REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
17-05-2019	Master's Thesis	

4. TITLE AND SUBTITLE
THE THREAT OF TRADITIONAL ATTACKS AND CYBER WARFARE ON NATURAL GAS AND COAL

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Martorano, Eric, C, LCDR, SC, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Civilian Institutions Office (Code 522)
Naval Postgraduate School
1 University Circle, Herrmann Hall Rm HE046
Monterey, CA 93943-5033

10. SPONSOR/MONITOR'S ACRONYM(S)
NPS CIVINS

11. SPONSORING/MONITORING AGENCY REPORT NUMBER

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This thesis' focuses on the critical infrastructural security of the gas and coal industries, which account for 50% of our nations domestic energy consumption. I believe that maintaining energy security is a fundamental responsibility because it ensures the well being of our society. Our ability to maintain critical infrastructural security is dependent on public awareness and support of our critical infrastructure, and to understand the risks that threaten it. In addition, effective government leadership in response to terrorist attacks, private sector cooperation, planning for emergencies that involve supply disruptions, and ensuring adequate resource allocation to provide energy source diversification can ensure infrastructural security. The objectives of infrastructural security cannot be achieved without the means of innovative technology, up-to-date information systems, adequate funding, and equipped personnel.

15. SUBJECT TERMS
Energy security, critical infrastructural security, government leadership and resiliency in response to terrorist attacks, mitigating supply disruptions, effective resource allocation, and energy source diversification.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPONE NUMBER (*Include area code)*
U	U	U	UU	29	

THIS PAGE INTENTIONALLY LEFT BLANK

THE THREAT OF TRADITIONAL ATTACKS AND CYBER WARFARE ON NATURAL GAS AND COAL

Eric C. Martorano

A thesis submitted to the faculty at the University of Kansas in partial fulfillment of the requirements for the degree of Masters in Business Administration in Petroleum Management in the Kansas School of Business.

2019

Approved by:

Dr. Shapour Vossoughi

ABSTRACT

Eric C. Martorano:
The Threat of Traditional Attacks and Cyber Warfare on Natural Gas and Coal
(Under the direction of Dr. Shapour Vossoughi)

Herein, I will focus on the critical infrastructural security of the gas and coal industries, which account for 50% of our nations domestic energy consumption. I believe that maintaining energy security is a fundamental responsibility because it ensures the well being of our society. Our ability to maintain critical infrastructural security is dependent on public awareness and support of our critical infrastructure, and to understand the risks that threaten it. In addition, effective government leadership in response to terrorist attacks, private sector cooperation, planning for emergencies that involve supply disruptions, and ensuring adequate resource allocation to provide energy source diversification can ensure infrastructural security. The objectives of infrastructural security cannot be achieved without the means of innovative technology, up-to-date information systems, adequate funding, and equipped personnel.

TABLE OF CONTENTS

CHAPTER 1: VULNERABILITIES

Introduction

Over the past two centuries, the United States has responded to numerous attacks deliberately intended to test our resolve and exploit our vulnerabilities with destructive prejudice. Despite the pain that results from these challenges, precious data can be taken from the lessons they impart, which can help formulate an adaptive and strategic response to future challenges that lie over the horizon. Our resiliency can be measured by our capacity to respond to crises; therefore, it is imperative to our national and economic security that we establish the defense mechanisms necessary to secure our energy resources. These mechanisms must be both institutional and industrialized. They must be robust, redundant, and capable of a rapid response to disruptions in our affected infrastructural sectors. In terms of our national security, the National Infrastructure Protection Plan of 2013 (NIPP 2013) addresses various infrastructural sectors, including agriculture and food systems, defense industrial base, energy systems, public health and health care facilities, national monuments and icons, banking and finance systems, drinking water systems, chemical facilities, commercial facilities, dams, emergency services, nuclear power systems, information technology systems, telecommunication systems, postal and shipping services, transportation systems, and government facilities.

Inextricable Interdependencies

Many of the sectors mentioned in NIPP 2013 are interconnected. Our ability to respond to attacks can be measured by how effectively we identify and mitigate single points of failure that may pose risk to these sectors during their operational process. A successful attack on our energy sector that damages our ability to generate power would result in a cascading effect of disastrous proportions because energy is a lifeline system that supports each sector, where each

sector influences each other both directly and indirectly. Natural gas and coal are used to generate energy in the power generation stations, which further provide this energy to processing stations, storage facilities, and natural gas and coal distribution systems. These inter-dependent relationships are indisputable!

Information Technology and Operational Technology Convergence

Power plant operators can continuously monitor and control different sections of a plant to ensure its proper operation, which is possible because of the development of remote command and control networking technology. Information technology (IT) and operational technology (OT) allow wireless exchange of data between various systems. IT systems compute the data integrated with the OT systems to monitor and control the operational processes occurring in a power plant. The interconnected IT and OT networks result in synergies that enhance the energy industry. However, because of the automation of several of the industrial processes, the gas and coal companies should manage their cybersecurity approach to protect the automated controls that manage processing and production. Understanding the systems and subsystems that encompass this integration is essential to grasp the fundamental concept related to the manner in which the industrial networking platforms enable energy production from gas and coal.

Enterprise Applications

Enterprise applications include various systems such as SAP and Oracle. SAP is an enterprise resource planning (ERP) software that can be deployed to help with financials, distribution, manufacturing, project management, and customer relation management. The enterprises that implement a vulnerability management process will experience a significantly less number of successful attacks. SAP has more than 320,000 customers in 190 countries, including more than 85% of the Fortune 2000 oil and gas companies. Oracle, which is used by

100% of the Fortune 100 companies, provides similar e-business enterprise platforms. ERP security is an important cog in the business management process. The IT security managers should regularly review all the connections, securing these connections whenever possible, and should not include open connections to the critical information systems within the organizations domain.

1. Industrial Control Systems

The industrial control systems (ICSs) use network connectivity to support the integration of hardware and software in distributed control systems, industrial automation and control systems, programmable automation controllers, control servers, intelligent electronic devices, and sensors. These systems are designed to be remotely controlled and, thus, link together time and place efficiently. Over time, technological developments have enabled these systems to become smarter by allowing remote access because data exchanges are made possible by internet connectivity via human–machine interfaces (HMI). Historically, the machines and related components used in industrial plants have employed computerized proprietary protocols, i.e., communication protocols owned by a single organization or individual. In fact, these dated machines lacked computing and communications technology. When compared to the modern advanced ICSs that can be controlled using wireless networks, such proprietary protocols kept these systems closed to external connectivity.

The advantage of traditional proprietary protocols was that external threats did not exist because it was a closed or “air-gapped” system. The obvious advantage of the current IT systems is that they possess efficiencies that outperform any dated system; however, due consideration must be given to the external cyber threats. Even though it is logical to argue the benefits of operational and market efficiency outweighs the cost of dealing with cyberattacks, the threat of

them are considerably serious. As these technological inputs continue to develop, they present opportunities to improve the capability of the energy industry; however, they also inevitably enhance the technological capabilities of the cyber attackers. This makes it crucial to maintain a concurrent cybersecurity strategy that does not lose sight of or underestimate such threats.

Massive amounts of throughput and continuity are required with respect to our coal and gas sectors to satisfy the aforementioned condition. The critical infrastructure of these sectors must be supported by ICSs that maintain a heightened level of cyber readiness. Maintaining this level of readiness can be a cumbersome task. Taking these systems down is not as simple as announcing a scheduled system outage, installing a patch, rebooting a server, and resuming normal operations. In addition, the ICSs are not similar to traditional home computers that can effortlessly deploy and update the anti-malware software. Further, malware was not considered when these systems were originally designed. Therefore, modern IT/OT integration requires robust security standards to prevent sabotage and industrial espionage. Additionally, these security practices must continue to evolve with the evolution of the threats.

2. Supervisory Control and Data Acquisition Systems

The supervisory control and data acquisition (SCADA) systems are a subset of ICSs. The SCADA systems involve sophisticated software and hardware elements that allow industrial organizations to achieve the following:

- ensure production safety at refineries;
- control production processes locally and remotely;
- monitor, gather, and process real-time data;
- directly interact with devices, such as sensors, valves, pumps, motors, and other devices, via HMI;

- record events in a log file.

The SCADA systems are essential for energy companies because they help to process data efficiently, thereby enabling smart decisions in real time, and communicate system concerns to mitigate interruptions. The programmable logic controllers and remote terminal units are microcomputers that transmit data to and from the sensors, end devices, and factory machines. These transmitted data are essential for plant managers and engineers to make important decisions. The corruption of these processes could be catastrophic if cyber attackers compromised the security of these systems. For example, if an attack resulted in a machine being unable to report a system malfunction to plant managers, product loss would occur and the damage would go undetected.

Cybersecurity programs are based on market solutions as well as shared practices that continue to evolve with the emergence of new threats. The Oil and Natural Gas Information Sharing and Analysis Center (ONG–ISAC) serves as a central point of coordination and communication to protect ONG exploration and production, transportation, refining, and delivery systems by analyzing and sharing trusted and timely cyber threat information, including the vulnerability and threat activity specific to the ICSs and SCADA systems. The mission of the ONG–ISAC is structured around the following four cornerstones:

1. anonymous sharing;
2. authenticated information sharing;
3. industry-owned and -operated;
4. protection from the Freedom of Information Act disclosure and anti-trust violations.

Which is the Most Vulnerable Energy Source?

Any energy source that is relied upon in an unrelenting manner is most at risk. America's electrical power grid is certainly among the most vulnerable. It comprises more than 200,000 miles of high-voltage transmission lines, several thousand power plants, traditional and non-traditional electric utilities, and millions of electronic controls and computers routing these systems. Approximately 1,075 gigawatts of electrical power is distributed across one electric power grid consisting of three systems–the Eastern Interconnect, the Western Interconnect, and the Texas Interconnect. The computers managing this monumental task were designed in the 1960s to integrate our power grid as a means to manage the generation, supply, and distribution of electricity. Over time, the complexity and sophistication of these systems have increased the efficiency of the industrial process; however, they have also become increasingly vulnerable and extremely difficult to secure.

This correlates with critical coal and gas infrastructure because approximately 35% of the electricity is produced by the combustion of coal, whereas 27% of the electricity is produced by the combustion of natural gas. Further, 19% of the electricity is produced from nuclear power plants, which would be the most ecologically disastrous target if a terrorist attack was successfully executed. A nuclear power plant is a likely target for sabotage due to the potential impact; however, because of heavy operative protocols and security, nuclear power plants are not necessarily the most vulnerable. Regardless, attacks against any of these facilities would directly affect the electrical grid of our nations.

Historically, the United States has enjoyed a geological and geographical position that has yielded a considerable competitive advantage with respect to the manner in which we produce, consume, and market the nation's energy resources. The mobilization of the modern gas

industry in 1998 by Mitchell Energy in Texas allowed the United States to become a significant force during the unconventional gas revolution. America's capacity to produce gas domestically has shielded us from foreign influence, minimizing the vulnerability of the nation's critical infrastructures. As the production of natural gas in the U.S. continued to grow, our exporting facilities in the contiguous 48 states developed to satisfy the increased demand. In 2017, the United States became a net natural gas exporter, indicating that we export more amount of natural gas than the amount that we import (see Figure 1). In 2018, the U.S. natural gas exports doubled from that in 2017 for the first time in 60 years and have further continued to increase.

Despite our advantageous natural gas position in the world, the U.S. has more than 300,000 miles of inter- and intrastate transmission gas pipelines in addition to 2.1 million miles of distribution pipelines. These pipelines fuel our industry and heat our homes. Ensuring the cybersecurity of gas pipeline companies is a major enterprise risk, and their stakeholders seek to ensure that such risks are appropriately managed. Managing such risks involves protecting the use of the ICSs that control the pipelines. As mentioned previously, these interconnected systems are not only limited to the pipelines but are also utilized across the entire energy industry, including the coal plants. The heavy reliance on these pipelines to distribute gas across the country emphasizes the interdependency among our energy and transportation sectors.

Midstream Vulnerabilities

The gas pipelines lie underground, indicating that they are safer than the above-the-ground systems. Multiple system backups and redundancies that enable failsafe environments secure the production, storage, and transportation of natural gas. LNG transportation is a precise process, where the natural gas is compressed and cooled to −260 °F. At this temperature, it becomes liquid and takes up only 1/600 of the space that it occupies in a gaseous state. This

indicates that it can be pumped into a specifically designed tanker, shipped long distances over water, and stored or re-gasified, fed into pipelines, and sent to consumers in global territories with independent laws and security postures. The aboveground risks must be well understood, managed, and mitigated. Despite the organization of the U.S. gas infrastructure, the disposition of a highly combustible commodity, such as natural gas, presents a target-rich environment for terrorists. Further, physical attacks and numerous plots have been both planned and perpetrated to achieve significant damage and disruption.

CHAPTER 2: DEFINING THE THREAT

History of Threats and Attacks: Traditional vs. Cyber

Extremists, eco-terrorists, and "hacktivists" have been determined to disrupt the transportation of gas and resort to sabotage to achieve their goals. In 2012, Anson Chi corresponded with Ted Kaczynski, the "Unabomber," and unsuccessfully attempted to bomb a natural gas pipeline in Plano, Texas. In December 2010, eco-activists opposing the construction of two LNG pipelines in Virginia trespassed onto the property of an employee of the State Water Resources Control Board. A banner reading "Stop Poisoning Our Community" was subsequently hung, and these same activists communicated plots against the LNG export terminals along the U.S. coast on the "Anonymous Contributor" website. The anonymous author posted the following threatening message:

"When we have done everything we can to prevent this pipeline with legal means, we will resort to sabotage and we will defeat this symbol of domination, exploitation, global capital, global pillage..."

Considering the amount of gas that the U.S. continues to import, disruption attacks against our geographic neighbors and trading partners would cause volatile supply disruptions and hinder free trade. Between October 2008 and July 2009, Canada's natural gas pipelines in British Columbia were bombed six times by unknown eco-terrorists. These bombings were uniquely disturbing because these natural gases contained deadly concentrations of hydrogen sulfide. In 2013, Colombia's FARC rebels bombed the rail line of Colombia's largest coal exporter, decommissioning the train for four days. Incidentally, the exports were not impeded by this event because the company had sufficient stock at the port to continue exporting.

To date, the most sophisticated cyberattack was Stuxnet, which was a virus developed by the U.S. and Israel to strike the Iranian nuclear facilities at Natanz in 2010. In 2014, other sophisticated attacks were successfully conducted when the hackers cut off a German steel mill operator's ability to shut down its blast furnaces by taking control of the mill's production software. The workers helplessly watched while the furnaces burned and destroyed the plant. In 2012, an organized "spear-phishing" attack targeted the computer network of Saudi Arabia's state-owned oil firm, Aramco, infecting 30,000 computers, which required weeks to contain. However, ultimately, this attack failed to achieve its objective, i.e., to disable Aramco's ability to supply oil. In 1982, the Central Intelligence Agency allegedly planted a Trojan horse into the USSR's Tran-Siberian Pipeline's SCADA system to disable its pumps and compressors, which caused a massive 3-kiloton explosion. The construction of this pipeline was controversial because it delivered natural gas to Western Europe during the Cold War.

Not all the cyberattacks are committed with intent to cause physical destruction. For example, some attacks are motivated by market fraud and corporate espionage. In 2014, the Department of Justice (DOJ) filed charges against five Chinese military hackers for cyber-

espionage against SolarWorld, a U.S. Corporation, for hijacking critical and sensitive manufacturing information. According to the DOJ, Chinese solar manufacturers "dumped" products into the U.S. markets at prices well below the fair value, stole thousands of files, including information on SolarWorld's cash flow statements, manufacturing and production data, and privileged legal information related to the ongoing trade litigation.

Top Ten Cybersecurity Threats

How can attackers identify the systems used by their targets? All an attacker would have to do is to visit the website of a supporting vendor, such as Honeywell, read the press releases of past initiatives to identify the systems that have been implemented to formulate a strategy, and begin planning an attack. The following list identifies the top ten cybersecurity threats:

1. Lack of awareness and training
2. Remote work
3. Using IT products with known weaknesses
4. Limited cybersecurity culture
5. Insufficient data network separation
6. Insufficient physical security of the data rooms
7. Software weaknesses
8. Outdated control systems
9. Onshore and offshore facility connections
10. Plant shutdown

CHAPTER 3: RISK EXPOSURE AND IMPACT ON STABILITY

1. Gas Processing and Production

Most of the gas processing is performed at the wellhead; however, the complete processing of natural gas is conducted at the processing plants. Much of the natural gas that we consume is primarily obtained from methane. Gas is easier to process when compared to processing and refining oil. Prior to delivering to the end user, natural gas must be separated and purified by removing ethane, propane, butane, and pentanes. There are four main processes involved in the removal of these impurities.

1. Elimination of the oil and condensate
2. Elimination of water
3. Separation of the natural gas liquids
4. Elimination of sulfur and carbon dioxide

Scrubbers and heaters play a major role during the removal process. Scrubbers are designed to remove the particle impurities, and heaters ensure that the temperature of the gas does not become considerably low. These management systems are used in a variety of applications, including separators, tanks, heaters, incinerators, and flare stacks. These systems are designed to protect heaters from explosions. Conceptually, the fire triangle, which is obtained when the fuel or flammable materials are heated, is observed when the stored energy begins to react with the oxygen in the air, generating heat. This creates a vicious cycle that causes the fire to spread. To stop the spread of the fire, one of these elements should be eliminated to break this triangle. If an attacker was to gain control of the combustion or compression process and impede the ability to purge these systems, it could result in a deadly explosion, damaged equipment, and halted production.

Another management system that could be disastrous if its processes are compromised is the vibration-monitoring systems (VBSs). A VBS comprises wireless transmitters and sensors that provide intelligent monitoring and early detection of the damaged rotating machine parts. These systems directly impact a plant's distribution of the product to the end users. A VBSs optimal performance is critical because they enable plants to maintain peak efficiency by preventing unplanned downtime, reducing maintenance costs, and improving reliability. Following the processing of natural gas, its storage can be just as vulnerable if compromised. In addition, the tank inventory systems control the commands that change any alarm affected by the gas' level, temperature, and pressure.

Fiscal Metering

The flow computers facilitate fiscal metering, which involves custody transfer. Fiscal metering of gas involves a highly specialized process because gases are more difficult to measure when compared to liquids and are highly affected by the parameters of temperature and pressure. The ability of a flow computer to calculate the gas quantities based on these parameters are of paramount importance, and quantity measurement is imperative when upstream companies sell gas to midstream companies. Here, a small error could result in wastage of millions of dollars. The security measures for such computers make them extremely difficult to access; however, one should not underestimate the motivations of a disgruntled employee or an agent working for a hostile group or nation. These are not attacks in the traditional sense; when the production accounting systems can be manipulated to commit market fraud.

Market Fraud

How can hackers commit market fraud? Precise inventory levels are critical to a gas company's economic viability, and even a slight error, e.g., a fraction of a percent, could result in

millions of dollars in losses. For example, the hackers could manipulate a company's supply data by transmitting fake information to managers who make decisions based on this data. If these decision makers were deceived and ultimately exhausted their supply, their inability to deliver gas to customers and satisfy obligations could lead to changes in gas prices, resulting in huge losses that could possibly bankrupt the given company. By successfully installing malware, hackers can also manipulate stock figures, where systems, such as SAP, are used by deliberately understating the data about the stock of the affected companies to control the price of the stock. Such attacks can be achieved by exploiting SAP or Oracle Management plant connectivity applications that transfer data from the task management systems to the SAP systems.

Coal Processing and Production

Several methods are used during the coal extraction processes from both the surface and underground mines. Monumental labor efforts are involved in these processing plants to produce the final product. In **surface mining**, the ground covering the coal seam must be initially removed to expose the coal seam for extraction. Further, surface topography controls are employed in various surface mining methods, e.g., mining contour, area strip, or open-pit mining. The methods employed for loading, transporting, and storing coal are predominantly different. For example, contour mines are the most common in the hilly Appalachian terrain of the eastern United States where the overburden (see Figure 2), i.e., a material that lies above a coal seam, must be transported. **Underground mining** (see Figure 3) is observed when any ore body is a considerable distance below the surface, the amount of waste to be removed for obtaining the ore through surface mining is prohibitive, and underground techniques should be considered.

The functional **processing** involved in coal preparation is common among different plants. The sequences can be given as follows:

1. crushing and breaking;
2. sizing;
3. storage and stockpiling;
4. density separation;
5. froth flotation;
6. coal drying;
7. refuse and tailings management.

In 2017, approximately 757 million short tons of coal were produced in 24 states, among which five states produced approximately 538 million short tons (approximately 71% of the total U.S. coal production). The five largest coal-producing states (see Figure 4) with respect to the production in million short tons and their share of the total U.S. coal production in 2017 can be given as follows:

- Wyoming (316.5 million short tons; 41% of the total U.S. coal production in 2017)
- West Virginia (92.8 million short tons; 12% of the total U.S. coal production in 2017)
- Pennsylvania (49.1 million short tons; 6% of the total U.S. coal production in 2017)
- Illinois (48.2 million short tons; 6% of the total U.S. coal production in 2017)
- Kentucky (41.8 million short tons; 5% of the total U.S. coal production in 2017)

Cybersecurity Challenges in Mining

To date, there have been no successful attacks against coal plants, resulting in damage or denial of services. The Trump administration and Department of Energy (DOE) suggest that coal's security strengths compared to gas are related to cybersecurity due to the dispersed and exposed nature of the gas pipelines that feed power plants, leaving them difficult to defend. In contrast, it is physically difficult to penetrate coal plants. Some argue that although coal plants are easier to guard physically, they still have numerous digital networks and computer systems controlling heavy machinery that can be hacked.

Generally, the IT security expenditures in mining are small when compared to other business expenditures. The processes have become computerized to promote efficiency relative to managing of company data, operations, and assets. However, the risk has increased because the use of such digital technologies has increased and they have become more interconnected. The use of process control networks (PCNs) to monitor and control industrial infrastructure and processes has become more common in the mining industry. PCNs communicate the commands and data between traditional control and measurement components as well as SCADA equipment. Historically, PCNs have been protected from hackers using the so-called "air gaps" that isolate them from unsecured networks and have been considered to be low risk from a cybersecurity perspective because they can only be accessed by onsite mining staff. However, this has subsequently changed. Today's mining operations have become integrated into company-wide networks. These networks enable the employees to operate assets remotely to manage various functions, including the circulation and detection of flammable or harmful gases as well as machine temperature monitoring and controls. If these systems were to be hacked and sabotaged, an inability to control the systems could lead to injury and/or death, equipment

damage, cessation of production, and interruption in the supply of utilities. These forms of attacks can be committed from accidentally inserting a thumb drive containing malware to sights that are traditionally sealed off from outside networks. Highly sophisticated email or browser-based attacks include phishing, Trojans, and worms.

Distribution and Transportation

The annual coal distribution report (ACDR) provides detailed information about U.S. domestic coal distribution according to the origin state, destination state, consumer category, and transportation method. The ACDR also summarizes a nation's foreign coal distribution based on the coal-producing nation. Note that all the data for the 2017 report are final, current, and contain the following.

- The total coal distribution for 2017 was 767.7 million short tons.
- The distribution to foreign and domestic destinations was 767.8 million short tons.
- Railroads moved approximately 68.6% of the domestic coal (see Figure 5), river barges accounted for 12.1%, trucks approximately 9.3%, and tramway, conveyor, and slurry pipelines accounted for 10.0%. Great lakes and tidewater pier transport modes accounted for less than 0.1% of the total shipments.
- The electric power sector received approximately 92.5% of domestic distribution, whereas commercial, institutional, and industrial plants received the remaining 7.5%.
- In 2018, U.S. coal exports were the highest in five years (see Figure 6).

Freight Rail Security

The transportation of coal by rail affects the communities through which the coal passes. For example, trains that haul coal temporarily block the roads, causing traffic congestion on major roadways that could potentially delay or otherwise impede emergency responders or

temporarily cut off residents from emergency services. Thus, a well-timed attack against a coal-transporting train could be deadly. A national response to such terrorist attacks would be costly and further compound the success of these attacks. The Department of Homeland Security (DHS) and Department of Transportation (DOT) prescribed "voluntary" security practices for railway HAZMAT carriers, including scheduled training drills, criminal background checks on employees, and a designated liaison to the government emergency response agencies. Many believe that compliance with these security practices should be mandatory; however, the rail industry has claimed that these practices and preplanned responses in their training programs have been in place well before the government issued its recommendations. Following the 9/11 terrorist attacks, the rail system identified its vulnerabilities and made significant changes to its operations. The rail system has the best safety record among that of any transportation method used in the United States. The 9/11 terrorist attacks continue to increase fears in American society, and subsequent attacks against the passenger rail systems in London, Madrid, and Mumbai have raised concerns about possible terrorist disruptions to the American freight rail transportation.

Fuel on Hand

Although efficient in minimizing the inventory holding costs, just-in-time delivery faces the risk of shortages when supply lines are disrupted. These supply lines can be exposed to both physical and cyber threats. Some argue that the benefit of "fuel on hand," which means fuel sources, such as gas, that is stored onsite in substantial amounts will make fueled power plants more resilient in its response to a disruption caused by an attack. Others argue that the risk of stockpiling a highly combustible gas sensitive to temperature and pressure creates a considerable opportunity for failure and mishap. A recent announcement from the DOE stated that cyber and

physical threats could be mitigated at coal plants because they can store months of "fuel on hand" to survive supply disruptions that could not be mitigated by natural gas facilities because of their reliance on the pipeline networks.

President Trump and Energy Secretary Rick Perry announced the halt of coal retirement to create a "strategic energy generation reserve" with the same intent as that of the U.S. Petroleum Reserve, which was created in 1973 in response to the 1970's energy crisis. This crisis was caused by an oil embargo imposed by the members of the Organization of Arab Petroleum Exporting Countries, which resulted in fuel shortages and excessive prices. The halting of coal retirement was further solidified in 2017 when President Trump signed an Executive Order (see Figure 7) directed at the Environmental Protection Agency to begin the complex and lengthy legal process of repealing the then President Obama's Clean Power Plan (CPP). The CPP would have closed hundreds of coal-fired power plants, halted the construction of new ones, and replaced them with wind and solar farms.

Proponents of the Trump administration's move believe that the exposures to threats can be minimized if electric generation facilities can maintain coal and nuclear stockpiles onsite. In case of attack, the Energy Department would exercise emergency authority under a pair of federal laws, i.e., the Defense Production Act of 1950 and the Federal Power Act, and order operators to purchase coal from at-risk facilities, which is an unprecedented intervention with respect to the energy markets. However, the opponents of the Trump administration's move believe that federal intervention to rescue a dying industry will damage the energy market because it orders customers to purchase expensive electricity from designated power plants. The federal government centralizing its authority in any market would distort the demand signals and disrupt competition. I believe that our nation's energy security is the most secure when diverse

means of power generation are available that serve as a contingency plan to protect our citizens in case of a disaster.

CHAPTER 4: CHALLENGES AND RECOMMENDATIONS

Current and Potential Issues

Although no actual cyberattack or physical attacks have succeeded against the U.S. gas and coal infrastructures, credible threats and attempts continue to occur. A successful attack against our energy infrastructure that result in instability or loss would leave our civilization in a state of panic, similar to the one our society witnessed during 9/11. This makes such threats more difficult to address for decision makers, especially because we cannot physically notice such threats and the types and methods of attacks. Unlike a physical attack, cyberattacks can cause immense damage before they are even detected.

Private Industry and Government Cooperation

From a legal perspective, there are no set reasonable standards of IT security compliance mandatory for a private enterprise to follow. This is largely because 80% of the energy infrastructure is owned and managed by the private sector. Regardless, there is some functional level of government cooperation with respect to energy security. The DOE provided technical assistance to help the states develop energy assurance and resiliency plans with support from the National Association of State Energy Officials.

Cyber Readiness Funding, Legislation, and Policy

Because of slow government action, the private sector has been forced to take cybersecurity seriously and is expected to spend more than $1 trillion on digital security globally through 2021; however, no specific figures were available with respect to energy sector spending. Through the American Recovery and Reinvestment Act (ARRA) of 2009, the DOE

allocated $38 million in grants to assist states in developing plans designed to respond to the energy supply shocks, provide training to improve coordination between federal and state personnel, improve recovery and restoration capabilities, and address vulnerabilities. These plans are also designed to address supply disruptions to the nation's energy resources, including electricity and natural gas, in response to the cybersecurity threats.

In 2018, Rick Perry established the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at the DOE, and $96 million in funding for the office was included in President Trump's fiscal year (FY) 2019 budget request to strengthen the DOE's efforts related to cybersecurity and energy security. The creation of a CESER office will elevate the DOE's focus on energy infrastructure protection and will enable coordinated preparedness and response to cyber, natural, and man-made threats. The DOE has announced $28 million in funding for 11 research partnerships, aiming to improve the technologies that combat cyberattacks. This funding will come from the CESER and fund four national laboratories and several large electric utilities as research partners. Although paling in comparison to private sector spending, these can be considered to be meaningful first steps.

Figure 1

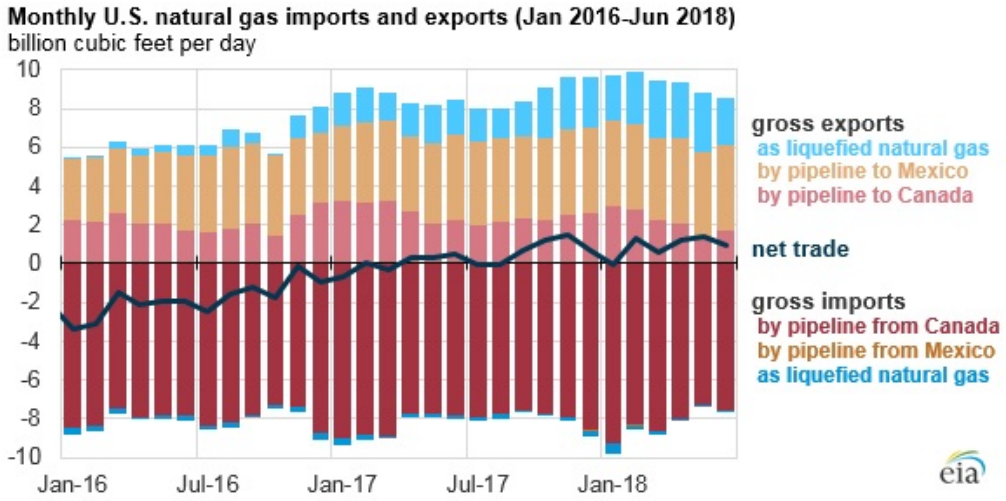

Figure 2

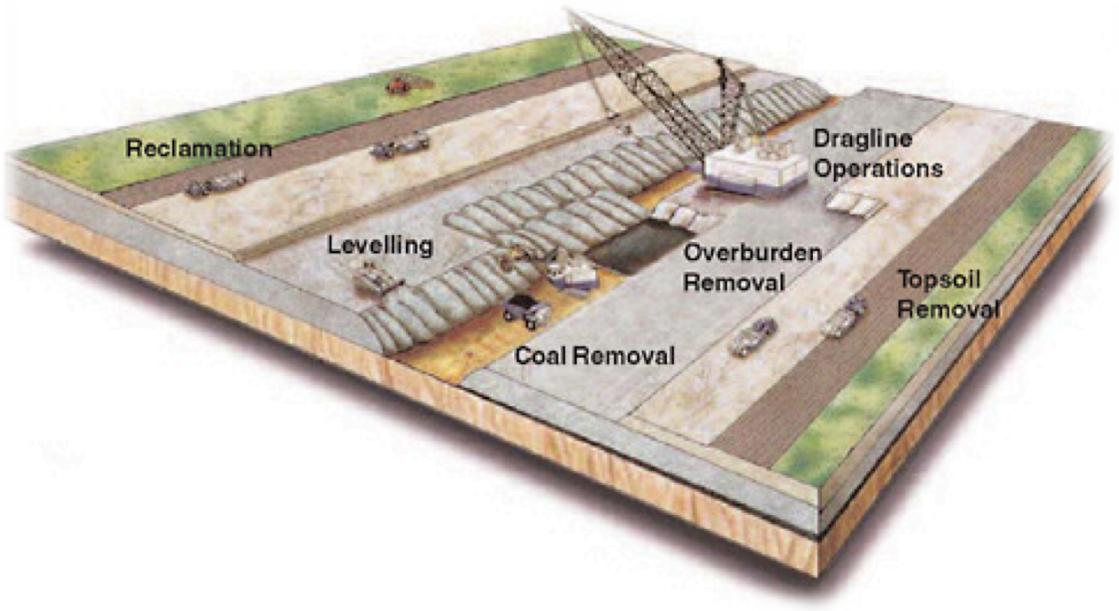

Figure 3

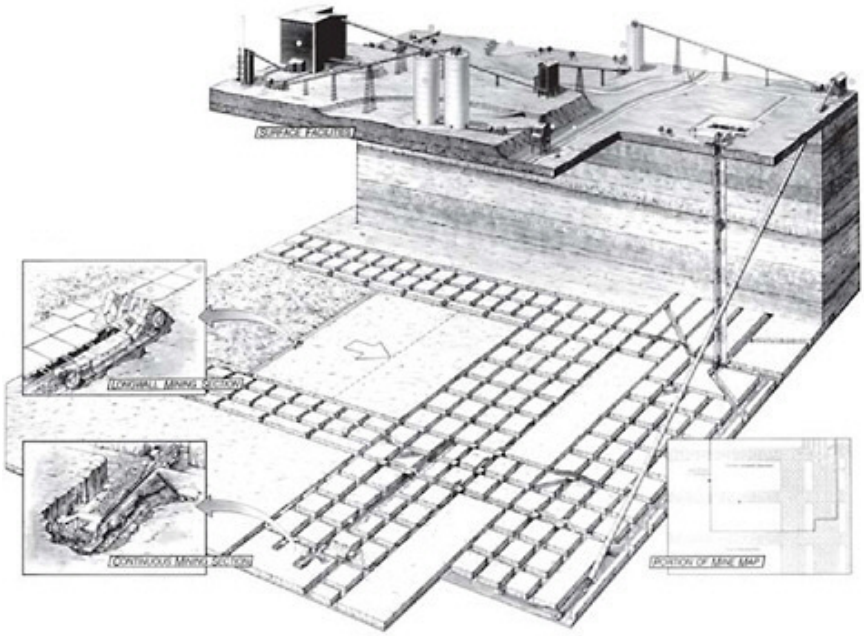

Figure 4

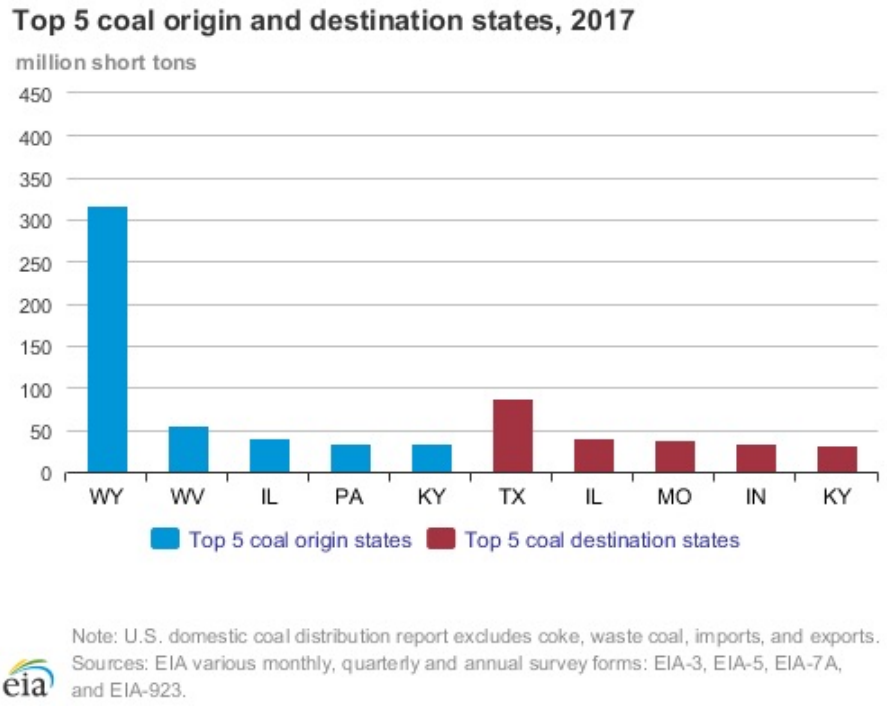

Figure 5

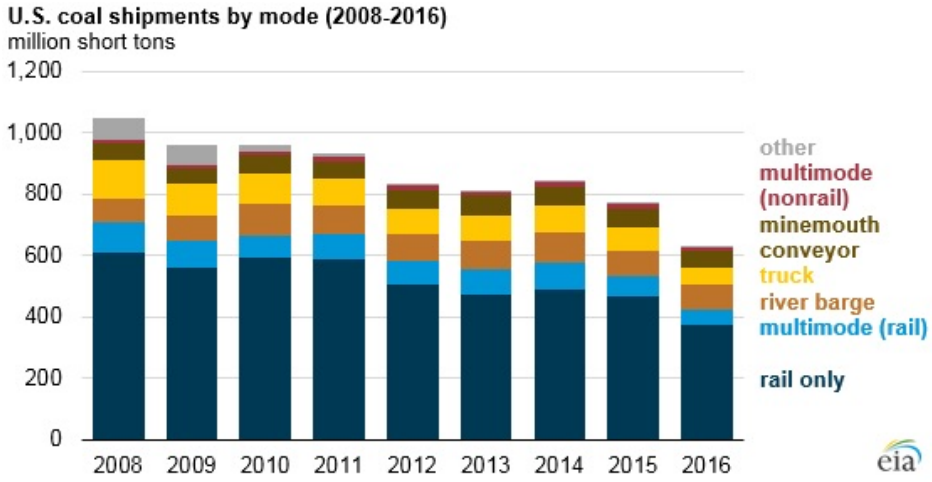

Figure 6

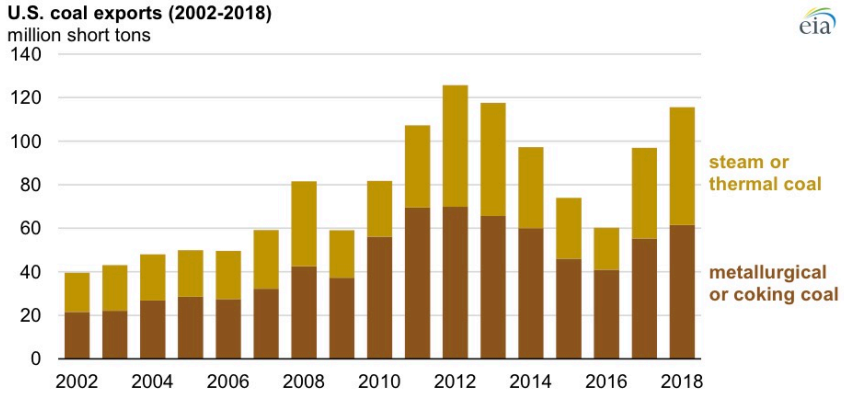

Figure 7

References

United States, Congress, "National Infrastructure Protection Plan." National Infrastructure Protection Plan, 2013, www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

"U.S. Energy Production & Consumption." U.S. Energy Facts - Energy Explained, Your Guide To Understanding Energy - Energy Information Administration, 15 May 2016, www.eia.gov/energy-explained/?page=us_energy_home.

"SAP Customer Reviews | Software & Technology Solutions." SAP, www.sap.com/about/customer-testimonials.html. Accessed 27 Feb 2019.

"Oracle on the Forbes Best Management Consulting Firms List of 2019." Forbes Magazine, www.forbes.com/companies/oracle/#63541db3509c.

Haughn, Matthew. "What Is Industrial Control System (ICS)? - Definition from WhatIs.com." 16 Mar 2016. https://whatis.techtarget.com/definition/industrial-control-system-ICS.

"Proprietary protocol." www.pcmag.com/encyclopedia/term/49868/proprietary-protocol. Accessed 27 Feb 2019.

"ONG-ISAC: Oil and Natural Gas Information Sharing and Analysis Center." https://ongisac.org. Accessed 01 Mar 2019.

"Electric Power Grid." United States Nuclear Regulatory Commission - Protecting People and the Environment, 21 Mar 2019. www.nrc.gov/reading-rm/basic-ref/glossary/electric-power- grid.html.

"U.S. Energy Information Administration - EIA - Independent Statistics and Analysis." What Is U.S. Electricity Generation by Energy Source? - FAQ - U.S. Energy Information Administration (EIA), 1 Mar 2019. www.eia.gov/tools/faqs/faq.php?id=427&t=3.

Dyl, Katie. "U.S. Net Natural Gas Exports in First Half of 2018 Were More than Double the 2017 Average - Today in Energy - U.S. Energy Information Administration (EIA)," 27 Mar 2019, www.eia.gov/todayinenergy/detail.php?id=37172.

Marie, Chloe. "Research Guides: Natural Gas Pipeline: Home." Home - Natural Gas Pipeline - Research Guides at Penn State School of Law-University Park, 6 Jul 2018, https://pennstatelaw.libguides.com/naturalgaspipeline.

"Plano Blast Suspect Corresponded with Unabomber." Dallas News, 30 Jun 2014, www.dallasnews.com/news/plano/2014/06/29/plano-blast-suspect-corresponded-with-unabomber.

Anonymous Contributor. "Virginia: On Eve of ACP Decision, Banner Dropped at Board Member's Home." It's Going Down, 12 Dec 2017, https://itsgoingdown.org/virginia-eve-acp-decision-banner-dropped-board-members home.

Bright, Arthur. "Bombings of Canadian Pipelines Spark Ecoterrorism Fears." The Christian Science Monitor, The Christian Science Monitor, 17 Oct 2008, www.csmonitor.com/World/terrorism-security/2008/1017/p99s01 duts.html.

Kimball, Jack. "Colombian Rebels Blow up Biggest Coal Exporter's Railway." Reuters, Thomson Reuters, 14 Mar 2013, www.reuters.com/article/us-colombia-cerrejon-attack-idUSBRE92D13H20130314.

"Cyberattack on a German Steel-Mill." Sentryo, 29 Dec 2016, www.sentryo.net/cyberattack-on-a-german-steel-mill/.

Nichols, Megan Ray. “10 Cybersecurity Threats Facing The Oil And Gas Industry.” Manufacturing.net, 31 Jul 2018, www.manufacturing.net/article/2018/01/10-cybersecurity-threats-facing-oil-and-gas-industry.

“Natural Gas Processing” NaturalGas.org, 25 Sep 2015, www.naturalgas.org/naturalgas/-processing-ng/.

“Mine Spoil Waste.” www.encyclopedia.com/environment/encyclopedias-almanacs-transcripts-and-maps/mine-spoil-waste. Accessed 27 Mar 2019.

Clark, George B., and William Andrew Hustrulid. “Mining.” Encyclopedia Britannica, Encyclopedia Britannica, Inc., 25 Apr 2017, www.britannica.com/technology/mining/-Underground-mining.

“U.S. Energy Information Administration - EIA - Independent Statistics and Analysis.” Annual Coal Distribution Report - Energy Information Administration, 5 Nov 2018, www.eia.gov/coal/distribution/annual/.

Kaplan, Eben. “Rail Security and the Terrorist Threat.” Council on Foreign Relations, Council on Foreign Relations, 8 Mar 2007, www.cfr.org/backgrounder/rail-security-and-terrorist- threat.

Northey, Hannah, and Peter Behr. “WHITE HOUSE: Trump Orders DOE to Halt Coal, Nuclear Retirements.” WHITE HOUSE: Trump Orders DOE to Halt Coal, Nuclear Retirements -- Friday, 1 Jun 2018, www.eenews.-net/stories/1060083235.

Talton, Ellis, and Remington Tonar. “A Lack Of Cybersecurity Funding And Expertise Threatens U.S. Infrastructure.” Forbes Magazine, 28 Apr 2018, www.forbes.com/sites-/ellistalt-on/2018/04/23/the-u-s-governments-lack-of-cybersecurity-expertise-threatens-our-infrastructure/#5d1f2beb49e0.

Hartman, Kristy. “ Protecting the Nation’s Energy Infrastructure: States Address Energy Security.” National Conference of State Legislatures, 2013, www.ncsl.org/documents-/energy/EnergySecurityFinal-10-13.pdf.

“Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response.” Energy.gov, 14 Feb 2018, www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity energy-security-and-emergency.

“Department of Energy Invests $28 Million to Advance Cybersecurity of the Nation's Critical Energy Infrastructure.” Energy.gov, 1 Oct 2018, www.energy.gov/articles/department-energy-invests-28-million advance-cybersecurity-nation-s-critical-energy.