CYBERSECURITY:
HOW SAFE ARE WE AS A NATION?

A Thesis
submitted to the Faculty of
The School of Continuing Studies
and of
The Graduate School of Arts and Sciences
in partial fulfillment of the requirements for the
degree of
Master of Arts in Liberal Studies

By

Lisa A. Ferdinando, B.A.

Georgetown University
Washington, D.C.
April 12, 2016
ABSTRACT

We live in a connected world. From the ordinary to the extraordinary, networks and connectivity power our day, keep us running and help us along with our professional and personal endeavors. Public transportation relies on networks to whisk people to their destinations. Doctors share medical research with the world and consult with patients remotely. Students around the world connect, exchange ideas and learn; schools offer online classes to make learning accessible to the world. Our nation’s critical infrastructure such as banking, gas and electricity, water and transportation relies on the grid. Connectivity has revolutionized the way we travel, communicate and do business. Convenience is a click away.

But with this connectivity comes a dark side; our networks are vulnerable to intrusion by a myriad of actors, including cyber criminals, rogue nation states, hackers seeking to make a political point, cyber terrorists and others with malicious intent. Cybercrimes cost the American economy billions of dollars each year; the impacts of these crimes are far-reaching, they erode trust in the system and instill fear (Spinello 2011). Cybersecurity is a top priority of the U.S. government. Administration officials, all the way up to President Barack Obama, have expressed concern about troubling activity by adversaries, including those who have breached our nation’s critical
infrastructure. The threat against our networks is constant. Officials have named China, Russia, Iran and North Korea as nation states that have infiltrated U.S. cyber targets. Experts have warned of the possibility of a major cyberattack. The consequences could be dire if a rogue nation or cyber terrorists struck our critical infrastructure. In an executive order addressing the dangers and vulnerabilities in cybersecurity, President Obama declared a “national emergency to deal with this threat” (White House 2015).

The nation needs to stay one step ahead. As this paper will demonstrate, the adversaries are relentless. They have already stolen sensitive information, and compromised the privacy of millions of Americans. With our infrastructure vulnerable, our national security depends on a strong cyber culture. To stay ahead of the threat, cybersecurity needs to be steeped into the national consciousness through education, sustained messaging and increased cooperation among businesses and government.

My research examines the vulnerabilities, and cites case studies, national policy and expert analysis. I will explore the ways forward, drawing from the national conversation and most recent developments on the issue. My hypothesis is that we need a national shift in thinking on cybersecurity; we need to strengthen the cyber culture. To that end, I will look at societal changes using the examples of two issues that are independent of each other, smoking and seat belt use. With both those issues, society changed its behavior over time in the face of dangers and consequences. I believe society will change as well in regards to strengthening its cyber culture. It only takes one person to click or open a document with malware to let the adversaries into our networks. Change must happen. The threats are only growing more complex; the adversary is only more determined.
DEDICATION

To my family, loved ones and friends,

and most especially my mother who supported me through this and everything in my life.

-L
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>ii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td>iv</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER 1. A NATION CONNECTED</td>
<td>3</td>
</tr>
<tr>
<td>Vulnerabilities in Critical Infrastructure</td>
<td>9</td>
</tr>
<tr>
<td>Breaches in OPM, Other Government Networks</td>
<td>14</td>
</tr>
<tr>
<td>CHAPTER 2. U.S. GOVERNMENT AND MILITARY</td>
<td>16</td>
</tr>
<tr>
<td>U.S. and Adversaries: A Level Playing Field</td>
<td>16</td>
</tr>
<tr>
<td>Cyber Component in Current Military Operations</td>
<td>19</td>
</tr>
<tr>
<td>North Korea and Devastating Sony Hack</td>
<td>21</td>
</tr>
<tr>
<td>Defense, Intelligence Officials on Vexing Threat</td>
<td>23</td>
</tr>
<tr>
<td>Worldwide Threat Assessment</td>
<td>26</td>
</tr>
<tr>
<td>Turning to the Advice of ‘Ethical Hackers’</td>
<td>27</td>
</tr>
<tr>
<td>An Alarming Trend: Ransomware</td>
<td>29</td>
</tr>
<tr>
<td>CHAPTER 3. NATIONAL VULNERABILITIES</td>
<td>32</td>
</tr>
<tr>
<td>President Obama’s Plan for the Nation</td>
<td>33</td>
</tr>
<tr>
<td>Cyber: A ‘Serious and Significant Attack Vector’</td>
<td>34</td>
</tr>
<tr>
<td>Threats from Nation States</td>
<td>35</td>
</tr>
<tr>
<td>The Business of Hacking</td>
<td>43</td>
</tr>
<tr>
<td>Threats from the Inside</td>
<td>46</td>
</tr>
<tr>
<td>Infrastructure at Risk for Attack</td>
<td>48</td>
</tr>
<tr>
<td>CHAPTER 4. EXAMINING CYBER SOLUTIONS</td>
<td>50</td>
</tr>
<tr>
<td>Examining the Threat from China and Russia</td>
<td>52</td>
</tr>
<tr>
<td>Stronger Culture, Stronger Protections</td>
<td>55</td>
</tr>
<tr>
<td>Creating a ‘Healthy Cyber Ecosystem’</td>
<td>63</td>
</tr>
<tr>
<td>CHAPTER 5. ASSESSMENT ON CULTURE CHANGE</td>
<td>66</td>
</tr>
<tr>
<td>Social Engineering: Targeting the Weakest Link</td>
<td>72</td>
</tr>
<tr>
<td>Often Overlooked Danger: Public Wi-Fi</td>
<td>77</td>
</tr>
<tr>
<td>CONCLUSION A CULTURE CHANGE</td>
<td>82</td>
</tr>
</tbody>
</table>
INTRODUCTION

The United States is intimately interwoven in the cyber realm. The examples are all around us: from the everyday social interactions to the banking and financial industries, to the critical infrastructure on which the nation relies, and to the sophisticated national security apparatus that protects the nation. Even those who are not connected could still feel the impacts of cybercrime, including through increased costs, or if their personal information gets stolen, or if terrorists struck the nation’s critical infrastructure.

Connectivity has brought convenience right to our collective fingertips. A business transaction is just a click away, an engineer at the electric company can control the grid from a computer, and our “smart” homes “talk” to the grid to maximize energy savings. But with the convenience comes risk; networks are vulnerable to intrusions by a myriad of actors. The U.S. government warns that adversaries are constantly trying to breach critical networks. Officials have named China, Russia, Iran and North Korea as nation states that have infiltrated our networks. Experts have warned of the possibility of a major cyberattack. In an executive order addressing the dangers and vulnerabilities in cybersecurity, President Barack Obama declared a “national emergency to deal with this threat” (White House 2015).

This thesis will highlight the need for strong cyber protections and examine proposals for safeguarding the country. I will present the hypothesis that change in our national cyber culture is needed. My hypothesis is that a shift will happen, but it will take time. To test my hypothesis, I will examine how society’s behavior changed in regards to two independent actions: smoking and using a seat belt. I grew up in a time when
smoking was glamorized in advertisements and in popular culture. In addition, most people did not wear a seat belt. I find it fascinating how the culture shifted over time in response to sustained messaging, education about the dangers, and the threat of sanctions and other repercussions. As I will explain, smoking and not wearing a seat belt can have impacts beyond just the one primary person; the same holds true in cybersecurity.

This thesis will lay out the importance of connectivity in our society – from the individual user to national security and the military. I will examine the vulnerabilities, cite case studies, and look at the consequences the cyberattacks have or could have on society. To best frame my research, I will include recent cyber events and examine the national policy and expert analysis from the government and private sector. I will explore the ways forward, drawing from the national conversation and policy developments.

As this paper will demonstrate, the adversaries are relentless. They have already breached critical networks and infrastructure, stolen sensitive information, and compromised the privacy of millions of Americans. With our infrastructure vulnerable, our national security depends on a strong cyber culture. To stay ahead of the threat, cybersecurity needs to be steeped into the national consciousness through education, sustained messaging and increased public-private cooperation. The threats are only growing more complex; the adversary is only more determined.
CHAPTER 1
A NATION CONNECTED

From the ordinary to the extraordinary, networks and connectivity power our day, keep us running and help us along with our professional and personal endeavors. The great domains are land, sea, air, space and now cyberspace. “Cyberspace” goes beyond just the Internet. According to counterterrorism and cybersecurity expert Richard Clarke, who served in several presidential administrations, cyberspace includes the Internet as well as “all of the computer networks in the world and everything they connect and control.” Cyberspace, according to Clarke, includes transactional networks that are used for credit card or financial transactions, and even networks for control panels that run pumps and generators (Clarke 2010, 70).

To illustrate just how connected we are, imagine this: an average American rouses from sleep with an alarm on his smartphone, then does a variety of tasks before even leaving bed, such as reading emails, logging on to his bank account, and checking his sleep patterns as recorded by an app on his phone. He starts his “smart” coffeemaker, then jumps in the shower where he uses water from the local utility that runs on the grid. Rushing out of his “smart” home, he starts his car and enables his home security system with a few taps on his smartphone. The public transportation he uses relies on networks to ferry passengers to their destinations. While walking to his building, he checks his vital signs and how many steps he has taken, and gets the weather report from his smartwatch.

After using his fingerprint and code to electronically enter the building, he might correspond via secure connection with a colleague thousands of miles away. The building
and the streets around him are protected by local, state and federal authorities who rely on networks for critical information. While logged on to his work computer, he could pay his mortgage, send sensitive information to his health provider, check on his wife and sleeping baby at home through an online feed from the baby monitor, retrieve banking documents, and update his personnel records with his new address or information on his spouse and children. And all this could happen before he even has his morning coffee!

As this simple and quite typical scenario indicates, not only are we connected as a society -- we are hyper-connected. We live in the age of the “Internet of Things,” or IoT, where our connected devices such as appliances can track our usage, be controlled remotely, and tell us when maintenance is needed, according to the Center for Strategic and International Studies. IoT devices usually have an IP address, onboard computing power, and most have network connectivity, often wireless, according to CSIS. These devices go beyond just the day-to-day things in our lives, but can be industrial machines that automate activities such as inventory control, and arranging shipping and delivery, CSIS said in a report, Managing Risk for the Internet of Things. The document outlined how IoT devices are vulnerable to hacking. It points out that many of these devices lack the computing power to carry out security functions like a traditional computer does (Lewis 2016).

Connectivity has revolutionized the way we travel, communicate and do business. Convenience is a click away. News, ideas and information buzz around the globe. Financial transactions happen in seconds. Networks store a whole host of information. From medical and financial records, personnel employment data, private records, tax
information, school records, Social Security numbers, to government data, the list goes on about the sensitive data stored on networks.

Connectivity moves the nation forward. Commuters sit back as the high-speed rail whisks them into the city. Financial brokers make trades as they eye the stock ticker. During your shopping excursion, the clerk relies on connectivity for quick credit card transactions, or to check if an item is in stock. Doctors share medical research with the world and consult with patients remotely. Students around the globe connect, exchange ideas and learn; schools hold online sessions to make learning accessible to the world.

It is a given that businesses and institutions will likely have an Internet presence now to include a website and one or more social media pages. The online world is a social gathering spot where people connect and share ideas. To illustrate how many people are online and use social media, consider this: the world’s population is more than 7 billion (U.S. Census Bureau 2016). Facebook averaged 1.5 billion monthly active users around the globe for September 2015 (Facebook 2016). Meanwhile, Instagram boasts more than 400 million monthly active users (Instagram 2016).

Most of the adult population in the United States are connected. In 2015, only 15 percent of American adults surveyed said they did not use the Internet. That is compared to 2000, when nearly half of American adults were offline (Anderson and Perrin 2015). Now, with connectivity so ingrained in society, the majority of Americans rely on electronic transactions, including credit and debit cards, for their in-person financial transactions and carry less than $50 on any given day (Kieler 2014). The networks are buzzing with activity: in an Internet minute, there are 20 new victims of online identity
theft, 204 million emails are sent, and Amazon makes $83,000 in sales. There will be 50 billion networked devices by 2020 (World Economic Forum 2016).

While networks can be used for good, the bad guys are out there as well. It is a rough neighborhood of thieves, conmen and even terrorists. Hackers are seeking to compromise sensitive information, launch malicious programs, steal identities, hack into your bank or credit card account, trick people into handing over account information, and otherwise wreak havoc. Malware has infected computers and exposed vulnerabilities.

A news report on hacking of Utah state systems described the persistent attacks from malware this way: “Most of the time, the hackers are not sitting in front of a keyboard and screen, but programs set in motion by them are sweeping state systems, searching for signs of weakness. Think of it as a constant stream of searchlights, crisscrossing your neighborhood, looking for an open garage door” (Mullahy 2016).

Cybercrimes are far-reaching; they erode trust in the system and instill fear. They impact individuals, businesses, financial institutions, consumers and the economy. According to the United Nations, cybercrime is an enterprise that exceeds a trillion dollars a year in online fraud, identify theft and lost intellectual property. The crime affects millions of people around the world, as well as businesses and governments worldwide (United Nations 2016).

In addition to computers and networks, any device that has connectivity, such as baby monitors, home security systems, and our “smart” cars and appliances, are all susceptible to hackers. Developers might also put in “trapdoors” in the code so they can go back later if they need to add updates, or so they can enter places they aren’t supposed
to be, according to cyber expert Richard Clarke. And it is the stuff that James Bond movies are made of, he said. Those with malicious intent, including espionage or sabotage, could write in special lines of code to tell a copier to save and then email copies of the document it is copying, or perhaps the code would direct the copier to malfunction and overload, thus starting a fire that sabotages a business (Clarke 2010, 72).

While the American public might not need to be overly concerned that their copier is being used for nefarious purposes, the point is that any device with connectivity is vulnerable. Security experts urge continued vigilance because the threat is only increasing. And the way adversaries can get in is pretty easy: we let them in. Phishing is a common technique to lure people into revealing sensitive information in an effort to compromise their bank, credit card or other personal accounts. In a phishing attempt, cyber crooks send an email purportedly to be from a legitimate business. The recipient is asked to click on a link and enter sensitive information. The thieves then hijack that account to steal what they can or try to lure the victim’s contacts into the scheme. Another consequence of clicking on a phishing attempt could be that the link directs the person to malicious page that infects the computer (Norton 2016).

The more advanced cousin of phishing is spear phishing. A phishing attempt could be an email addressed to someone along the lines of “Dear Valued Customer” and sent out to the masses. A spear phishing attack, in contrast, is tailored to its target. A spear phishing attempt could appear to be from a legitimately sounding source such as a bank, government entity, or even the head of the targeted company, and be addressed to an employee or employees.
Of the more than 1,000 items in my email “junk” folder, I see messages purportedly from FedEx, Google, Facebook and LinkedIn, all urging me to click on links to read messages from people I don’t know, retrieve a package “containing confidential personal information,” or add an unknown friend to my social network. Even though these are low-tech and obvious attempts riddled with typos, clicking on a link could still do harm. As the Norton anti-virus computer company succinctly describes it: “Phishing is essentially an online con game and phishers are nothing more than tech-savvy con artists and identity thieves” (Norton 2016).

In the commercial world, hackers have compromised banks and financial institutions, and staged major breaches of large retailers such as Home Depot, Target and Staples (Hardekopf 2014). According to Target, “criminals forced their way” into its system and gained access to information of 110 million credit and debit card accounts in 2013. The retailer said after the intrusion was discovered it moved to immediately close the access point in which the attackers entered (Target 2016). The entry point was reportedly not Target itself, but allegedly a Pennsylvania-headquartered firm that does contract business electronically with Target. That firm, Fazio Mechanical Services, said it was the victim of a “sophisticated cyberattack operation.” It reportedly fell victim to a phishing attack in which malware was installed into its system. The attackers allegedly used Fazio’s system as a “backdoor” to make their way into Target’s system (Krebs 2012).

As illustrated in the Target example, even with the best outside defenses, a system is still vulnerable because of the human factor. Despite the heightened awareness to
phishing, an employee could easily fall prey by hurriedly or even accidently clicking on a legitimate-looking link, thus opening up the network to a whole host of problems. Critical infrastructure, businesses or government agencies could have the strongest authentications, firewalls and protections in place. However, hackers can walk right in to the network, if an employee opens the cyber door for them.

Once malware is in place, viruses and worms can infect systems. Denial-of-service (DoS) attacks have inundated servers and caused them to crash, thus denying legitimate users access to a site. In distributed denial-of-service (DDoS) attacks, the attack uses a botnet, or a network of hijacked computers, to launch a DoS attack. The attack is coming from many places, perhaps around the world, thus the “distributed” in the DoS attack (Department of Homeland Security 2013).

**Vulnerabilities in Critical Infrastructure**

Just as the lives of the collective public have shifted online, so have the systems that power and control the nation’s critical infrastructure. In the last 25 years, the move from analog to digital has made work easier and more efficient, according to Michael Assante, director of Industrial Control Systems, Supervisory Control and Data Acquisition Networks at the SANS Institute. Operators can control systems remotely and oversee various sites, while managers can run refineries and the electrical grid, and control temperatures in nuclear cooling towers, he notes (Assante 2014).

In the same way the everyday individual is at risk for hacking and cyberattacks from a range of actors, so are the systems for the nation’s critical infrastructure. National leaders and computer experts warn that it is not a matter of *if*, but *when* a major
cyberattack occurs (Rainie, Anderson and Connolly 2014). The U.S. government has acknowledged the severity of the threat. In February 2013 President Barack Obama signed an executive order for Improving Critical Infrastructure and Cybersecurity (White House 2016).

Connectivity keeps the nation’s lights on, the water flowing, machines running, and the systems operating in the military and national security arenas. A cyberattack that sabotages the power grids, transportation, gas or chemical plants, food infrastructure, hospitals, or communication systems, to name a few, could have devastating impacts. It could directly or indirectly result in loss of life, while causing calamity, and spreading widespread terror and fear. Imagine a dam bursting open, airplanes and public transportation impacted, controls at pipelines and bridges taken over by terrorists, chaos on the roads without stop lights, commerce impacted, financial institutions crippled, cash machines dead, water or food supplies tainted, supermarkets forced to close, or cities plunged into darkness. Vulnerable populations would be at risk; looting and a breakdown in law and order could add to the chaos and further exacerbate the disaster.

President Obama described the cyber threat as one of the gravest national security dangers (White House 2014). U.S. national and economic security depend on the nation's critical infrastructure operating in the face of such threats, the president said in the 2013 Executive Order, “Improving Critical Infrastructure Cybersecurity.” It is a national imperative to make sure these networks are protected, the president said (White House 2013).
Then-U.S. Defense Secretary Leon Panetta warned in 2012 of the possibility of a catastrophic event in which terrorists strike the nation’s critical infrastructure. Foreign cyber actors are probing America’s critical infrastructure networks, and targeting the nation’s computer control systems that operate chemical, electricity, water and transportation, according to Panetta.

“We know of specific instances where intruders have successfully gained access to these control systems. We also know that they are seeking to create advanced tools to attack these systems and cause panic and destruction and even the loss of life,” he said at a New York event for business executives in national security. He said terrorists could gain control of the switches, and perhaps in conjunction with a physical attack, contaminate water supplies, shut down the power grid across large parts of the country, or seek to harm critical military systems and communication networks. “The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability,” Panetta warned (Panetta 2012).

The consequences to national security underscore the importance of changing the cyber culture, especially since the government is not responsible for the systems that keep the country running. The majority of critical infrastructure operations in the United States are operated through private enterprises, with nearly 70 percent of the nation’s homes powered through private utilities (Cardwell 2013). Public water utilities serve about 80 percent of the U.S. population (Little 2012).
Flippant attitudes and disregard for cybersecurity are how problems could arise, perhaps with technicians and engineers who run the utilities taking for granted measures to protect their networks. Just as an individual might be nonchalant about protecting personal computers or employing simple safeguards, a worker at a small utility might think, “Why would we have to be so uptight about cybersecurity? Who would want to attack our power plant in the middle of nowhere?” In the same manner in which the retailer Target was allegedly breached, a phishing attack on a small network could be used as a “back door” to gain access to a larger system. But an attack on any utility or any target of national significance could not only cause damage but also strike terror in that population and larger populace, leaving citizens fearfully wondering, “What’s next?” The elderly or those with health conditions could face catastrophic consequences in the event of a power disruption.

The government has identified infrastructure systems that used default or weak passwords, no passwords, or the same passwords for various systems. In addition, viruses have been introduced into systems after USB drives or other external media have been plugged into networks. The Department of Homeland Security’s Industrial Control Systems Cybersecurity Emergency Response Team, or ICS-CERT, assists government and private entities and shares the information in an effort to prevent cyberattacks against critical infrastructure (Department of Homeland Security 2016).

ICS-CERT reported that two researchers with the private firm InfraCritical used readily available tools and located IP addresses of critical infrastructure devices. Some of the logon passwords were weak, default or non-existent. DHS worked in identifying
about 7,200 devices that were at risk and directly related to control systems. Someone with malicious intent could have easily used the readily available tools to find those Internet-facing devices, thereby opening the systems up for attack, it said. ICS-CERT reported an increasing trend in cyberattacks against energy and pipeline infrastructure around the world. It has been tracking threats and responding to intrusions into infrastructure such as oil and natural gas pipelines and electric companies at what it describes as an “alarming rate” (Department of Homeland Security 2012).

The critical infrastructure is a symbolic target, whether an attack causes significant damage or not. A Pew Research study found experts believe the nation’s infrastructure is at risk and cyberattacks are likely to increase. Attacking a power grid or other industrial control system is “asymmetrical” and “effective” (Rainie, Anderson and Connolly 2014).

While early control system breaches were random and infections may have been an accident, today industrial control systems are the object of targeted attacks by “skilled and persistent adversaries,” according to cyber expert Michael Assante. As the nation shifts to digital systems for its critical infrastructure, it sees improved efficiencies and productivity but also the dangers increase. The situation, he said, has severely exposed the nation’s “soft underbelly” (Assante 2014).
Breach in OPM, Other Government Networks

The U.S. government’s Office of Personnel Management said in June 2015 it discovered the background investigation records of current, former, and prospective federal employees and contractors had been stolen. The data included the Social Security numbers of 21.5 million people -- applicants as well as family members of applicants. In addition, some 5.6 million fingerprints were compromised. In addition, OPM said it discovered a separate breach in 2015 in which the personnel data of 4.2 million current and former federal employees was stolen. That information included the full name, date of birth, home address, and Social Security numbers of the personnel. (Office of Personnel Management 2016). OPM has not said how the massive breaches occurred.

Federal workers expressed outrage not just because their data was breached, but that the information of their family was compromised, and that the federal government has not indicated how the attack happened or who was possibly behind it.

OPM is not the only government target that has been breached. The White House, State Department, and the National Oceanic and Atmospheric Administration have seen their websites and networks intruded into by cyber attackers (Storm 2014). In addition, the Department of Defense’s Office of the Chairman of the Joint Chiefs of Staff was forced to take its unclassified email system offline in 2015 after a spear phishing attack allowed cyber intruders to enter, according to news reports. The spear phishing attack was reportedly quite sophisticated with characteristics that have officials probing whether Russia was behind the breach (Starr 2015). According to a news report, the attackers could see unclassified emails of the Joint Staff. The email system was taken offline for 10
days, affecting thousands of employees (Karambelas 2016). The head of U.S. Cyber Command and the National Security Agency, Navy Adm. Michael Rogers, said the attack was a “different scheme and maneuver that I had not seen before” (Paletta 2015).

As this chapter outlined, the nation is connected in virtually every aspect of society, from businesses, banking, social interactions, infrastructure to national security. Consequently, with the connectively comes the collective vulnerability and complex challenges posed by cyber threats.

The Federal Bureau of Investigation leads the national effort to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud, according to its Cyber Crime website. “We are building our lives around our wired and wireless networks,” it said. “The question is, are we ready to work together to defend them” (Federal Bureau of Investigation 2016)?

The answer must be a resounding YES.
CHAPTER 2
U.S. GOVERNMENT AND MILITARY

There is no relenting in the cyber war that happens every day against government targets. Networks are bombarded with cyberattacks, with attempts at breaching the fortified systems growing more and more sophisticated (Paletta 2015). The threats against U.S. critical infrastructure and the economy are constant (Department of Homeland Security 2014). With the United States relying so heavily on connectivity, officials have warned just how damaging an attack could be. Leaders at all levels, all the way to the president of the United States, have repeatedly voiced concerns about the possible impacts a cyberattack could have on the nation.

U.S. and Adversaries: A Level Playing Field

In 2015, several months before retiring as the highest-ranking U.S. military officer, the then-chairman of the Joint Chiefs of Staff, Army Gen. Martin E. Dempsey, shared his serious concerns about the impact of cyber terrorists. "As the senior military officer of the most powerful military on the planet, I like to have the playing field tilted to my advantage," he said, in an interview in Rome. “I'd like the enemy to play uphill and us to play downhill, and in cyber, it's pretty level. There are actors out there who can compete with us on literally on a level playing field, and I don't like that.”

Since the U.S. military depends on commercial networks, the strongest military cyber defense still could be threatened by a weak link elsewhere, Dempsey said. "We have authorities and capabilities that allow us to do a pretty good job of defending ourselves," he added. "The vulnerability of the rest of America is a vulnerability of ours,
and that's what we have to reconcile." He said what is needed is legislation on cyber to allow information sharing between the government and the private sector while safeguarding civil liberties. "We haven't done enough -- that's just not internal to the military," Dempsey said. “We haven’t done enough as a nation" (Ferdinando, Department of Defense 2015).

This is indeed a great paradox. Despite being unequivocally the superpower in the physical realm, the balance of power in the cyber realm is a vastly different scenario. On land, in the sea and in the air, the United States military is a fighting force of unmatched power, boasting the world’s most sophisticated equipment and technology supported by a highly trained fighting force. The U.S. is ranked the most powerful conventional military power in the world, with its defense spending far outpacing that of any other nation (Global Firepower 2016). For fiscal year 2017, the U.S. defense budget request totaled $582.7 billion -- $523.9 billion in the base budget and $58.8 billion in the overseas contingency operations fund (Garamone 2016).

The Department of Defense’s budget request includes $6.7 billion in fiscal year 2017 for defensive and offensive cyberspace operations, capabilities, and cyber strategy (Department of Defense 2016). The overall federal budget includes more than $19 billion for cybersecurity, more than a one-third increase from the previous budget plan, President Obama pointed out. He said the fiscal year 2017 federal budget plan includes modernizing federal IT by replacing and retiring outdated systems that are vulnerable to attack (White House 2016).
In 2009, the secretary of defense directed the commander of U.S. Strategic Command to establish the U.S. Cyber Command; full operational capability was reached in late 2010 (U.S. Strategic Command 2016). Cybercom, the fifth combatant command, defends Department of Defense networks, helps other federal agencies and provides cyber capabilities for defending the nation. It also provides cyber warfighting capabilities, as it is doing now in the fight against Islamic state terrorists in Syria and Iraq (Department of Defense 2016).

In comparison to the government’s cyber budget, hackers would need to spend very little to stage an attack and do harm to federal networks, according to the chief information officer for the Department of Defense, Terry Halvorsen (Ferdinando, Department of Defense 2015). Anonymous and behind a keyboard, hackers could be at various locations throughout the world working in tandem. Malicious software, including viruses, Trojan horses, worms, keystroke loggers, and spyware, could be stealing data, sabotaging systems, seeking further vulnerabilities and running amok.

A cyberattack could leave the nation reeling. President Obama’s Comprehensive National Cybersecurity Initiative describes the cyber threat as “one of the most serious economic and national security challenges we face as a nation.” To underscore the complexity of the issue, the White House acknowledges that “we as a government or as a country are not adequately prepared to counter” the threat (White House 2016).
Cyber Component in Current Military Operations

In the 2015 DoD Cyber Strategy, Secretary of Defense Ashton Carter said state and non-state actors are planning “disruptive and destructive” cyberattacks on the nation’s critical infrastructure. Adversaries are seeking to steal U.S intellectual property, including secrets related to technological advancements and the military, he said. Attackers could sabotage electronic health records, target an industrial control system of a utility, and otherwise be a significant risk to the U.S. economy and national security, he said. “The increased use of cyberattacks as a political instrument reflects a dangerous trend in international relations,” Carter stated.

Vulnerable data systems present state and non-state actors with what Carter described as an “enticing opportunity to strike the United States and its interests.” It is assumed that during a conflict, the adversary will seek to target “U.S. or allied critical infrastructure and military networks to gain a strategic advantage,” the defense secretary said (Department of Defense 2015).

He outlined the problem this way:

We are vulnerable in this wired world. Today our reliance on the confidentiality, availability, and integrity of data stands in stark contrast to the inadequacy of our cybersecurity. The Internet was not originally designed with security in mind, but as an open system to allow scientists and researchers to send data to one another quickly. Without strong investments in cybersecurity and cyber defenses, data systems remain open and susceptible to rudimentary and dangerous forms of exploitation and attack. Malicious actors use cyberspace to steal data and intellectual property for their own economic or political goals. And an actor in one region of the globe can use cyber capabilities to strike directly at a network thousands of miles away, destroying data, disrupting businesses, or shutting off critical systems (Carter 2015).
Carter said there is no distinction between a physical attack against the United States and one in cyberspace. “I don't care if you do it with a keyboard or a bomb, an attack on the country is an attack on the country,” he said. “It's a serious business.” Other nations are still working out their cyber policies and their position on cyber in national and foreign policy, Carter said. As far as he is concerned, he said, in his job of protecting the defense networks and the nation, “an attack is an attack” (Carter 2016).

Cybercom is deploying “cyber tools” in the current military efforts against Islamic state terrorists in Syria and Iraq, Carter said. Those efforts are aimed at disrupting the terrorists’ ability to operate and communicate over the virtual battlefield, he said. “We can't allow them to freely command and control forces that are enemy forces, so it's just like any other war. We have to attack their command-and-control,” according to Carter.

The offensive cyber efforts are being directed particularly at Syria, in an effort to cause them to lose confidence in their networks, and interrupt operations and their ability to control the population and the economy, Carter said. Using cyber against an adversary is an important new capability, Carter said. "This is something that's new in this war, not something you would have seen back in the Gulf War. It is an important use of our Cyber Command -- and the reason that Cyber Command was established in the first place" (Ferdinando, Department of Defense 2016).

In 2012, then-Secretary of Defense Panetta described cyberspace as the “battlefield of the future.” Adversaries of the United States are developing the capability to go after the nation’s power grid and financial and government systems to “virtually
paralyze this country,” he said. But the greater danger, he said, goes beyond criminal activities. An attack could be catastrophic, he said. “A cyberattack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attack on 9/11” (Panetta 2012).

To illustrate the problem: trained, sophisticated hackers have already launched targeted attacks against individuals, institutions and communities. Imagine what cyber terrorists could do if they launched a coordinated attack on critical infrastructure systems.

A cyberattack against Saudi Arabia’s state oil company Aramco in 2012 did widespread damage, according to Panetta. He described the virus called Shamoon as “very sophisticated” and said it included a “wiper” that was coded to self-execute. The malware replaced crucial systems files with an image of a burning American flag and overwrote the data on the machine, Panetta explained. The malware ended up rendering useless 30,000 computers, he said (Panetta 2012). The New York Times said U.S. intelligence officials believe Iran was behind the attack. The report cites security experts as saying an insider with privileged access to the network was involved in the attack, which the report said could have been launched through a USB memory stick that was inserted into a networked computer (Perlroth, 2012).

**North Korea and Devastating Sony Hack**

In highlighting the cyber threat, security experts and national leaders point to the crippling attack in 2014 by North Korea against Sony Pictures Entertainment. The attack was likely in retaliation for the movie “The Interview,” a comedy in which two American journalists are sent to North Korea to assassinate the country’s dictator, Kim Jong-un.
The depiction of Kim Jong-un enraged Pyongyang and North Korea allegedly took action, unleashing the wrath of its cyber army in a sustained attack that threatened Sony employees and the public, destroyed data, stole and revealed trade secrets, and released sensitive information to the Internet (Elkind 2015).

In addition to the sheer impact of the breach, another worrisome part of the intrusion is this: the attack was so sophisticated that 90 percent of Internet defenses in private industry might not have detected it, according to Joseph Demarest, the assistant director of the Federal Bureau of Investigation’s cyber division. At a Senate hearing, he said the malware would likely have challenged even a state government (Gibbs 2014).

In the hack, Sony employees logged on to the network and saw a ferocious skeleton above the images of two Sony executives, as threats scrolled underneath, according to an in-depth investigative report by Peter Elkind in Fortune. The malware wiped clean data on thousands of personal computers and servers, and then with a special deleting algorithm, overwrote the data on the computers, leaving the computers as essentially dead shells, according to Elkind. There was more to come. In the ensuing weeks, hackers released a trove of confidential information, including Social Security numbers of thousands of employees, unfinished movie scripts and unreleased movies (Elkind 2015).

The hackers also threatened the American public with 9/11-style attacks on theater-goers. A group claiming to be responsible for the hack warned “how bitter fate those who seek fun in terror should be doomed to … The world will be full of fear. Remember the 11th of September 2001. We recommend you to keep yourself distant
from the places at that time. (If your house is nearby, you’d better leave)” (Peterson 2014). Sony pulled the initial release of the movie, but eventually opened it to a limited number of theaters (Elkind 2015).

The incident left the company in shock, the nation concerned and the federal government outraged. In response to the attack, the Obama administration slapped new sanctions on North Korea for that country’s “ongoing provocative, destabilizing, and repressive actions and policies particularly its destructive and coercive cyberattack on Sony Pictures Entertainment,” according to the White House statement on the executive order on the additional sanctions (White House 2015).

Defense Secretary Ash Carter slammed North Korea for the attack, saying Pyongyang accompanied the hack with “coercion, intimidation, and the threat of terrorism.” He described the intrusion as “one of the most destructive cyberattacks on a U.S. entity to date.” It further spurs the national dialogue on cybersecurity and the need for improved defenses, he said (Department of Defense 2015).

**Defense, Intelligence Officials on Vexing Threat**

The Department of Defense’s roughly 7 million networked devices and 15,000 network enclaves, including sophisticated weapons systems, are protected by U.S. Cyber Command. The command’s mission is three-fold mission. According to Defense Secretary Carter, the mission includes: to defend DoD networks and weapon systems; help other federal agencies defend the nation against cyberattacks from abroad, especially if they would cause loss of life, property destruction, or significant foreign policy and economic consequences; and provide offensive cyber options that can be used in a
conflict, like currently is the case in Iraq and Syria. The investments for those three missions total $35 billion over the next five years, he said in a speech in San Francisco (Department of Defense 2016).

The commander of Cybercom, Adm. Michael Rogers, detailed to Congress in 2015 the challenges in improving the military’s cybersecurity posture in uncertain threat conditions. Protecting the systems is critical, especially considering the overlap and dependency between real-life national security and military operations with the networked realm, he told lawmakers.

“Cyberspace is more than a challenging environment; it is now part of virtually everything we in the U.S. military do in all domains of the battlespace and each of our lines of effort,” Rogers told the U.S. Senate Armed Services Committee. “There is hardly any meaningful distinction to be made now between events in cyberspace and events in the physical world, as they are so tightly linked.” Adversaries are staking out the nation’s vulnerabilities and leaving their “cyber fingerprint,” he said. In addition, other countries are developing capabilities and attaining accesses for potential hostilities, “perhaps with the idea of enhancing deterrence or as a beachhead for future cyber sabotage,” Rogers warned.

He said private security researchers have reported numerous malware finds in the industrial control systems of energy sector organizations. “We believe potential adversaries might be leaving cyber fingerprints on our critical infrastructure partly to convey a message that our homeland is at risk if tensions ever escalate toward military
conflict,” he said. While Rogers did not reveal which countries, he did say there are “multiple” nations investing in cyber warfare capabilities (Rogers 2015).

In a previous appearance before Congress, Rogers said China and “one or two” other countries have the capability to inflict serious harm on the nation’s electric grid and other critical systems. “All of that leads me to believe it is only a matter of when, not if, we are going to see something dramatic,” he told the House (Select) Intelligence Committee (Rogers, National Security Agency 2014).

Cyber is on the minds of all the military services. Each has their own cyber unit -- Army Cyber, U.S. Navy Fleet Cyber, Marine Forces Cyber, Air Force Cyber, and Coast Guard Cyber Command. The branches carry out their own training and participate in joint exercises based on cyberattack scenarios (U.S. Cyber Command 2015).

A hacker can spend a "fairly small sum of money and cause us to spend quite a bit of money," the Department of Defense’s Chief Information Officer Terry Halvorsen told a cybersecurity conference in Washington. "Right now, we are on the wrong side of that cyber-economic curve," he said. A strong cyber culture and discipline would raise the cost of entry, thus thwarting some of the smaller players, according to his assessment. “Today almost anybody with a laptop, a little bit of sense and a little bit of money can go on the Internet, download some tools and cause a problem," he said (Ferdinando, Department of Defense 2015).

Still, even the most fortified defenses are only as strong as the weakest link. We have already seen what can happen with an infection -- personal data gets stolen,
websites go down and financial information is compromised. But what could happen if a system gets hijacked, its controls taken over?

**Worldwide Threat Assessment**

The director of National Intelligence, James R. Clapper, leant his voice to the chorus of administration officials expressing concern about the cyber threat. Testifying to Congress about the 2016 Worldwide Threat Assessment of the U.S. Intelligence Community, Clapper noted the “consequences of innovation and increased reliance on information technology in the next few years on both our society’s way of life in general and how we in the intelligence community specifically perform our mission will probably be far greater in scope and impact than ever.”

Russia has increased its “assertiveness” in cyber intrusions against the United States, Clapper said. Other cyber threats come from China, North Korea, Iran and non-state actors, he said. Cyber is quite unlike conventional warfare, where if you were to attack the United States physically, there would most certainly be a response. There is no shortage of targets for cyber attackers either. Clapper points out that adversaries are “emboldened” and “undeterred” in conducting reconnaissance, espionage, and even attacks in cyberspace because of the “relatively low costs of entry, the perceived payoff, and the lack of significant consequences.” Russia and China are among those who “view offensive cyber capabilities as an important geostrategic tool and will almost certainly continue developing them while simultaneously discussing normative frameworks to restrict such use,” he said (Clapper 2016).
As cyber is the new frontier of warfare, the United States is seeking to establish a set of international principles dealing with cyber military operations, akin to rules of engagement in traditional warfare, like prohibiting attacks on the networks of protected sites such as hospitals. President Obama hosted his Chinese counterpart, President Xi Jingping, for a state visit in September 2015, with the leaders agreeing to deepen cooperation in cybersecurity (White House 2015).

Defense officials say the next conflict will likely have a major cyber component in which adversaries such as a nation state or terrorists use cyber warfare against the United States. Army Col. Carmine Cicalese, a cyber expert with Army Operations Center, G-3/5/7, described how hackers are constantly looking for vulnerabilities in the Army’s networks and how their attacks are increasing in complexity. The Army, he explained in an interview, relies on networks for a host of critical tasks, from using sophisticated weapon systems to executing wartime operations. An adversary who compromises the network could compromise the mission. “That threat is out there; it’s every day,” he said. “We're dependent on our networks. We're dependent on our communication systems, so that's a vulnerability and a non-lethal vulnerability, at that, where they could have an effect.” In the next war, "someone's screens are going to go blank,” he said. “We don't want them to be ours” (Ferdinando 2014).

**Turning to the Advice of ‘Ethical Hackers’**

Realizing the formidable adversaries out there in cyberspace, the government acknowledges it needs to tap into the expertise of those who know best about hacking – the hackers themselves. Each year, thousands of hackers and cybersecurity insiders
gather for the Black Hat and Def Con hacker conferences in Las Vegas. Then-NSA and Cybercom director Army Gen. Keith Alexander had addressed both meetings. In 2013, he told the Black Hat gathering that the hackers in the room are the “technical foundation for our world’s communications.” The issue, however, is how to best defend the nation while safeguarding civil liberties, he said. Despite being jeered and heckled by audience members for alleged NSA activities, Alexander acknowledged the government needs help. “The reason I’m here is because you may have some ideas of how we can do it better. We need to hear those ideas,” Alexander said (K. Alexander 2013).

In employing a practice used in the private sector, the Department of Defense launched a cyber bug bounty program. The “Hack the Pentagon” program, which launches in April 2016, is controlled and limited in duration, according to the Pentagon. In the carefully vetted exercise ethical, or “white hat,” hackers will be able to search publicly facing Department of Defense websites for vulnerabilities, with possible “monetary awards and other recognition” for their discoveries, according to a Pentagon statement. Internal networks and sensitive mission-facing program are off limits, the Pentagon said. The program, according to the Department of Defense, is the first of its kind in the federal government. “I am always challenging our people to think outside the five-sided box that is the Pentagon,” Defense Secretary Carter said in the announcement. “Inviting responsible hackers to test our cybersecurity certainly meets that test. I am confident this innovative initiative will strengthen our digital defenses and ultimately enhance our national security” (Department of Defense 2016).
The Hack the Pentagon program is a way to get the “good guys” involved, according to a Defense official. The department is not worried about criminals, or “black hat hackers,” taking part in the exercise. “Bad guys are not sitting there and thinking to themselves, ‘Oh wow, this is excellent, I’ve been waiting for the Department of Defense to do a bug bounty.’ They’re already there, attacking us every single day,” the Defense official said (Pellerin 2016).

Industry relies on “ethical” hackers to point out vulnerabilities. Private companies that already have bug bounty programs include Apple, AT&T, Facebook, Hewlett-Packard, Microsoft, Paypal, and Samsung, just to name a few. Crowdsourcing for vulnerabilities allows hackers, who must adhere to the rules of the program, to bring their varied expertise to the table and put a set fresh of eyes on a system, with monetary rewards or other incentives in helping the company patch its weaknesses (Bugcrowd 2016). In fact, Facebook said it has paid more than $4.3 million to more than 800 people around the world in its bug bounty program since it started it in 2011. Highlighting the expertise and interest around the world, in just 2015 alone, Facebook said it received more than 13,000 submissions, coming from more than 5,500 people in 127 countries (Facebook 2016).

**An Alarming Trend: Ransomware**

Cyber experts and federal authorities are warning users about another growing trend: hackers using ransomware to extort money from users. With this technique, hackers infiltrate a network and hold a computer, network or smartphone “hostage,” until the user pays a ransom to have the system unlocked. The victims usually pay in hard-to-
trace cyber currency called bitcoins (Finkle 2016). The FBI says anyone can be targeted, from an individual to a government agency.

Hollywood Presbyterian Medical Center in Los Angeles was a victim of such an attack in February 2016. The hospital said the cyberattack did not impact the delivery and quality of patient care (Stefanek 2016). However, several people told a local news station they were impacted by the hack and concerned about the situation, including family members caring for elderly loved ones. The medical center’s president and chief executive officer, Allen Stefanek, told NBC Los Angeles that investigators say the attack appeared to be random (Crouch 2016).

The medical center paid in bitcoins the equivalent of $17,000, Stefanek said. He said the malware used against the medical center “locks systems by encrypting files and demanding ransom to obtain the decryption key.” The medical center decided “in the best interest of restoring normal operations” it would pay the ransom, Stefanek said (Stefanek 2016).

Subsequently, the Los Angeles County Department of Health Services found itself a victim of ransomware and its access to its data blocked. The agency was able to isolate infected devices, according to the Los Angeles Times, and has not paid a ransom. A South Carolina school system in February 2016 paid attackers $8,600 to regain control of its system (Hiltzik 2016).

Apple users were targeted in March 2016 with the first known ransomware attack against Apple, according to a Reuters report. The infection was in an update to a popular program called Transmission, which is used for peer-to-peer data sharing, the report said.
Apple and Transmission quickly acted, but not before more than 6,000 users were infected. The Reuters report quotes security experts as saying hundreds of millions of dollars are paid to cyber criminals each year (Finkle 2016).

The amount extorted from individuals in a ransomware attack generally ranges from hundreds to thousands of dollars, according to the FBI. The ways that users can be infected include by clicking on infected sites, usually lured by an email or popup ad, or by downloading programs infected with the malware.

The ransomware highlights another disturbing development in the complex, ever-evolving cyber realm, once again showing how vulnerable we all are, and how readily criminals will steal from, coerce and victimize any target, whether a hospital, school, government entity or individual.
CHAPTER 3
NATIONAL VULNERABILITIES

The persistent threats from foreign cyber attackers are a real danger, so much so that they rise to the level of a national security concern, according to President Obama, in an executive order on April 1, 2015, that blocks the property of individuals outside the United States who engage in significant cyberattacks against the nation. The increasing “prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States,” he said. “I hereby declare a national emergency to deal with this threat” (White House 2015).

Cybersecurity breaches are an all too common occurrence; seemingly every day a new attack, data theft or other intrusion makes the news. The U.S. Cyber Command protects Department of Defense networks and works to guard other federal agencies from malicious activity; the FBI, Secret Service, and Department of Homeland Security are among the agencies that investigate cybercrimes. But it is still up to private industry to secure its own networks. As the case with Sony Pictures Entertainment, a private entity is no match for a sophisticated hacker, most especially a determined nation state.

Cyber intruders have already been accused of entering our nation’s critical systems. What will happen when the next generations of rogue elements breach our critical systems with the intent of doing harm, launching a terrorist attack, or
manipulating systems to harm civilians? This chapter will examine the threat and vulnerabilities of our critical infrastructure and national security networks.

**President Obama’s Plan for the Nation**

In February 2016, President Obama presented his Cybersecurity National Action Plan to the nation. The plan outlines new initiatives to safeguard against malicious cyber activity. Protecting the country, Obama noted, is no longer just about military might and a kinetic response. “It also requires us to bolster our security online,” he said. The latest network intrusions in the news indicate that “cyber threats pose a danger not only to our national security but also our financial security and the privacy of millions of Americans,” the president said. He described his plan as an aggressive effort that addresses both the short- and long-term strategy in cybersecurity. The government needs to play “catch-up,” he acknowledged, saying federal IT systems are seriously antiquated and at risk. His current budget proposal includes a $3.1 billion Information Technology Modernization Fund. “We have software in the federal government now where the software operator does not exist anymore, and yet we're expected to provide the kinds of service, security, and privacy to Americans based on these leaky systems -- so that's going to have to change” (White House 2016).

The situation of our national networks, as Obama outlined, is cause for great concern and raises many questions. The United States does a magnificent job in protecting itself militarily, sparing no expense it seems in the physical defense of our nation. The cyber field seems akin to the days of the Wild West, when criminals defiantly carried out their crimes and the law was racing to stay ahead.
Cyber: A ‘Serious and Significant Attack Vector’

In an interview with CBS 60 Minutes, CIA director John Brennan said there are safeguards to protect the nation from cyberattacks. But he acknowledged it is not an easy task; the threat is one of the concerns that “keeps me up at night.” And for good reason. As he described it, the cyber dimension is a “very serious and significant attack vector for our adversaries if they want to take down our infrastructure, if they want to create havoc in transportation systems, if they want to do great damage to our financial networks.”

Even though nation states have breached U.S. networks, they did not have the intent to sabotage or carry out actions that would harm systems or civilians, he said. However, adversaries that have that intent, think Islamic state terrorists or other terror or rogue groups, don’t have the capability, Brennan said, adding that otherwise they would have already been deploying those tools (CBS 2016).

In the 2016 Worldwide Threat Assessment, the director of National Intelligence, James Clapper, points out another vulnerability in the networks that have brought convenience to our lives: the manipulation of artificial intelligence that is used for autonomous decision making.

“As we have already seen, false data and unanticipated algorithm behaviors have caused significant fluctuations in the stock market because of the reliance on automated trading of financial instruments,” Clapper said. While systems that use artificial intelligence can have benefits, they are susceptible to a “range of disruptive and deceptive tactics that might be difficult to anticipate or quickly understand,” the DNI chief said. “Efforts to mislead or compromise automated systems might create or enable further
opportunities to disrupt or damage critical infrastructure or national security networks” (Clapper 2016).

**Threats from Nation States**

The United States is concerned about the increasing number of state and non-state actors that have cyber capability or are seeking ways to infiltrate important systems. Russia, China, North Korea and Iran make the list of nations the United States is concerned about, according to officials.

In a speech to Fordham University on “National Intelligence, North Korea, and the National Cyber Discussion,” Clapper outlined Russia’s “broad range of highly sophisticated technical and human intelligence capabilities” in its cyber arsenal. If the United States and Russia were enmeshed in a conflict, “some U.S. critical infrastructure networks will be at risk.” The threat from Russian hackers, he explained, is more sophisticated than that coming from China, North Korea or Iran.

Iran and North Korea are aggressive in going after U.S. networks, while China is focused on blatantly stealing business and technical secrets, Clapper said. China, he said, is “cleaning us out” and “robbing our industrial base blind” through vulnerabilities that can be easily fixed with a patch. “We know we’re supposed to do those simple things, and yet we don’t do them,” he said (Director of National Intelligence 2015).

China is alleged to be behind the hacking of the U.S. government’s Office of Personnel Management’s network and the theft of the background records of millions of current and former federal employees, including security clearance information. In an interview with *The New York Times*, James Lewis, a cybersecurity expert at the Center
for Strategic and International Studies, said the OPM cyberattack does not have the hallmarks of hackers just looking to profit off of the stolen data. Instead, he said, it appears the perpetrator is looking to mine data out of the millions of records. “They didn’t go to sell the data, which is what criminal groups usually do,” he is quoted as saying. “It’s biographic databases that really give an intelligence benefit -- and that get into an opponent’s skin.” Security clearance information includes that person’s foreign contacts, Lewis points out. He said that is a gold mine for a hacker who wants to see who from their country has contacts with Americans in government (David Sanger 2015).

The theft of the records of nearly 26 million people, including fingerprints and highly personal information, from the OPM system is a cause for tremendous alarm. What is the thief planning to do with that massive amount of information? The records give our adversaries a stunningly detailed picture of the composition of the federal workforce – the full identities of the workers, their home addresses, name of family members and contacts. While not every federal employee would be of interest to a foreign entity, think about the employees in high-level or top secret positions in nuclear and space programs, in the Department of Defense, White House, CIA, FBI, NSA, State Department and so forth. Through the records, the lives of agents in intelligence or other

---

1 The Office of Personnel Management announced separate incidents in 2015. According to the OPM website: “In June 2015, OPM discovered that the background investigation records of current, former, and prospective federal employees and contractors had been stolen. OPM and the interagency incident response team have concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases ... approximately 5.6 million (of the records) include fingerprints. ... Earlier in 2015, OPM discovered that the personnel data of 4.2 million current and former Federal government employees had been stolen. This means information such as full name, birth date, home address and Social Security numbers were affected.”
sensitive positions worldwide could be pieced together. Who is to say this information won’t be sold or passed to an adversary? In the wrong hands, this data could put lives and national security missions in jeopardy.

It is also troubling because the inspector general at OPM had warned about the vulnerabilities, according to The New York Times. The report quotes a U.S. official as saying “The mystery here is not how they got cleaned out by the Chinese. The mystery is what took the Chinese so long” (David Sanger 2015). In another disservice to the American people, Donna Seymour, the chief information officer for OPM, resigned days before she was to testify to the House Committee on Oversight and Government Reform. The hearing was canceled; the American people never got to hear from the person who was in charge of the systems and who could explain what went wrong. That testimony could have given those impacted in the theft the answers they deserve, while providing insights to government and private industry about ways to avoid such a breach and how to move forward (Yoder 2016).

The list of purported Chinese hacks goes on. China is also suspected of being behind an iCloud hack in 2014 that potentially obtained passwords, messages, photos and contacts (Reuters 2014). It is also allegedly behind the 2014 break-in of the United States Postal Service network in which the home addresses, Social Security numbers and employment information for all employees were stolen, according to the Washington Post. The news report went on to say that customers’ credit card information was not affected, leaving experts to speculate that the hackers may have thought the U.S. postal service was like China’s, which keeps detailed records on its citizens. Afterwards,
Postmaster General Patrick Donahoe said it is “an unfortunate fact of life these days that every organization connected to the Internet is a constant target for cyber intrusion activity” (Nakashima 2014).

China was allegedly being cyberattacks that stole design plans for more than two dozen major weapons systems, according to a Washington Post report citing a private Pentagon document. Those plans included the F-35 Joint Strike Fighter (Nakashima, Washington Post 2013). China later debuted its alleged copycat aircraft, the J-31 fighter (Weisgerber 2015). According to a CNN report, documents leaked by former NSA contractor Edward Snowden indicate that U.S. authorities believe China stole "many terabytes of data" related to the F-35 fighter jet (Boykoff 2015).

Separately, five members of China’s military were indicted in U.S. District Court in the Western District of Pennsylvania in May 2014 for alleged hacking, marking the first time in the United States that charges have been brought against a state actor for this type of allegation, according to then-Attorney General Eric Holder. The five members of China’s People’s Liberation Army are on the FBI’s “Cyber’s Most Wanted” list. They were charged on 31 counts, including aggravated identity theft, economic espionage and theft of trade secrets in the U.S. nuclear power, metals and solar products industries.² According to the FBI, the men infiltrated the computer networks of six American firms and stole proprietary information to include email exchanges among employees and trade secrets for nuclear plant designs (FBI 2016).

² The full indictment can be found at the Department of Justice’s website at https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf
“The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response,” Holder said. The Chinese government has “blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries,” according to FBI Director James Comey (Department of Justice 2014).

Cyber counterterrorism expert Richard Clarke puts the situation in perspective: hacking is a vastly improved way for nation states to do espionage. Instead of being on the ground and putting your life at risk for a limited number of documents over the years that may or may not be reliable, you can get an unimaginable amount of data straight from the source. Noting how the F-35 hack was alleged to have netted “many terabytes,” Clarke explains how just one terabyte of information is equivalent to the amount of information in more than 3,000 encyclopedias. To physically move that many documents, one would need a small moving van and a forklift, he said. Could you imagine driving a van up to a government building in the hopes of “sneaking out” that same amount? For comparison, Clarke noted how convicted spy Robert Hanssen, who worked for the FBI and passed information to Russian and Soviet agents, passed a minuscule amount in comparison to the F-35 hack (Clarke 2010, 234). After his arrest in 2001, the FBI said Hanssen provided some than 6,000 pages of information to Moscow over two decades of spying (FBI 2001). Again, it took two decades to pass that very limited amount of paperwork. China allegedly obtained a small truckload of documents in one cyberattack.

The breadth and depth of alleged China hacking on U.S. systems is stunning. The alleged hacking can be seen as a long-term strategy to build an intelligence profile and
give China, albeit unfair and through theft, a competitive edge on the world stage. I seriously question what it is doing with the personal data of millions of government employees; in addition, I have many concerns as well about the threat from Russia.

Defense officials have accused Russia of penetrating U.S. government and private sector networks. Russia is allegedly behind a “Trojan Horse” malware program that infiltrated the systems for critical infrastructure and could have caused an economic catastrophe, according to an ABC News report that cites a Department of Homeland Security bulletin. The bulletin in 2013 said the malware was in place for at least two years, but that it made no attempts to harm the critical systems. The news report said DHS sources think the Russians may have infiltrated the systems as a threat or to have a strategic placement inside critical infrastructure in the event of a conflict with the United States (Cloherty and Thomas 2014).

Russia has deployed the use of cyber tools in times of conflict. Clarke explains in his book how the Georgian government was the victim of DDoS attacks and its government website defaced during its war with Russia in 2008. Through a barrage of attacks, Georgians were not able to access news sites to see what was going on during this critical time. Online banking operations, credit card systems and mobile phone operations went down as well, Clarke said. “At their peak, DDoS attacks were coming from six different botnets using both computers commandeered from unsuspecting Internet users and from volunteers who downloaded hacker software from several anti-Georgia websites,” he said (Clarke 2010, 20).
In addition, in December 2015, during a frigid Ukrainian winter, power went out in a wide area of Ukraine. Ukrainian officials blame Russia for the outage in a cyberattack, as part of its conflict with Ukraine over Crimea, according to Jose Pagliery with CNN Money. In addition, phone lines were jammed so customers could not report the outage, the reporter said (Pagliery 2016). Targeting the population and civilian infrastructure are against the internationally accepted rules of engagement in conflict. Such behavior is extremely troubling.

Russia is also allegedly behind infiltrations of the State Department and White House networks. Investigators believe the cyber assailants got access to the White House following a successful phishing attempt through the State Department, according to CNN. The hackers allegedly accessed emails and the daily schedule of President Obama. While that information was not classified, it did contain sensitive information not released to the public, including the movements and daily appointments of the president (Perez 2015).

According to Clarke, Russia in 2008 launched malware that hacked the government’s unclassified NIPRNET. From there, it searched for thumb drives and when it found them, it downloaded itself to those external drives. When those external drives were used in the classified SIPRNET computers, the malware then jumped to the classified system, Clarke said. “Within hours, the spyware had infected thousands of secret-level U.S. military computers in Afghanistan, Iraq, Qatar, and elsewhere in the Central Command,” he said (Clarke 2010, 172).
While not alleged to be a government official, on the FBI’s Cyber Most Wanted list is a Russian man who is believed to reside in Russia. The FBI describes Evgeniy Mikhailovich Bogachev as “one of the FBI’s most wanted – and most prolific – cyber criminals.” The FBI is offering a reward up to $3 million for information that leads to his arrest and/or conviction. He is alleged to have been the administrator of the GameOver Zeus botnet believed to be responsible for the theft of more than $100 million from businesses and consumers in the United States and around the world, according to the FBI. The agency describes GameOver Zeus as an extremely sophisticated type of malware that stole banking and other credentials, or created false webpages where victims would enter their banking information (FBI 2016).

Looking at the threats from other nation states, U.S. officials accuse Iran of hacking U.S. and international firms and stealing sensitive information for at least two years (Winter 2014). In addition, the United States accused Iran of intruding into unclassified Navy computers in 2013. The Wall Street Journal cites an official as saying the breach was "enabled by vulnerabilities that were discovered and exploited in older systems and network architecture." According to the news report, the contract with Hewlett-Packard Co. for the database did not require the contractor to provide security for some databases, so security was not regularly maintained. This gave an easy way for hackers to enter the system and then travel deep within the Navy Marine Corps Intranet network, according to sources cited by The Wall Street Journal. The sources are quoted as saying no classified information or emails were reached. This intrusion, according to the report, is the only known time that Iran has broken into U.S. military networks (S.
Gorman 2014). Also of serious concern, Iranian hackers are alleged to have infiltrated the controls of a dam in Rye, New York, according to a separate report in *The Wall Street Journal*, citing former and current U.S. officials (Yadron 2015).

North Korea is said to have its “Bureau 121” unit of elite hackers, according to a man who said he trained with them before fleeing the repressive, isolated nation. In an interview with the Reuters news agency, defector Jang Se-yul said there are 1,800 hackers in the unit. He said members of the North Korean hacking team were handpicked by the regime and are considered the elite in the reclusive nation (Ju-Min Park 2014).

North Korea has been aggressive and provocative with its cyber intrusions, according to the director of National Intelligence, James Clapper. Pyongyang is making a lot of noise and wants to be recognized as a leader on the world stage, he said. Cyber is a powerful new realm for the North Koreans, he said, adding that they “can exert maximum influence at minimum cost.” The hacking of Sony Pictures Entertainment shows they have the capabilities and can get recognized internationally for their cyber exploits, Clapper said. “That’s why we have to push back. If they get global recognition at a low cost with no consequence, they’ll do it again, and keep doing it again until we push back, and of course others will follow suit” (Director of National Intelligence 2015).

**The Business of Hacking**

Of course, the threat against the United States doesn’t stop at a few nation states. Criminals and other saboteurs are on the hunt as well for any vulnerability, whether in a targeted strike or random attack. Each day, an average of nearly 1 million pieces of malware are released (Harrison 2015). Selling malicious code or stolen data is big
business; breached credit card information and personal data is for sale online. There are sites where people can buy malware, or even order services such as having someone carry out a denial of service attack on a competitor (ABC News 2016).

The people who write the malicious codes are not just ordinary crooks, according to Larry Ponemon, founder and chairman of the Ponemon Institute. His Michigan-based group researches data protection and information security policies. “The people building today’s hacking tools have Ph.D.s in math and physics,” Poneman said in an interview with Forbes. Why do they do it? It is a lucrative criminal trade for those who take part in the schemes. Hacking tools can go for “tens of thousands of dollars at a minimum,” Poneman said. While the cost for the malware might seem high, he said, the “ill-gotten gains can be great” (Banham 2015).

There are many tricks cyber attackers use to try to reach the inbox of someone who will open the attachment or click on the link. Emails from foreign locations might be routed directly to junk or spam folders. However, if it appears the email originated inside the United States, then it might have a chance making it into the victim’s email account.

Hacking is not just a one-way activity with U.S. getting pummeled and adversaries infiltrating our networks. The United States has sophisticated cyber capabilities and is actively seeking to recruit both military and civilian personnel to work in the cyber corps. According to a news report citing documents released in the Snowden breach, the National Security Agency hacked into Chinese telecommunications firm Huawei Technologies. The NSA allegedly noted that many of its “targets” communicate over Huawei products and it wanted to make sure it knew how to “exploit these products”
and “ensure that we retain access to these communication lines,” according to The Washington Post (Wan 2014). The Snowden documents allegedly revealed “extraordinary amounts of detail about clandestine efforts to spy on systems around the world,” including on telephone conversations in the United States and on technology companies including Google, Facebook and Apple (Harris 2014). The scale of the spying even surprised hackers, according to Shane Harris in his book @War: The Rise of the Military-Internet Complex (Harris 2014, 67-68).

The U.S. is widely thought to be behind the Stuxnet computer worm that targeted Iran’s nuclear program (Sanger 2012). The Stuxnet malware is described as the “world’s first digital weapon,” according to WIRED reporter Kim Zetter, in her book Countdown to Zero Day. The worm targeted Iran’s Natanz nuclear facility and was aimed at sabotaging or at least severely delaying Iran’s nuclear program (Zetter 2014). Stuxnet disrupted the Iranian nuclear program for years before its detection. There were two versions of it. The second part was so advanced it was like the “work of an in-group of top-notch industrial control system security experts and coders who lived in an exotic ecosystem quite remote from standard IT security,” according to an investigative report in Foreign Policy by Ralph Langner. It was “equipped with a wealth of exploits that hackers can only dream about,” Langer said (Langner 2013). ³

Using Stuxnet as an example, pretty much nothing can stop expert hackers. According to Richard Clarke, “The really good cyber hackers, including the best

---

³ For further details on Stuxnet, read the in-depth Foreign Policy report by Ralp Langner, which can be found here: [http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/](http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/)
government teams from countries such as the U.S. and Russia, are seldom stumped when trying to penetrate a network, even if its operators think the network is not connected in any way to the public Internet.” Their greatest trick, he said, is to leave no trace, except when they want you to know they were there (Clarke 2010, 127).

**Threats from the Inside**

In addition to external dangers, our networks are also threatened in the inside by the very people entrusted with their keep. Think about a disgruntled employee, employee-turned-spy, or someone looking to make a political point or perhaps even just to profit from the data. The Edward Snowden case revealed details about NSA activities and ignited fierce debate in the United States and abroad about surveillance methods. But the leak also revealed that our networks and the sensitive information they contain are vulnerable from the inside. What would happen if someone in the inside wanted to sabotage our networks or cause harm to civilians?

In another high-profile case, Army Pvt. Bradley (Chelsea) Manning was sentenced to 35 years in prison in 2013 for leaking a trove of documents to WikiLeaks. Those 700,000 files included thousands of diplomatic cables, a video from a 2007 U.S. helicopter attack in Baghdad in which journalists and other civilians were killed, information on Guantanamo detainees, and reports from the wars in Iraq and Afghanistan, according to *The New York Times* (Charlie Savage 2013).

Manning, a low-level intelligence analyst in Iraq, was sent to the warzone with a Top Secret clearance despite his chain of command questioning whether he was mentally fit for the deployment, according to feature story on Manning in *New York Magazine.*
Manning displayed serious red flags including aggression, anger, and unpredictable behavior; he was the target of bullying and had emotional struggles with his gender identity, writer Steve Fishman said in the magazine feature. All those issues were known before deployment. However, the desperate need for analysts in Iraq trumped any concerns about his personal behavior. Fishman said that during the deployment, Manning’s master sergeant even removed the bolt from his weapon due to concerns about his behavior. Manning said information security was so low that he easily accessed the sensitive documents and copied them to a CD, Fishman reported. The only reason he was caught at the time was because he talked about his exploits in an online chat with a former hacker who turned Manning in (Fishman 2011). The Manning case raises many questions, including: If he showed mental distress and emotional problems before deployment, why was he deployed in the first place? Were there no safeguards to putting external media in the computers? How could he so easily access material he had no business being in, such as the State Department cables?

While authorities were able to quickly apprehend Manning once he was identified as the leaker, other cases are not so clear cut. In fact, Snowden is reportedly in Russia, while other cyber criminals are far and wide in any part of the world. It can be extremely hard to catch a hacker, as cybercrime knows no geographical borders and takes place in the vast anonymous world of cyberspace. Assaults can be in any part of the world pummeling networks, hacking systems and stealing precious data. Investigations that cross borders would need international cooperation to apprehend suspects. To that point,
there is little expectation that Russia or China will turn over to the United States the men on the FBI’s Most Wanted Cyber list.

**Infrastructure at Risk for Attack**

In addition to the threat from external and internal forces, another vulnerability is that the systems of our critical infrastructure are standardized. “In fact, all modern plants operate with standard industrial control system architectures and products from just a handful of vendors per industry, using similar or even identical configurations,” according to an in-depth report that was examining the Stuxnet worm. “In other words, if you get control of one industrial control system, you can infiltrate dozens or even hundreds of the same breed more,” reporter Ralph Langner said. Another vulnerability is the workforce itself, he said. “The sober reality is that at a global scale, pretty much every single industrial or military facility that uses industrial control systems at some scale is dependent on its network of contractors, many of which are very good at narrowly defined engineering tasks, but lousy at cybersecurity,” he said (Langner 2013).

And if generators were destroyed in a cyberattack, as Richard Clarke points out in his book, it could take months to replace them since they have to be custom built. “Having an attack take place in many locations simultaneously, and then happen again when the grid comes back up, could cripple the economy by halting the distribution of food and other consumer goods, shutting down factories, and forcing the closure of financial markets,” he said (Clarke 2010, 170).

It only takes *one* person to let the adversary in. Imagine it this way: a worker at a government agency or public utility receives an email addressed to the individual or their
office about some mundane matter, like renewing transit benefits, construction on a local road, or a “Sssshhh! We’re having a surprise party for Jane in accounting.” Would an average person really think a criminal enterprise or foreign entity would be targeting them specifically, and most especially in a mundane notice about something that directly pertains to their life? Would they not have even thought twice before clicking or opening the attachment?

As demonstrated in this chapter, the challenges and vulnerabilities are far and wide for our nation’s networks. The threats are coming at us from all directions. Stronger defenses are needed in the framework of our cyber architecture and in regards to the human element of those who use these networks.
“Make no mistake, we are not winning the fight in cyberspace,” Senator John McCain, the chairman of the Senate Armed Services Committee, said in his opening statement at a September 2015 hearing on Cybersecurity Policy and Threats (McCain 2015). The hearing brought together Obama administration heavyweights in cybersecurity: the director of National Intelligence, James Clapper; the deputy secretary of defense, Robert Work; and the head of U.S. Cyber Command and the National Security Agency, Navy Adm. Michael Rogers.

The debate, as it has for years, continues on Capitol Hill and with the American public about what is the right strategy to protect the nation, while safeguarding privacy. Some industry insiders worry about too much involvement by the government, saying they fear that would amount to government surveillance. On the other hand, some lawmakers and even industry members say a greater partnership between the government and the private sector is needed to stay one step ahead of these malicious and evolving challenges. In my view, the threat is too daunting and the stakes are too high; collaboration between the government and industry is needed.

President Obama says his Cybersecurity National Action Plan, or CNAP, which was introduced in February 2016, is an important step forward in protecting government and the American people. It provides investments in cybersecurity, and works to recruit the best in IT and cybersecurity. The administration is also creating the first-ever federal
chief information security officer who will be responsible for cybersecurity activities across the federal government, and who will ensure the government is interacting with the private sector as well. The White House describes the national action plan as a culmination of seven years of effort that encompasses lessons learned with valuable input from industry and other stakeholders. The action plan includes establishing a commission on cybersecurity. It also encourages Americans to take steps to protect their own accounts including with two-step authentication, and seeks to enhance efforts to strengthen cybersecurity in critical infrastructure (White House 2016).

Lawmakers have charged that the Obama administration has not taken a strong enough response in the face of the troubling cyber actions from China, Russia, Iran and other aggressive adversaries. “Not surprisingly, the attacks continue,” McCain told the Senate Armed Services Committee. “Our adversaries steal, delete, and manipulate our data at will, gaining a competitive economic edge and improving their military capability. They demonstrate their own means to attack our critical infrastructure.” They are pushing the limits of acceptable behavior, even purposely leaving traces of themselves behind, the veteran Arizona Republican said. That audacity and boldness, he said, is demonstrating that these adversaries “feel confident that they can attack us with impunity and without significant consequences” (McCain 2016).

Without retaliatory action, the adversaries are emboldened further, lawmakers and experts say. “We need to impose costs for bad cyber behavior on those who are currently acting with impunity,” according to Frank Cillufo, associate vice president and director at the Center for Cyber and Homeland Security at George Washington University. He said
what is needed is a strong cyber deterrence strategy that is articulated and demonstrated. “The threat tempo is magnified by the speed at which technologies continue to evolve and by the fact that our adversaries continue to adapt their tactics, techniques and procedures in order to evade and defeat the latest prevention and response measures,” he said (Hearing Transcript 2016).

Cillufo spoke at a hearing of the House Subcommittee on Cybersecurity, Infrastructure Protection and Security Technology on emerging cyber threats to the United States. The February 26, 2016, hearing brought together private industry experts for robust discussion on the way forward; I will be referring to the hearing throughout this chapter. The testimony from the industry members provided unique insight into their view of the cyber threat and suggestions on the way forward.  

Exchanging the Threat from China, Russia

Cybersecurity was a prominent theme when President Obama hosted his Chinese counterpart, Xi Jinping, for a state visit at the White House in September 2015. The two presidents announced they agreed to cooperation in the cyber realm, including not to conduct or support cyber-enabled theft that results in a competitive edge.

In a joint news conference following their talks, Obama said the United States will be looking to China to see if it lives up to its promises. “I raised once again our very serious concerns about growing cyber threats to American companies and American citizens. I indicated that it has to stop,” Obama said.

---

“What I’ve said to President Xi and what I say to the American people is the question now is ‘Are words followed by actions?’ And we will be watching carefully to make an assessment as to whether progress has been made in this area,” Obama said.

The American president noted “progress” with China. “We’ve agreed that neither the U.S. nor the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage. In addition, we’ll work together, and with other nations, to promote international rules of the road for appropriate conduct in cyberspace,” he said (White House 2015). The United States and China also welcomed a United Nations accord in which the signatories pledged not to target one another’s critical infrastructure in peacetime, according to The New York Times. The Times says that “leaves open many questions, since there are many definitions of what constitutes critical infrastructure” (Julie Hirschfeld Davis 2015).

The United States finds itself in a precarious position on what to do about China. On the one hand, China obviously is a tremendous economic partner to the United States and provides merchandise that dominates the American marketplace. In that regard, the United States has to maintain some cordiality. However, just as with human rights and other issues in China, cyber is an important topic that needs to stay on the forefront of U.S.-China relations.

The Council on Foreign Relations points out that the United States and China are also seeing increased cooperation in security, energy, and climate change as well, while cyber does remain an issue of concern. “The United States and China have serious
differences on cyberattacks and the rules of cyberspace as well as how to ensure the security of the hardware and software of each country’s information and communications infrastructure,” according to Adam Segal, the director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations. Segal writes, in an assessment about the China-U.S. cyber situation, that neither side is willing to change its behavior. “The perceived benefits from intelligence gathering are too high, the costs inconsequential,” he said (Council on Foreign Relations 2015).

Senator McCain and other lawmakers have called for tough actions against China for its cyber intrusions on U.S. networks. “After much hand-wringing, it appears the president will not impose sanctions in response to China’s efforts to steal intellectual property, pillage the designs of our critical weapons systems, and wage economic espionage against U.S. companies,” McCain said. China’s state visit instead resulted in “more vague commitments not to conduct or knowingly support cyber-enabled theft of intellectual property,” he told the Senate Armed Services Committee (McCain 2015).

While they do pose a threat to the United States, the Chinese cyber activities appear to be for Beijing’s own benefit in the world stage. But Russian actions are far more troubling. Russia has infiltrated our critical networks, and has shown it will deploy cyber tools in times of conflict affecting civilian populations.

The Russians are “very determined and they're very well resourced,” according to Jennifer Kolde, the lead technical director at FireEye Threat Intelligence, a California-headquartered network security company. She spoke at the February 2016 House subcommittee hearing on cybersecurity. Her firm tracks hundreds of threat groups, she
said, including those believed to be Russian nation-state hackers. “They've been extremely aggressive within victim environments,” she said, explaining that often cyber attackers disappear once they are detected. “We've had engagements where we've been working with Russian threat groups where they fight very strongly to stay within that network, and they do so with a great deal of skill and adaptability that challenged even our responders to keep ahead of them,” she said (Hearing Transcript 2016).

Cybersecurity has been a concern of the U.S. government for years. The Comprehensive National Cybersecurity Initiative was established by President George W. Bush in January 2008 (White House 2016). But the threat was on the radar even before that. The chief of staff for President Bill Clinton, John Podesta, in 2000 highlighted how the Internet brings new possibilities, while also challenging values and underscoring the need for new protections. “Because we are so interconnected, more people now have easier access to our most personal information, from bank statements to our medical history. International narcotics traffickers can communicate with each other via computer messages. Hackers can destroy cyber property by defacing homepages and maliciously manipulating private information,” he said (Podesta 2000). When Podesta spoke more than 15 years ago, he and others in government or the public likely could have never imagined how complex the cyber issue would be.

**Stronger Culture, Stronger Protections**

Threats in cyberspace only continue to increase, according to Jennifer Kolde with FireEye Threat Intelligence. She said criminals are getting more creative; malicious activity from threat groups is evolving faster than the public sector’s ability to keep up.
Kolde told the February 2016 House hearing on cyber threats that there is an increase in the sophistication in tools and techniques used by some nation-states and criminal groups. “This includes tools that can evade traditional operating system security and security software, or that reside only in computer memory and leave very few forensic traces. We also see increased efforts by the attackers to hide in plain sight so that hacker activity is indistinguishable from legitimate user behavior without using advanced detection methods,” she said.

Kolde is among those who support increased partnership and automated information sharing between the private sector and government. “However, the information shared cannot consist solely of technical indicators, but must be enhanced with contextual data that will allow defenders to prioritize alerts and respond faster and more effectively with appropriate countermeasures,” she said.

While it is impossible to stop all attacks, Kolde said, security firms should be prepared to “detect and respond to malicious activity across the entire attack life cycle,” making it harder for adversaries to operate in cyberspace. “This should not be achieved by implementing compliance-type checklists, but through a risk-based approach where organizations identify critical assets and implement appropriate countermeasures based on a real world understanding of how attackers operate,” she said (Hearing Transcript 2016).

The Cybersecurity Information Sharing Act of 2015 takes steps to strengthen the nation’s cybersecurity, including by making it easier for private companies to share cyber threat information with each other and the government. It is meant to “improve
Texan Republican John Ratcliffe, the chairman of the House Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, said the bill establishes the Department of Homeland Security National Cybersecurity and Communications Integration Center as the “sole civilian interface for sharing cyber threat information with the federal government.” It also protects companies from being sued for sharing information with the government and with other firms, he said. Ratcliffe said he hopes the bill will encourage the private sector to share information with the government. “The act bolsters DHS' ability to deploy intrusion detection and prevention capabilities across our federal government. These capabilities will ensure the proper capabilities to defend government networks from nation-state attacks,” he said (Hearing Transcript 2016).

The text of the bill was included in a massive spending bill that President Obama signed into law on Dec. 18, 2015, possibly averting a government shutdown. According to the legislation, the government is limited in using the information it receives to “certain cybersecurity purposes and responses to imminent threats or serious threats to a minor.” The government can prosecute crimes such as fraud, espionage or those posing an imminent threat, according to Everett Rosenfeld of CNBC. The legislation has both strong supporters who says it is a step forward, and vociferous detractors who say it
promotes government spying and interference through its vague language, Rosenfeld reports (Rosenfeld 2015).

Among the critics is Sen. Ron Wyden, a Democrat from Oregon, who described the cybersecurity bill as a dangerous piece of legislation that could allow the government to use backdoor procedures to investigate companies and snoop on their customers. “Americans demand real solutions that will protect them from foreign hackers, not knee-jerk responses that allow companies to fork over huge amounts of their customers’ private data with only cursory review,” he said (Wyden 2015).

Information sharing between the government and private sector can help identify the threats quicker, according to Issac Porche, the associate director, Forces and Logistics Program, the RAND Army Research Division at the RAND Corporation. He spoke at the February 2016 House subcommittee hearing on cybersecurity. “Given the time taken to identify a malicious intrusion and determine its extent, which is usually measured in months, the bad actors are long gone, along with your data. If government entities and the private sector are sharing information quickly and often, they have a better chance of being able to anticipate and prepare for the eventual attack,” he remarked. “Ultimately, perhaps ideally what is needed is the ability to track cyber intruders, criminals and other hostile actors with the same freedom of maneuver and speed these adversaries enjoy in cyberspace today. And achieving this goal will required sustained, long-term efforts to develop policy and technology,” he said (Hearing Transcript 2016).
Adam Bromwich, the vice president of security and response at the cybersecurity company Symantec, underscored to the hearing the importance of collaboration, saying the bottom line is not that one company is trying to get a competitive edge. “We are all contributing and sharing with the community to better uncover, understand, and protect against advanced attacks. The cyber threat landscape is always evolving, but so, too, are new security technologies. Preventing cybercrime is a shared effort, and your work to inform the public is an important part of that,” he told lawmakers (Hearing Transcript 2016).

In an example of a big tech company working with government, Microsoft has teamed up with cities and governments to improve cybersecurity for the public. “Microsoft remains committed to supporting national and city governments in developing a unified approach to cybersecurity,” according to Adrienne Hall, Microsoft’s general manager for issues and crisis management. Those efforts including having Microsoft CityNext take part in the Rockefeller Foundation’s 100 Resilient Cities, to help cities around the world implement stronger cyber defense by providing information on best practices and cybersecurity strategies. “We hope that this partnership further emphasizes the need for cities to develop holistic strategies, and will help leaders enhance services, manage operations, and protect citizens,” Hall said, in a press release (Hall 2015).

Computer security is not well regulated, and threats and vulnerabilities need real solutions, not a quick fix or a “patch and pray” effort, according to a report in The New York Times on cybersecurity. Some firms have even run into trouble for not adhering to
mandated standards for protecting data. The government can issue fines to companies like banks and hospitals and others for cybersecurity transgressions (Perlroth 2014).

For example, the U.S. Securities and Exchange Commission announced in September 2015 that R.T. Jones Capital Equities Management, a St. Louis-based investment adviser, agreed to a $75,000 fine and settled charges of not having proper cybersecurity measures in place. The SEC said those lax controls led to a breach that compromised the personally identifiable information of approximately 100,000 people. The SEC said the firm failed to adopt any written policies and procedures, as required by law, to ensure the security and confidentiality of the personal information and to protect it “from anticipated threats or unauthorized access.” The firm “failed to conduct periodic risk assessments, implement a firewall, encrypt [personally identifiable information] stored on its server, or maintain a response plan for cybersecurity incidents,” according to the SEC (U.S. Securities and Exchange Commission 2015).

In May 2013, the Department of Homeland Security, National Protection and Programs Directorate, held a roundtable on cyber risk culture. The meeting in Arlington, Virginia, brought together a variety of stakeholders, including insurance carriers, risk managers, information technology and cyber experts, owners and operators of critical infrastructure. According to the DHS report on the meeting, participant Laurie Champion, Managing Director of Enterprise Risk Management, Aon Risk Solutions, Global Risk Consulting, noted that those at the roundtable could not agree on who “owns” the cyber risk, whether it is private industry, government or a combination of the two. Ownership of the risk will have impacts in a number of areas, including cyber risk management,
threat information sharing, cost sharing, and finding solutions, she pointed out (Department of Homeland Security 2013).

The government can levy fines on certain firms that act irresponsibility in regards to their customers’ personal data. But what about OPM? Has there been any punishment for that massive breach? And a larger question arises, what is the appropriate action for an inadvertent slip? Who is to blame when an individual takes the bait in a phishing attempt or clicks on a bad link and the network gets infected, money is lost, and sensitive data gets compromised? There are laws against committing fraud and other crimes in cyberspace, but what about those who allow the hackers to come in through negligence? Is there accountability procedures for personal actions?

It is a nebulous area. No longer are scams now limited to a single victim. Now, the whole network and all those whose information it holds are at risk. I am interested in seeing how regulations will play out. There needs to be accountability. However, the execution and enforcement of regulations would certainly need to be further examined. For example, if you blame the person who clicked on a phishing link, you are blaming the victim of the attack, as pointed out by George Washington University’s Frank Cillufo during the February 2016 House subcommittee hearing (Hearing Transcript 2016).

Phishing and spear phishing attacks can be pretty sophisticated; I’ve received several emails from Georgetown University or those claiming to be affiliated companies asking me to take a survey or click on a link. Were those phishing attacks or legitimate messages? Whether to click on a link is a decision that could have a serious impact.
Cillufo asked lawmakers a rhetorical question, “How many companies, even the largest, went into business thinking they were defending themselves against foreign intelligence services? That’s precisely what’s happening today, companies taking on nations or being exploited by nations.” A new way of tackling cyber is needed, as the “current approach or business as usual is doomed for failure, as it is completely reactive,” he remarked. The private sector would benefit from assistance from the government, he said. “The U.S. government must give companies who now find themselves at the tip of the spear, the framework, parameters and tools that they need in order to engage in active defense to protect themselves and their customers,” he said (Hearing Transcript 2016).

Cybercrime has wide reverberations, with the costs trickling down to everyone. The head of Cyber Command and NSA, Adm. Michael Rogers, spoke in a March 2016 House Armed Services Subcommittee hearing on Emerging Threats and Capabilities. The burden of cybercrime weighs on the entire economy, he said. “Literally every American who has connected to a network has been affected, directly or indirectly, by cybercrime,” he said. Rogers noted how millions of Americans have had their personal information stolen or had accounts compromised. “Even if we have so far avoided such problems, however, we all pay higher prices for our computers and software, our Internet service, and the goods we buy as a result of cyber-enabled theft,” he said (Rogers 2016).

The director of National Intelligence James Clapper told an audience at Fordham University that segmenting data is another way to protect yourself. “A single breach shouldn’t give attackers access to an entire network infrastructure and a mother lode of proprietary data,” Clapper said. He compared it to a scene in the movie Titanic, where
researchers showed the ship had segmented areas meant to contain any flooding, aimed at keeping the ship afloat. “But the forensic analysis in the film showed that the bulkheads didn’t go high enough, and so the water spilled over the top of each section into the next section until the entire ship was flooded. So we tell the private sector: Don’t let that happen to your data. Make sure a single breach won’t sink your entire company, your entire enterprise,” he said (Clapper 2015).

Industry could also have an “air gapped” network that is not connected to the larger network or the Internet. But, according to a report in Slate magazine, this is a “one of the most drastic, inconvenient, and difficult-to-maintain computer security measures,” typically used in high-level security situations. It points out that researchers at the Fraunhofer Institute for Communication, Information Processing, and Ergonomics reported that the air gap can be bridged by high-frequency audio signals. “It’s not just that the things we can’t see -- the electromagnetic and acoustic waves -- can serve as access points for attackers. It’s that we don’t yet have any thorough understanding of what all the possible access points to computer systems are, or what their complete ‘attack surface’ looks like,” Slate reporter Josephine Wolff said (Wolff 2013).

**Creating a ‘Healthy Cyber Ecosystem’**

The Department of Homeland Security has an interesting take on cyber protections and the cyber environment. Cyber is like any natural system in the physical realm, according to the 2011 report, Enabling Distributed Security in Cyberspace, Building a Healthy and Resilient Cyber, Ecosystem with Automated Collective Action. Just as in the physical world, there are many steps that can be taken in cyber to create a
“healthy cyber ecosystem.” It points out that in a healthy system, cyber devices collaborate in order to protect the larger system or each other. The “cyber ecosystem” should run like a human body, it explains.

For example, there are a number of alerts and warnings on the human body: the senses alerts the brain to dangers, the skin serves as a firewall, while internally the body’s immune system attacks viruses, repairs breaches, builds immunity and strengthens defenses. Externally, organizations such as the Centers for Disease Control and Prevention issue warnings about health concerns, so individuals and society can anticipate threats, take preventative steps, and immediately take action if needed.

Just as natural defenses are automated, the cyber ecosystem would be improved with automated responses to threats, the report said. “If cyber devices communicated in near real-time with each other about attacks, and took coordinated security-hardening response actions consistent with a defined policy framework, then critical business, mission and privacy objectives could be better supported, and many security risks could be managed proactively and dynamically,” it said (Department of Homeland Security 2013).

Florida Republican Representative Daniel M. Donovan Jr had a similar analogy when examining the threat from cyber. He looks at it as a disease. But then how do you approach care? Questions arise, he said, such as as“(do) we wait for the disease to happen, and then we find a cure? Do we wait for attacks, because I suspect there's different ways that people attack our systems, and then try to figure out how to deal with
it? Or do we anticipate what is the next method of attack and try to protect ourselves from that before it happens” (Hearing Transcript 2016)?

Of course, the answer is the latter. The best way is to protect oneself in cyberspace, whether an individual, a small company or a big enterprise, is by anticipating threats, looking at trends, learning from worst-case scenarios, and evolving with the environment. Taking those bold steps and real action, instead of thinking “it will never happen to me” is part of the culture change, as the national conversation focuses on the dangers that are lurking in the vast expanse of cyberspace, just beyond our fingertips.
CHAPTER 5

ASSESSMENT ON CULTURE CHANGE

A critical element in protecting the nation against threats in the rapidly evolving cyber domain is right at our fingertips – literally, according to the Department of Defense’s chief information officer. In a keynote address to a cybersecurity summit in Washington last year, Terry Halvorsen shared with the hundreds of participants his biggest concern: “What keeps me awake is 'Will we get the cyber culture right?'”

The United States is perhaps more dependent on cyber than any other nation in the world, he said, adding that it is at least certainly true for the U.S. military. While the connectivity gives America powerful advantages in warfare and business, it also makes it the "most vulnerable to cyber interdiction," Halvorsen said. "Culture is the hardest thing to change," he said. "That's why it keeps me awake at night" (Ferdinando 2015).

In this chapter, I will explore the central theme of my thesis: that the cyber culture must evolve with the threats in cyberspace. My hypothesis is that there will be a culture shift. Cybersecurity will be engrained in the national consciousness, but it will take time. I will examine culture changes using two independent issues, seat belt use and cessation of smoking. I picked those issues because they are relevant to my generation: I grew up when smoking was glamorized in advertisements and in popular culture. In addition, most people did not wear a seat belt when I was growing up. I find it fascinating how the culture shifted over time in response to sustained messaging, education about the dangers, and the threat of sanctions. As I will explain, smoking and not wearing a seat belt can have impacts beyond just the one primary person; the same holds true in cybersecurity.
My hypothesis will look at the shift in human behavior and apply that to cybersecurity. I believe that Americans will shore up their personal defenses and strengthen the national cyber culture once the dangers and costs of bad behavior are fully realized.

In my assessment, changes pointing to a safer cyber culture are already afoot: think about the national conversation going on about cybersecurity, and the steps businesses and governments are taking to address the threat and educate the workforce. Cybersecurity classes are mandatory at some workplaces. Americans have taken action as well. Just as most people secure their home routers now, change is coming because of sustained messaging about the dangers and people are modifying their behavior as the threat evolves. But cybersecurity needs to move to a higher level of consciousness. All the training in the world could go out the window if just one employee, out of the many thousands targeted, clicks on a link with malware. There is much to lose: the mission of governments and businesses is at risk; national security can be jeopardized. Workplaces as a whole may understand the threat, as they depend on the networks to successfully execute their missions. It is vitally important to get that awareness and concern into the consciousness of all users.

Now let’s examine culture change in the United States and put my hypothesis to the test. To do so, we have to go back a few decades. Think back to the days of when smoking was glamorized and when hardly anyone used a seat belt. Think about riding in the station wagon, the children piled in the back. The parents enjoyed their cigarettes, while the kids jumped all around in the backseat, with no seat belts to restrict their movements. That behavior was perfectly acceptable; there were no seat belt laws then
and smoking was widely accepted. But, wow! Imagine if that scenario happened today! Frantic motorists would be calling the police; people would be snapping photos and shooting videos on their smartphones to share with authorities. Our carefree family could be slapped with citations for not wearing seatbelts, not properly restraining children, and, depending on which community they were driving in, even a citation for smoking in a vehicle with children.\(^5\) Who knows, they may have even received a child endangerment or reckless driving charge as well.

The point of this scenario is to illustrate how behaviors change over time. Laws and regulations evolved. The culture shifted. Americans modified their behavior in the face of danger and to avoid sanctions. Even though smoking was once widely accepted and the norm, Americans have largely given up that habit. The Centers for Disease Control and Prevention says 19 percent of adults in the United States were smokers in 2011, compared to 42.4 percent in 1964.\(^6\)

The culture shifted in the face of very real health dangers, as well as sanctions in the way of higher costs per pack and increased inconveniences in finding a place to smoke. In addition, studies have shown smoking is a public safety hazard that can hurt more than just the smoker. Second-hand smoke can have adverse health impacts on others. Just as smoking can harm others, poor cyber behavior can impact others.

\(^5\) Several states and communities, and Puerto Rico have laws prohibiting smoking in cars when children are present. For more information see: [http://www.no-smoke.org/learnmore.php?id=616](http://www.no-smoke.org/learnmore.php?id=616).

\(^6\) For more information, see: [http://www.cdc.gov/tobacco/data_statistics/tables/trends/cig_smoking/](http://www.cdc.gov/tobacco/data_statistics/tables/trends/cig_smoking/).
Many states have restricted or banned smoking public venues such as restaurants, beaches, parks and even near the entrances of some buildings. Americans also faced sustained messaging on the dangers of smoking. After fierce debate and opposition, laws were passed and a culture shift happened in the United States. No longer is smoking widely advertised or thought of as the glamorous habit of rock stars and celebrities (Centers for Disease Control and Prevention 2014). Even cigarette maker Philip Morris agrees: “Cigarettes are addictive and cause serious diseases in smokers. For those concerned about the health risks of smoking, the best thing to do is quit” (Philip Morris USA 2016). Could you imagine today’s stance in the 1950s and 1960s, when even Fred Flintstone was marketing cigarettes?  

Conversely, in regards to seat belts, most Americans now buckle up when driving a vehicle. Recognizing the dangers, states began enacting laws for seat belt use. And there was vocal opposition. “The government is not going to tell me what I can do!” But it is a public safety issue. Just like smoking can impact more than just the smoker, a crash can impact more than just a driver who is not wearing a seat belt. Think about all the emergency personnel who rush to the scene and their resources used, in addition to the

---

7 However, smoking and the use of other tobacco products are popular throughout the rest of the world. The World Health Organization describes the tobacco epidemic as “one of the biggest public health threats the world has ever faced, killing around 6 million people a year.” For more information see: http://www.who.int/mediacentre/factsheets/fs339/en/.

8 For an example of a cigarette ad featuring Fred Flintstone, see: https://www.youtube.com/watch?v=bdHS1quSHMw.
medical personnel and resources for the medical care. It has been determined that wearing a seat belt prevents injuries.\(^9\)

While the laws and penalties vary by state, throughout the United States, except in the state of New Hampshire, it is illegal to operate a vehicle without wearing a seat belt (National Highway Transportation Safety Administration 2015).\(^{10}\) Again, in this example, Americans faced sustained messaging about the sanctions and dangers and modified their behavior. In an action that was barely a passing thought in years past, now most drivers buckle up when they are operating a vehicle. The National Highway Traffic Safety Administration says the nationwide rate for seat belt use was 87 percent in 2014, compared to 14 percent in 1983.\(^{11}\)

It is my hypothesis that just like the smoking and seat belt issues, society will shift toward a safer cyber culture. Culture changes don’t happen overnight, and there are often skeptics, opponents and detractors. It is my view that change in cybersecurity will happen over time. It is necessary because cybersecurity affects more than just the user who clicks on a wrong link. The entire network is at risk. Education and sustained messaging are needed. The consequences of poor cyber behavior must resonate with the user. Those

\(^9\) Those emergency and medical resources could be used elsewhere, instead of treating injuries that could have been avoided. There are also secondary costs such as higher insurance premiums, long-term medical treatment and other costs. For more information see: http://www.cdc.gov/motorvehiclesafety/seatbelts/facts.html.

\(^{10}\) New Hampshire does not have primary or secondary seat belt laws for adults, although it does have laws for drivers and passengers under the age of 18, according to the National Highway Traffic Safety Administration.

\(^{11}\) For more information, see: http://www-nrd.nhtsa.dot.gov/Pubs/812149.pdf and file:///C:/Users/Owner/Downloads/GHSA-Present.pdf.
risks could include the loss of productivity or work because of a cyberattack, increased costs to the consumer, and repercussions for employees. Americans must take on a greater responsibility in safeguarding themselves and their networks. Our behaviors must evolve to keep pace with the complex, evolving threat. Cybersecurity needs to be ingrained into the national consciousness.

In examining a culture change, I want to look at some insights into attitudes on the topic, as well as insights into human behavior. Why do we act the way we do? We know a “bad apple spoils the bunch.” But do “good apples” rub off on each other? Would “good cyber behavior” rub off on employees?

According to a World Bank Group report on human behavior, individuals are “social animals who are influenced by social preferences, social networks, social identities, and social norms.” Most people, according to the report, care about what others are doing and how they fit in with the group. People will “imitate the behavior of others almost automatically” (World Bank Group 2015). In applying that theory to cyber, then good cyber habits would rub off in a culture that promotes them. Members of the group would like to mimic their colleagues. If a company’s leadership demonstrates and instills in the workforce the importance of cybersecurity and good cyber behavior, the mindset could rub off on the individual workers and those in that culture.
**Social Engineering: Targeting the Weakest Link**

Computers can be relied on to do exactly what they are programmed to do, with zero variations. We, the humans who use the systems, are still the wildcard.

Computer expert and “good hacker” Lillian Ablon of the RAND Corporation said the “human element is becoming increasingly prevalent in cyber and computer network operations and is also the most unpredictable factor in cybersecurity” (Ablon 2015). She explained how at the Def Con hacker conference she won the challenge of getting specific information about a Fortune Top 10 company. And for her, it was extremely easy. She explains, “I dug for open source information online, and then conducted a live social engineering phone attack on employees with the audience watching. I gained key insights into the company and could have successfully installed malware on its computers.” (Ablon, The Good Hacker: Q&A With Lillian Ablon 2015).

A classic example is someone calling and pretending to be from “tech support” wanting to “help” you repair your computer. The caller might try to gain remote access to your computer. From there, the scammer might install malware in which you will need to pay money to have your computer “fixed,” or the caller may direct you to a website that will infect your computer. “These scammers are taking advantage of your reasonable concerns about viruses and other threats. They know that computer users have heard time and again that it’s important to install security software,” according to the Federal Trade Commission. In addition, some scammers even pull off the con by placing ads online so consumers will call them to seek help for their computer (Federal Trade Commission 2016).
Prolific hacker Kevin Mitnick, who spent several years in jail because of computer and communication-related crimes, said it is much easier to “hack” a human than a computer. In an interview with the Computerworld website, he explained that there is a simple explanation why. “Computers follow instructions, they don't vary,” he said. Humans are the opposite. Mitnick highlighted how people are swayed by their emotions and various things going on in their lives. It is not difficult to socially engineer people, “especially if they haven't been burned before,” according to Mitnick (Elgan 2016).

A skilled hacker conducting social engineering knows exactly what to say and do in order to infiltrate a target. Think James Bond in the cyber world. And unlike an intrusion or robbery in the “real world,” the hacker faces no physical danger I can think of, and for the most part there is no risk of immediate arrest. The hackers can hit a seemingly endless number of targets looking for a vulnerability. And, in some parts of the world, hackers act with impunity.

A survey commissioned in 2015 by CompTIA, the IT industry trade association, indicates that while some progress has been made in instilling the message of cybersecurity in the public consciousness, there is still a ways to go. The survey looked at 1,200 full-time workers across the United States. Forty-five percent of the respondents said they did not receive cyber training at work. In a press release on the study, Kelly Ricker, a senior vice president at CompTIA, said organizations need to take steps to make sure they have effective training in place. "Companies cannot treat cybersecurity training as a one-and-done activity. It needs to be an ongoing initiative that stretches to all employees across the organization,” Ricker said.
In the same press release, CompTIA announced the results of a social experiment it commissioned. The experiment involved leaving flash drives out in public places and seeing what happened. Would someone actually place a flash drive into their computer, putting their computer and network at risk? The flash drives were left around in major cities, including Chicago, San Francisco and Washington, D.C. The results: one in five times, the devices were inserted into computers, which could have exposed the person and their networks to malware. "We can't expect employees to act securely without providing them with the knowledge and resources to do so," Todd Thibodeaux, president and CEO of CompTIA, said in the press release. “Employees are the first line of defense, so it’s imperative that organizations make it a priority to train all employees on cybersecurity best practices” (CompTIA 2015).

Our actions in cyberspace need to match up with our actions in the physical realm. To illustrate, think about what your reaction would be if a stranger walked up to you in person and said “Hello, I am with First Fidelity Bank and I need you to update your account information. Please write your logon information on this sticky note and I will verify your account.” Crazy, right? What if you worked at the front gate at the White House, and foreign agents walked up to the entrance and said, “Hi, we need access to the computers.” Would you buzz them in and let them wander around the West Wing? Those scenarios are exactly what is happening in cyberspace. Adversaries have “knocked” through phishing attempts and the cyber door was opened for them. Through these attacks, adversaries have entered critical networks and threatened national security and the privacy of Americans.
Even the director of National Intelligence, James R. Clapper, agrees that people need to be aware of the threat and act accordingly. “Teach folks what spear phishing looks like. So many times, the Chinese and others get access to our systems just by pretending to be someone else and then asking for access, and someone gives it to them,” he told an audience at Fordham University (Clapper 2015).

The importance of being aware of the dangerous out there, and getting the cyber culture right cannot be understated, according to Army Col. Carmine Cicalese of Army Operations Center, G-3/5/7. In an interview about Army cybersecurity, he talked about practicing “good cyber hygiene.” The behavior of every soldier is of concern to the Army, since one careless move can let the adversary in and threaten the mission, he pointed out. "Everybody has a part in this,” he said. The threats against Army computer systems are unrelenting, he said. His advice to his troops is simple: "Don't bite on the phishing scams.” National security depends on it; any disruptions could prevent communications and impact the mission, whether in the battlefield or elsewhere, Cicalese said. In a message that is relevant to any workplace, Cicalese said cybersecurity needs to resonate at all levels, from the highest-ranking executive to the most junior personnel (Ferdinando 2014).

The threat of cyberattacks is a part of the reality in operating in this vast, open arena. Crime is unfortunately a sad reality that people in the physical realm face. It is also a grim reality in cyberspace. Just as one takes steps and is educated in crime prevention, proactive and preventative steps need to be taken as well in the cyber world. Even with a culture shift in cybersecurity, not everyone is going to behave correctly and demonstrate
good cyber sense. And those are the people the hackers are betting on. But it’s not only
the “careless” people who slip. It could be someone in a split-second who just wasn’t
paying attention while clicking through emails. Or the con could be so convincing that
the users are just fooled.

“If it happens in the physical world, it's happening in the cyber world, and
increasingly you're seeing those two worlds converge, especially with the advent of the
‘Internet of Things’ and ‘Internet of Everything,’” according to Frank Cillufo with
George Washington University. He spoke at a House hearing on cybersecurity. There will
be a cyber dimension in every form of conflict now and in the future, he said. “Whereas
technologies will continue to evolve and change, human nature remains pretty
consistent,” Cillufo said (Hearing Transcript 2016).

In some workplaces, external media is prohibited from networked computers,
ports are locked, websites blocked, links are disabled in emails, and only administrators
can download programs. Access to certain networks are limited; data might be
segmented. Those simple measures can certainly stop infections or limit damage. But the
risk also comes from infected links that could be innocently shared on social media.
Friends and contacts might post a link with an eye-catching headline. People are more
inclined to click on a link if a friend shares it, according to Dave Weinstein, New Jersey's
director of cybersecurity. Weinstein was quoted in the Asbury Park Press newspaper on a
story about the dangers of social media. For example, scroll through a social media feed
and you might see your contacts sharing links to: Win Tickets for a Disney Vacation! See
Adorable Pictures of Celebrity Baby! Take this Quiz to Find Your Soulmate! Those links
could be marketing ploys or even have malware attached, infecting your computer and allowing access to the network, according to Weinstein (Willis 2016).

**Often Overlooked Danger: Public Wi-Fi**

There is another danger, and one that doesn’t get nearly the same amount of attention as phishing – and that is public Wi-Fi. People tend to assume the connection is safe because it is free, open and available to everyone, akin to a public meeting spot. But eavesdroppers could be intercepting all the unencrypted information you send, including usernames and passwords. Wi-Fi monitoring programs are readily available online for free. And this danger is not just for people using the public connections for recreational activities like surfing the Internet and going on social media sites. Guess what happens when you are on the public network for work purposes?

“If you're using Wi-Fi in a public place and you're not getting hacked, it's only because there's nobody around bothering to do it,” Robert Graham, CEO of tech consultant Errata Security, said, according to USA Today tech reporter Byron Achohido. Eavesdroppers just need to sit within 100 feet from the target, Rick Farina with AirTight Networks said in the same news report.

For example, Tom Brennan with security consultant Access IT Group, told Achohido about a tech systems manager in New York City whose network was infiltrated after he used a public Wi-Fi connection during a lunch break in a public park. Eavesdroppers stole the username and password the manager used to connect to the company’s network. Later, a hacker used that information to access the server. "People
Intercepting data traffic is simple, according to *PCWorld* contributor Eric Geier. He likens it to listening in on someone’s walkie-talkie or on a CB radio conversation. “Like CBs and walkie-talkies, Wi-Fi networks operate on public airwaves that anyone nearby can tune into,” he writes. “You can snag emails, passwords, and unencrypted instant messages, and you can hijack unsecured logins to popular websites,” Geier said. He demonstrated how easy it was to intercept communications by using a wireless network analyzer. Geier points out that he was only monitoring the electronic traffic, since gaining access to another person’s account is illegal. However, in his experiment, he used his own smartphone to send messages and use social media, which he intercepted on his laptop. He entered his own Facebook account through the intercepted information (Geier 2013).

“It takes zero hacking skills to surreptitiously monitor and/or hijack communications over a public Wi-Fi network. Widely available freeware makes eavesdropping on emails and web browsing as simple as pressing a button,” according to *Forbes* technology writer Amadou Diallo. Eavesdroppers can also set up their own Wi-Fi spot or spoof sites to look like the legitimate site, and they can monitor all the unencrypted information you send. A way to protect yourself, according to Diallo, is to make sure the information you send is encrypted, either through secure sites or by using a Virtual Private Network, or VPN (Diallo 2014).
Private Wi-Fi connections can be vulnerable to eavesdropping as well. The director of Cox Business Segment marketing, Lisa Majdi, writes in a column for *Forbes*, there are a number of steps a business can take to protect itself. In an often overlooked danger, a router that is out in the open can easily be reset by hitting a button, she said. Hitting reset can circumvent many security measures, Majdi writes. She recommends keeping the router locked in a location with restricted access. “Changing your router’s passphrase may seem like another obvious precaution, but you might be surprised: the most common way for people to access a business’ Wi-Fi without permission is by using the default router passphrase which has never been updated,” she said.

She said businesses should make sure the router is also using the encryption protocol WPA, which means “Wi-Fi Protected Access.” She points out that older routers might be set to the “extremely hackable” encryption protocol of WEP, or “Wired Equivalent Privacy,” she explains. Another vulnerability is having a single public network for both employees and customers, which can open up your data and network to risk, Majdi said. Businesses can create separate access points through a Service Set Identifier, or SSID. That can “isolate your business’ computers and devices from guest devices, meaning that customers or other guests of your business can’t interact with or undermine your company’s proprietary devices or data,” Majdi said (Majdi 2016).

The vice president of specialty casualty division at Liberty International Underwriters, Oliver Brew, said while it is impossible to stop all cyberattacks, companies can take important steps to mitigate risks. Those steps start with instilling a strong cyber culture in the workforce. Brew spoke at a one-day Department of Homeland Security
roundtable on cybersecurity in 2013. Businesses can promote several key areas, he pointed out: leadership; education and awareness; technology designed to promote security and to protect privacy; and information sharing. It is important for information sharing to happen within the organization, as well as among businesses, and in public-private partnerships. Each pillar is not independent; they must be done in tandem with the others, he said (Department of Homeland Security 2013).

In addition, at the DHS roundtable, an IT professional said companies are “getting lucky every day” and should take those near-misses into account as well when they are developing their cyber policies and sharing best practices. “The IT professional concluded that if an adversary dedicates the time to getting into a company’s assets, the adversary will succeed – a fact of life that supports the argument that companies should adopt risk mitigation rather than risk avoidance strategies,” the read-out report on the DHS meeting said (Department of Homeland Security 2013).

In a series in May 2015, the Washington Post examined what it called the “Net of Insecurity: A Flaw in the Design.” Reporter Craig Timberg outlined how the threat in cyberspace began with the first widely spread worm in 1988 that wreaked havoc, crashing machines and causing millions of dollars in damage. The architects of the Internet created an open space for researchers and scientists to share data, he said. They never imagined it would be used for criminal enterprises; they never imagined that users would attack other users, Timberg said (Timberg 2015). But that is the reality of today.

The dangers noted in this chapter have one thing in common: they are preventable. It would like to think that many more Americans are aware of at least some
threats and might think twice about clicking on a link in an email addressed to “Dear Valued Customer” and asking them for their password information. But the threats are not always that obvious.

Cybersecurity is uniquely different from physical security. For example, a workplace might have security personnel at the front door. There are a limited number of entryways into an office building. However, in cybersecurity, everyone who has direct and even indirect access to a network is a guard who could repel adversaries – or let them in. Contractors and employees could be connecting into the network from all around the globe. That is a lot of people responsible for keeping the network safe from adversaries.

The threat is dynamic and complex. Hackers have moved beyond the typo-laden emails in stilted English. Their crimes transcend borders; they act with impunity in carrying out attacks against U.S. targets. Now, adversaries are gaining access through sophisticated spear phishing attacks, preying on the human and technical vulnerabilities in the system. And once the malware infiltrates a network, it may be extremely difficult for the computer technicians to detect and neutralize the danger. Or the damage could already be done, the data stolen, and the cyber attackers long gone.

In my research of this paper over the course of the semester and in previous courses and experiences, I assess that a culture shift is under way. It will be excruciatingly painful, as we have already seen. It is important to note, not everyone is swayed by risk and danger. People still smoke. Not everyone buckles up. But quitting the habit and using a seat belt are examples of important steps for public health and safety. Cybersecurity is an important issue for the health and safety of our networks.
CONCLUSION

A CULTURE CHANGE

The goal of this thesis was to underscore the severity of the problem the nation faces in regards to cybersecurity. As the experts and national leaders indicate across the board, the threat is only increasing in frequency and severity. Adversaries are ever-exploiting vulnerabilities in the system; criminals are constantly evolving to steal data, make a profit or lure people into revealing sensitive information. National leaders, businesses and government understand the urgent need to do more. As a result, the national conversation on cybersecurity includes varied viewpoints from government, academia, and the private sector. Change is needed to ensure better security for our networks, including starting with the most important factor: the human element.

My hypothesis is that the country will improve and strengthen its cyber culture, but it will take time. In testing my theory, I applied culture change in two independent areas, cessation of smoking and increased seat belt use. In those instances, Americans changed their behavior in the face of threats, sanctions and harm to themselves. I believe the same changes will happen over time in regards to cybersecurity.

In the first chapters of this thesis, I highlighted how the nation depends on connectivity for an increasingly number of activities. Connectivity is a part of the national fabric, important in so many aspects, from our everyday lives to our nation’s critical infrastructure. It plays a vital role in the communications and weapons systems used by the military.
The cyber threat is an increasingly vexing problem; seemingly every day a new report emerges about a data breach or some type of cyberattack. Consumers, governments and businesses are more vulnerable than ever, as so much of our lives are taking place in the cyber realm. The convenience is unmatched; no more having to wait in lines at the bank, commerce is no longer limited by geographic location, far-flung friends can chat instantaneously, and businesses can wheel and deal with clients on the other side of the globe. Photographs are stored in the cloud, newspapers and books are available online, and a homeowner can even control a thermostat or appliance with a few taps of the smartphone. But as outlined in this paper, everything that is connected is at risk. Cyber threats have exponentially increased – by more than 10,000-fold – over the last dozen years (Perlroth 2014).

In later sections of this thesis, I discussed the vulnerabilities in our national infrastructure and critical systems. I examined the threats posed by sophisticated hackers including nation states such as Russia, China, North Korea, and Iran. From there, I assessed the political context and the national debate in cybersecurity. In the final chapter, I examined culture change and human behavior, and applied my hypothesis to cybersecurity.

As explained throughout this paper, the hackers of today are no longer just the whiz kids or bored teenagers looking to get some laughs or raise a few eyebrows. Now, sophisticated hackers have infiltrated our critical infrastructure, carried out espionage, stolen confidential information, and compromised the personal information of millions of Americans. Among the hackers are nation states that are posing real threats to U.S.
security. Russia has demonstrated advanced capabilities that are truly worrying; China has blatantly stolen trade and business secrets. Meanwhile, Iran and North Korea have acted aggressively. While terrorists do not have the capability to attack our systems, they do have the intent. There is even a market for cyber crime: programmers and coders sell malware, and stolen credit card data is for sale online. All of this paints a troubling picture. Investments are needed to strengthen our defenses and update antiquated systems. The cyber protections need to stay one step ahead of the relentless adversary. Criminals send the bait out to users through phishing scams, hoax websites or bad links. Malware can be launched through a variety of ways, including through an infected link, a USB stick with the malicious program on it, or through opening documents or downloading programs that contain malicious code. Common sense says be careful, don’t click on links, but sometimes a deal is “too good to be true” or in a split-second we get a seemingly irresistible popup ad or link about a celebrity and we just aren’t thinking about cybersecurity.

As I demonstrated in this paper, we rely heavily on computers and networks throughout our comings and goings each day. Cybersecurity lapses could be everywhere: whether a flawed or absent password, a disgruntled employee with a score to settle, or poorly designed or implemented cybersecurity measures. A breach could be a denial of service attack, a group “defacing” a web page in protest of an issue, or it could be more serious as the theft of significant amounts of money, exposure of government and military secrets, or sabotage on the nation’s infrastructure. With all its defenses, even the
White House, the Department of Defense and other government networks have been victims of cyberattack.

The United States has devoted significant attention to the issue, requesting billions in the budget for cybersecurity, creating a Cyber Command and focusing time and attention in battling cybercrime. President Obama has called for stronger cybersecurity laws. Stiffer penalties are needed to enforce cybersecurity standards. For example, only certain companies such as hospitals and financial institutions face possible sanctions due to cyber negligence (Perlroth 2014). Legislative action is needed to ensure that cybersecurity stays on the forefront of efforts in protecting the individual and the nation.

As demonstrated in this paper, U.S. critical infrastructure is vulnerable to attack. It needs reliable and tough cyber protections, and systems not entirely reliant on a network. A critical component in keeping the infrastructure safe, as President Obama has called for, is constant cooperation between the federal government and the private operators. Other ways to strengthen the public-private partnership are to share best practices, engage in dialogue, and seek solutions in a cooperative manner. With the vast amount of government documents, personnel records and other files, it would be unrealistic to have federal entities or critical infrastructure keep hard copies of everything, but a recommendation could be to store information in internal, off-line systems.

As evident from developments in recent years, the cyber threat could be from the inside as well. While the cases of Edward Snowden and Army Pvt. Bradley (Chelsea)
Manning underscored the complexity and severity of this threat, there are other less publicized cases of internal breaches. What is needed is continual screening of those with access to computer systems. Actions can include reporting suspicious activity, monitoring systems for unauthorized access, and even keeping track of the actions of those who conduct authorized work.

The security of the nation is in a precarious position in regards to cyber. The government does not oversee many of the systems of the critical infrastructure since they are in private hands. In outlining the importance of public-private collaboration, the White House said it supports the sharing of “actionable threat information and warnings,” and helping impart best practices for the “most vulnerable critical infrastructure companies and assets” (White House 2014). Since small utilities might not readily have the know-how, resources or technical expertise to keep up with the evolving cyber threat, it is critical they maintain and strengthen ties with the federal government.

Dangers lurk at every click in cyberspace. Nefarious actors lie in wait for a vulnerable target, seeking to steal account information, syphon money away from victims, compromise sensitive information, and put Americans at risk. Malware surreptitiously waits on a USB stick. Nation states infiltrate our critical networks.

The American people need to be increasingly vigilant. Our national security depends on it.
REFERENCE LIST


—. 2016. Statement by Pentagon Press Secretary Peter Cook on DoD’s 'Hack the Pentagon' Cybersecurity Initiative. March 2. 


