Government Department of Homeland Security, 2016) We were, effectively, figuring it out as we went along. (Lewis, 2015)

Almost immediately after the formation of DHS, President Bush signed into effect Homeland Security Presidential Directive 7 in December 2003, "which establishe[d] a national policy for Federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks" (Bush, 2003). This document specifically mentions cybersecurity as it pertains to critical infrastructure and mandates the maintenance of a committee to oversee homeland security in cyberspace. By encouraging collaboration and information sharing among various federal, state, and local departments and agencies, the directive established a precedent to holistically protect critical infrastructure on all fronts–including the new digital battlefield (Bush, 2003).

Early Safeguards

Prior to the mid 2000s, government efforts focused on curtailing hacking activity through prosecution and passive cyber defense. Critical infrastructure systems were not always connected to the internet, providing a relatively strong defense mechanism against miscellaneous forms of digital threats. For, as the New York Times highlights,

> For years, the conventional wisdom was that the industrial control technology, while electronic, was separate from the outside world. The communications software was specialized and proprietary, designed for closed, industrial networks. They were assumed to be isolated, so-called air gap systems. (Lohr, 2015)

However, as Stuxnet illustrated in 2009, air gap systems are no longer an effective means of protecting these systems, drastically changing the digital playing field (Zetter, An Unprecedented Look at Stuxnet, the World's First Digital Weapon, 2014). It is as if the enemy suddenly developed the trebuchet and is now able to lob explosives over the moat and walls that once defended the castle so effectively. Advanced malware is now able to transcend the digital and move through the physical world in ways never seen before.

Prior efforts focused almost exclusively on passive cyber defense, or simply building more intelligent digital walls around systems and fending off attacks as they occur. Unfortunately, while these methods are the easiest to implement and often intuitive, they are inadequate to deter attacks and do little to mitigate or prevent damage once an infiltrator gains access to a network (Bryant, 2015). These defenses therefore fail relatively quickly when faced with an Advanced Persistent Threat and are extremely susceptible to zero-day attacks. We will discuss modern alternatives further in following sections.

Present (2013 to 2016)

So I said to the customer: "Have you tried turning it off then turning it back on again?"

I never sold another HAL9000 again.

–Dr. Andrei Smyslov, 2001: A Space Odyssey (Clarke, 1968)

Recent Legislative Developments

In February of 2013 President Barack Obama signed into effect Presidential Policy Directive 21, (Obama, PPD-21, 2013) refocusing efforts to defend critical infrastructure on increasing overall network security and resiliency (U.S. Government Accountability Office, 2014). This shift illustrated a deeper understanding of homeland security and network theory, embracing the idea that withstanding an attack intact is more important than defending against one and being crippled should safeguards fail. A second piece of legislation from the same month, Executive Order 13636, outlined the following to encourage communication between the public and private sectors on matters of digital security:

1. the National Institute of Standards and Technology shall lead the development of a cybersecurity framework that will provide technology-neutral guidance;
2. the policy of the federal government is to increase the volume, timeliness, and quality of cyber threat information sharing with the U.S. private sector;
3. agencies with responsibility to regulate the security of critical infrastructure shall consider prioritized actions to promote cyber security; and

4. DHS shall identify critical infrastructure where a cybersecurity incident could have a catastrophic effect on public health or safety, economic security, or national security. (Obama, EO 13636, 2013)

Additionally, in December of 2013, the National Infrastructure Protection Plan (NIPP 2013) was updated to,

> Reaffirm the role of various coordinating structures (such as sector coordinating councils and government coordinating councils) and integrate cyber and physical security and resilience efforts into an enterprise approach for risk management, among other things. (U.S. Government Accountability Office, 2014)

Therefore, with these policy directives we began to see a sea change in the way critical infrastructure security was viewed as a whole, transitioning from a concrete, physical, defensive, government-driven stance to one of greater understanding, resiliency, holistic consideration, and public-private sector cooperation.

With major cyberattacks in the headlines, lawmakers began to better understand the severity of digital threats to connected critical infrastructure and their potential impact on the American people–finally acting to bolster cyber defense spending, cross-departmental efforts, research and development, and training. The U.S. government began to realize terrorism, warfare, and crime had transcended the physical and moved into what the Department of Defense declared, “the fifth domain of warfare” (U.S. Government Accountability Office, 2014).

Modern Defenses

As discussed earlier, air gaps and passive cyber defense were formerly the primary means of defending critical infrastructure control systems from digital attacks. However, with the spread of IoT networks and connected equipment, air gaps are rarely an option because new sensors and appliances inherently require internet connectivity to function properly, if at all. Our networks have moved beyond departmental siloes cut off from the outside world and are more integrated and cloud-dependent than ever. Subsequently, higher walls won't keep the enemy out, and neither will digging a wider moat. We have to devise and implement new means of protecting these systems against increasingly sophisticated international adversaries.

At this point we must come to terms with the fact that merely passively defending is not enough, for modern adversaries must be repelled and struck back to prevent continued assault. Much like swatting a mosquito, simply bushing off the aggressor is not sufficient to prevent further harassment–so we must therefore stop the attack at its source. According to the article U.S. Policy on Active Cyber Defense, "Practical cyber defense approaches range from stopping an attack to punishing attackers so that they do not want to attack again, which an assortment of strategies in between" (Flowers & Zeadally, 2014). This method of deterring attackers through retaliatory punishment is called active cyber defense and is defined in context of Department of Defense networks as:

> [The] synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerability... It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and

> mitigate malicious activity on DoD networks. (U.S. Department of Homeland Security, 2011)

However, in order to do so we must contend with preexisting legislation, which strictly limits retaliatory measures available to companies and government agencies.

Subsequent Complications

Policy enacted in the late 1980s focused primarily on curbing and prosecuting hacking activity under the Computer Fraud and Abuse Act (CFAA) of 1986, limiting modern defenders' abilities to digitally track and retaliate against attacking Advanced Persistent Threats (APTs). This legislation effectively makes hacking of any form illegal, generally including retaliatory force (Doyle, 2014). Later amended and expanded under the 2002 USA PARTIOT and 2008 Identity Theft Enforcement and Restitution Acts, it now dictates extremely vague cases under which the Judicial Department may prosecute hackers–or simply digital trespassers–of any sort with exceedingly harsh penalties, creating a legal grey zone in which we must tread carefully (Hathaway, et al., 2012).

Presidential Policy Directive 20 (PPD-20) was a confidential document leaked during the Snowden Revelations which outlined the role active cyber defense was to take in federal policy. Commentary on the article in Der Gruyter suggests,

> The definition of active cyber defense that can therefore be inferred from PPD-20 is a subset of DCEO [Defensive Cyber Effects Operation] including: operations and related programs or activities conducted by or on behalf of the U.S. Government, that manipulate, disrupt, deny, degrade, or destroy computers, information or communication systems, networks, physical or virtual infrastructures controlled by computers or

> information systems, or information resident thereon for the purpose of defending or protecting U.S. national interests against immediate threats or ongoing attacks or malicious cyber activity occurring inside or outside cyberspace. (Flowers & Zeadally, 2014)

The top secret document indicates the U.S. government authorizes retaliation against attacking computer systems regardless of their location or sovereignty. It does, however, mandate that these operations are conducted in a way minimizing collateral damage and abiding by international combat law. (Flowers & Zeadally, 2014)

One of the major challenges associated with cyberspace is the lack of national boundaries, enforceable rules of combat/treaties, and internationally recognized regulatory committees (Chayes, 2015). Criminals and adversaries are able to transverse space and time anonymously and with complete disregard for geopolitical boundaries, making active cyber defense problematic. International law dictates that retaliation in self-defense is an acceptable use of force, however it becomes tricky when attacking an enemy's system technically violates another nation's sovereignty (Flowers & Zeadally, 2014). To add another layer of complexity, attackers routinely relay network traffic around the world through thousands of nodes, making it virtually impossible to identify the originating system with absolute certainty and requiring defenders to cross countless borders to find the perpetrator. Subsequently, to deter an attacker a government entity may need to relay malicious network activity across uninvolved nations' telecommunications networks and noncombatant systems, creating a legal quagmire (Hathaway, et al., 2012).

Future (2016 Onward)

We need not to be let alone. We need to be really bothered once in a while. How long is it since you were really bothered? About something important, about something real?

–Guy Montag, Fahrenheit 451 (Bradbury, 1953)

The Crux of the Problem

We are experiencing a rude awakening in the area of cybersecurity, for U.S. defenses have fallen behind in the global digital arms race and need to quickly play catchup. This lapse, however, should not solely be blamed on slow government action, but rather our adversaries' early willingness to undertake illegal cyberespionage and cyberattack operations against civilian organizations during peacetime. Countries such as China and Russia–and the rogue nation states that serve as their proxy cyber armies–are responsible for inordinate numbers of attacks against U.S. corporations and government networks, bombarding our systems with an inundation of DDoS attacks, APTs, and vicious malware. They are not playing by the rulebook because, frankly, there is not one in cyberspace.

Therefore, rather than attempting to control this wild realm just beyond our cable modems the government ought to accept the system's open nature and adjust our cyber command operations accordingly. As discussed by the New York Times article, "An Elizabethan Cyber War", we ought to return to the days of the Spanish armada and embrace the privateer mindset rather than viewing cyberspace as another frontier for the cold war among China, Russia, and the United States. For, as the article suggests,

> Instead of trying to beat back the New World instability of the Internet with an old playbook, American officials should embrace it. With the conflict placed in its proper perspective, policy makers could ratchet down the rhetoric and experiment with a new range of responses that go beyond condemnation but stop short of all-out cyberwar — giving them the room to maneuver without approaching cyber conflict as a path to Defcon 1. (Hirsch & Adelsberg, 2013)

Only with a new combination of bolstered network resiliency, innovative active defense measures, policy reform, and novel thinking can we truly reestablish U.S. cyber superiority. It will take time to move the cogs and gears of government, but in reality what other options do we possess? After all, "In these legally uncharted waters, only Elizabethan guile, not cold war brinkmanship, will steer Washington through the storm" (Hirsch & Adelsberg, 2013).

Emerging Methods

The primary focus of current critical infrastructure security efforts is to bolster the resiliency of the system as a whole, ensuring that our nation's most vital industries and activities can withstand what would currently be crippling incidents. Whether physical or digital, these attacks ought not be able to overload or disable a critical infrastructure system due to redundancy and load balancing throughout the network. However, we might need to be a little more creative than gates, guns, and guards when attempting to increase critical infrastructure network resiliency.

Computing resources are less expensive than they have ever been–meaning that redundancy using virtual networks and offsite emergency backups has never been so simple or accessible. Organizations, whether public or private, need to be willing to invest more resources

in novel ways because the reality is that today, according to FBI Director Robert Mueller, "There are only two types of companies… those that have been hacked and those that will be" (Sengupta & Perlroth, 2012).

Companies and government agencies alike ought to draw inspiration from the financial sector, which has established private cybersecurity command centers, completely redundant emergency networks, and strictly controls the flow of information throughout their systems. We need to develop virtualized emergency networks that function as contingency networks should a local one be compromised, geographically redundant automatic data backups to limit the destruction caused during APT incursions or ransomware, and segregate various parts of our networks from one another behind thick walls–all while locking down the individual machines themselves. Our defenses need to extend beyond antivirus to the hybrid environments that now define the modern organizations' IT systems, shielding everything from the cloud down to individual networked devices. We may not be able to keep everyone out all the time, but we can at least make it difficult to enter (firewalls, network scanning, strong passwords), tougher to pilfer anything once inside the network (advanced encryption, segregated systems), and even harder still to do permanent damage (offsite backups, redundant virtual networks, data breach insurance).

Cybersecurity is rapidly evolving, so we must look to new technologies and training to combat social engineering and increased use of Zero-Day attacks. Researchers at the Massachusetts Institute of Technology recently developed the AI^2 cybersecurity system that combines artificial intelligence, machine learning, anomaly detection, and human intervention to reliably detect up to 85% of attacks (Noyes, 2016). Investment in hybrid systems, which leverage computational power to perform pattern recognition and aid human-based attack detection could

yield tremendous gains. Startups like Cylance and Carbon Black are already utilizing similar technologies in their endpoint solutions to achieve very positive results. Extensive and engaging training will also prove key, for a network is only as secure as its users' habits. And finally, enabling active cyber defense will be crucial for large corporations and government entities, for passive defense can only protect a network for so long against an APT (Chayes, 2015). However, in order to do so we must reform the now-bloated and unconstitutionally vague Computer Fraud and Abuse Act to untie defenders' hands and enable legal active defensive measures (Wu, 2013).

By reforming outdated and vague cybercrime policy we can quickly and effectively increase critical infrastructure cyber resiliency with the implementation of active defense policies within both government agencies and the private sector. However, in addition to adjusting policy we must also alter our collective mindset and understand that security can never be complacent or stagnant. Adversaries continually evolve and innovate, making our defense methods obsolete shortly after their development.

The Red Queen

I suggest that we step back for a moment and look to our childhoods for inspiration. Think back to the wonderful, sweetly whimsical, and surprisingly profound story of Through the Looking Glass by Lewis Caroll. In this second book of the series Alice finds herself in a chessboard land as a white pawn and encounters the Red Queen, a motherly chess figure who gives her a tidbit of advice. Just as the landscape is about to change with a new turn, the Queen hurridly says to Alice, "My dear, here we must run as fast as we can, just to stay in one place. And if you wish to go anywhere you must run twice as fast as that!" (Caroll, 1871). This small comment was the foundation for the biological concept of the Red Queen Hypothesis, which

suggests animals must adapt as quickly as possible simply to keep up with those around them (Sanders, 2013). Cybersecurity, in much the same way, takes her statement to heart. We must innovate as quickly as possible simply to keep up with those who wish to harm us–and redouble our efforts further should we hope to one day gain the upper hand in the perpetual game of castle siege that is the modern internet.

Conclusion

If you took a moment to read "For the Bristlecone Snag" you likely assumed that Zackary Scholl wrote poetry in his spare time as English major at Duke University. Now a PhD candidate in computational biology, as an undergraduate he coded an artificial intelligence algorithm to write the poem in 2011, which was later published in the university's literary magazine (Merchant, 2015). Scholl's program subsequently passed the Turing Test, a proposal created by Alan Turing–the creator of the Nazi code-breaking predecessor to the first true computer, that loosely states if a machine can play "The Imitation Game" and convince an interviewer they are speaking with another person it has reached a level of complexity suggestive of true intelligence (Oppy & Dowe, 2016). The poem might not have been a brilliant piece of literary genius, but it passed as the work of an undergraduate English major making a stab at heavy-handed poetry and proved that in 2011 machines were surpassing a level of processing complexity about which the science fiction writers of old merely dreamed.

Passing the Turing Test indicated that artificial intelligence was to the point where it was both ready for widespread use and powerful enough to surpass human computational abilities in certain fields, like Big Data. We have reached a point where these "intelligent" machines control much of our lives and are interconnected across the globe with numbers (estimated 22.9 billion devices) that surpass that of the global human population (Statistica, 2014). They sit in our pockets as personal assistants named Siri, Cortana, and Alexa; analyze massive amounts of weather and agricultural data to predict commodities prices using the IBM Watson platform; and stop our cars automatically if a small child chases a ball into the street.

Computers have done incredible things for our lives and will increasingly continue to do so, however we must also learn to protect ourselves. We need not guard against the technology

itself, but rather those who wish to pervert it for personal gain or others' pain. Under the threat of global terrorism and organized crime we must come to understand that cyberspace is truly a digital battlefield and has real-world consequences when critical infrastructure is directly affected. We must not forget to stay vigilant. And we must always remember to keep running.

Bibliography

Acharya, S. (2015, December 25). Whaling attacks targeting employees for illegal wire transfers on the rise. *International Business Times*.

Ackerman, S. (2014, October 24). How Y2K Changed the Field of Cybersecurity Technology. *Security Magazine*.

Adams, R. (1972). *Watership Down.* Avon Books.

Anonymous. (n.d.). *Official Anonymous Profile*. Retrieved from Facebook: https://www.facebook.com/OffiziellAnonymousPage/

Asimov, I. (1950). *I, Robot.* United States: Gnome Press.

Bellware, K. (2015, May 14). Washington Post's Mobile Site Hacked By Syrian Electronic Army. *The Huffington Post*.

Bradbury, R. (1953). *Fahrenheit 451*.

Bryant, W. D. (2015). Resiliency in Future Cyber Combat. *Strategic Studies Quarterly*(Winter), 87-107.

Bumiller, E., & Shanker, T. (2012, October 11). Panetta Warns of Dire Threat of Cyberattack on U.S. *The New York Times*.

Bureau, D. (2013, April 5). 'Hacktivists' deface North Korea's Twitter & flickr accounts. *DataQuest*.

Bush, G. W. (2003, December 17). Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. Washington, DC, United States of America: The White House.

Caroll, L. (1871). *Through the Looking-Glass, and What Alice Found There.* (J. Tenniel, Ed.) United Kingdom: Macmillan.

Chayes, A. (2015). Rethinking Warfare: The Ambiguity of Cyber Attacks. *Harvard National Security Journal, 6*.

Chui, M., Löffler, M., & Roberts, R. (2010, March). The Internet of Things. *McKinsey Quarterly*.

Clarke, A. C. (1968). *2001: A Space Odyssey.* United Kingdom: Hutchinson.

Clinton, W. J. (1996, July 15). Executive Order 13010: Critical Infrastructure Protection. Washington, DC, United States of America: The White House.

CNN (Producer), & Vollmann, M. T. (Director). (2016). *The 414s: The Original Teenage Hackers* [Motion Picture]. United States of America.

Corrigan, S. (2008, July). *Introduction to the Controller Area Network (CAN).* Retrieved from Texas Instruments: www.ti.com/lit/an/sloa101a/sloa101a.pdf

Doyle, C. (2014). *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws.* Congressional Research Service.

Drozhzhin, A. (2015, August 6). Black Hat USA 2015: The full story of how that Jeep was hacked. *Kaspersky Lab Daily*.

Fitzpatrick, D., & Griffin, D. (2016, April 15). Cyber-extortion losses skyrocket, says FBI. *CNN*.

Flowers, A., & Zeadally, S. (2014). US Policy on Active Cyber Defense. *Homeland Security & Emergency Management, 11*(2), 289-308.

Friedman, T. (2005). *The World is Flat: A Brief History of the Twenty-First Century.* United States of America: Farrar, Straus and Giroux.

F-Secure. (2015, April 9). Business Executives As Targets Of The Whaling Season.

General Electric. (2016). *RailConnect 360*. Retrieved from GE Transportation: http://www.getransportation.com/railconnect360

Gertz, B. (2015, January 22). NSA Details Chinese Cyber Theft of F-35, Military Secrets. *The Washington Free Beacon*.

Greenberg, A. (2016, March 10). Thousands of Trucks, Buses, and Ambulances May Be Open to Hackers. *WIRED*.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012, August). The Law of Cyber-Attack. *California Law Review, 100*(4), 817-885.

Hirsch, J. C., & Adelsberg, S. (2013, May 31). An Elizabethan Cyberwar. *The New York Times*.

Hoffman, C. (2013, April 20). Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats. *How-To Geek*.

IBM (Director). (2011). *IBM Centennial Film: Wild Ducks - Celebrating 100 years of Visionary Clients* [Motion Picture]. United States of America.

Kaplan, F. (2016, February 19). 'WarGames' and Cybersecurity's Debt to a Hollywood Hack. *The New York Times*.

Kushner, D. (2014, September 8). The Masked Avengers. *The New Yorker*.

Lasker, L., Parkes, W. F. (Writers), & Badham, J. (Director). (1983). *WarGames* [Motion Picture].

Lewis, T. G. (2015). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (2nd Edition ed.). Hoboken, NJ, United States of America: Wiley.

Leyden, J. (2008, January 11). Polish teen derails tram after hacking train network. *The Register*.

Lohr, S. (2015, October 14). G.E. Navigates, Carefully, the Industrial Internet of Things. *The New York Times*.

McAfee. (2011). Combating Advanced Persistent Threats.

Merchant, B. (2015, February 5). *The Poem That Passed the Turing Test*. Retrieved from Motherboard: http://motherboard.vice.com/read/the-poem-that-passed-the-turing-test

Morozov, E. (2008, August 14). An Army of Ones and Zeroes. *Slate*.

National Initiative for Cybersecurity Careers and Studies. (n.d.). *Explore Terms: A Glossary of Common Cybersecurity Terminology*. (U. S. Security, Producer) Retrieved from https://niccs.us-cert.gov/glossary

Norte, J. C. (2016, March 6). Hacking industrial vehicles from the internet.

Noyes, K. (2016, April 18). AI + humans = kick-ass cybersecurity. *PCWorld*.

Obama, B. (2013, February 12). Executive Order 13636: Improving Critical Infrastructure Cybersecurity. Washington, DC, United States of America: The White House.

Obama, B. (2013, February 12). Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. Washington, DC, United States of America: The White House.

Oppy, G., & Dowe, D. (2016, February 8). *The Turing Test*. Retrieved from Stanford Encyclopedia of Philosophy: http://plato.stanford.edu/entries/turing-test/

Oxford Dictionaries. (2015). Black Hat Definition.

Oxford Dictionaries. (2015). White Hat Definition.

Perlroth, N. (2015, October 14). Online Attacks on Infrastructure Are Increasing at a Worrying Pace. *The New York Times*.

Riley, M. (2014, July 21). How Russian Hackers Stole the Nasdaq. *Bloomberg Businessweek*.

Rothman, L. (2014, December 31). Remember Y2K? Here's How We Prepped for the Non-Disaster. *TIME Magazine*.

Rouse, M. (2014, December). *Definition: Security Information and Event Management (SIEM)*. Retrieved from TechTarget: http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

Sanders, R. (2013, June 20). The Red Queen was right: Life must continually evolve to avoid extinction. *Berkeley News*.

Scholl, Z. (2011). For the Bristlecone Snag. *The Archive(Fall)*. Duke University.

Schutgens, M., van Beek, J. (Producers), & Busstra, H. (Director). (2015). *Zero Days: Security Leaks for Sale* [Motion Picture].

Sengupta, S., & Perlroth, N. (2012, March 4). The Bright Side of Being Hacked. *The New York Times*.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY, United States of America: Oxford University Press.

Squatriglia, C. (2008, January 11). Polish Teen Hacks His City's Trams, Chaos Ensues. *WIRED*.

Statistica. (2014). *Internet of Things (IoT): number of connected devices worldwide from 2012 to 2020 (in billions)*. Retrieved from Statistica: The Statistics Portal: http://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Symantec. (n.d.). *Malware*. Retrieved from Norton by Symantec: https://us.norton.com/security_response/malware.jsp

Tafoya, W. L. (2011, November). Cyber Terror. *FBI Law Enforcement Bulletin*. United States Federal Bureau of Investigation.

The Economist. (2010, July 1). War in the fifth domain. *The Economist*.

The White House. (1984, September 17). National Security Decision Directive Number 145: National Policy on Telecommunications and Automated Information Systems Security. Washington, DC, United States of America: The White House.

U.S. Coast Guard. (2016). *Transportation Worker Identification Credential (TWIC)*. (U. S. Security, Producer) Retrieved from National Maritime Center: https://www.uscg.mil/nmc/twic/

U.S. Department of Homeland Security. (2011). *Department of Defense Strategy for Operating in Cyberspace.*

U.S. Federal Bureau of Investigation. (2009, April 1). Spear Phishers.

U.S. Government Accountability Office. (2014). *MARITIME CRITICAL INFRASTRUCTURE PROTECTION: DHS Needs to Better Address Port Cybersecurity*.

U.S. Government Department of Homeland Security. (2016). *Critical Infrastructure and Key Resources*. Retrieved from Information Sharing Environment: https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources

Verizon. (2015). *2015 Data Breach Investigations Report.*

Waldrop, M. M. (2016, February 09). The chips are down for Moore's law. *Nature*.

Wasik, B. (2013, May 14). In the Programmable World, All Our Objects Will Act as One. *WIRED*.

Wu, T. (2013, March 18). Fixing the Worst Law in Technology. *The New Yorker*.

Zetter, K. (2011, July 11). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. *WIRED*.

Zetter, K. (2014, November 3). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *WIRED*.

Zetter, K. (2015, September 17). Hacker Lexicon: A Guide to Ransomware, the Scary Hack That's on the Rise. *WIRED*.

Zetter, K. (2016, March 3). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *WIRED*.

Appendix A: Critical Infrastructure

Critical infrastructure is defined by the US government as, "so vital that [its] incapacity or destruction would have a debilitating impact on the defense or economic security of the United States," (Clinton, 1996) and is therefore its responsibility to protect as a matter of homeland security. These infrastructures consist of 16 sectors, including the following: the chemical industry (including oil production, refining, and storage), select commercial facilities, communications equipment and crucial nodes, critical manufacturing, dams, the defense industrial base (US military, defense contractors, and supporting services), emergency services (medical, police, fire, and rescue), energy production and transmission, financial services, food and agriculture, government facilities, healthcare and public health, information technology systems, nuclear facilities (reactors, materials, and waste), transportation systems (air, sea, and land), and water and wastewater systems (Obama, PPD-21, 2013). According to the order,

> Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats").

We as a nation must be conscious of potential threats in every domain and wary of complacency towards unseen foes.

Basic and rapidly evolving theory related to critical infrastructure security focuses primarily on increasing resilience of systems as a whole to withstand attacks on crucial nodes (Lewis, 2015). Most US critical infrastructure systems are structured similarly to the global airline industry in that their networks consist of hubs and spokes, with any given network overly dependent a handful of the former. Therefore, should one hub be knocked out by an incident of

some sort, the system itself goes down under the weight of instantaneous overload. For example, when winter storms in the Northeastern US cause one or more hubs to temporarily go offline the system bogs down (think LaGuardia, JFK, and Newark shutting down during a blizzard), leaving passengers stranded and planes grounded across the nation. Critical infrastructure functions in much the same manner, so should a critical hub of the electrical grid go down, an entire seaboard may experience rolling (or permanent) blackouts until the network can normalize once again. Subsequently, we as a nation must focus greater attention and resources towards improving the resilience of the entire system rather than simply bolstering hubs' excess capacity and security (Lewis, 2015).

The major challenge associated with improving resilience is that both the system design and efficiency are stacked against the federal government's favor. Eighty-five percent of our nation's critical infrastructure is owned by the private sector (U.S. Government Department of Homeland Security, 2016) and therefore driven by profit, creating a system in which lean design prevails. These companies are heavily regulated but ultimately governed by shareholder interest, encouraging limited redundancy to cut costs. Nodes are constructed with continuity of service in mind, but the lack of network resilience is concerning. Eliminating excessive redundancy saves money, and therefore they have been designed with a cost-benefit ratio in mind–a ratio that the private sector has pushed to the very limits of safety to ensure the highest level of profitability possible (Lewis, 2015). Therefore, conflicts arise with the federal government and Department of Homeland Security in terms of mandating stronger network resilience. Frankly, companies do not want to do it, and the government has a hard time determining who is responsible for expenses associated with protecting nodes and strengthening spokes. It is a difficult question that

is made exponentially more challenging to answer when confronted by the treats associated with global terrorism.

According to the 2013 Presidential Directive on Critical Infrastructure Security and Resilience (PPD-21):

> Three strategic imperatives shall drive the Federal approach to strengthen critical infrastructure security and resilience:
>
> 1. Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;
> 2. Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and
> 3. Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure. (Obama, PPD-21, 2013)

Without government oversight we cannot trust the private sector to tackle these challenges properly, however we also cannot mandate they pay for all protective measures–leading to the tricky question of, "Who should pay the bill?" We do not have the answer yet–however we are slowly discovering the emerging challenges associated with public-private partnerships in all 16 critical infrastructure sectors.

Appendix B: Cyber Terminology

The following is an overview of basic cyber terminology.

Cybersecurity

Cybersecurity has been defined by the federal government as,

> The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. (National Initiative for Cybersecurity Careers and Studies, n.d.)

Inordinately challenging for defenders, cybersecurity is a never-ending game of castle siege. Defenders must be right 100% of the time, which is technically impossible, while attackers must only find an overlooked chink in the castle defenses to enter and pilfer or destroy the palace. Therefore, cybersecurity is a game of continual active defense. Passivity and stagnancy are rewarded with catastrophic damage, for systems must be continually patched, updated, and modified to protect against unseen foes. As described in Cybersecurity and Cyberwar, "[Cybersecurity] is associated with the presence of an adversary. In that way it's a lot like war or sex; you need at least two sides to make it real… [It] only becomes a cybersecurity issue if an adversary seeks to gain something from the activity" (Singer & Friedman, 2014). Unfortunately, as our defenses evolve, so do our attackers' techniques–forcing us to stay one step ahead, a daunting and effectively impossible task.

Cybercrime

Cybercrime tends to focus on the extraction of financial resources, intellectual property, or sensitive information from compromised networks but includes a broad range of activities. "Cybercrime, as we now think of computer crime, is most often defined as the use of digital tools

by criminals to steal or otherwise carry out illegal activities" (Singer & Friedman, 2014). We will cover the most prevalent forms of cybercrime in a later section.

Cyberespionage

Cyberespionage is a variation of cybercrime that focuses primarily on the theft of sensitive information or intellectual property. It normally involves government agencies and the pilfering of secrets from classified computer networks (Singer & Friedman, 2014). Cyberespionage is generally perpetrated by hostile governments and has reached as far as the White House's nonessential internal network and F-35 Joint Strike Fighter's classified stealth radar and engine plans (Gertz, 2015). The latter breach stole over 50 terabytes of information form Northrop Grumman, severely compromising the project and enabling the Chinese government, "to include the design and technology in Beijing's new stealth jet, the J-20" (Gertz, 2015).

Cyberterrorism

The Center for Strategic Information Studies has defined cyberterrorism as, "the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population" (Tafoya, 2011). Furthermore, it involves, "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information" (Tafoya, 2011). Therefore, these types of attacks must be directed at noncombatant civilians and cause significant damage to be labeled cyberterrorism, exactly like its physical sibling. This form of cyberattack is the most concerning for operators of critical infrastructure, as system nodes are relatively susceptible to such threats and can cause major damage and potential casualties.

Cyberwar

Cyberwar, or Information Warfare (IW), tends to be coupled with active physical war situations and very rarely occurs on its own. While many consider cyberespionage or general cyberattacks to fall under this categorization, the US government only considers a cyberattack an act of war if it were to, "proximately result in death, injury, or significant destruction" (Singer & Friedman, 2014). Therefore, the attack must have major physical consequences to fall under this category, which can also include acts of cyberterrorism.

Appendix C: Threats

Cyberattacks come in many forms and are distinguished by the technology used to achieve their end goal. Each of the following sections discusses a major offensive vector or actor. Multiple technologies are often used in tandem to gain entry to a particular system, and depending on the attackers' sophistication and end goals the incident may occur over the course of seconds, days, or even months.

Bot-Net Operators

Bot-Net Operators use networks of computers infected with malware to launch various forms of attacks, such as sending phishing emails or spam, coordinating denial of service attacks, or distributing malware. Their services are often available for purchase on the black market via the dark web as hired guns, a means of bolstering an attack's intensity when attempting to take down a website or overload a specific server. The software responsible for forming a bot-net is propagated via various forms of malware (U.S. Government Accountability Office, 2014).

Business Competitors

Corporate cyberespionage (or defending against it) may play a role in a business' ongoing daily operations. As depicted in the 2009 movie "Duplicity", intellectual property theft is a major business in everything from weapons manufacturing to consumer packaged goods, forcing corporations to guard against attacks from both external and internal actors (U.S. Government Accountability Office, 2014).

Criminal Groups

Both organized syndicates and smaller independent cells are responsible for various internet cybercrime schemes. Their end goal usually involves the theft of personal information to

commit identity fraud or extortion (U.S. Government Accountability Office, 2014). Recent trends indicate these groups are flocking to ransomware, a form of malware that takes one's system hostage with malicious encryption and threatens to delete all locked data if a payment is not received within a certain time period (Zetter, Hacker Lexicon: A Guide to Ransomware, the Scary Hack That's on the Rise, 2015).

A disturbing new tactic involves targeting hospitals in developed countries with strains of this type of malware. By accidentally clicking a phishing link or plugging in an infected USB thumb drive, a user in a hospital system can inadvertently spread the malicious program and lock patient records, which are so critical and time-sensitive that the hospital must pay the ransom rather than fight the attack or take precious time to rebuild their systems from backups (Fitzpatrick & Griffin, 2016).

Hackers

Hackers are individuals or groups who work to break into computer networks and systems for various reasons, most notably, "the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons" (U.S. Government Accountability Office, 2014). The field has become drastically easier to enter with the advent of attack scripts and protocols, network sniffing devices, simplified password brute-forcing, and many others. "Thus, while attack tools have become more sophisticated they have also become easier to use" (U.S. Government Accountability Office, 2014). The following are key categories of hackers based on their motivation and intent.

Blackhat

Blackhats are individuals who hack into networks or devices using previously unknown vulnerabilities and/or social engineering for malicious intent. These hackers generally do so for

individual financial gain or–less commonly–patriotic or ideological reasons (Oxford Dictionaries, 2015). Blackhats may also work in teams to form Advanced Persistant Threats (APTs), which we will discuss shortly.

Whitehat

Whitehats are individuals who hack into computer networks for testing and vulnerability detection purposes. They often work as freelance contractors, for cybersecurity and penetration testing firms, or simply submit problems they discover to technology companies in return for compensation through bug bounty programs (Oxford Dictionaries, 2015).

Greyhat

Very few things in life are black and white, and the shadowy world of hacking tends to follow the same trend. Greyhats are individuals who, "[do not] work for their own personal gain or to cause carnage, but they may technically commit crimes and do arguably unethical things" (Hoffman, 2013). As discussed in the movie "Zero-Days," these hackers are faced with difficult moral choices when presented with vastly different compensation on the black and white markets for finding a bug in a popular system's code. A Greyhat must sometimes decide between a bug bounty program payout of $30,000 and a black market value of $1,000,000 or more (Schutgens & van Beek, 2015).

Hactivist

These hackers are individuals or groups who take driving social or political change into their own hands using little more than a laptop and high-speed internet connection (Singer & Friedman, 2014). They are digital activists, whose tools have morphed from throwing paint on wealthy, fur-clad women in front of New York Fashion Week tents to taking down child pornography websites, crashing terrorist organizations' servers, and defacing North Korea's

twitter and flickr accounts (Bureau, 2013). These methods are usually legally-questionable and difficult to attribute unless a group directly claims responsibility.

The most feared, revered, and interesting of these hacktivist groups is Anonymous, a very loosely organized collective of hackers scattered across the internet who periodically rally around a common cause. As discussed in The New Yorker magazine, it is less an organization proper and more of a "shape-shifting subculture" that has been described as "a series of relationships" (Kushner, 2014) branching across the dark web and sites like 4chan to encourage sociopolitical change. "Among Anons, personal identity and the individual remain subordinate to a focus on the epic win–and, especially, the lulz" (Kushner, 2014). The group has declared "war" on individuals like Donald Trump and terrorist groups like ISIS and is nearly impossible to track or repel. Its sheer size, rather than its actual sophistication, makes it inherently difficult to stop. Most members are not experienced hackers but simply interested individuals dabbling in light hacking and taken by the group's shadowy ideology. Their battle cry is, "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us." (Anonymous, n.d.).

Insiders

According to the 2015 Verizon Data Breach Report, 20.6% of all system compromises/damages are classified as insider misuse (Verizon, 2015). These incidents occur when a user with legitimate access to a network abuses their privileges to commit an internal cybercrime. These users are often disgruntled employees or contractors who were recently terminated or simply careless with introducing malware into a network environment. "The insider may not need a great deal of knowledge about computer intrusions because his or her knowledge of a target system is sufficient to allow unrestricted access to cause damage to the system or to steal system data" (U.S. Government Accountability Office, 2014).

Nations

Nations with cyber command programs, especially those hostile to the United States, are of grave concern when protecting critical infrastructure. These programs may take the form of organized military units, such as the US Air Force's Cyber Command, or loosely connected hacker crime syndicates hired by the Russian government. Cyberespionage and cybercrime against civilian targets and government agencies are commonplace, such as the Sony Hack by North Korea, which we will discuss later–however the consequences of a full-out cyberwar could be devastating to a nation's critical infrastructure (Singer & Friedman, 2014). Small or underdeveloped nations with relatively incapable traditional military forces are now able to launch dangerous, full-scale cyberattacks against more powerful states with little expense or difficulty. Nations build up stores of uncovered zero-day exploits, or unknown vulnerabilities in code, and silently infect other nations' military networks as a potent insurance policy should an attack occur on their own systems (Schutgens & van Beek, 2015). According to the 2014 GAO Maritime Security Report, "Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power–impacts that could affect the daily lives of citizens across the country" (U.S. Government Accountability Office, 2014).

Phishers

Criminals utilize phishing to collect private information and perpetrate financial fraud against individuals or businesses. Individuals often do not commit the crimes themselves, instead selling personal and medical information on dark web marketplaces for use by organized crime, often in Eastern Europe or Russia. Phishers use various methods to collect information, however the most common are spam (Nigerian businessmen, wealthy Namibian heiresses, online

pharmaceuticals sales), spyware (key loggers and sniffing applications), and malware (U.S. Government Accountability Office, 2014).

Spammers

This category of cybercriminal usually overlaps with phishers but may not be the actual perpetrator of information theft. Spammers are obviously responsible for unsolicited emails and fictitious social media posts or connection requests, however they may also offer a for-hire botnet to send out phishing information for other criminals. These systems may also be used to launch denial of service attacks to crash an email server by sending millions of messages per second to one or multiple specific address, temporarily crippling an organization's ability to communicate digitally.

Spyware and Malware Authors

These groups create malicious computer programs and launch attacks on vulnerable systems. Due to its inherent system architecture and ubiquity, the Windows operating system is most often targeted, however Android malware is on the rise (Verizon, 2015). Mac OSX malware is still limited but increasing at a breakneck pace, while ransomware across all platforms has become the new trend within the field (Fitzpatrick & Griffin, 2016). Authors will often repackage or alter previously developed malware to evade virus detection software and bypass traditional system defenses.

Terrorists

Groups such as the Syrian Electronic Army and ISIS have become potential threats to critical infrastructure but have so far stuck with supporting their radical causes through defacing websites, hacking social media profiles, and crashing web servers (Bellware, 2015). These groups have aspirations, "to destroy, incapacitate, or exploit critical infrastructures in order to

threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence" (U.S. Government Accountability Office, 2014). They would most likely attack targets with the greatest potential impact for loss of life, such as nuclear power plants or drinking water facilities. Additionally, much like organized crime syndicates, they often use fraud, malware, and phishing to fund their operations (Singer & Friedman, 2014).

Appendix D: Attacks

The following sections discuss varied forms of cyberattacks, grouped according to the technology each uses. Some are very temporary, inundation-like assaults that overwhelm individual computers or websites, while others are more complex programs that infiltrate a closed network silently to perform a specific task over an extended period of time. Each was created for a different purpose and has evolved over time, many now incorporating aspects of social engineering and various technologies from multiple categories.

Denial of Service

DoS attacks, as they are usually abbreviated, consist of an operator using a host machine to flood another system with an overload of traffic in hopes of temporarily disabling or crashing it by exhausting system resources (U.S. Government Accountability Office, 2014). Much like hitting a person with a firehose, the target may be able to withstand the onslaught at first but collapses within a short period of time.

Distributed Denial of Service

These attacks, a variant of Denial of Service attacks, use multiple machines or networks distributed across the internet to simultaneously fire millions of requests at a server or website per second (U.S. Government Accountability Office, 2014). They are much more difficult to withstand than DoS attacks because more machines fire at full bore against one target, as if thousands or millions of firehoses were aimed at one person. DDoS attacks, as they are abbreviated, easily crash websites or servers and can destroy physical components through overheating under extreme processing loads. The server does its best to manage the heightened traffic but does not always know when when to shut down to protect itself, often resulting in permanent damage.

These attacks are relatively easy to coordinate and often launched by hacktivists to prove a point. They can be launched from several machines or utilize thousands of hijacked computers and servers around the world, which we witnessed during the Russian invasion of Georgia. Various crime syndicates, Russian patriots and extremists, and potentially the government itself fired DDoS attacks against Georgian government servers, banking websites, and communications providers, temporarily crashing vital internet services (Morozov, 2008). This attack cannot be considered a true act of cyberwar because it did not cause loss of life or crippling damages, however it was associated with active military conflict between nations (Singer & Friedman, 2014).

Malware

Norton by Symantec, one of the most reputable endpoint virus protection programs and successful international cybersecurity companies, defines malware as the following,

> Malware is a category of malicious code that includes viruses, worms, and Trojan horses. Destructive malware will utilize popular communication tools to spread, including worms sent through email and instant messages, Trojan horses dropped from web sites, and virus-infected files downloaded from peer-to-peer connections. Malware will also seek to exploit existing vulnerabilities on systems making their entry quiet and easy. (Symantec, n.d.)

Malware is somewhat of a catch-all term for what the public generally considers generic viruses. As mentioned in the above definition, various forms exist and are categorized by their propagation mechanisms and characteristics. Complex malware may span multiple categories and pull from the nastiest traits of each to more effectively compromise a system and spread. The following represent the top categories of malware identified currently.

Ransomware has become a major new threat due to its striking profitability. The program is installed through a phishing email and takes over one's system, often spreading through a network like wildfire. Unless quarantined, certain strains can make their way into centralized servers to take an entire organization hostage. The program, "locks your keyboard or computer to prevent you from accessing your data until you pay a ransom, usually demanded in Bitcoin" (Zetter, Hacker Lexicon: A Guide to Ransomware, the Scary Hack That's on the Rise, 2015). However, since their emergence in 2005 the programs have evolved into more sophisticated systems, now encrypting the victim's information so that only the hacker can unlock it. In this way, if a target lacks regular, secure, offsite backup systems they can either lose vast amounts of information or sizable sums of money. Currently ransomware is expected to cost businesses at least $1 Billion in 2016 alone (Fitzpatrick & Griffin, 2016).

Trojan Horses, or simply "Trojans", are exactly what their name implies–a seemingly innocuous or helpful program that users willingly install on their system that then infects their device with spyware, other forms of malware, or even a botnet network client. They can secretly operate in the background and log users' keystrokes and relay passwords back to a command server, cause annoying popups on the desktop, or take over the machine entirely (U.S. Government Accountability Office, 2014).

Viruses are the most commonly known threat online and, "can copy [themselves] and infect a computer without the permission or knowledge of the user" (U.S. Government Accountability Office, 2014). As we all likely know from experience, viruses often take over computers and limit removal efforts or evade detection by antivirus programs while spamming one's email contacts to spread the infection. Sometimes these programs erase data, corrupt system files, disable programs, or perform a myriad of other insidious digital actions to achieve

an end goal of some sort. A distinguishing factor of viruses from other forms of malicious computer programs is that they require human action, like opening an infected PDF file, to propagate (U.S. Government Accountability Office, 2014).

Worms are the most dangerous and advanced in this family of infectious code because they are, "self-replicating, self-propagating, self-contained program[s] that use network mechanisms to spread" (U.S. Government Accountability Office, 2014). The disturbing and unique trait these programs possess is that they require no user intervention to move throughout a network and can rapidly, efficiently, and cripplingly infect vast numbers of devices without detection. They are the most complex and effective attack vectors the security community has encountered to date, forming the digital missile that carries a cyber weapon payload directly into the heart of an enemy network (Singer & Friedman, 2014). The world's first advanced cyber weapon, an extremely sophisticated worm developed by the U.S. and Israeli governments, is detailed in the following paragraphs to provide insight into the potential ramifications of weaponized computer programs.

Stuxnet was an astounding piece of digital engineering, for it did what no other worm had managed to do before–jump across thin air to transverse the boundary between digital and physical, wreaking havoc on equipment connected to the industrial control system responsible for Iran's nuclear enrichment program. The worm was released into networks at contracting companies responsible for the engineering and development behind Iran's nuclear program, evading detection through cloaking, mutation, and slow but steady progress. It eventually made its way via intranet connections into the peripheral network at Iranian nuclear enrichment labs, which were separated from the control room by an air gap. Stuxnet then infected the physical media used to transfer files between the two networks, evading virus detection through the use of

unknown vulnerabilities, called zero-day exploits, and entered into the heart of their nuclear operation (Zetter, An Unprecedented Look at Stuxnet, the World's First Digital Weapon, 2014).

The worm would rev enrichment centrifuges up and down repeatedly at night to wear out their motors and delay program progress, all while feeding operators normal operating values to evade detection. Thousands of centrifuges burned out at alarming rates due to the worm's clandestine infection over the course of months, yet Iranian computer experts were unable to locate the cause. International investigators monitoring the program were also at a loss, for as WIRED points out,

> What the inspectors didn't know was that the answer they were seeking was hidden all around them, buried in the disk space and memory of Natanz's computers. Months earlier, in June 2009, someone had silently unleashed a sophisticated and destructive digital worm that had been slithering its way through computers in Iran with just one aim — to sabotage the country's uranium enrichment program and prevent President Mahmoud Ahmadinejad from building a nuclear weapon. (Zetter, How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, 2011)

Thus, the first advanced cyber weapon was unleashed upon the world, utilizing four zero-day exploits and multiple modules that could be turned on or off, depending on the type of system it was infecting (Zetter, How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, 2011). According to Bloomberg Businessweek, those who designed the code had a thorough understanding of the way the Iranian nuclear program was assembled, what equipment they used, how contractors worked together through intranet connections, and what the operating limits were for the custom-built centrifuges used in their facilities (Riley, 2014).

It took over one year for the Iranian government to begin putting the pieces together. One night a control center computer unexpectedly began an endless restart cycle, prompting officials to call in international computer security experts to dissect the situation. Researchers discovered packets of foreign code throughout the machine in secret directories, however it took much longer to diagnose the problem as a cyber weapon. Few in the cybersecurity community wanted to touch the worm, either out of sheer disinterest or some other suppressing force, but eventually Symantec and F-Secure cracked small snippets of the worm's code, discovering what was at the time, "the most complex malware ever written — a piece of software that would ultimately make history as the world's first real cyber weapon" (Zetter, An Unprecedented Look at Stuxnet, the World's First Digital Weapon, 2014).

Phishing

Phishing is a type of cyberattack that crosses over into the physical world through social engineering. According to the GAO Maritime Security Report, phishing is defined as, "A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information" (U.S. Government Accountability Office, 2014). It serves as a potent entryway for malware into otherwise secure networks or method for extracting sensitive personal information and has become increasingly sophisticated. Traditional phishing involves sending out thousands of emails to random individuals and hoping someone takes the bait (for lack of a better term), clicking on an email's malicious link or entering their banking password into a seemingly legitimate login page. However, since its introduction the technique has evolved and become more targeted, as discussed in the following paragraphs.

Spear phishing is a variant of phishing that consists of cybercriminals targeting, "select groups of people with something in common—they work at the same company, bank at the same financial institution, attend the same college, order merchandise from the same website, etc." (U.S. Federal Bureau of Investigation, 2009). This method is highly effective because individuals are inherently more likely to trust their local bank or supervisor than a Nigerian businessman who just won an international lottery. Currently, email sender names and occasionally addresses can be spoofed/faked with relative ease, making a phishing attack more deceptive and difficult to detect.

Whale phishing is a newer trend within the cybercrime community that targets employees handling major financial transactions within larger corporations. Also called a Business Email Compromise (BEC), this method utilizes a phony email sent by a member of senior management to an employee directing them to wire money to an offshore account. The email address is either spoofed or hacked, making the employee believe they are simply following legitimate directions (Acharya, 2015). However, it has recently evolved further, incorporating various social media channels to increase a sender's perceived legitimacy and reach. Whalers do so because these executives, "have access to lots of valuable or competitive intel, system access or even just to the right social network or endorsement" (F-Secure, 2015). This method meets with a startlingly high rate of success due to its extremely targeted, personal nature and employees' willingness and obligation to follow superiors' orders.

Zero-Day Attacks

Zero-Day attacks are effectively the Achilles' heels of the technology industry. They represent a gap in the armor, a glitch in the code, a hole in the fence that enables hackers to swiftly and secretly gain entry into an otherwise protected system. These are, "the hacking

world's most potent weapons: They exploit vulnerabilities in software that are yet unknown to the software maker or antivirus vendors" (Zetter, How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, 2011). Their name originates from the fact that upon discovery there have been zero days to patch the vulnerability, making them extremely valuable yet exceedingly rare. "Out of more than 12 million pieces of malware that antivirus researchers discover each year, fewer than a dozen use a zero-day exploit" (Zetter, How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, 2011). Therefore, a general rule of thumb when diagnosing malware and attributing development is that using one Zero-Day in a malicious program or attack indicates a sophisticated hacker or group, while using multiple suggests government involvement (Schutgens & van Beek, 2015).

These attacks are the cyber weapons of the future, for they afford access to secure systems without alerting antivirus programs, intrusion detection systems, or network administrators. They are nuclear weapons of the cyber battlefield, and when coupled with a dedicated group of hackers little can be done to stop or delay a total system compromise.

Advanced Persistent Threats

Advanced Persistent Threats are groups of highly capable hackers sponsored by crime syndicates or governments responsible for the most sophisticated of cyberattacks. According to McAfee's definition of the term,

> APTs are to intrusion detection what stealth aircraft are to radar. They are targeted attacks designed to evade conventional detection. Once "inside" and disguised as legitimate traffic, they can establish covert, long-term residency to siphon your valuable data with impunity. (McAfee, 2011)

These attacks generally occur in the following stages and are extremely difficult to prevent, detect, or mitigate due to their sophistication and perseverance:

1) Incursion: During the first stage of an attack hackers gain entry into a system and establish a reliable access point from which to explore the network and launch highly targeted covert operations. APTs are long-tail games rather than traditional "smash and grab methods" (McAfee, 2011) and utilize a variety of techniques and tools to compromise a target's network.
2) Discovery: Upon gaining access, an APT begins to map out the network structure and composition to better understand how their target works and where valuable data is most likely stored. Attackers are methodical about executing the intrusion and usually stay within compromised systems, watching and waiting, for over six months. During this period, they search for various vulnerabilities and may install malware on client devices to log keystrokes and access secure data.
3) Capture: Once infiltrators have mapped out a network's architecture and better understand how it functions from a whole-system perspective, they begin accessing data in hopes of uncovering sensitive and/or valuable information. Furthermore, they may install more malicious code on servers to gather intelligence on users' activity and credentials, silently collecting information with every passing keystroke.
4) Exfiltration: Finally, once the target's devices are totally compromised the attackers can begin pulling data out of their system, absconding with intellectual property and sensitive materials.

   (McAfee, 2011)

In this manner, APTs are potent tools for infiltrating and exploiting target systems, becoming increasingly more important in international cyber command operations as governments rely more heavily on digital espionage.

Advanced Persistent Threat teams are expensive to maintain and equip properly, generally limiting their operations to governments and organized crime syndicates. They have become increasingly more common as technology prices decrease and more of the developing world comes online, however the most advanced attacks are still perpetrated by governments due to the time, expense, and complexity associated with discovering zero-day exploits and infiltrating heavily protected systems (F-Secure, 2015).

Acknowledgements

I would like to thank Professor Ostergaard and Dr. Iarossi for their patience and kindness throughout this process, their investment of time and energy in my personal and academic development, and their mentorship and friendship. I am so grateful to have worked on this project under your guidance and to have you both in my life. Thank you.