2-2013

Evaluating the National Preparedness of the United States Against an Electromagnetic Pulse Threat

Matthew W. West

APUS Library Capstone Submission Form

This capstone has been approved for submission to and review and publication by the APUS Library.

Student Name [Last, First, MI] *	West	Matthew	W
Course Number [e.g. INTL699] *	HLSS699	**Paper Date** [See Title pg.]	02/2013
Professor Name [Last, First] *	Bundy, Edwin		
Program Name * See list	Homeland Security		
Keywords [250 character max.]			
Passed with Distinction * Y or N	Y		
Security Sensitive Information * Y or N	N		
IRB Review Required * Y or N	N	If YES, include IRB documents in submission attachments.	
Turnitin Check * Y or N	n/a	All capstone papers must be checked via Turnitin.	

* Required

Capstone Approval Document

The thesis/capstone for the master's degree submitted by the student listed (above) under this title *

EVALUATING THE NATIONAL PREPAREDNESS OF THE UNITED STATES AGAINST AN ELECTROMAGNETIC PULSE THREAT

has been read by the undersigned. It is hereby recommended for acceptance by the faculty with credit to the amount of 3 semester hours.

Program Representatives	Signatures	Date (mm/dd/yyyy)
Signed, 1st Reader * [capstone professor]		
Signed, 2nd Reader (if required by program)		
Recommendation accepted on behalf of the program director *	Kelli Frakes Digitally signed by Kelli Frakes DN: cn=Kelli Frakes, o, ou, email=kfrakes@apus.edu, c=US Date: 2016.08.16 10:09:46 -04'00'	
Approved by academic dean *	Digitally signed by Mark T. Riccardi DN: cn=Mark T. Riccardi, o=American Public University System, ou=Academics, email=mriccardi@apus.edu, c=US Date: 2016.08.24 15:49:21 -06'00'	

* Required

AMERICAN PUBLIC UNIVERSITY SYSTEM

Charles Town, West Virginia

EVALUATING THE NATIONAL PREPAREDNESS OF THE UNITED STATES AGAINST AN ELECTROMAGNETIC PULSE THREAT

A research paper submitted in partial fulfillment of the requirements for the degree of

MASTER OF ARTS

in

HOMELAND SECURITY

by

Matthew William West

Department Approval Date:

DEDICATION

This paper is dedicated to my parents, Robert and Kathy West, who gave me support throughout my life and encouraged me to pursue my dreams. To my grandparents, whose wisdom and stories of the “good old days” taught me how to make things work without modern technology, and to my wife, Rachel West, who has wholeheartedly stood beside me, supported and motivated me to chase my dreams!

ACKNOWLEGEMENTS

I wish to thank the professors, faculty, and staff of the American Military University's Department of Homeland Security and the Department of Emergency Management who taught me how to look beyond the obvious. Special thanks to Dr. Edwin Bundy, as his guidance throughout my research was invaluable. I would also like to thank Beth West, whose journalistic experience helped keep me on the right page.

Finally, I would like to express my gratitude to my supervisors and coworkers at the Union Pacific Railroad Police Department, who have supported me in my educational endeavors.

ABSTRACT

EVALUATING THE NATIONAL PREPAREDNESS OF THE UNITED STATES AGAINST AN ELECTROMAGNETIC PULSE THREAT

by

Matthew William West

American Public University System, November 27, 2012

Charles Town, West Virginia

Professor Edwin Bundy, Professor

This paper evaluates the threat that an electromagnetic pulse presents to the infrastructure of the United States of America. Several key reference materials were studied and evaluated for this research project. Of particular interest, the *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures* (2008) is the primary reference of this research project. This U.S. government publication is the most comprehensive overview of EMP threats that is available through the public domain. This document, coupled with online publications such as *Future Science* (Emanuelson, 2008), help examine just how vulnerable the United States is to an EMP threat and how the nation, as a whole, is not prepared for such an event.

TABLE OF CONTENTS

CHAPTER PAGE

Chapter I: Introduction

In the late 18th and early 19th centuries, the Industrial Revolution began in the United States and Europe, opening the door for a variety of new technology and inventions that would forever change the way human beings lived. Inventors such as Robert Stephenson, who pioneered the steam locomotive; Edward Butler with his gas powered internal combustion engine, and Dr. Rudolph Diesel and his engine that ran on peanut oil, all transformed transportation to allow for expedient travel across vast areas. When these marvels of transportation were first introduced they were considered a novelty and only a handful of businesses and people were able to afford them as they were considered expensive luxuries that were not easy to maintain. As technology progressed, and mass production was introduced, internal combustion powered vehicles became readily available and affordable to the general public. With an estimate of over 200 million vehicles on the road in the U.S. today, the automobile has become a fundamental part of our economy as a way to transport goods and ferry people to and from their jobs (Associated Press, 2003).

Toward the middle 19th and early 20th centuries, several other inventions were introduced that would change the way Americans live. Thomas Edison, Alessandro Volta, Nikola Tesla, and George Westinghouse all played an important role in bringing electricity and lighting to the average consumer. With the advent of readily available electricity, other inventions flourished to take advantage of this power source. Heating and cooking could now be done quickly and efficiently without the use of gas, wood, or oil and keeping food and medications safely stored was another direct benefit of electricity.

The advent of electricity also allowed communication to improve. No longer were people forced to converse with pen and paper that took days or weeks to deliver by courier, but thanks to telegraphs, telephones, and radios, communication became instantaneous, whether it originated from across the street or across the globe.

Fast forward to today and it is amazing how much technology has advanced over the last 200 years. Particularly in the last four decades, the increase of electronic technology has grown exponentially. Mammoth mainframe computers of the 1960s and 1970s gave way to desktop-sized computers in the 1980s and 1990s. By early 2000, laptop computers began to take a stronghold in both the workplace and home. During the same time frame, the Internet became readily available, and affordable allowing people to connect to one another instantaneously in a variety of media forms such as email, instant chat, and video conferencing. Computer technology then rapidly combined with cellular radio technology to open the doors to communications on-the-go without wired power, telephone cords, or network cabling.

As electronic technology becomes more and more intertwined with our everyday lives, our dependency on it has grown. Checkbooks are rapidly becoming a thing of the past, with cash rapidly following pace as credit cards, smart phone applications and Internet banking have changed the way we handle our financial transactions. Electronic computer technology has tightly interwoven itself into the supply chain, public safety services, military defense systems, and virtually every aspect of our daily life. As unique as each system is, ultimately they are all intertwined, and depend on one common denominator…power.

Just over 150 years ago, electricity was considered a convenience, almost a novelty if you will, however; in today’s American society, electricity is crucial as millions of people have become dependent. Should our power generating stations, or any component of the electrical grid be compromised for an extended length of time, it would mean an almost certain collapse of modern society as we know it.

It may be hard to imagine any one event that could wipe out an electrical grid system that could bring America to its knees, but the reality is, a large-scale electromagnetic pulse (EMP) could quickly, and unexpectedly, turn the power off for some time. What makes this even more nerve-racking is that this threat not only comes from a man-made device, but from a source of power that Mother Nature herself sends our way.

Chapter II: Electromagnetic Pulse (EMP) Threats

High-Altitude Electromagnetic Pulse

Electromagnetic energy is found in abundance throughout the universe and is an important aspect of everyday life. Our main source of electromagnetic energy is derived from the sun and is an essential part of nature; however, technical advancements over the last century have taught us how to harness and concentrate electromagnetic energy. We can see it in the form of visible light, listen and view it in the form of radio and television waves, and even use it to heat food in the form of microwaves. (Encyclopædia Britannica Inc., 2012)

While the advances of electromagnetic energy have helped transform society to become more productive, it is also being looked at as a weapon to topple developed nations. Hollywood movies such as *Battleship, Battle Los Angeles, Transformers,* and the *Matrix* have introduced the term EMP into main stream vocabulary, and have raised awareness of nations competing to complete a functional EMP weapon, when in reality; EMP weaponry has been around since the detonation of nuclear weapons.

In 1958, space scientist James Van Allen announced his discovery of radiation belts (now known as the Van Allen Radiation Belts), that encircle the earth, and are held together by the earth's magnetic field. (Krulwich, 2010) Ironically, according to Krulwich, Van Allen agreed to work with the United States government to see if a nuclear blast could potentially disrupt this field.

Nearly four years later, on July 8, 1962 at approximately 11:00 pm (Honolulu time), the Starfish Prime project was completed, and Van Allen's work was about to be tested. On the Johnston Atoll, the United States military launched a rocket-propelled hydrogen bomb and exploded it 400 kilometers directly above the test facility. (Vittitoe, 1989, p. 3) Conventional explosives such as dynamite, TNT, or C4 release energy in the form of heat and light, while a nuclear blast will release large amounts of X-rays and gamma rays. (Plait, 2012)

Aside from creating a dazzling light show for people living on the Hawaiian Island chain, the explosion and subsequent release of the X-ray, gamma rays, and electrons caused the unexpected result of knocking out nearly 300 streetlights and damaging a microwave link belonging to a telephone company on the Island of Oahu located nearly 800 miles away from ground zero. (Emanuelson, EMP History, 2008) Additionally, several satellites were destroyed as a result of the blast due to radiation being trapped by the earth's magnetic field, and creating its own artificial Van Allen Belt. (Plait, 2012)

Russia began testing a series of high altitude nuclear devices between 1961 and 1962, known as the "K tests" as they were detonated over the airspace of Kazakhstan. Since the tests commenced over a highly populated area with abundant industry, the results of the nuclear detonation created a much larger recorded electromagnetic pulse effect. This larger high-altitude electromagnetic pulse (HEMP) caused damage to diesel generators; disrupted telephone, microwave, and radio communications; and created a fire in an electrical generator station. (Daniel, 2009) Although much of the Russian tests are still classified, the information that has been ascertained shows that the scientists conducting the high altitude nuclear tests were very much aware, and deeply interested in, the electromagnetic pulse phenomenon.

As both countries raced to build their nuclear program, they began to understand more and more about how electromagnetic pulses worked. One such discovery of this research revealed that the HEMP created three distinct pulse waves, the E1, E2, and E3 waves, each occurring at separate time intervals from the initial explosion.

The first wave, known as the early-time waveform (E1), happens almost instantaneously after a high-altitude nuclear explosion. Its speed is so fast that common surge and voltage protectors designed to suppress lightning strikes are not quick enough to stop the pulse. (Emanuelson, 2010) It is the E1 wave that is devastating to electronics as it generates extremely high voltages in sensitive electronic devices such as computers and other electronic devices, especially those coupled with short wire systems such as WiFi antennas and other short cables such as those used for computer and information networking.

Up to one second after the initial explosion and E1 wave, the intermediate-time wave form is created. Known as the E2 wave, it has characteristics similar to the electromagnetic pulses generated by lightning, and in most of the research, it is appears to be largely ignored. In theory, common products used to protect electronic equipment against lightning strikes could prevent damage to electrical devices from an E2 pulse. Emanuelson (2010) did point out the probability that there would be a high likelihood that the original E1 pulse could easily disable protection devices, rendering them useless against the following E2 pulse.

Appropriately named the late-wave pulse, the E3 pulse is the last in the chain of EMPs. Similar to a solar flare striking the earth, the E3 actually is able to displace the normal magnetic field of the earth and last a few seconds to hundreds of seconds before the magnetic field is restored. (Daniel, 2009) Pulses create by the E3's magnetic energy field has the most affect on long transmission lines and antennas. Phone systems, power grids, data lines, and radio communications would be the most susceptible to damage or substantial disruption from an E3 pulse.

Ironically, as devastating as a high-altitude nuclear weapon is to electronic equipment through its EMP, the actual weapon itself is essentially harmless to humans as the nuclear radiation fallout is contained well above the earth’s atmosphere and is filtered out naturally as the early tests in the 1960s nuclear tests conducted by the United States and Russia both revealed.

What makes the HEMP such a strategic weapon is its potential to impact a large geographic area. A comprehensive Nuclear Environment Survivability study, released by the United States Army in 1994, estimated that a HEMP could have crippling effects on various electronic dependent systems for hundreds of thousands to even millions of square miles, and even went as far as saying, “HEMP has the greatest range of damage of all nuclear effects.” (Department of the Army, 1994, p. 61)

To put this in perspective, the United States encompasses approximately 3.5 million square miles of land, this would mean that if a HEMP has an effective radius of one million square miles, it would directly impact nearly one-third of the United States. If a HEMP of this magnitude were detonated somewhere between Chicago and New York City, power and electronic devices for hundreds of millions of people living in this radius could be severely disrupted or destroyed.

In a 2004 congressional hearing, it was stated that if a nuclear device was detonated 500 kilometers above the United States, that the entire nation would be impacted by the resulting EMP wave. Congressman Curt Weldon (Pennsylvania) best described this HEMP scenario as being the “…ultimate terrorist threat”. (Committee on Armed Services, 2004, p. 12)

The threat of a man-made electromagnetic pulse is a grave reality. Countries such as North Korea, Pakistan, Russia, China, and Iran have the potential capability to launch a HEMP attack based on their current nuclear threat. During a 1999 meeting at the Duma International Affairs Committee, Russian delegates stated that they could (in retaliation for the United States involvement in Kosovo) launch a high altitude nuclear explosion from a submarine that would "shut down everything." (Committee on the Judiciary, 2005) In August of 2012, media outlets across the U.S. reported that a Russian nuclear attack sub had operated for several weeks undetected in the waters of the Gulf of Mexico. During the same time frame, several Russian Cold War era long range-bombers were reported to have entered restricted U.S. airspace. While it is unknown exactly why Russia conducted these maneuvers, we should take heed at the stealth and speed at which an attack could occur.

While less devastating, a nuclear bomb being detonated at or near ground level would emit a source region electromagnetic pulse (SREMP). Geographically speaking, the SREMP would affect metallic lines, such as phone, Ethernet, and power lines for up to 70 miles, causing great voltage spikes that could heavily damage any device that was connected to them. (Department of Homeland Security, 2012)

Non-Nuclear Electromagnetic Pulse Threat

Aside from a high altitude nuclear threat, other non-nuclear electromagnetic pulse (NNEMP) threats exist that pose a limited risk to our electronic infrastructure. A majority of these threats are found in the form of radio frequency weapons (RFW). Since the 1960s, RFW have historically been used to disable radio, microwave, and satellite communications; however, it has been found (through mainly accidental applications) that radio frequencies have caused the disabling of vehicles, created disruptions in public utility systems, and have even caused pipeline explosions. (Department of Homeland Security, 2012)

Learning from incidents where radio waves or other directed energy sources have crippled electronic systems, the United States military has been studying how the effects can be built into a weapon platform; however, the process has been slow and expensive. Working for more than four decades, the United States military has been trying to perfect radio frequency and other directed energy weapons with limited success.

In a 2008 article, *Wired Magazine* highlighted a RF weapon built for the United States Army called the Active Denial System. Similar in looks to a common radar system, the weapon is mounted on a multipurpose heavy tactical truck. When activated, the weapon, which emits a high frequency radio wave, is pointed at a human combatant and causes them to become extremely hot. There is concern that if the weapon is used multiple times on a single subject, or left on too long, it could cause third-degree burns or even death. (Hambling, 2008) Other similar radio frequency weapons work on a variety either ultra-low or ultra-high frequencies, but their primary intended effect is to provide a non-lethal threat on humans, and not the ability to take out electronics systems.

This does not mean that all non-nuclear electromagnetic weaponry is being designed strictly for non-lethal human applications. In 2001, the United Kingdom announced a missile system that, when launched, would deploy a small explosion before reaching the target, releasing small RF transmitters that would send out a pulse disabling electronic command centers, and any other weapons that used electronic systems. (Information Handling Services, 2001)

One of the most recent and successful developments of a non-nuclear electromagnetic pulse device was publicized by *Popular Science Magazine* in 2010. Built by Eureka Aerospace, the EMP cannon has the ability to disable a vehicle's electronic system within an approximate 650 foot range. (Hsu, 2010) While the cannon is relatively bulky in size, work is underway to condense the cannon into a suitcase-sized device so that it may be used by law enforcement to quickly disable cars, eliminating dangerous vehicular pursuits. While the *Popular Science* article did not go into detail about the military applications, it would not take much imagination to come up with numerous defense applications for the device.

If this technology becomes widely available to either military or law enforcement, we should be concerned about what would happen should it wind up in the wrong hands. Since the cannon has limited range, and appears to have a concentrated energy beam, this would mean only electronics in which the device was aimed directly at would be in harm's way. Imagine an extremist who wanted to take out a flood control system, damage the power grid, or disrupt any other critical infrastructure that was dependent on electronic control systems. The results could still have a negative effect on millions of people.

Space Weather Events

Our solar system's sun provides the building blocks essential for life on earth. It causes plants to grow, shapes our weather, and even directs our gravitational pull; without the sun, planet earth could not sustain human life. Prior to the 19th century, the only negative effects the sun had on humans was the risk of UV exposure (sunburn), dehydration, and drought. Today, with the United States' dependency on electricity and electronic systems, the sun has created an electromagnetic pulse threat in the form of solar flares and Coronal Mass Ejection (CME).

According to NASA (2010), solar flares are defined as a sudden release of electromagnetic energy from the solar atmosphere. These radioactive waves spread across the entire electromagnetic wave spectrum, producing anything from long wavelength pulses to x-ray and gamma radiation. The explosive energy released by solar flares is the equivalent of millions of 100 megaton hydrogen bombs being detonated.

Solar flares are a natural occurrence, and have been studied for over 150 years. During that time, scientist have classified solar flares by using an alphabetical scale of A, B, C, M, and X with each letter representing a 10 time increase in energy output. (Fox, 2011) According to Karen Fox with NASA (2011), the "C" level solar flares are not even noticeable to us on earth and it is not until "M" level ratings that we begin to see the negative effects of radio blackouts and radiation danger that pose a potential danger to astronauts. It is the "X" class solar flares that are of potential concern to our nation's electronic infrastructure. These flares have the potential of knocking out satellites, communication systems, and even the electrical grid across the planet. (Fox, 2011)

A CME is one of the largest and potentially most devastating space weather solar threats. CMEs are large bubbles of plasma that erupt with tremendous force, sending charged particles toward the earth at the rate of over 4.4 million miles per hour. (SRI, 2012) Like a "X" class solar flare, CMEs have the potential to cause major disruptions in the earth's magnetic fields. In testimony given by Director Brandon Wales of the Department of Homeland Security's National Protection and Programs Directorate Infrastructure Analysis and Strategy Division, a Coronal Mass Ejection is the biggest concern for Homeland Security officials as it pertains to a space weather electromagnetic pulse threat. (DHS, 2012) Unlike a HEMP from a high altitude nuclear device that produce E1, E2, and E3 EMPs, solar flares and CMEs produce effects that are similar to an E3 wave length, making electrical components connected to long metallic lines more susceptible to failure.

Solar storm is the name given to a solar flare event or CME that is strong enough to disrupt the earth's magnetic field. These storms have three stages to them, although according to Dr**.** Daniel N**.** Baker with the University of Colorado Laboratory for Atmospheric and Space Physics, solar storms come in three phases. The first wave is composed X-ray, high-energy sunlight, and ultra-violet rays that effect radio communications. Secondly, a wave of radiation follows, creating a hazard of exposure to astronauts and aviation personnel who fly at high altitudes for long periods of time. Finally, the CME particles hit and interact with the earth's magnetic field causing major fluctuations, although the three events do not necessarily happen each time. (Lovett, 2011)

From a historical aspect, solar flare and CME events have only been recorded since the late 19th century. British astronomer Richard Carrington was one of the first scientists able to observe and record an extreme solar flare event and link it to earth-related events. Carrington's observations were originally published in the *Monthly Notices of the Royal Astronomical Society*, vol. 20, 13-15, 1860. In his report, Carrington documented that he was mapping "solar spots" that he was observing by using a telescope that projected the sun through tinted plate onto a media in which Carrington could literally trace solar flares..

On September 1, 1859, Carrington noticed an unusually bright light being displayed, to the point where he believed that that the tinted plate filtering the light had broke. Realizing that this was not an equipment malfunction, and instead, an anomaly of the sun, he ran to get a witness, but by the time he returned, the initial event had passed. (Carrington, 1859) It was what happened when the solar event hit the earth's magnetic field that intrigued scientists.

Hours after the solar event impacted, telegraph operators began to report that their telegraphs were sparking, and even that the operators themselves had been shocked. The aurora borealis was so bright, people could clearly read newspapers during the dark of night and it was reported that the northern lights could be seen as far south as Cuba. Even a day after the initial event, telegraph operators could send limited messages through the line without battery power as the residual magnetic energy provided enough electricity to send a signal. (Klein, 2012)

Even though the telegraph was the most advance electronics system in Carrington's time, scientists still benchmark this event, known as the Carrington Event, as being the most powerful solar flare event ever recorded. According to an article on History.com (The History Channel), ice core samples were taken during a research project to compare solar flare events over the past 500 years, and the Carrington Event was revealed to be at least two times larger than any other solar event. (Klein, 2012)

Dr. Sten Odenwald, a NASA astronomer, created a website dedicated to space weather that includes a history of the most notable solar weather events recorded since the 1859 Carrington Event. From August 28, 1862 until October 29, 2003, ninety-eight major solar weather events were reported. Most of these events were reported to be an unusually bright display of the aurora borealis allowing it to be seen in a greatly extended geographic area than normal.

Since technology was fairly limited during the first half of the recorded solar weather events, telegraph lines appeared to be the only thing documented as being affected by the storms. As technology advanced, more and more problems were being associated with these solar storms. In 1821, the New York Central Railroad had to halt operations due to signal and switch failure as well as a fire that erupted in a control tower. On March 25, 1940, a solar storm created extremely high voltage spikes in which telegraph and telephone lines designed to carry around 48 volts suffered voltage spikes upwards of 600 volts; in addition, power generating stations in

New York reported voltage fluctuations of nearly 1,200 volts. (Odenwald, 2003) Other anomalies that have been documented as a result of solar storms include: carbon filaments in lamp posts spontaneously glowing, loss of radio communications, and electrical grid failures.

Chapter III: EMP Threats to the U.S. Infrastructure

Threat Against National Power Grid

Modern society has become so dependent on technology that it has become interwoven into nearly every aspect of our lives. If you think about it, when you get up in the morning to brush your teeth, the light switch you flip sends electricity from the power grid to the light bulb, causing it to illuminate. Water from the faucet is being electronically monitored and pumped from a well, and monitored and pumped through a waste water disposal plant. The toothbrush and toothpaste you are using were more than likely manufactured at a production plant using modern automated technologies. As one could imagine, this scenario could continue on and on, into an almost indefinite loop. What this scenario reinforces is the fact that just about every item we use today is dependent on electricity in some form or fashion.

The United State's power grid is considered to be the largest power generation and distribution center in the world. There are over 10,000 power generating plants in the U.S., using a variety of electrical generation resources such as: coal, hydro-electric, nuclear, and natural gas as their primary energy source. An additional 5,000 distributed energy facilities (solar and wind generation) transfer approximately 830 gigawatts of electricity over 211,000 miles of high voltage lines. (The Energy Library, 2009) According to the Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (2008), which will be referred to as the EMP Commission Report, "The electrical power system is the largest single capital-intensive infrastructure in North America" (p 17) and is one of the few critical infrastructures that, if it were to fail, could stop the normal daily lives and activities of all Americans.

In order to maintain and regulate the electricity throughout the United States, Canada, and parts of Mexico, the entire grid is overseen by the North American Electric Reliability Corporation (NERC). The duties of the NERC are to ensure proper reliability standards, enforce these standards, and ensure the security of the entire grid. (NERC, 2012)

In the U.S., the power grid is then broken down into three major sections: the Eastern Interconnection, the Western Interconnection, and the Texas Interconnection. Each interconnection is responsible for generating and monitoring the power needs for its geographical region (each region has several sub-regions that help monitor and regulate). All interconnections in the United States operate on alternating current (AC) at a rate of 60 Hz. Due to the fluctuating demand of electricity, each interconnect is tied into one another in order to help with fluctuating electricity needs. In order to better control such needs, the point where these grids converge must be able to convert the alternating current to direct current (DC), allowing more control over voltage regulation from one grid to another. (Prince, 2009) (The Energy Library, 2009)

Knowing how interconnected the power grid is, and how it helps maintain the social and economic sustainability to the over 300 million people in North America, it is much easier to see how the sudden lack of electricity could have a devastating impact. While storms, mechanical failure, and human error have all produced blackouts over the decades, all have been temporary and fairly short lived, but the chaos these blackouts sometimes bring leave lasting impressions. Solar storms and an E3 pulse generated from a high-altitude nuclear attack have the capability of knocking out a majority of the U.S. power grid, damaging expensive and hard to replace electrical components and potentially leaving hundreds of millions of people without power for up to months at a time.

In its April 2008 report, the EMP Commission, with the assistance of numerous respected scientists from around the country, studied the potential vulnerabilities found within the power grid as a result of an HEMP attack or solar weather event. To fully understand the impact, the commission broke its study down to the three basic components of the power grid: electricity generation, transmission, and distribution.

First, we will look at the vulnerabilities in the generation phase. Power generating plants (as with most critical infrastructure control facilities) have a series of electronic and manual control systems that act as a check and balance in the case of power fluctuations, sudden power loss to control systems, or unexpected shut down of the generator itself. Solar weather, E2, and E3 pulses are not of much concern to as they pertain to the generating plants themselves; however, in the event of a nuclear induced EMP, the E1 pulse poses the greatest threat.

Since the E1 pulse has the potential to destroy computer circuitry and other voltage-sensitive electronic devices, systems that monitor temperature, voltage, pressure, and other critical parameters may be at risk, although should any of these systems fail individually, protective systems are built in to create a “soft shutdown” of the equipment to prevent damage. Even with secondary systems in place, an E1 pulse has the potential to damage these protective systems and even the main control system that regulates the soft shutdown procedures. In the event that a plant had an unregulated shutdown, severe damage to equipment could occur that not only would be expensive to repair, but could take months or years to do so. (EMP Commission, 2008, pp. 29, 30)

Older power plants may be somewhat protected from an E1 pulse, simply because of the physical structures they are constructed in, and the mechanical controls that they utilize have limited electronics and wire. Currently in the United States, there are approximately a little over 1,100 coal fired plants; of these, a majority are more than 40 years old (Peltier, 2011), meaning that the operating systems have few electronic dependencies. As these plants began to retire, new, high-tech plants such as natural gas, wind, and solar are being built.

Newer plants will become more dependent on computerized operating systems, making them much more vulnerable to E1 pulses. Regardless of the age and the type of monitoring system, a HEMP that injects itself into the power grid will send an instantaneous E1 pulse that would directly impact numerous plants. If a large majority of power plants were hit with an E1 pulse, it could cause an instant collapse of power production. (EMP Commission, 2008, p. 30)

What really makes the power grid so vulnerable to failure is the hundred of thousand plus miles of extra high-voltage (EHV) electrical lines that span North America. During a solar storm or E3 pulse, the earth's magnetic field becomes distorted and as nature attempts to reset its magnetic field, it creates electrical charges that stream back through the magnetic field, usually from the earth's core outward to space. (Flatow, 2012) These electrical charges are attracted to long metallic lines and towers (such as EHV transmission lines) where amperages from these electromagnetic charges can be found in upwards of tens of thousands of amps.

This increased amperage can then travel through the power lines and back to the source (power generating station) or an end user (to a manufacturing plant or your home computer). (Forstchen, 2008) Electric transformers would take the brunt of damage caused by an E3 pulse or solar storm, due to their inherent design that makes them dependent on magnetism. (RAF Tabronics, 2007) Geographic location of the power plants and the EHV lines themselves may also make them more susceptible to increased geomagnetic induction. According to the NERC, locations where EHV lines run on or near igneous rock formations or large bodies of water stand a much higher risk of the geomagnetic interference. (NERC, 2011, p. 32)

In the NERC's 2011 Workshop Summary Report (2011, p. 34), researchers analyzed data to see what kind of impact that a solar storm, such as those experienced in 1859 or 1921, would have on transformer durability. Research indicated that there was a potential for 20 percent of 345-kV transformers, 28 percent of 500-kV transformers, and 32 percent of 765-kV transformers could be damaged or fail. The study shows that nearly 350 high-voltage transformers would fail nationwide in a matter of hours, 94 of which would be generating station step-up transformers. Even if only 50 percent of the predicted failures occurred, a majority of the grid would be shut down for a relatively long duration of time.

While utility companies and transformer manufacturers often have residential and light business transformers in reserve to deal with replacement during large scale storms, EHV step-up and step-down generators found at power generation stations and sub-stations are not easily replaced. In 1989, a solar storm hit earth causing wide spread electrical grid problems, including the Hydro-Quebec grid failure that left millions in the dark for over nine hours. In the Hydro-Quebec incident, the solar weather caused five main lines to trip, creating a voltage loss of 9,450 megawatts (MW) while it was under a load of 21,350 MW. This sudden decrease in power created a chain reaction of failures, bringing down the entire grid in a matter of 90 seconds. (Thompson, 2012)

A 1991 report from the Oak Ridge National Laboratory, titled *Electric Utility Industry Experience with Geomagnetic Disturbances* examined actual events recorded by electrical utility companies during geomagnetic storms. According to the report, during the same 1989 solar event that caused the Hydro-Quebec grid failure, an EHV step-up transformer at the Public Service Electric & Gas Company's Salem 1 Nuclear Plant succumbed to a critical failure directly related to the electromagnetic interference. In this case, the transformer suffered damage beyond repair to the low voltage windings, thermal insulator degradation, and a melted conductor. (Barnes, Rizy, & McConnell, 1991, p. 12) Since step-up transformers must be particularly engineered for their specific application, replacement times for these large generators can be upward of two years, as such was the case with this incident.

Nuclear power plants also pose a unique danger in the event of grid collapse. Even if a nuclear power plant is safely taken off line, the stored nuclear rods must be continuously cooled. Backup generators are installed at these plants to provide power in the event of power grid loss; however, should the generators be damaged by E1 or E2 pulses, or generator fuel supplies be depleted, a repeat of the 2011 Fukushima, Japan tsunami disaster could be repeated. (Pry, 2011) It is unknown exactly how much fuel each United States nuclear power plant has onsite for emergency power. We can gain a little bit of insight on fuel supply based on the comments made by the Exelon Corporation on its preparations for Hurricane Sandy. Referencing their New Jersey Oyster Creek Nuclear Power Plant, Exelon stated that they would be able to run on backup generators for approximately two weeks before needing to be refueled. (Associated Press, 2012)

Other anomalies to the power grid that have been reported during geomagnetic events, and were included in the Oak Ridge report (pp. 12-16), included a report of surge arrestor failures as a result of oversaturated transformers; relay failure as a result of transformer problems or interference from geomagnetic charge; and voltage regulation problems from the failure of static VAR compensators (SVCs) that provide rapid voltage regulation in high voltage lines.

In the EMP Commission Report (EMP Commission, 2008, pp. 43-44) many of the same historical failures were studied as documented in the Oak Ridge Laboratory report; however, in the EMP Commission report, several distinctions were made on the difference between an EMP disruption on the power grid versus historically large area outages, such as those created by hurricanes or other natural events.

One distinction made by the commission (pp. 43-44) was that traditionally during past grid failures, only one (or very few) critical hardware failed, which caused a domino effect in shutting down the remainder of the system. In the likelihood of a HEMP or extreme solar weather event, multiple stations would hit simultaneously causing cascading failures in more than just one system. Components during historical events have also tripped or shutdown as they were originally designed to do. In an EMP event, it is likely that numerous components would not only be tripped, but would be heavily damaged, meaning total replacement.

Secondly, telecommunications have historically worked during prior grid failures. This still allowed for monitoring of substations and remote infrastructure by trained personnel. In the case of an EMP, telecommunications would most likely be disrupted, making remote monitoring, and even remote controlling of these systems impossible, resulting in potential system failures in these systems. Due to the unreliability of these control systems, properly diagnosing the full extent of damage would be a long and tedious task.

Finally, the enormous scope of grid failure would make it logistically impossible to get trained personnel to the entire damaged infrastructure within a timely manner. In a worst case scenario, the EMP Commission believes that nearly 70 percent of the North American power grid could be shut down as a result of an EMP event. (EMP Commission, 2008, p. 44) As a result of such a catastrophic failure, a large number of components could be damaged that would exhaust replacement supplies on hand. Infrastructures such as transportation, manufacturing, and general commerce would shut down in a cascading effect. This would result in a breakdown of virtually every type of service known, and would be reminiscent of the problems experienced by the devastation of hurricane Katrina, but on a much larger scale.

Based off the summary solutions published in the NERC summary, several steps are already in place to help diminish potential problems when geomagnetic storms are predicted or in progress. These steps include: (NERC, 2011, pp. 36-42)

- Establishing protocol and operating procedures when a solar storm threat is imminent
- Reducing electrical output and loads (usually by a 10% reduction)
- Avoid taking EHV lines out of service for maintenance
- Monitor real-time geomagnetic events through the use of sensors and monitoring stations

Although major power utility companies have realized just how vulnerable the North American power grid is to the effects of EMPs and have taken steps to mitigate potential problems, many still do not have a backup plans in case of a large damage or shutdown. Realizing that the United States does not have a reasonable backup plan in the event of a wide scale failure of transformers and other components, the EMP Commission has requested that the power industry work with the Department of Energy (DOE) and Department of Homeland Security (DHS) to institute a plan on how to recover from an EMP event.

Some of the steps presented by the EMP Commission (2008) that power companies should implement in order to prepare for a catastrophic EMP event include:

- Retrofit, modify, and upgrade existing equipment with commercially available products.
- Create contingency planning at a national and regional level
    - Define government and industry roles
    - Prioritize service
- Availability of replacement and backup components
    - Create modular transformers that would run at limited capacity
    - Assure that components can be adequately transported in the case of fuel and transportation shortage
- Extend “black start” capabilities of power plants
    - Have alternative fuels available to power generation equipment

Funding many of the proposed upgrades to harden our electrical grid does not come cheap. Significant hardening the power grid would cost billions of dollars in equipment, labor, and testing. As with many government mandates, it appears that the utility companies would have to foot the bill, which would mean that the cost for such upgrades would dramatically increase consumer electrical costs.

Impact on SCADA Systems

Our modern industrial age is more dependent on technology than ever before. Industries may now monitor and regulate complex control systems from thousands of miles away. Known generically as Industrial Control Systems (ICS), these systems help monitor, regulate, and control critical infrastructure and other important industries such as oil and gas production, power production and distribution, and water quality monitoring.

In particular, an electronic system known as the Supervisory Control and Data Acquisition (SCADA) is the primary monitoring and control systems used by industries that need to have real-time information to control systems over a large geographic area. Typical SCADA systems are characterized by information being processed in a central control station which, through either an automated process or through manual input from an operator, sends the data back to field devices (remote station devices) that may then open or close control valves, circuits, or alarms. (Stouffer, Falco, & Kent, 2006, pp. 2-1) Often, field devices are found in extreme remote areas or in environments where physical human monitoring would be hazardous.

SCADA systems are very complex control systems that involve a variety of technology components. In the control center, known as the Master Terminal Unit (MTU), there are an abundance of computer servers, hardware, and other software systems interconnected between themselves and the field devices through a combination of telephone, radio, or satellite communication devices. (Stouffer, Falco, & Kent, 2006, pp. 2-6) Field devices are not as complex as the MTU, but still must rely on hardware, software, and telecommunication systems.

Since SCADA systems are reliant on electricity and telecommunications, this makes them particularly vulnerable electromagnetic pulses. With their integrated circuits and reliance on antennas to communicate, SCADA can quickly fall victim to an E1 pulse from a HEMP attack. Depending on their environment, many SCADA field devices may be ruggedized and enclosed in a metal protective box, however; because of exposed antennas and short length wires (fed to routers or computer systems), field devices are very vulnerable. (EMP Commission, 2008, p. 5)

According to the EMP Commission's report (2008, pp. 5-7), operational SCADA components were subjected to an E1 magnetic pulse at a governmental EMP testing facility.

After the test, results showed that virtually every system reported some sort of failure. The severity of each failure ranged from catastrophic failures such as the shorting of circuitry to nominal failures that were cured by conducting a reboot of the system. Based off the data presented, the study found that the sheer number of failures alone, despite their severity level, would cause SCADA systems to ultimately fail completely.

Historically, failure of certain SCADA systems have proven to be catastrophic, not just to the system it controls, but to the general public as well. On July 10, 1999 in Bellingham, Washington, a SCADA system that was not functioning properly failed to release extreme pressures that had built up on a damaged gasoline pipeline. Creating a rupture in the line, over 230,000 gallons of gasoline were released in a nearby creek, which then ignited, killing two 10 year old boys and an 18 year old man. (Singel, 2008)

In 1980, a radar signal interfered with a SCADA system that controlled a valve in a natural gas pipeline in The Netherlands. The improperly operating valve sent shockwaves through the pipeline resulting in an explosion. Nineteen years later after The Netherlands incident, a ship's radar, located 25 miles off the coast of San Diego, California, interfered with a SCADA control system for the San Diego aqueduct system. Workers were able to manually avert the disaster, but had it not been detected in time, severe flooding could have occurred, placing people and property in danger. (EMP Commission, 2008, pp. 2,8)

SCADA systems also have failed as a result of malicious computer virus attacks. In 2003, a nuclear power plant in Ohio lost its safety monitoring system for nearly five hours. In the same year, a SCADA system controlling a portion of the power grid was infected with a virus that knocked out power to over 50 million people. (Singel, 2008) Even though these two attacks were induced by a manmade computer virus, it illustrates just how important SCADA systems are to safety, and in an EMP event, similar failures could occur.

In order to ensure safe operation of these complex systems, SCADA systems are engineered and designed with the forethought that a system failure is inevitable at some point and time. Alarms, redundancy systems, rerouting, and automated safety shutdown procedures are a common part of SCADA design, but as the EMP Commission points out, these designs are engineered for a single point system failure and not for multiple failures that an EMP would create. (EMP Commission, 2008, p. 9) Charles Perrow best summed up the complexity and venerability of SCADA systems by stating, “We have produced designs so complicated that we cannot possibly anticipate all the possible interactions of the inevitable failures; we add safety devices that are deceived or avoided or defeated by hidden paths in the systems”. (Perrow, 1999, p. 11)

Solar storms and E3 pulses do not pose much of a threat to SCADA systems, except for the connection to the commercial power grid or commercial telephone line. It is the E1 and E2 pulses that pose the greatest threat. Hardening SCADA systems to prevent EMP interference are easier done in self-contained structures, such as a production plant, where there are no external field units. Shielding network cabling and having control systems enclosed in electromagnetic resistant protective cases, commonly known as a Faraday cages, would help prevent damage from E1 and E2 exposure.

SCADA field units, on the other hand, may be harder to protect, as many of them rely on wireless communication and solar and battery power. Even if protected by a Faraday enclosure, the exposed antennas and power sources still would make them susceptible. As with the power grid, new technology designed to suppress the quick voltage spikes generated from an EMP should be integrated into the antenna and power inputs to prevent damage.

Telecommunications

Prior to the mid-20th century, most people related the term “telecommunications” to the thought of hard-wired telephone systems that connected homes, businesses, and operating systems to one another, and overall, this was very true. During this timeframe, wireless communications generally consisted of two-way radio systems, microwave communication (for long distance phone service) or limited satellite communication. Bulky, and expensive, wireless communications were primarily used by large businesses or governmental entities. Fast forward to the 21st century and we find that telecommunications has engulfed almost every aspect of technology. Meshing copper landlines with fiber optics, cellular radio communication, satellite, microwave, and computer-based internet telephony systems has allowed us to communicate in ways never before thought possible.

This interwoven technology, which is 100 percent power dependent, drives our daily and business lives. Global positioning systems (GPS) use satellites to communicate with land based transponders to pinpoint specific locations. Used on land or on water, GPS has enabled us to track logistics, view battlefield assets in real time, or give directions to the nearest supermarket.

Cellular, microwave, telephone, and internet protocol (IP) systems allow us to conduct transactions without the physical use of cash. Gas stations with pay at the pump, remote automatic teller machines (ATMs), and online banking are all dependent on telecommunications to operate efficiently and effectively. With our “cashless” society that depends on credit/debit cards, American society has become ever so dependent on telecommunications for everyday financial transactions.

Government entities have now built their entire infrastructures around telecommunications. Public safety services rely on GPS, two-way radios, wireless broadband, and mobile computing to dispatch calls for service. Police departments use license plate readers to instantaneously check for stolen cars, in-car computers to check criminal databases and complete reports. Fire and ambulance services use similar systems to find the quickest route when responding to emergency calls and are able to update hospitals with real time patient information while still en route to the emergency room.

Businesses use an abundance of telecommunication equipment to conduct day to day business. Smartphones use high-speed cellular technology to allow employees to conduct business on the road. World-wide business meetings take advantage of video conferencing to allow participants to meet without leaving their home offices. Business computing systems use hardwired Ethernet cables and wireless networking (WiFi) to backup, store, and distribute software and files to end users using remote servers, and more recently, cloud technology.

As a nation, we have become so dependent on the entangled web of telecommunications that any prolonged interruption could mean potential economic collapse and the stoppage of many services. A prolonged loss of telecommunications could be just as devastating as a prolonged loss of electricity.

Many telecommunication facilities, both wired and wireless, have been hardened against electromagnetic interference from the beginning. Cellular towers and landlines must be engineered to prevent bleed-over and interference from other telecommunication devices. Their components are magnetically shielded and in the case of cellular sites, lightning arrestors and other voltage regulation devices are already installed to prevent damage to the delicate systems.

Fiber optic lines, which are already considered less susceptible to EMPs, are quickly replacing aging copper telephone lines. (EMP Commission, 2008, p. 67)

Admittedly, there seems to be very little research on just how an EMP would affect telecommunication systems nationwide. Based off historical records, such as the Carrington event, and other subsequent solar storms, we have learned that solar weather, with its E3 pulse like characteristics, can have a severe impact on long metallic transmission lines, however; these lines were connected above ground, and today, most telecommunication wires are being installed subterranean. According to a 1984 report from Manuel Wik, a defense administrator in Stockholm, Sweden who studied EMP effects on telecommunication devices, buried telephone cables are less susceptible to EMP effects based off extra insulating factors.

Despite the limited testing, government officials still believe that telecommunication equipment will be affected as a whole, especially in the case of a HEMP event. We know that E3 type pulses can disrupt wireless communication due to interference with radio waves as they travel through the atmosphere. In more recent times, the temporary loss of cellular, microwave, satellite, and conventional radio communications have all been recorded during solar storm events.

Even with basic hardening techniques that are applied to telecommunication facilities, there are still numerous common building components that can act as a conductor, especially to an E1 and E2 pulse. Radio towers, guide wires, metallic fencing, electrical plumbing, climate control systems, and even the metal reinforcement inside concrete structures can create system breaches. (Wik, 1984)

Studies on the power grid and SCADA systems have revealed that E1 pulses can disable sensitive electronic circuitry, such as the components that control and monitor a variety of our telecommunications infrastructure. It is strongly believed by the United States government that much of the (civilian) telecommunications systems would develop circuitry damage, particularly at repeater stations, greatly crippling our communications infrastructure. (Committee on National Security, 1997)

Even if the telecommunications systems prove to be more resilient than the U.S. power grid, there are still a couple of factors that would hinder communications. First, and foremost, is power. Today, a majority of telecommunication systems have alternative power sources, such as generators and battery backup that allow communications to continue, even during a continued power outage. On average, most telecommunication systems can operate on backup power for up to 72 hours before either fuel or battery supplies need to be replenished. (EMP Commission, 2008, p. 68) In the worst case scenario of a 70 percent outage of the nation's power grid, replenishing such supplies would be next to impossible due to logistical failures.

On October 29, 2012, Hurricane Sandy slammed into the New Jersey shore, negatively impacting not only New Jersey, but New York City as well. A day after the storm hit, it was estimated that Verizon Telecommunications Company lost nearly 25 percent of its regional cell network, emergency 9-1-1 centers were knocked out of operation, and numerous land line systems were down because of flooding at key telecom stations. (Carew, 2012) Several days later, Broadband for America (2012) stated several key Internet infrastructures were damaged, knocking out Internet access to key areas of the Northeast Coast.

Seven years prior to Hurricane Sandy, another major hurricane named Katrina knocked out telecommunications systems along the Gulf Coast state of Louisiana on August 29, 2005. Entire radio, telephone, and Internet services were knocked completely out of service. Police officers for the City of New Orleans could not communicate for days, 9-1-1 centers were either off-line or overwhelmed, and backup generators for all systems could not be refueled. (Henry, 2006)

Secondly, the most common failure of telecom systems, and one deemed most probable in the event of an EMP, or any large scale disaster, is the overloading of the telecommunications network. People commonly experience this congestive effect when participating in large events where thousands of people are gathered, such as professional sporting events. Often, it is difficult to make or receive cellular calls at these events as the cellular towers are taxed beyond their operating call loads. With an EMP event already causing degradation of telecommunication services, even nominal traffic on these systems could cause connection failures, preventing emergency and government responders from communicating as needed.

Traditionally, telecommunication providers have been able to quickly respond to a disaster, quickly restoring services within a matter of hours, days, or at the most, weeks. Such a rapid response and recovery time is due in part of preexisting contingency planning, and pooling of resources. In a majority of these circumstances, areas are still confined within relatively small geographic areas, and not the hundreds of thousand square miles that is predicted from an EMP event.

Since 1951, the United States Government has utilized telecommunications as a means to warn the general population of any imminent threats to the country. Originally known as the Control of Electromagnetic Radiation system (CONELRAD), established during the Cold War by President Truman to warn Americans of a nuclear attack, the system has grown and morphed into what is known today as the Emergency Alert System (EAS). According to the Federal Emergency Management Agency (FEMA), “The Emergency Alert System is one of the many means used by alerting authorities to send warnings via broadcast, cable, satellite, and wireline communications pathways". (FEMA, 2012) According to FEMA, this is one of the primary communication tools that allow the President to communicate to the nation.

Concerns have been raised about how the EAS would work in an EMP event, particularly a high-altitude nuclear strike. According to the EMP Commission (2008, p.149), the primary EAS signal sent out by the President is transmitted on high-power AM radio stations, known as primary stations, that then send the alert messages to other AM and FM radio stations. The secondary AM/FM stations then continue the leap-frog effect, and transmit to other public communication providers.

According to the EMP Commission's 2008 report (pp. 154-155), an assessment of the EAS was conducted to include site surveys and EMP testing. The Commission seemed content that many of the commercial communication nodes had adequate backup power, such as generators or batteries, and felt confident that these systems would continue to work. While testing the radio equipment against an EMP field, the report noted that an AM receiver/decoder failed in dormant mode and an AM radio also failed. FM communications only reported erratic signals at high EMP levels.

Even though the EMP Commission states that they feel confident that the EAS will function at a "near normal fashion" (2008, p. 155), their own testing should prove contrary to their belief. Indicating that the origination of the EAS is from high-powered AM radio stations, and based off of their own testing that primarily affected AM radios, it can easily be deduced that the initial warning system could fail as a result of an E1 pulse damaging source radio and satellite components as well as the E3 pulse blocking the transmission signals from traveling normally through the atmosphere.

On November 9, 2010, a nationwide test of the EAS was conducted under normal (stable) conditions. According to the Society of Broadcast Engineers, a majority of broadcast stations received the EAS alert, but due to other technical difficulties, the test message did not reach some viewers or listeners. (SBE, 2010) With the test not reaching end users under normal conditions, this reaffirms that the EAS may not be successful in alerting the American public under an EMP event.

Since in-depth testing of EMP effects has not been thoroughly conducted, the exact effects that an EMP event would have on the North American telecom infrastructure is unknown. Telecom systems are becoming more and more hardened against EMP events as modern technology, such as fiber optic lines, is rapidly replacing older, more vulnerable components such as the traditional copper telephone lines. Retrofitting of older systems and buildings can be very costly for telecommunication companies; however, incorporating electromagnetic interference resiliency is currently being incorporated into the costs of new construction and upgrade implementations. (FEMA, 1984)

Transportation

According to the United States Census Bureau (2012), in 2009, there were over 254 million registered vehicles and nearly 116,000 public transportation vehicles operating on an excess of 4 million miles of roadway in the U.S. Other estimates about our transportation industry indicate that rail transportation accounted for well over 24,000 locomotives pulling an estimated 1.5 million railcars over 170,000 miles of train track, and in the airline industry, 24,000 flights serviced nearly 400 airports, while over 25,000 shipping containers traversed the 325 seaports in America . (Ritter, Barrett, & Wilson, 2007, p. xxi)

With the astonishing number of vehicles travelling across America, one does not have to look at statistics to realize just how vital transportation is. As people begin to move out from the perceived urban decay of large cities and into the suburbs and small bedroom communities surrounding metropolitan areas, the use of automobiles, buses, and passenger rail has made us even more dependent on transportation than ever before. Even individuals who live inside the larger cities often must drive or commute to work as they may live too far from their job to walk or ride a bike.

Without reliable and regular transportation, businesses in the United States would not be able to function adequately and efficiently. Personally owned vehicles and public transportation provide a means and a way to shuffle employees to and from work. If personal and public transportation were to cease, businesses would suffer greatly as they would have no way to adequately staff their factories, warehouses, or stores.

Thanks to our modern computer age, our economy has never been so dependent on transportation for the manufacturing and selling of goods as it is today. Several decades ago, it was traditional for retailers to keep a stockroom full of merchandise to keep their shelves from running bare. Usually, shipments were brought in by truck at a particular day and time. This meant that retail managers had to forecast their sales and hope that they did not over or under stock their products. Manufacturers also had to predict how sales were going to be in order to adjust assembly line flow. Needless to say, this was not a very efficient approach.

In the late 20^{th} century, the just-in-time (JIT) manufacturing and logistics approach was adopted by most manufacturers and retailers. This concept, used widely by Toyota in Japan, reduces stockroom space (allowing for more retail sales space) and reduces inventory costs.

(Abilla, 2007) Today JIT is dependent on both computer technology and quick transportation of goods.

A large retail store such as Target or Wal-Mart is an excellent example of how JIT works. As customers check out items at the register, computers monitor the current stock, and as they get low, send a message either to management or through other automated systems that new stock needs to be ordered. Orders are then placed to the manufacturer, who begins to produce the needed product.

If produced overseas, the product must quickly be produced and shipped, usually via intermodal containers, to the United States where it is then hauled by train and/or truck to the retailer, all of which takes place in the matter of days. Should transportation be disrupted for any length of time, products would quickly disappear from the shelves. According to the EMP Commission (2008, p. 112), in the event of a complete breakdown of transportation, most stores in large cities only have enough food staples to last several days.

Today's modes of transportation depend on electricity both directly and indirectly. Internal combustion engines operate off a spark or heat source to ignite the fuel in the engine's cylinders. To accomplish this, a direct current battery sends power to a coil, which is a basic transformer/inducer. Power then is distributed to the spark plugs that ignite the engine. A vehicle's alternator or generator charges the battery and keeps other electrical components such as the radio and other power accessories running.

Up until the late 20th century, cars and trucks (light and heavy duty) had a basic electrical system as previously described. As automobile technology has advanced, so has the dependency on computerized control systems. Even the most economically priced vehicles on the market today have more components and controls dependent on the small onboard computer system than ever before.

Since E3 pulses and solar weather events do not affect a vehicle's electrical system, the real threat comes from the E1 and E2 pulses found in a HEMP attack. During the Starfish Prime and Russian "K Project" tests of the 1960s, automobiles, locomotives, and airplanes did not have the sensitive electronics that are incorporated into their construction as they are today, so the effects on their components are truly unknown.

Automobiles and Trucks

Limited EMP laboratory testing has been done on automobiles and trucks (to include truck-tractors) to test the impact that an EMP would have on their electrical systems. The only published report on the testing is found in the EMP Commissions report (2008, pp. 115-116). During that test, a total of 37 automobiles (passenger cars) and 18 trucks (pickup trucks and semi-tractors) were tested in a simulated EMP environment. E1 waves were produced at various increments until a failure was observed or the 50 kV/m threshold reached (2008, p 115). Vehicles were tested in a running and non-running condition.

Testing indicated that all cars and trucks functioned normally when exposed to an EMP while in the non-running condition. When testing began while the vehicles were fully operational, three automobiles and three trucks exhibited complete engine failures at a pulse measured at 30 kV/m or higher. A majority of the other automobiles and trucks tested resulted in what the EMP Commission referred to as "annoyances" (p. 115), such as blinking dash lights or check engine lights that remained on.

Since only a brief overview of the testing was released, it is unknown if a particular manufacturer fared better than another or if gasoline engines experience more or less problems than their diesel counterparts. The final outcome of the EMP Commission's tests shows that two out of three cars on the road during an HEMP event would succumb to some sort of failure, most likely one that would result in having to merely restart the vehicle. Trucks, on the other hand, could experience up to a 70 percent malfunction rate with 15 percent experiencing engine stall. (2008, pp. 115-116)

There is no doubt that criticism has been targeted at the testing methods and the data provided. Data provided in the report do not provide information if one manufacturer fared better than the others or if gasoline powered vehicles performed better or worse than a diesel powered vehicle. A concern about the maximum threshold level should also be noted: It appears that major problems began appearing in vehicles at the 30 kV/m to 50 kV/m threshold range. According to the U.S. Army, in the case of a HEMP the magnitude of the energy field could reach up to 50 kV/m (Department of the Army, 1994, p. D6); however, estimates from the Russian "K projects" estimate pulses in upwards to 100 kV/m, (Daniel, 2009) which has raised some concerns as to why the EMP Commission did not test at higher EMP field rates.

According to Emanuelson's online article about the effects an EMP has on vehicles (2008), the EMP Commission testing was faulted from the beginning. Emanuelson stated that funding was very limited for the EMP vehicular testing so vehicles had to be borrowed from other governmental agencies with a guarantee that they would be returned in working order. As a result of these demands, the vehicles were not tested to the full capacity of the laboratory. Dr. William Graham, who is a member of the EMP Commission, elaborated on this topic in a radio interview by saying that they were only allowed to test up to the first threshold of failure, which was well below what a HEMP event would generate and it was believed that should testing have been allowed to realistic HEMP environmental levels, there would have been a much higher failure rate. (Pry, 2011)

An indirect threat to vehicular traffic is the impact a HEMP would have on the rest of the traffic infrastructure. Using the worst-case scenario of a 70 percent power grid failure, a majority of traffic control devices, such as traffic lights, street lighting, and drawbridges would be inoperable. Even if backup power was installed and operational, many of these devices depend on electronic circuitry that would be directly impacted by the E1 and E2 HEMP threat.

Just as with the testing conducted on automobiles and SCADA devices, a series of tests was run by the EMP Commission on traffic control devices. According to the testing data, EMP energy was directed to a fully operation traffic light control system. E1 pulses up to 15 kV/m were induced, and four main disruptions were observed (EMP Commission, 2008, p. 114):

> 1. Forced Cycle: At field levels of 1 to 5 kV/m, the light was forced to cycle from green to red without going through yellow. This is a transient effect that recovers automatically after one cycle.
> 2. Disrupted Cycle: At field levels of 5 to 10 kV/m, the normally programmed cycle times became corrupted and changed to a cycle different from that originally programmed. The controller had either been damaged or needed to be manually reset.
> 3. No Cycle: At 10 to 15 kV/m, the side street lights at an intersection never turned green. The controller had been damaged.
> 4. Flash Mode: Also at 10 to 15 kV/m, the intersection went into a mode in which the lights in all directions were flashing. This mode can cause large traffic jams

because traffic flow is severely reduced in this situation. The controller has either been damaged or needs to be manually reset.

Just as with the automobile testing, it appears that the thresholds were conducted at artificially low levels. Considering that controller damage was noted on the traffic control systems at 10-15 kV/m, which would simulate the EMP effects felt on the outer limits of an HEMP attack, a more concentrated and realistic level of 50-100 kV/m, would almost certainly induce widespread damage to the electrical components based off the limited data provided. Regardless of the amount of component damage or the exact functionality of traffic control devices, there would be enough disruption to cause severe traffic jams in most heavily populated metropolitan areas.

Fuel supplies will potentially be the largest concern in a major EMP event. Major hurricanes that have shown us how fuel supplies are impacted the United States as roads become impassable and electricity is cut off for days or weeks at a time. Gas stations that are lucky enough to have operational backup generators to run gas pumps may only have a couple of days worth of fuel to meet their demand.

A severe solar weather event causing grid disruptions for weeks or months at a time would cause refineries to go immediately offline, halting production of various types of common fuels that we are dependent on. Should refinery production cease, or be severely limited in output, a nationwide fuel shortage would quickly cripple our economy and social stability.

Of grave concern would be the impact that a HEMP would have on the fuel distribution network. Due to the combined E1 through E3 waves, power grid and SCADA systems could fail, resulting in pipeline and refinery failure. Gas stations would not be able to distribute or be resupplied with fuel, and traffic control device disruption would cause massive traffic jams. There, of course, is also the potential for a large number of vehicles being disabled due to electronic system control failures. In such an event, all modes of transportation would come to a literal halt.

In 2006, the American Trucking Associations (ATA) published an article showing just how dependent America is on the trucking industry alone. Illustrating the cause and effect of a nationwide truck stoppage, a one month timeline (see Appendix A for the detailed timeline) shows how hospitals, retail outlets, financial institutions, and critical infrastructures would ultimately fail, leading to complete economic, governmental, and social collapse. (Holcomb, 2006)

Preventing a systematic failure of the automobile transportation system during an EMP event is problematic, merely because of the number of correlated systems involved. Lacking true testing data, we are unaware of just how a vehicle's electrical components would react to a full scale HEMP. Traffic control systems would cease to operate properly, and it is doubtful that enough components could be supplied if over one-third of the United States was impacted. Businesses would have to shut down as employees would not be able to get to work, and even if some could, keeping shelves stocked after merchandise is exhausted would be next to impossible without reliable transportation.

Railroad Infrastructure

Since the mid-19th century, the United States has been dependent on the railroad infrastructure to move an abundant number of people and cargo quickly and efficiently across the continent in a matter of days instead of months. As automobiles and airplanes came into existence, long distance passenger rail quickly subsided and most of the large railroads quickly shifted to primarily hauling freight. A majority of the main arterial lines utilized by the Class I railroads such as Union Pacific (UP), Burlington Northern Santa Fe (BNSF), Norfolk Southern (NS), and the CSX railroads, have been in place for over 150 years.

In 2005, over 1.8 million tons of freight were carried throughout the United States by the major Class I railroads with coal making up over 42 percent of all freight. (Rails West, 2010). In 2012, railroads such as BNSF saw more than a 75% increase in carloads of petroleum thanks to the oil fracking boom going on throughout the U.S. (Market Wire, 2012) With a majority of electricity being produced by coal fired power plants and the increased demand for fuel transport from newly drilled oil fields, railroads are just as important to the national infrastructure as ever.

Nearly 11 million railcars transported intermodal containers (comprised of shipping containers and truck-trailers) filled with a variety of goods from coastal shipping ports to key trucking facilities across the U.S. (Rails West, 2010) As mentioned, intermodal shipments are comprised of a variety of commodities and can include anything from automobile parts from China being shipped to a U.S.-based assembly plant, to beer being shipped from Mexico being forwarded to local distributorships. Keeping the trains running is just as important to our economy and our supply chain as keeping tractor-trailers running on the roads. Aside from the fact that energy production is heavily dependent on the railroads, so are the producers and retailers that rely on just-in-time shipments of their products.

Like most industries in the 21st century, railroads have become greatly dependent on technology to allow for more efficient operation. Automated control systems, often located in centralized dispatch centers, monitor a railroad company's entire train networks, train dispatcher then communicate with train crews across the United States using a myriad of telecommunication systems such as microwave radios, conventional VHF radio, fiber optic, and traditional analog lines to ensure safe railroad operations. (Hines, 2012)

Similar to a standard traffic light system, the railroads signal control system is designed in a series of "blocks," all interlinked with phone and wireless technology. Sensors are either bolted or welded onto the tracks that allow small electric currents to flow as a train's solid metal axle creates a circuit from one side of the rail to the other. As with a conventional sensor activated traffic signal, the railroad signal will change the signal indication at the other end of the block (usually at a rail siding), giving notice to an oncoming train. (EMP Commission, 2008, p. 110) The same basic principles also operate the grade crossing signal devices.

Inherent to the designs of their signal and telecommunications equipment, railroads are very susceptible to both, solar weather and HEMP events. Acting as a large antenna, the tens of thousands of miles of steel rail lines can act a super conductor for E3 pulses, mimicking the same risks of extreme voltage spikes that can occur in high voltage power lines. Railroads depend on low voltage direct current systems for dependable railroad signal operations. It has been found that EMP energy amounts as little as 1 kV/m can cause railroad systems to malfunction, while amounts up to 15 kV/m can cause permanent damage to the signal systems. (EMP Commission, 2008, pp. 109-110) In addition, high levels of E1 and E2 pulses can destroy the delicate circuitry housed on the railroad right of way.

Radio communications also are placed in jeopardy as solar weather events can disrupt the long distance microwave communications between train dispatchers and train crews and E1 and E2 pulses can affect the repeater stations and other delicate telecommunication devices. It is possible that point-to-point communications between trains (within about a five mile range) could be maintained as much of the two-way VHF radios used by train crews are ruggedized and hardened due to the harsh vibrations and other environmental hazards they are exposed to.

Basic diesel locomotive design has changed little since the late 1950s. Despite the thought that the large diesel motors drive the wheels, the fact is the huge engines power a generator that produces AC or DC power to the traction motor that then turns the axles. Earlier models of diesel locomotives were relatively simple, and were mechanical in nature. An engineer monitored and regulated traction (drive) power, braking pressure, and slack action, all by his/her intuition and experience. Technology used in today's diesel locomotives rely heavily on microprocessors. Computers virtually control all functions of the locomotive, throttle, braking, and electrical output is all controlled by electronic wire, and not manual controls.

There has only been one study of the effects that an EMP would have on a locomotive. Conducted by the Swiss on an electro-mechanical locomotive (which unlike the diesel electric, depends on an external power source to operate), the test found that damage to electrical components began at the 8 to 16 kV/m range while damage to modern diesel locomotives could potentially occur at the 20 to 40 kV/m range. (EMP Commission, 2008, pp. 111-112) During a HEMP event, pulses in excess of 40 kV/m could realistically be seen.

Diesel locomotives also depend on radio communications paired with computerized control systems to communicate with multiple locomotives attached to the train. With this newer technology, locomotives can be placed unmanned at the rear of a train. Known as a distributive power unit (DPU), power demand and braking are calculated by the lead (front) locomotive and information is constantly relayed and monitored by both the rear and lead units. (Union Pacific, 2012) In the event of a loss of communication, as is the case with any locomotive system failure, locomotives are design to initiate an emergency braking procedure to prevent accidents. Should the computer controlled braking system fail, a manual override is located on the dashboard of both the engineer's and conductor's consoles. This braking system is mandated by federal statute under 49 CFR § 229.47 (Justia, 2012)

As long as locomotives are operational, railroads have an advantage over more modern forms of transportation that are 100 percent technology dependent. The fact that railroads have been in business since before commercially available electricity, modern backup protocols still allow for trains to move under conditions when power may not be restored.

Automated switches have manual override levers that allow trains to navigate sidings and yards and track warrants (bulletins giving to train crews, giving specific instructions on train movement) are issued to trains to control individual train movement from one point to another during signal outages. (Pacific Southwest Railway Museum Association, 2012)

Lack of testing has left it unclear as to what the overall impact and effect an EMP event would have on the railroad's infrastructure. Railroads have been one of the most resilient entities of modern times. The industry survived through civil war and numerous major natural disasters. Known for having detailed emergency response and recovery plans a majority of larger railroads are able to move freight within days.

During the Year 2000 (Y2K) computer bug scare, the railroads began to prepare for a system-wide power outage. According to *Computer World Magazine* (1999), the Union Pacific Railroad began stockpiling nearly 500 generators to be placed at signal control points. In case more generators where needed, the UP had a contingency plan to convert the diesel generators on their refrigerated cars to help power critical infrastructure. (Computer World, 1999)

As prepared as railroads are against all types of disasters, both natural and manmade, it is unclear exactly what the railroad's contingency plans would be for a sustained power outage where a majority of signals and radio systems would fail, and fuel would be in short supply.

Even if railroads were able to ration fuel reserves to keep key trains going, the system would have to come to a halt for an undetermined amount of time until every train on the system could be pinpointed geographically to allow for the safe movement of trains. This could take days or weeks before this could be accomplished safely, while in the meantime, the much needed fuel and other urgently needed resources would sit idle.

Aviation

Compared to the railroads and automobiles, commercial aviation is a relatively new mode of transportation. In the earliest era of commercial aviation history, production aircraft, like the early automobile, depended on carbureted engines, mechanical gauges, cables, and hydraulic systems to operate the aircraft. As time advanced, so did the technology, fuel management, navigational devices, and the jet turbine engines themselves become dependent on computerized control systems. Most recently, the standard hydraulic and cable steering control systems have been replaced with computerized technology, commonly referred to as “fly-by-wire.”

Aircraft technology has allowed aircraft to fly at higher altitudes, reduce fuel usage, and improve safety dramatically through technology such as anti-collision warning devices, auto-pilot, and wind shear monitoring equipment. On the ground, air traffic controllers monitor flights across the world through a system of radar, satellite, and telecommunications systems. These complex systems work seamlessly together to provide safe travel through congested skies.

Researching data for the effects of an EMP on aircraft (both military and commercial) has been a difficult task. Virtually all of the military testing is classified and tests against commercial aircraft, which are typically conducted by the aircraft manufacturers, are considered proprietary information and are not available through the public domain. It is possible to piece together some of the information based off the limited open source information available.

Obviously the greatest risk an EMP would have on modern aircraft is the susceptibility to the numerous electronic devices that control the cabin environment, flight controls/instrumentation, and radio communications, as these systems are entirely dependent on microchip technology that is sensitive to even the smallest increase in electromagnetic energy or static charge.

On average, every commercial aircraft is struck by lightning at least once a year in which little or no effects to operating systems is reported. (Hickman, 2012) Airplane design in itself acts as its own Faraday cage where the highly conductive aluminum skin of the aircraft allows lighting to flow across the outside, protecting the internal components. If the fuselage is not sealed properly, the electrical current, which contains the same elements of an E2 electromagnetic pulse, can enter into the planes electrical system causing a potential system disruption. (Rupke, 2006)

In order to protect electronics from rogue currents, today's modern aircraft incorporate electromagnetic shielding on wiring and hardened cases enshrouding the computer processors to protect against EMP. Despite the hardening efforts, the actual nose of the aircraft that houses the radar system, known as the radome, is the most venerable to EMP intrusion since it is unable to be shielded. (Rupke, 2006) To prevent a backflow of current entering the electrical system through the radome, Rupke (2006) explains that metallic strips are placed inside the nose that transfer electrical current to the shell of the plane, additionally, lightning surge protectors are installed on all critical electronic control devices.

Although there are numerous safety systems in place to protect commercial aircraft from lightning strikes, it is unknown how these systems would be affected by the initial E1 pulse. As discovered with the power grid, an E1 EMP can cause the surge and voltage spike safety devices to fail, allowing E2 generated pulses to enter protected systems. In a HEMP event, the E1 and E2 event would happen within a fraction of a second between each other, possibly not allowing these electrical safety devices to provide adequate protection.

Aircraft sitting at terminal gates may actually be more susceptible to an EMP than those in the air. Most aircraft awaiting passenger loading and unloading sit at the gates with their fuselage doors open, and are connected to external commercial power systems. In this condition, the aircraft is now susceptible to a “back door” intrusion of an electromagnetic pulse that could cause system failures and either disable or prolong the grounding of air traffic. (Nordwall, 1998) Space weather events can adversely affect aircraft, and their passengers that fly at high altitudes, particularly over the polar regions of the planet.

A comprehensive study by the International Civil Aviation Organization (ICAO), which is a specialized agency of the United Nations (UN), published a report titled, *Space Weather Effects in Regard to International Air Navigation* (2011). According to the report, the greatest concern was electromagnetic radiation at high altitude generated by a solar weather event. Aside from radioactive contamination to the aircrew and passengers, the high altitude radiation can damage sensitive electronic avionics. Numerous malfunctions have already been reported in aircraft during space weather events. Reports of auto-pilot systems resetting and avionics going into loop testing mode have been just a few of the documented electronic system failures directly related to a solar event. (ICAO, 2011, pp. 34-35)

Research on the EMP Commission’s report does not go into specific detail about any testing or data relevant to EMP testing on aircraft; however, the commission reported that members had met with Boeing Corporation staff to address specific questions they had about how they build their aircraft to hold up against and EMP. According to Boeing, its commercial aircraft is designed to handle a “non-hostile electromagnetic environment.” (EMP Commission, 2008, p. 123) It is unclear as to what Boeing means by a “non-hostile electromagnetic environment” as it did not provide any data or other type of clarification. The EMP Commission did appear to show some concern that not enough EMP testing has been conducted on newer aircraft, such as the Boeing 777, that is a “fly by wire” design, and even with multiple redundancies; the commission still had concerns about the electronic dependencies on newer aircraft. (EMP Commission, 2008, pp. 124-125)

In order to conduct safe and efficient air travel, commercial, private, and governmental aircraft are heavily dependent on radio and satellite communication. This complex communication system not only allows pilots to communicate aircraft to aircraft, and from aircraft to air traffic control (ATC), but radars and GPS tracking allow real time tracking of all aviation traffic worldwide. Today, tracking of aircraft has become more and more dependent on satellite GPS tracking than with the traditional land based radar systems, although the two systems are still dependent on one another.

Solar weather has been known to affect radio communications in several ways. In the case of GPS systems, a solar storm can disrupt these systems by increasing the error of the computed position, prevent a receiver from locking onto the satellite system, and create radio interference due to the solar radio noise. (ICAO, 2011, p. 32) High frequency (HF) radio systems used to communicate during transoceanic flights can experience radio blackouts lasting from minutes to days during severe solar weather events. (ICAO, 2011, pp. 29-30)

Loss of radar tracking and communication to the air traffic controllers would create a detrimental effect to the safety of aircraft operations. Radars help the ATC space out incoming and outgoing flights to prevent collisions, and in today’s busy airports such as Los Angeles

International or LaGuardia, the loss of radar tracking would mean disastrous results. The Federal Aviation Administration's (FAA) radar system is designed to overlap, so in the event of a single radar failure, or if radar must be taken offline for maintenance, surrounding radar sites will still allow for system-wide tracking. In the case of an either a HEMP or solar weather event, a large portion of the FAA's radar system could be temporarily or permanently taken off-line.

During the EMP Commission's analysis of the FAA's radar network and ATC systems, it was found that many vulnerabilities existed that could prove detrimental to the ATC network. Obviously, the abundance of electronic control systems proves to be susceptible to E1 and E2 pulses. Using data from other tests from electronic control systems that are similar in design and function to the ATC system, the commission reported that EMP levels as low as 4 kV/m would cause a distinguishable disruption to the system, while levels as high as 15 kV/m would cause permanent damage. (EMP Commission, 2008, p. 126) In the same report, the commission also showed concern that due to the age of the ATC system and the mixing of technology ranging from the most current technology to components that are over four decades old would mean a delay in replacement and calibration of equipment.

Protecting our aviation critical infrastructure against any form of EMP threat will be an expensive and drawn-out process. Updating and retrofitting the United States ATC system would be entirely cost prohibitive to a struggling airline industry and the shrinking budget of the FAA. Even the EMP Commission acknowledges that there is no easy workaround to quickly fix this problem and has suggested that a special committee or government program be created to work with the FAA to find a way to get the ATC network back up and running as quickly as possible after an EMP event. (2008, p. 128)

EMP Risk Assessment

In the occurrence of a devastating EMP event, citizens, businesses, and governmental entities need to be prepared to respond and recover as quickly as possible. As evident from Hurricane Katrina, a complete collapse of the economic and social infrastructure can rapidly develop when everything comes to a halt. Hurricane Katrina taught the nation just how unprepared we were for such a disaster that abruptly halted transportation, utilities, communications, and medical and food supplies. Extreme civil unrest and violence quickly arose as law enforcement was unable to adequately respond.

Depending on the type of EMP event encountered, it is quite possible that we could see the same collapse of infrastructure and society without the physical damage that is brought on by natural disasters. In the case of a HEMP triggered by a nuclear warhead, the power grid, communication devices, transportation, fuel distribution, food, water, medical, and other critical infrastructures could fail unexpectedly within hours or days. Fuel supplies would dwindle within weeks as refineries could not be brought back online. Vehicles would not be able to transport goods or services and store shelves would quickly run dry.

With our increasingly cashless financial system, credit cards, debit cards, and checks would become immediately useless. From the consumer to the manufacturer, electronic monetary transactions would cease, and those with cash would find that the quick collapse of our technology dependent financial system would create rapid inflation.

Government infrastructure would struggle or even fail at multiple levels (local, state, and federal) if such a devastating event covered a large geographic region of the United States. Chaos and confusion would be imminent until clear communication and understanding of the event is established. In the EMP Commission's 2008 report, continuity in governmental operations during an EMP threat was addressed and it was acknowledged that such operations were critical to the welfare of the United States. The particulars of how this was to be accomplished were still listed as classified and not available for public release. (2008, p. 172)

Even if communication could be established by governmental and business entities, there would be a great struggle in trying to restart the entire U.S. infrastructure from scratch. Since a HEMP event would be an intentional act by a hostile country, the threat of invasion must also be contemplated, meaning that there must be a way to ensure that the United States' capability to withstand an attack on our own soil must be contemplated.

An extreme solar weather event, such as the 1858 Carrington solar flare would most likely have a less dramatic effect than a HEMP event, however; if the worse-case scenario of 70 percent of the U.S. power grid failing, much of the same infrastructure breakdowns found in a HEMP event could be seen in a solar weather event, albeit at a slower pace if power cannot be quickly restored.

It is essential that the business and governmental stakeholders develop contingency plans through risk management to help mitigate the effects of an EMP event. In order to better prepare, the following factors must be evaluated by both the public and private sectors to ensure they can operate efficiently: (Fink, 2002, pp. 38-40)

- Evaluate the intensity that an EMP event would have on the industry, and how much can be endured on the stakeholders and infrastructure
- Evaluate how normal operations would be affected for the industry
- Evaluate how fast could normal operations be restored and if all repair parts and tools could quickly be accessed.

Contingency planning to ensure key energy supplies would need to be brokered through a collaboration of public and private entities. An example of this would be to work with Mexico and key Latin American countries to ensure that emergency fuel supplies could be obtained from their refineries and shipped relatively quickly via rail, since this would be the most stable form within the transportation infrastructure systems.

The United States could also look at the possibility of adding emergency interconnections to the power grid system in Mexico to allow for an increase in supplemental power. A permanent hard line connection should not be established as this could cause EMP feedback through the high-voltage lines, potentially harming Mexico's power grid; however, temporary interconnects could be designed and established where a physical connection of high voltage line would have to be established before the transfer of power could begin.

Most of how we have learned to prepare and respond to disasters stems from prior lessons learned. Hurricanes and floods occur on a regular basis throughout the nation and with the advancement in meteorology, can be predictable. Earthquakes and tornadoes are more spontaneous, but we have learned to identify the areas in which they are most prone and try to mitigate damage through architectural design, shelters in place, and public awareness. In those areas that are prone to the more common natural disasters, a majority of the business, governmental, and critical infrastructures are hardened against the most probable threat.

Manmade disasters are much less predictable that natural ones. Chemical spills, industrial fires, radiation leaks, explosions, and contamination are just a few of the disasters that we have dealt with since the industrial revolution began. Industries such as chemical plants, refineries, and nuclear power plants all have a potential risk developing a catastrophic event. While the probability of such an event occurring may be low due to modern industrial safety practices and redundant safety systems, these industries must still maintain a contingency plan for a worst case scenario.

Steven Fink (2002, p. 46) has illustrated what he calls a Crises Barometer (see Appendix B). This barometer is set up as a plotting chart using an X/Y axis so that businesses can forecast the risk of catastrophic events. The “X” axis measures the probability factor of the event from 0 to 100 percent while the “Y” axis measures the impact that will be inflicted upon the business, 0 being no impact while 10 having severe impact. Four zones are then created to help assess how critical each event would have.

In an event that had 0 to 50 percent probability but an impact rating of 0 to 5, it would be categorized as a “Green Zone” or “Low/Low” risk. Events with a 51 to 100 percent probability but with an impact value less than 5 is placed in the “Gray Zone” or “Low/High” risk. Anything listed with a probability less than 50 and an impact value higher that 5 is rated in the “Amber Zone” or as “High/Low” risk. Finally, events with a greater than 50 percent probability and greater than a 5 impact rating would be placed in the “Red Zone” or “High/High” risk category.

Even though natural and manmade EMP events have been well documented over the last 100 years, the strongest of them were during a time when the modern electrical grid was nonexistent and microcomputer technology had not even been thought of. Based on what limited information we have, we can still try to assess what our risk rating is and plan accordingly.

Many of the manmade threats of an EMP attack against the United States still remain classified; however, we do know that China and Russia pose the most significant threat through the means of a HEMP. According to Emanuelson (2008), probability of the United States coming under a HEMP attack in the next 10 years ranges between 20 to 70 percent, depending on the source. Emanuelson continues that the threat of a solar weather EMP threat has more than a 50 percent occurrence rate over a 10 year span.

Using Fink's "Crisis Barometer," we can plot that both types of EMP events will have a dramatic impact on our national infrastructure, placing it above a 5 impact rating. Even at a the lower end of Emanuelson's prediction of a 20 percent probability of a HEMP, this still places the risk in the "Amber Zone" while the 70 percent prediction places the EMP threat in the "Red Zone," yet no serious contingency plans have publicly been established by either the business sector or the government sector to deal with an infrastructure collapse brought forth by an EMP event.

Summary

There is some debate over just how much of an impact an EMP event would affect the North American continent. Recently, entities such as the Federal Energy Regulatory Commission (FERC) were at odds with the North American Electric Reliability Corp (NERC) over the impact an EMP would have on the power grid, yet at the time of the 2004 and 2008 EMP Commission reports, both sides had agreed that an EMP posed a significant threat to the U.S. power grid. (Behr, 2011) Despite the disagreement, we should look at the facts that have been presented and make an informed decision based on the facts that we do know.

An electromagnetic threat to the United States is real. Since the 1859 Carrington event, the effects that space weather has had even the most rudimentary electrical devices have been noteworthy from sparking telegraphs to damaged transformers at nuclear power plants, the warning signs from a never-before-seen storm is there. The same holds true for manmade electromagnetic pulse events, between the Russian "K Projects" and the Starfish Prime experiments of the 1960s, the quest for EMP weapon development, and EMP mitigation has been ongoing, shrouded by the mystery of classified governmental programs.

In the early European days, before world travel was widespread, it was known for hundreds of years that all swans were white, as there had never been a swan by any other color ever seen before. Once worldwide travel was possible, European travelers were astonished when they arrived in Australia to find that swans there were black. This anecdote has recently been made famous by Nassim Nicholas Taleb, who states that "black swan" events, "Lie outside the realm of regular expectations, carry an extreme impact, and human nature makes us concoct explanations for their occurrence after the fact." (Casti, 2011)

To put this in perspective, an EMP event could easily be considered a "black swan" event. Most people do not expect an EMP event to occur, and in reality, do not know the first thing about them, but when an EMP event does propagate across the United States, the damage and devastation that could occur will have a definite extreme impact on our lives. The threat of an EMP event is definitely out there. Questions such as "Where will it occur?", "When will it occur?", "How will it occur?", and "What will the damage be?" have yet to be answered, and may not be able to be answered until after the fact.

It is evident that our government has shown great concern. With the creation of the EMP Commission, many questions about our nation's susceptibility from an EMP threat still remain. There are still those out there that are skeptical whether or not we are crying "wolf", but we cannot afford to ignore this threat as we have too much at stake.

References

Abilla, P. (2007, March 23). *Ford's Contribution to Just-In-Time*. Retrieved November 15, 2012, from Shmula.com: http://www.shmula.com/fords-contribution-to-just-in-time/371/

Associated Press. (2003, August 30). *Americans' Love Affair with Cars, Trucks and SUVS Continues*. Retrieved September 26, 2012, from USA Today: http://www.usatoday.com/news/nation/2003-08-30-outnumbered-cars_x.htm

Associated Press. (2012, October 30). *Nuclear Plants Partly Shut Down as Sandy Hits*. Retrieved November 17, 2012, from CBS News: http://www.cbsnews.com/8301-201_162-57542293/nuclear-plants-partly-shut-down-as-sandy-hits/

Barnes, P., Rizy, D., & McConnell, B. (1991, November 25). *Electric Utility Industry Experience with Geomagnetic Disturbances*. Retrieved November 2, 2012, from Oak Ridge National Laboratory: http://www.ornl.gov/~webworks/cpr/v823/rpt/51089.pdf

Behr, P. (2011, August 26). *Disputes Dog Efforts to Protect Transmission Grid From 'High-Impact, Low-Probability' Threats*. Retrieved November 23, 2012, from The New York Times: http://www.nytimes.com/gwire/2011/08/26/26greenwire-disputes-dog-efforts-to-protect-transmission-g-30509.html?pagewanted=all

Broadband for America. (2012, November 1). *Hurricane Sandy Affects Internet Infrastructure Locally, Access Internationally*. Retrieved November 10, 2012, from Broadband for America: http://www.broadbandforamerica.com/blog/hurricane-sandy-affects-internet-infrastructure-locally-access-internationally

Carew, S. (2012, October 30). *Hurricane Sandy Disrupts Northeast U.S. Telecom Networks*. Retrieved November 10, 2012, from Reuters: http://www.reuters.com/article/2012/10/30/us-storm-sandy-telecommunications-idUSBRE89T0YU20121030

Carrington, R. C. (1859, November). *Description of a Singular Appearance Seen in the Sun on September 1, 1859*. Retrieved October 25, 2012, from The SAO/NASA Astrophysics Data System: http://adsbit.harvard.edu/cgi-bin/nph-iarticle_query?bibcode=1859MNRAS..20...13C

Casti, J. L. (2011, November). X-Event: The Collapse of Everything [Kindle Version). Kindle Locations 626-627. Harper Collins, Inc.

Committee on Armed Services. (2004). *H.A.S.C. No. 108–37*. House of Representatives, Committee on Armed Services, Washington D.C.

Committee on National Security. (1997, July 16). *Threat Posed by Electromagnetic Pulse (EMP) to U.S. Military Systems and Civil Infrastructure House of Representatives*. Retrieved October 5, 2012, from U.S. House of Representatives: http://commdocs.house.gov/committees/security/has197010.000/has197010_1.HTM

Committee on the Judiciary. (2005). *Terrorism and the EMP Threat to Homeland Security*. Subcommittee on Terrorim, Technology and Homeland Security, United States Senate. Washington D.C.: United States Government Printing Office.

Computer World. (1999, July 19). *Union Pacific's Contigency Plan*. Retrieved November 17, 2012, from Computer World: http://www.computerworld.com/home/features.nsf/all/990719up

Daniel, P. (2009). *Strong Electromagnetic Impulse Generation*. Retrieved October 14, 2012, from Environment and Electrical Engineering: http://eeeic.eu/proc/papers/61.pdf

Department of Homeland Security. (2012, September 12). *The Electromagnetic Pulse (EMP) Threat: Examining the Consequences*. Retrieved October 20, 2012, from Department of Homeland Security: http://www.dhs.gov/news/2012/09/12/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity

Department of the Army. (1994). *Test Operations Procedure (TOP) 1-2-612 Nuclear Environment Survivability*. U. S. Army White Sands Missile Range, Headquarters, U.S. Army Test and Evaluation Command. Aberdeen: Department of the Army.

DHS. (2012, September 12). *The Electromagnetic Pulse (EMP) Threat: Examining the Consequences*. Retrieved October 25, 2012, from Department of Homeland Security: http://www.dhs.gov/news/2012/09/12/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity

Emanuelson, J. (2010, September). *E1 E2 and E3*. Retrieved 10 15, 2012, from Futurescience LLC: http://www.futurescience.com/emp/E1-E2-E3.html

Emanuelson, J. (2008). *EMP Effects on Vehicles*. Retrieved November 17, 2012, from Future Science: http://www.futurescience.com/emp/vehicles.html

Emanuelson, J. (2008, May). *EMP History*. Retrieved October 14, 2012, from Future Science LLC: http://www.futurescience.com/emp/EMP-history.html

EMP Commission. (2008, April). *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*. Retrieved September 8, 2012, from EMP Commission: http://www.empcommission.org/

EMP Commission. (2004). *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Volume 1: Executive Report 2004*. Retrieved 09 08, 2012, from EMP Commission: http://www.empcommission.org/

Encyclopædia Britannica Inc. (2012). *electromagnetic radiation*. Retrieved October 14, 2012, from Encyclopædia Britannica Online: http://www.britannica.com/EBchecked/topic/183228/electromagnetic-radiation

FEMA. (1984, June). *Attack Environment Manual: Chapter 4: What the Planner Needs to Know About Electromagnetic Pulse*. Retrieved November 10, 2012, from Federal Emergency Management Agency: http://www.lrc.fema.gov/downloads/attack_env_4.pdf

FEMA. (2012, June 8). *Emergency Alert System*. Retrieved November 10, 2012, from Federal Emergency Management Agency: http://www.fema.gov/emergency-alert-system-eas

Fink, S. (2002). *Crisis Management*. Lincoln: iUniverse, Inc.

Flatow, I. (2012, January 27). *How 'Space Weather' Affects Planes And Power Grids*. Retrieved October 27, 2012, from National Public Radio: http://www.npr.org/2012/01/27/145990089/how-space-weather-affects-planes-and-power-grids

Forstchen, W. R. (2008). *"EMP 101" A BASIC PRIMER & SUGGESTIONS FOR PREPAREDNESS*. Retrieved October 26, 2012, from One Second After: http://www.onesecondafter.com/pb/wp_d10e87d9/wp_d10e87d9.html

Fox, K. C. (2011, August 09). *Solar Flares: What Does It Take to Be X-Class?* Retrieved August 25, 2012, from NASA: http://www.nasa.gov/mission_pages/sunearth/news/X-class-flares.html

Hambling, D. (2008, October 10). *Army Orders Pain Ray Trucks; New Report Shows 'Potential for Death'*. Retrieved October 21, 2012, from Wired.com: http://www.wired.com/dangerroom/2008/10/army-ordering-p/

Henry, R. (2006, April 18). National Science Board Workshop Task Force on Hurricane Science and Engineering. Pensacola, Florida: University of Louisiana, Lafayette. Retrieved November 10, 2012, from http://www.nsf.gov/nsb/committees/archive/hurricane/3/henry.pdf

Hickman, L. (2012, May 16). *Should you be worried about lightning striking your plane? French president François Hollande's flight was forced to land after being hit this week. But is there any real danger?* Retrieved November 22, 2012, from The Guardian: http://www.guardian.co.uk/world/shortcuts/2012/may/16/worried-lightning-striking-plane

Hines. (2012). *Union Pacific Harriman Dispatch Center*. Retrieved November 17, 2012, from Hines Online: http://www.hines.com/property/detail.aspx?id=467

Holcomb, R. (2006, July 14). *When Trucks Stop, America Stops*. Retrieved November 14, 2012, from American Trucking Associations: http://www.trucking.org/newsroom/white papers/when trucks stop america stops.pdf

Hsu, J. (2010, January 20). *Electromagnetic Pulse Cannon Could Demo Car-Stopping Power Next Month*. Retrieved October 25, 2012, from PopSci: http://www.popsci.com/technology/article/2010-01/electromagnetic-pulse-cannon-could-demo-car-stopping-power-next-month

ICAO. (2011). *Space Weather Effects in Regard to International Air Navigation*. Retrieved November 22, 2012, from International Civil Aviation Organization: http://www.icao.int/safety/meteorology/iavwopsg/Space%20Weather/Manual%20on%20Guidance%20on%20Space%20Weather.doc

Information Handling Services. (2001, January 5). *Jane's Intelligence Watch Report - Daily Update 2001*. Retrieved October 25, 2012, from Jane's Defense & Security News: https://janes-ihs-com.ezproxy2.apus.edu/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1111221&Pubabbrev=IWR

Justia. (2012). *Title 49 Code of Federal Regulations*. Retrieved November 10, 2012, from Justia.com US Law: http://law.justia.com/cfr/title49/49-4.1.1.1.22.3.24.5.html

Klein, C. (2012, March 14). *A Perfect Solar Superstorm: The 1859 Carrington Event*. Retrieved October 25, 2012, from History: http://www.history.com/news/a-perfect-solar-superstorm-the-1859-carrington-event

Krulwich, R. (2010, July 01). *A Very Scary Light Show: Exploding H-Bombs In Space*. Retrieved October 14, 2012, from National Public Radio: http://www.npr.org/templates/story/story.php?storyId=128170775

Lovett, R. A. (2011, March 2). *What If the Biggest Solar Storm on Record Happened Today?* Retrieved October 25, 2012, from National Geographic Daily News: http://news.nationalgeographic.com/news/2011/03/110302-solar-flares-sun-storms-earth-danger-carrington-event-science/

Market Wire. (2012, August 06). *Despite Facing Steep Drop in Coal Shipments, Union Pacific and Canadian Pacific Railway Showing Strong Gains*. Retrieved November 17, 2012, from Investorpoint: http://www.investorpoint.com/news/COMMODIT/53302341/

NASA. (2010, October 14). *What is a Solar Flare?* Retrieved October 25, 2012, from National Aeronautics and Space Administration Goddard Space Flight Center: http://hesperia.gsfc.nasa.gov/sftheory/flare.htm

NERC. (2012). *About NERC: A Company Overview*. Retrieved October 27, 2012, from North American Electric Reliability Corporation: http://www.nerc.com/page.php?cid=1|7

NERC. (2011, October). *Geo-Magnetic Disturbances (GMD): Monitoring, Mitigation, and Next Steps A Literature Review and Summary of the April 2011 NERC GMD Workshop*. Retrieved November 8, 2012, from North American Electric Reliability Corporation: http://www.nerc.com

Nordwall, B. (1998). EMP, High-Powered Microwaves Pose New EW Threat to Aircraft. *Aviation Week and Space Technology , 149* (17), 68.

Odenwald, S. (2003). *Major Space Weather Events in History*. Retrieved October 25, 2012, from Space Weather: http://www.solarstorms.org/SRefStorms.html

Pacific Southwest Railway Museum Association. (2012). *14.0 RULES APPLICABLE ONLY WITHIN TRACK WARRANT CONTROL (TWC) LIMITS*. Retrieved November 17, 2012, from Pacific Southwest Railway Museum Association: http://www.sdrm.org/faqs/rulebook/warrant.html

Peltier, R. (2011, May 1). *Predicting U.S. Coal Plant Retirements*. Retrieved October 28, 2012, from Power: Business and Technology for the Global Generation Industry: http://www.powermag.com/coal/Predicting-U-S-Coal-Plant-Retirements_3632.html

Perrow, C. (1999). *Normal Accidents: Living with High Risk Technologies*. Princeton: Princeton University Press.

Plait, P. (2012, July 9). *The 50th anniversary of Starfish Prime: the nuke that shook the world*. Retrieved October 14, 2012, from Discover Magazine: http://blogs.discovermagazine.com/badastronomy/2012/07/09/the-50th-anniversary-of-starfish-prime-the-nuke-that-shook-the-world/

Prince, A. (2009, May 1). *Visualizing The U.S. Electric Grid*. Retrieved October 27, 2012, from National Public Radio: http://www.npr.org/templates/story/story.php?storyId=110997398

Pry, P. V. (2011, March 23). *Dr. Peter Vincent Pry Show*. Retrieved November 17, 2012, from EMPact Radio: http://www.blogtalkradio.com/empact-radio/2011/03/23/empact-radio-with-dr-peter-vincent-pry

RAF Tabronics. (2007). *Transformer Basics*. Retrieved November 1, 2012, from RAF Tabronics LLC: http://www.raftabtronics.com/TECHNOLOGY/ElectromagneticBasics/TransformerBasics/tabid/110/Default.aspx

Rails West. (2010). *http://www.railswest.com/railtoday.html*. Retrieved November 17, 2012, from Rails West: http://www.railswest.com/railtoday.html

Ritter, L., Barrett, J. M., & Wilson, R. (2007). *Securing Global Transportation Networks. A Total Security Management Approach*. New York: McGraw-Hill.

Rupke, E. (2006, August 04). *What happens when lightning strikes an airplane?* . Retrieved November 22, 2012, from Scientific American: http://www.scientificamerican.com/article.cfm?id=what-happens-when-lightni

SBE. (2010, November 10). *Emergency Alert System Issues* . Retrieved November 10, 2012, from Society of Broadcast Engineers: http://www.sbe.org/sections/gov_eas.php

Singel, R. (2008, April 9). *Industrial Control Systems Killed Once and Will Again, Experts Warn.* Retrieved November 8, 2012, from Wired Magazine Online: http://www.wired.com/threatlevel/2008/04/industrial-cont/

SRI. (2012, May 20). *Coronal Mass Ejection (CME).* Retrieved October 25, 2012, from Southwest Research Institute IMAGE Homepage: http://pluto.space.swri.edu/image/glossary/cme.html

Stouffer, K., Falco, J., & Kent, K. (2006, September). *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security.* Retrieved November 3, 2012, from National Institute of Standards and Technology: http://www.cyber.st.dhs.gov/docs/NIST%20Guide%20to%20Supervisory%20and%20Data%20Acquisition-SCADA%20and%20Industrial%20Control%20Systems%20Security%20(2007).pdf

The Energy Library. (2009). *North American Electricity Grid.* Retrieved October 26, 2012, from The Energy Library: http://www.theenergylibrary.com/node/647

Thompson, R. (2012). *Power Failure in Canada During 1989*. Retrieved November 2, 2012, from Australian Government Bureau of Meteorology Radio and Space Weather Services: http://www.ips.gov.au/Educational/1/3/12

U.S. Census. (2012). *U.S. Census Bureau, Statistical Abstract of the United States: 2012 Transportation*. Retrieved November 10, 2012, from U.S. Census Bureau: http://www.census.gov/compendia/statab/2012/tables/12s1069.pdf

Union Pacific. (2012). *It's Just Railroad Talk*. Retrieved November 1, 2012, from Union Pacific: http://www.up.com/aboutup/funstuff/rrtalk/train_types/index.htm

Vittitoe, C. N. (1989, June). *Did High-Altitude EMP Cause the Hawaiian Streetlight Incident?* Retrieved October 14, 2012, from University of New Mexico Electrical and Computer Engineering: http://www.ece.unm.edu/summa/notes/SDAN/0031.pdf

Wik, M. (1984). *Hardening of Telecommunication Networks Against Electromagnetic Pulses.* Retrieved November 10, 2012, from University of New Mexico: Electrical and Computer Engineering: http://www.ece.unm.edu/summa/notes/SDAN/0028.pdf

Appendix A

American Trucking Associations

A Timeline Showing the Deterioration of Major Industries Following a Truck Stoppage

(Holcomb, 2006)

The first 24 hours

- Delivery of medical supplies to the affected area will cease.
- Hospitals will run out of basic supplies such as syringes and catheters within hours.
- Radiopharmaceuticals will deteriorate and become unusable.
- Service stations will begin to run out of fuel.
- Manufacturers using just-in-time manufacturing will develop component shortages.
- U.S. mail and other package delivery will cease.

Within one day

- Food shortages will begin to develop.
- Automobile fuel availability and delivery will dwindle, leading to skyrocketing prices and long lines at the gas pumps.
- Without manufacturing components and trucks for product delivery, assembly lines will shut down, putting thousands out of work.

Within two to three days

- Food shortages will escalate, especially in the face of hoarding and consumer panic.
- Supplies of essentials—such as bottled water, powdered milk, and canned meat—at major retailers will disappear.
- ATMs will run out of cash and banks will be unable to process transactions.
- Service stations will completely run out of fuel for autos and trucks.
- Garbage will start piling up in urban and suburban areas.

- Container ships will sit idle in ports and rail transport will be disrupted, eventually coming to a standstill.

Within a week

- Automobile travel will cease due to the lack of fuel. Without autos and buses, many people will not be able to get to work, shop for groceries, or access medical care.
- Hospitals will begin to exhaust oxygen supplies.

Within two weeks

- The nation's clean water supply will begin to run dry.

Within four weeks

- The nation will exhaust its clean water supply and water will be safe for drinking only after boiling. As a result gastrointestinal illnesses will increase, further taxing an already weakened health care system.

Appendix B
Crisis Barometer
(Fink, 2002)