Electromagnetic Pulse Threats in 2010

by

Colin R. Miller, Major, USAF

Center for Strategy and Technology

Air War College, Air University

325 Chennault Circle

Maxwell AFB Alabama 36112-6427

November 2005

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Electromagnetic Pulse Threats in 2010	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,Air War College,Center for Strategy and Technology,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**28**	

This page intentionally left blank

CHAPTER 12
Electromagnetic Pulse Threats in 2010

Colin R. Miller

I. Introduction

Current U.S. military transformation strategy centers on information dominance, network-centric warfare, and expeditionary operations. Operations Desert Storm and Iraqi Freedom demonstrated a spectacular evolution of capability in these key areas. Certainly, adversaries learned from Saddam's poor decision to face American forces head-on and will increasingly employ asymmetric attacks to defeat U.S. forces in the future. Electromagnetic pulse (EMP) weapons represent one of the most likely and potentially devastating opportunities for this type of attack in the near future. Ranging from sophisticated intercontinental nuclear weapons specifically designed to generate EMP effects to relatively crude and cheap electromagnetic bombs, these weapons can destroy all electronic devices within a target area as small as an automobile or as large as the continental United States. As U.S. forces continue to modernize and rely on electronic systems for effectiveness, it will become increasingly probable that an adversary will use EMP to strike at America's Achilles' heel. This paper addresses the threat EMP weapons will pose to U.S. expeditionary operations in the near future in terms of their ability to deny access to foreign soil, level the playing field in theater wars, and/or attack the U.S. homeland as a retaliatory or preemptive strike. It begins by discussing the nature of EMP and its effect on vulnerable systems, and then outlines the different methods of generating EMP while categorizing them by probability of use, lethal range, types of (electronic) targets they affect, and who is likely to use them. The paper considers three near-term scenarios for adversary use of EMP and recommends cost-effective response measures. It proposes a diplomatic policy to levy drastic consequences on the perpetrator of an EMP attack, rapid establishment of an EMP-hardened expeditionary force, hardening critical elements of civil infrastructures, integration of EMP attack response in large-scale training scenarios, and congressional action to establish and mandate compliance with EMP hardening standards for future military and civilian systems.

II. U.S. Forces' Future Concept of Operations

The United States is the most technologically advanced society in the world, a position that has brought unprecedented wealth, strength, and influence. To maintain this position, the U.S. national security strategy (NSS) seeks to defeat global terrorism, prevent attacks against the U.S. and its friends, defuse regional conflicts, and prevent threats by enemies with weapons of mass destruction (WMD) while transforming America's national security institutions to better meet the challenges and opportunities of the twenty-first century.[1] Key to this transformation is a complete transition to expeditionary network-centric operations.

Expeditionary Operations and Network-centric Warfare

In the past, enemies needed great armies to threaten America, which allowed the U.S. to preposition formidable garrison forces against predictable threats. The future will be different. Because of technology proliferation, shadowy networks of terrorist will be able to cause massive damage, causing the United States to embrace a strategy of preemptive response. The U.S. will have to engage emerging threats wherever they surface, before they fully form.[2] To do this, the U.S. military is embracing an expeditionary force concept similar to what has traditionally served the Marine Corps well. U.S. forces are being packaged into "buckets of legos" that can be rapidly deployed and tailored to produce capabilities suited to the Joint Force Commander's (JFC's) needs. *Joint Vision 2010* states that these forces will be relatively light, flexible, and seamlessly interoperable—leveraging information technology to ensure decisive advantage.[3]

According to Defense Secretary Rumsfeld, "…we must achieve: fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battlespace."[4] "Network-centric warfare (NCW) generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, high tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization."[5]

Operations Enduring Freedom and Iraqi Freedom demonstrated the potential of NCW, allowing unprecedented speed and lethality through digital command, control, communications, and computers (C4) integrated throughout the battlespace. The ability of microchip-enabled systems to leverage combat power was eye watering and in the future will be paramount. Data links, displays, satellite communications, computerized

planning systems, GPS receivers, radios, smart munitions, vehicles, aircraft, and all other systems required to support the networked force will derive their power, and potentially their doom, from fragile electronic systems.

Electronic Circuit Vulnerability to EMP

Electromagnetic pulses damage electrical and electronic circuits by inducing voltages and currents that they are not designed to withstand. To understand how this occurs, it is necessary to understand both the characteristics of electromagnetic pulses and the circuits they offend. An electromagnetic pulse is defined by its rise time (measured in volts/second), its electrical field strength (measured in volts/meter (v/m), and its frequency content (measured in Hertz [Hz]).[6] These factors combine to determine the threat EMP pose to a given system.

Rise time (how long it takes the pulse to reach peak amplitude) is primarily a factor for protected systems, such as those employing surge protectors. When rise times are less than a few thousandths of a second, protection circuitry often cannot react in time.[7] Field strength defines the amount of energy available to transfer to the target system, and frequency determines the efficiency of that transfer. Electric field orientation is also critical but, for the sake of simplicity, is not considered in this paper. EMPs are typified by fast rise times, high field strengths, and broad frequency content—factors that combine to make them lethal to electronic systems.

EMP induce large voltage and current transients on electrical conductors such as antennas and wires as well as conductive tracks on electronic circuit boards.[8] When pulses enter a system through a path designed to gather electromagnetic energy, such as an antenna, they are said to have entered through the "front door." In contrast, when they enter through an unplanned path, such as cracks, seems, trailing wires or conduits, they have entered through the "back door."[9] The efficiency of the energy transfer from pulse to system depends upon the frequency compatibility between the pulse and the entry path and on the conductivity of the material. When system characteristics match the offending EMP pulse, higher levels of damage occur. In general, sophisticated integrated circuits with short signal paths are susceptible to high frequency pulses while large electrical systems, such as commercial power characterized by long transmission lines, are vulnerable to low frequency EMP. It follows that a broadband EMP weapon threatens a greater number of systems than

a narrowband weapon, though the power requirement for a broadband weapon is much higher.

Regardless of how EMP enters a system, it damages components simply by overloading them. For example, high density metal oxide semiconductor (MOS) computer chips, which rely on extremely narrow internal "wires" to connect densely packed components, are permanently damaged when exposed to more than tens of volts or a few tenths of an amp.[10] While it is extremely difficult to calculate the minimum field strength required to induce signals of this magnitude for all cases and systems, testing has shown that pulses of 10 kV/m are sufficient to cause widespread damage.[11] Ten kV/m could induce electrical charges a billion times more powerful than systems were designed for, not just burning them out, but in some cases melting critical components.[12] As a result, unhardened computers used in data processing systems, communications systems, displays, industrial controls, military systems (including signal processors and electronic engine and flight control systems), telecommunications equipment, radar, satellites, UHF, VHF, HF, and television equipment are all vulnerable to the EMP at and above this level.[13]

III. EMP Weapons

EMP weapons come in a variety of forms, differing in cost, complexity, and lethality to electronic systems. Regardless of the type, they offer the user many significant advantages. First, EMP weapons do not rely on in-depth knowledge of the systems they strike, attacking all electronic systems without prejudice. Second, they are effective in all weather. Third, they are area weapons, with scalable footprints. One weapon can kill electronic systems in an area the size of a tennis court or throughout the entire United States.[14] Fourth, they produce persistent and lasting effects through destruction of circuits. Fifth, to counter EMP, entire systems must be hardened from end-to-end, a costly defense effort. Sixth, and perhaps most importantly, EMP weapons don't hurt people directly. An adversary could potentially decimate U.S. war-making capability with EMP without inflicting casualties, thus minimizing potential political and military repercussions.[15] EMP weapons can be classified as nuclear, high power microwave (HPM), or electromagnetic bomb (e-bomb). Each has its own characteristics, but all are constrained by the fact that they need a clear line-of-sight to the target to be effective.

Nuclear High Altitude Electromagnetic Pulse (HEMP)

Nuclear devices that generate HEMP are the most sophisticated, expensive, and effective electromagnetic weapons. The U.S. military first witnessed their effects after a series of high-altitude nuclear tests on Johnston Atoll in 1962. These tests unexpectedly generated disruptions in electronic systems in Hawaii, over 1000 miles away, due to EMP effects. Electronic systems failed across the island, radio broadcasts were interrupted, streetlights burned out, and burglar alarms sounded.[16] The Soviets had similar experiences, damaging overhead and underground cables at distances of 400 miles from low yield (300 kiloton) high altitude nuclear tests.[17]

HEMP is generated as a side effect of high-altitude nuclear detonation interaction with the atmosphere. Gamma rays released by the explosion interact with air molecules, producing high-energy free electrons through Compton scattering. These electrons are then trapped in the earth's magnetic field, generating an oscillating electric current, which gives rise to a rapidly radiating coherent electromagnetic pulse. The pulse can span continent-sized areas, due to the vast line of sight provide by its altitude, and affect systems on land, sea, and air.[18]

Characteristics

The HEMP is composed of three components. The first (E1) is a high frequency (1 MHz-1 GHz) free-field energy pulse with a rise time of a few billionths of a second.[19] This component disrupts or damages electronics-based control systems, sensors, communications systems, computers, and similar devices. The second component (E2) is a medium frequency pulse, similar to lightning, that follows E1 by a few millionths of a second. The E2 component is not particularly dangerous to electronics, especially those hardened against lightning, except when the E1 pulse damages surge protection circuitry first. The third component is relatively low frequency (3-30 Hz) slower rising pulse that follows E2 by a couple thousandths of a second and creates disruptive currents in long transmission lines.[20] The sequence of E1, E2, and E3 is important, because each causes damage building on the preceding pulse.[21]

The strength of HEMP depends on the design and yield of the nuclear device. However, relatively low-yield weapons can have devastating effects. For example, a 1-2 megaton device detonated at an altitude of 250 miles would produce a field strength of 10-50 kV/m, enough to produce

extensive damage to electronics over the entire continental U.S.[22] This illustrates the most significant characteristic of HEMP: one or a few high-altitude nuclear detonations can cause widespread damage due to its high power, wide coverage, and broad bandwidth.

Proliferation

Generating HEMP is very difficult and expensive because it requires the ability to field both a nuclear weapon and a delivery system to get it to altitude. It is critical to note that HEMP occurs for nuclear detonations above 25 miles and is most effective above approximately 70 miles. The higher the burst is, the more widespread the effects due to line of sight.[23] Currently, the United States, Russia, United Kingdom, France, China, India, Pakistan, and Israel have the capability to produce HEMP, and 11 other countries are not far behind, either due to indigenous weapons programs or arms trading.[24] More than 128,000 nuclear warheads have been built worldwide since 1945, and many are unaccounted for.[25] In addition, over 10,000 missiles owned by 30 countries are capable of lifting a nuclear weapon over U.S. expeditionary forces.[26] Of particular concern is North Korea, which recently declared ownership of nuclear weapons and has a robust short and intermediate range ballistic missile program with many fielded systems.

High Power Microwaves

While EMP is usually associated with nuclear weapons, it can also be generated though non-nuclear means. High power microwave (HPM) weapons encompass a class of directed-energy devices that emit electromagnetic energy at high frequencies. By changing the power, frequency, and distance to the target, HPM weapons can produce effects that range from denying the use of electrical equipment to disrupting, damaging, or destroying it.[27] HPM weapons are in their infancy and demand a strong technology base for acquisition. The biggest challenges involve building systems small enough to be tactically useful while generating sufficient power levels to affect targets from sufficient standoff range and developing ultra-wideband antennas for certain systems.[28,29]

HPM operate predominantly in the 1 MHz to 1 GHz frequency range, though occasionally higher, and may operate in very narrow bandwidths. They are capable of very short rise times (on the order of a few billionths of a second) and in this way are similar to HEMP. In addition, HPM systems can be tailored to generate area effects or to restrict influence to

small geographic areas or systems, such as individual aircraft or vehicles.[30] Current systems generate power densities between 0.1 and 100 watts/square meter (w/m^2) at the target, which corresponds to an electrical field strength between 5 and 200 v/m.[31] This power level is well below the 10 kV/m required to guarantee circuit destruction.[32] The lower power can be a limitation but also provides the benefit of scalable effects. HPM, due to their high frequency, are inherently suited to attack any modern system built on integrated circuits, circuit cards, and relay switches, such as those used for military command and control.[33]

The United States is a world leader in the development of HPM weapons and is still a few years away from fielding a system capable of inflicting electronic casualties. Other countries known to have purchased or to be developing HPM for military purposes include Australia, the United Kingdom, Russia, and Sweden.[34]

Electromagnetic Bombs

Electromagnetic bombs offer another method to generate EMP through non-nuclear means. E-bombs may be differentiated from HPM by the fact that they use conventional explosives to destroy a pre-charged electric circuit in a way that produces a desired electromagnetic wave. Since they destroy themselves to generate the pulse, they are inherently single-use devices suited to projectile munitions or suitcase bombs. Two versions of the e-bomb are the explosively pumped coaxial flux compression generator (FCG) and the virtual cathode oscillator (vircator).

FCG and Vircator Characteristics

The explosively pumped FCG is among the most mature e-bomb technologies, being first investigated by both the U.S. and U.S.S.R. in the early 1950s. The main idea behind the FCG is that of using an explosive to rapidly compress a magnetic field, transferring the energy from the explosion into an EMP.[35] A typical design involves wrapping an electrical coil around a conductive sleeve, which then surrounds a shaped explosive charge. An instant before the detonation, the coil is energized via a capacitor bank or smaller FCG with about 1 million amps of electric current, which generates an enormous, rapidly decaying electromagnetic field. The sophisticated explosive then detonates from one end of the coil to the other, distorting the conductive sleeve and creating a traveling short circuit that collapses the electromagnetic field into a narrow wave front. Published results indicate rise times between 10 and a few hundred

millionths of a second, and peak energy output near 10 megaJoules, which equates to a field strength of 1 kV/m at a range of 1 mile.[36] If the FCG were loaded on a projectile and detonated within 175 meters of the target, the field strength would increase to 10 kV/m^2, ensuring massive electronic circuit destruction. FCG pulse frequencies are low, typically below 1 MHz, which makes them less likely than HPM-type weapons to enter systems through the "front door" or to damage integrated circuits and circuit boards directly, as most electronic systems aren't vulnerable to EMP below 200 MHz.[37] However, these pulses may enter various systems through back door channels and induce malicious currents in systems.

While FCGs are relatively simple and technically viable, their inherent low frequency limits their effectiveness against many targets. The vircator, in contrast, can produce a more lethal high frequency pulse while maintaining the low physical profile required for packaging in a projectile or bomb. The physics behind a vircator are significantly more complex than the FCG. The device accelerates a high current electron beam against a foil anode, developing a space charge region that oscillates at microwave frequencies. The charge region is placed in a tuned resonant cavity, producing very high power levels. The shape of the resonant cavity is then instantly changed via an explosive charge (usually from a cylinder to a horn). The horn acts as an antenna and radiates an electromagnetic pulse of up to 40 gigawatts at frequencies between 1 and 10 GHz.[38] If one assumes a semi-isotropic antenna pattern, a vircator could generate a high frequency pulse with a field strength of 900 v/m at a range of 1 mile, or 10 kV/m at 150 meters.

Proliferation

Open literature suggests that e-bombs are easy to build that they will undoubtedly find their way into the hands of terrorists in the very near term. One source even provides the design of a FCG that it claims can be built for under $400.[39] While it is true that the component parts are cheap, assembling a working device is not trivial. Challenges include generating high power levels to charge the coil, timing excitement of the coil with detonation, and shaping the charge to detonate in a precise geometric manner. Still, an FCG is among the most likely EMP weapons to be used against the U.S. in the near term.

Vircators, on the other hand, require a rather significant technology base for development. Countries known to be working on them include the United States and Australia.[40] However, any country that relies

primarily on information technology to sustain its economy is probably capable of fielding one, and once fielded, they could proliferate rapidly, since safeguards employed to control weapons lethal to humans may not be used. Indeed, evidence suggests that e-bombs are already proliferating. A 1998 newspaper article claimed that the Swedish National Defense Research Institute purchased a Russian "suitcase bomb" for $100,000 that uses electromagnetic waves to destroy all electronics within its "blast radius."[41]

IV. 2010 EMP Threat Assessment and Scenarios

A significant amount of open-source literature proclaims that the sky is falling regarding EMP, primarily because the United States is becoming increasingly reliant on computers and information systems for its vitality and defense while systems that generate EMP are proliferating. Table 1 summarizes some of the approaching EMP threats in terms of their likelihood and severity of consequences to provide a realistic basis to discuss scenarios and responses. The table includes the author's subjective assessment of the probability of use, lethal range (based on 10 kV/m field strength at the target), most vulnerable targets (based on frequency class of weapon), and potential users in the year 2010. All data were derived from unclassified sources. The most likely threat was use of an explosively pumped flux compression generator, and the most dangerous was nuclear high altitude EMP. Though the threat of EMP existed during the Cold War, the probability will be considerably higher in 2010, as illustrated by the following plausible scenarios.

Weapon	Probability of Use	Lethal Range	Vulnerable Targets (Based on Frequency)	Potential Users
Nuclear HEMP	Moderate	Up to 1,500 mile radius	Electronics, computer chips, sensors, communications, vehicles, power transmission systems, civilian infrastructure	Nuclear powers with ballistic missile technology, Rogue states
HPM	Low	See note	Integrated circuits, circuit cards, relay switches	US, UK, Australia, Russia, Sweden
FCG	High	175 meters	Unprotected systems connected to long-run wires greater than 250 feet in length	Terrorists, Modern militaries
Vircator	Moderate	150 meters	Integrated circuits, circuit cards, relay switches	Any information age adversary
Note: Current HPM systems don't generate enough power to guarantee destruction of integrated circuits on a large scale.[42]				

Table 12.1 EMP Threats in the Year 2010

Scenario #1: China Isolates Taiwan

According to Taiwan's Ministry of Defense, China's electronic and information warfare capabilities will pose a real threat to Taiwan by 2010, as China becomes more proficient in using electromagnetic pulse bombs to paralyze Taiwan's command systems.[43] According to a white paper released by the Taiwanese government in 2002, Taiwan's capacity to endure the ravages of war is extremely limited. It will have to take offensive action in the form of a decisive naval and air battle to prevent

mainland troops from landing on the island.[44] This battle would probably involve joint U.S. forces, as the U.S.-Taiwan Relations Act pledges to "resist any resort to force or other forms of coercion that would jeopardize the security, or the social or economic system of the people of Taiwan."[45] Indeed, the United States responded promptly in 1996 with a build up of forces when Taiwan was threatened.

For its part, the United States will rely heavily on information superiority and network-centric operations to meet its Pacific commitments in 2010. According to Admiral Fargo, U.S. Pacific Command (USPACOM) Commander, USPACOM forces will exploit [informational] asymmetries for "significantly greater military capability" at lower personnel levels" through command, control, communications, computers, and reconnaissance (C4ISR) architecture.[46]

At dawn on Easter morning, 2010, Chinese special operations forces detonate a series of hand-carried flux compression generators near unprotected power transmission stations on the island of Taiwan. High energy, low frequency EMP couples with power transmission lines and overloads transformers, causing power failures at key air and missile defense sites. China immediately follows the attack with a salvo of CSS-6 GPS-guided intermediate range ballistic missiles, each carrying multiple conventional vircators.[47] The vircators detonate at precise locations above critical strategic targets, decimating computer-based systems with incredibly high power levels and small footprints, minimizing collateral damage. The attack destroys Taiwan's military command, control, and communications system and disrupts civil telecommunications, leaving the country in a communications blackout. The second wave of vircators immobilizes Taiwan's key defensive systems, including its high-tech F-16 fighters, air defense radars, and missile systems.

Meanwhile, China launches a separate EMP attack against the *USS Enterprise* carrier battle group, cruising in the Straits of Formosa. The attack involves a simultaneous wave of hundreds of air launched decoys intermixed with stealthy vircator-carrying cruise missiles. A few of the vircators get close enough to blast highly sensitive radar and communications antennas with high frequency EMP, blinding and segregating the fleet. The attack also affects key kinetic systems, grounding a large percentage of F-18 fighters and immobilizing radar-guided fleet defense missiles. Some airborne pilots are forced to bail out as their flight control computers fail.

Within an hour of such an attack, U.S. and Taiwanese forces would be unable to repel any Chinese follow-on invasion, much less wage an offensive. At the same time, U.S. leadership, half a world away, would

have little information and little time to order a response, and the event would expose America's Achilles' heel for the world to see. Crippled U.S. naval forces would have to limp home, while other similarly vulnerable forces hurriedly deploy to relieve them.

Scenario #2: North Korea Levels the Playing Field

After World War II, a republic was set up in the southern half of the Korean Peninsula while a communist-style government was installed in the north. During the Korean War (1950-1953), U.S. and other United Nations forces intervened to defend South Korea from North Korean attacks. An armistice signed in 1953 split the country in half at the 38th parallel. Since then, South Korea has undergone a technological revolution, which has driven economic growth 18 times that of North Korea, which has descended into poverty.[48] That is not to say, however, that North Korea is weak. North Korea has vast conventional forces, declared nuclear weapons, and the resolve to wage full-scale war against both South Korea and the United States.[49]

The United States and South Korea operate under the terms of the 1954 Republic of Korea-United States of America Mutual Defense Treaty, which binds both parties to defend each other. As part of this commitment, the U.S. maintains approximately 45,000 troops in South Korea with plans to reinforce them with up to 640,000 more, predominantly from USPACOM.[50] These troops, and their U.S.-equipped South Korean counterparts, represent a high-tech electronic force that relies on information superiority to overcome the larger North Korean army.

In March 2000 General Thomas Schwartz, then the U.S. commander in Korea, testified at a congressional hearing, "North Korea is the country most likely to involve the United States in a large-scale war."[51] North Korea has made it clear that it will strike all U.S. targets with all means if the U.S. strikes first. According to a Korean defense expert, North Korea plans to win without outside assistance through a massive conventional warfare campaign involving tactical aircraft, 600 high-speed landing craft, 140 hovercraft, 3,000 pontoon bridges, 700,000 troops, 8,000 heavy guns, and 2,000 tanks placed in more than 4,000 hardened bunkers within 150 km of the DMZ. North Korea plans to supplement this campaign with weapons of mass destruction.[52]

In the year 2010, tensions have increased between the United States and North Korea over the latter's nuclear weapons program. Now in the open, the U.S. has learned that North Korea has many more weapons than

feared, and recent intelligence indicates that they have sold at least one complete weapon to a terrorist organization. In response, the United States imposes sanctions on North Korea, builds up its troop strength to over 100,000 on the peninsula, and deploys two carrier battle groups to the region. With appropriate computerized mission planning tools in place and all combined and joint forces networked for dominant battlespace awareness and blue force tracking, the alliance is ready to strike. Under the cover of darkness, an all-stealth force of F/A-22s, F-117s, and B-2s strikes North Korea's nuclear production capability, after which all aircrews return safely to base. Six hours later, just before dawn, an eerie red-orange glow covers the southern sky as a North Korean Taepodong missile, carrying a small nuclear weapon, detonates high above the peninsula's southern tip. Minutes later, a vast conventional North Korean force emerges from hiding places underground and invades the south.

Even a small, relatively crude nuclear device detonated above the Korean peninsula would generate an EMP with field strength well above 10 kV/m, ensuring wholesale destruction of unprotected electronic systems.[53] The first-order effect on coalition forces would be a command, control, and communications (C3) blackout. The EMP would permanently destroy most computers and displays at the joint task force headquarters and combined air operations center and would wipe clean critical magnetically stored data. Radio, satellite, and cell phone communications would be permanently shut down, as well as wireline telephone systems relying on microprocessor control.[54]

The second order effect would be damage or destruction of major combat systems. Fielded forces would probably realize that something bad was happening but would have no way to access information and command systems to develop situational awareness and execute a response. The EMP would severely degrade the South Korean air defense system, if it did not destroy it all together. It would also immobilize unprotected vehicles (commercial and military) due to failures in electronic ignition systems and/or computerized engine controls. State-of-the-art aircraft such as the F-16, F-117, and F/A-22 would crash due to failure of fly-by-wire flight control systems and full-authority digital engine controls, and those on the ground would be inoperative. The EMP would also affect ships at sea, destroying or debilitating critical early warning radars as well as self-protection and offensive combat systems.

Third order effects would impact every soldier, sailor, airman, and Marine. This deadly shock to the network-centric and digitally magnified Western combat force would give North Korea a massive advantage for at least three reasons. First, North Korea would have achieved both tactical

surprise and information dominance. Second, North Korean forces would likely be less reliant on modern electronics for success, allowing them to withstand the EMP. Third, having foreknowledge of the attack, North Korea would be able to ensure their critical electronic systems were protected via sheltering, shielding, and positioning of the nuclear detonation.

Scenario #3 EMP Attack on U.S. Homeland

On July 15, 1996, President Bill Clinton issued executive order No. 13010, which identified infrastructures critical to the nation's survival: telecommunications, electrical power systems, oil and gas storage, transportation, banking and finance, water supply systems, and emergency services.[55] Unfortunately, these critical infrastructures were also singled out by a 2004 congressional report as being vulnerable to EMP attack. The report concluded that America's reliance on electronics makes "EMP one of a small number of threats that can hold [US] society at risk of catastrophic consequences."[56] It went on to say that EMP damage to electric power systems, telecommunications, energy, and other infrastructures could seriously impact the nation's financial system, means of getting food, water, and medical care to the citizenry, trade, and the production of goods and services. This vulnerability will present an increasingly attractive target to America's enemies as U.S. use of, and dependence on, electronics continues to grow, and nuclear weapons proliferate. In the context of theater operations, adversaries could use an EMP attack against the U.S. homeland as either a deterrent to U.S. involvement or as a preemptive strike to task saturate U.S. leadership and focus U.S. forces at home. Amazingly, Vladimir Lukin, a member of the Russian Duma, actually suggested such a course of action in 1999. Mr. Lukin told Representative Bartlett, who was part of a delegation sent to ease tensions with Russia over U.S. involvement in the Balkans, that if Russia really wanted to hurt the United States, they would launch a missile from a submarine, explode it high over the U.S., and shut down the U.S. power grid for six months.[57]

U.S.-Russian relations cool dramatically by 2010 due to tensions over U.S. military presence and action in the Caucuses. The Russians demand U.S. expeditionary forces withdraw within 72 hours or face dire consequences. Seeing no significant Russian troop build up in concert with the threat, the U.S. calls Russia's bluff, while attempting to negotiate a settlement. Twenty-four hours after the deadline, a Russian "spy

satellite" explodes over the central United States, releasing a high altitude electromagnetic pulse that blankets the entire continent.

The effect of a HEMP attack on the continental U.S. would be devastating, causing several trillions of dollars of damage (by conservative estimates) in cascading failures of interdependent infrastructures.[58] The primary avenue for destruction would be through electrical power and telecommunications, on which all other infrastructures, including energy, transportation, banking and finance, water, and emergency services, depend.[59] The cumulative effect of infrastructure failures would effectively send the country back in time. The majority of the US would be without electrical power. Telephones, televisions, and radios would be inoperative, and fuel/energy would be scarce. Most cars would not work, and public transportation—plane, rail, and bus, would be immobilized. Banking and financial services would become unavailable, and the amount in one's wallet or purse would define their liquid worth. At the same time, emergency services would have trouble functioning and responding to the disaster. The discussion below describes the most critical failures.

Electrical Power

The U.S. economy and functioning society is critically dependent on electricity. Fortunately, the electrical power system in North America is outstanding in its ability to deliver relatively cheap, high-quality power to end-users. At the same time, however, the system has become increasingly fragile. While demand for electrical power has increased dramatically over the last decade, little has been done to upgrade power transmission systems. At the same time, the few power generation systems added to the grid have been built at considerable distances from load centers for environmental purposes. The result is a system operating near peak capacity to move power from generation to load. The August 14, 2003 blackout provides a clear example of system fragility. At approximately 4:10 pm, a power surge of approximately 3,500 MW entered the New York power system.[60] Within seconds, 50 million North Americans found themselves without power, and thousands of businesses had to close operations.[61] The blackout was a wake up call to American leadership on the fragility of the infrastructure. The effects of an HEMP-induced blackout would be far more severe for at least three reasons. First, an HEMP attack would induce power surges simultaneously over the entire continent, degrading at least 70% of the nation's electrical service in an instant. Second, the late-time EMP component (E3) would couple more efficiently to long power transmission lines than naturally occurring

phenomenon do, and thus would produce far more damage than seen on August 14th. Third, the electrical power system requires proper functioning communications, financial systems, transportation, and fuel supply for operation, all of which would also suffer damage from HEMP, which would extend the recovery time to a period of months or a year.[62]

Telecommunications

Telecommunications are critical to modern society's function because they enable other key infrastructures like financial markets, transportation, and energy distribution; facilitate business and commerce; provide personal convenience; and allow for coordinated emergency response.[63] Fortunately, efforts have been underway since 1985 to harden critical parts of the U.S. telecommunications infrastructure from HEMP.[64] Its four major elements—wireline, wireless, satellite, and radio—have overlapping capabilities and different vulnerabilities to EMP. After an attack, some portion of the system would still be intact but would be overloaded by massive call volume, leading to significantly degraded service. In anticipation, the U.S. government developed national security and emergency preparedness (NS/EP) telecommunications services that guarantee government priority on surviving infrastructure. An unfortunate side effect of NS/EP, in the event of an HEMP attack, is that most civilian users would be locked out of the communications grid, making disaster response problematic. In many cases, authorities would have no way to contact citizens and provide instructions.[65]

Fuel/Energy

U.S. fuel and energy production and distribution systems depend heavily on electronic control systems that use real-time data flows for operation and use electronic sensors to monitor critical processes and react quickly to malfunctions. An EMP attack would fatally damage at least some of these electronics, causing ungraceful system shutdowns resulting in extensive damage, while providing an incomplete picture for troubleshooting and repair. Simultaneous failures in the electrical and communications sectors would also affect fuel and energy availability. Electrical power needed to operate valves, pumps, and other machinery required to deliver fuel wouldn't be available, and communications needed

to coordinate activities at refineries and ensure safety of on-site personnel and the surrounding environment would be scarce.[66] In the end, the fuel and energy shortage would probably persist for extended periods while interrelated infrastructures were repaired. Consequently, the U.S. could experience many casualties due to exposure if the attack occurred in the winter.

Transportation

The U.S. transportation infrastructure includes freight and commuter railroads, commercial air, roadways, and waterways, all of which are increasingly reliant on information technology and public information networks.[67] The push to achieve superior performance has led to tremendous reliance on electronics vulnerable to EMP. Examples include microprocessor-controlled internal combustion engines and electronic tracking of freight shipments outfitted with miniature radio frequency identification tags. The Commission to Assess the Threat to the United States from EMP Attack determined that significant degradation of U.S. transportation infrastructure would result from EMP attack. In particular, municipal road traffic would experience gridlock, traffic lights would fail, and many autos would shut down permanently. Railroad traffic would stop, and commercial air traffic would cease operations for safety reasons. Similarly, ports would stop loading and unloading ships until power and telecommunications infrastructures were restored.[68]

Banking and Finance

Almost all U.S. economic activity depends on proper functioning of the financial industry, built on a foundation of electronic technologies. Most financial transactions involved in preserving and promoting national wealth, as well as the preponderance of personal and institutional transactions, are performed and recorded electronically. In addition, the financial system depends on reliable and robust telecommunications to coordinate interrelated business, and electrical power to sustain operations.[69] The attacks of September 11, 2001 illustrated that disruption of critical infrastructures has a direct effect on financial markets and increases liquidity risks for the United States financial system. In response to this, the Federal Reserve Board identified key functions that require same-day recovery after an attack to ensure viability of the U.S. financial system. These functions included large-value inter-bank funds transfer capability, automated clearinghouse operations, key clearinghouse settlement utilities,

and treasury automated auction and processing system operation.[70] Each of these systems and their underlying infrastructures are potentially vulnerable to EMP. If they fail for greater than 24 hours, quite likely in this scenario, the viability of the entire U.S. economy would be at risk.

Emergency Services

EMP attack would severely debilitate emergency services required for adequate response, primarily due to service reliance on computer and communications equipment, but also due to their reliance on electricity.[71] Emergency services are also critically dependent on transportation, fuel for backup generators, and network equipment, all debilitated by EMP as previously discussed. Thus, emergency services represent another critical infrastructure in the chain of cascading failures that would contribute to the growing catastrophe.

V. Recommendations and Conclusion

EMP poses a massive threat to U.S. theater operations through its potential to isolate forces and deny access to regions, its ability to nullify the U.S. technology advantage, and its potential to produce a devastating national catastrophe. Even more ominous is the fact that the means to produce EMP effects, both nuclear and non-nuclear, are proliferating. National leaders must face the looming EMP threat immediately and develop measures that will reduce the likelihood of an EMP strike, maintain the military advantage in the event of theater attack, and increase the nation's chance for surviving a homeland attack. Through diplomacy, hardening of critical systems, training, and the establishment of industry standards to ensure future procurement of EMP-resilient systems, America can prevail against one of the most serious near-term threats.

Diplomacy

The first step in mitigating the possibility and consequence of EMP attack is deterrence. Rather than avoiding the issue of EMP, U.S. diplomats and senior leaders should transmit an unambiguous message about adversary use of EMP weapons. Specifically, the U.S. should openly classify nuclear EMP as a weapon of mass destruction (WMD), due to its huge footprint and devastating effects. Though nuclear EMP won't harm humans directly as long as they are kept clear of blast effects, second-order humanitarian consequences of a large-scale attack would be overwhelming. In addition, a homeland attack could threaten the ability of

U.S. leaders to govern and would probably wreck the U.S. economy. Therefore, the U.S. must consider such an attack a WMD strike and make it clear that the United States would respond in kind.

Hardening of Military Systems

A subset of critical military systems must be hardened to ensure survival in an EMP environment to bolster the credibility of deterrence and to ensure that the U.S. can meet national and military objectives at home and abroad even if attacked by EMP. The two ways to protect electronic systems from EMP both involve putting a physical electric shield around vulnerable electronics. The first method involves shielding the environment in which the electronics operate (such as an entire building), while the second involves shielding individual circuits.

EMP Hardening Techniques

Shielding the environment is a cost-effective solution for EMP protection when a large number of essential electronic devices are collocated. An air operations center (AOC) provides a good example. Incorporating a grounded metallic shield into the building structure and surge protecting power, communications, and antenna lines could protect an entire AOC from EMP. Mobile systems require a different means, such as a Faraday cage, which can protect individual components. A Faraday cage is simply a metallic mesh built around an electronic circuit (such as a fighter aircraft flight control computer) that protects it from EMP.

The cost of hardening systems against EMP in the design phase is relatively inexpensive, usually between 1% and 5% of system cost.[72] Unfortunately, the U.S. has only hardened a portion of its strategic force and virtually none of its tactical force.[73] Hardening systems after fielding is significantly more expensive. Making matters worse, U.S. forces are increasingly embracing commercial-off-the-shelf systems, dramatically increasing their vulnerability to EMP.

Priorities for Military EMP Hardening

Hardening the preponderance of fielded military forces is not fiscally viable in an era of constrained budgets. Therefore, the U.S. should focus on building EMP protection into future systems while retrofitting a subset of those already fielded. The Commission to Assess the Threat to the U.S. from EMP Attack determined that satellite navigation systems, satellite

and airborne intelligence and targeting systems, communications infrastructure, and missile defense are essential to U.S. success in regional conflicts.[74] Therefore, hardening efforts must ensure adequate capability in these areas after an EMP attack. In addition, the U.S. should harden a small but lethal "EMP-proof" strike force capable of exacting a high price on adversaries using EMP. This force should include tactical and strategic aircraft, special operations forces, and hardened support assets.

Civil infrastructure today is arguably America's greatest critical vulnerability and represents an attractive target for adversaries to use as a deterrent to U.S. military engagement abroad. Fortunately, affordable means exist to reduce vulnerability to acceptable levels within a few years, and certainly by 2010.[75] Electricity and telecommunications infrastructures should be protected first, since all other critical infrastructures depend on them. It would be impractical to protect the entire electrical power system from EMP attack due to the diverse range of equipment and designs involved, which makes the cost of retrofit prohibitive.[76] Therefore, the U.S. power system would almost certainly experience widespread blackouts following an HEMP attack. Realizing this, protective measures should focus on providing the quickest possible recovery through hardening of critical nodes. Efforts should prioritize identification and protection of regional power generation necessary for recovery and spares should be stockpiled at coal-fired and hydroelectric plants, which are resistant to EMP and offer the best chance for rapid repair. Other high-value and long-lead-time assets, such as power transmission components, should be protected at the system level, and auxiliary power and hardened communications must be made available at centers responsible for restoration.[77]

Telecommunications, like electrical power, cannot realistically be comprehensively protected. Hardening should focus on expanding capability of current emergency communications systems and identifying and protecting high-leverage communications nodes. For example, national security and emergency preparedness telecommunications services (NS/EP), already hardened against EMP, should be upgraded to increase the number of possible users, and should be monitored and tested to ensure upgrades don't introduce vulnerabilities. At the same time, key network elements, such as signal transfer points and wireless home locator registers, should be system-hardened against fast rise (E1) EMP, and the general capability of the telecommunications system to withstand sustained power failures should be improved.[78]

Training

Both military and civilian agencies need to start integrating EMP scenarios into training exercises. One of the immediate effects of an attack would be loss of communications and situational awareness, which could lead to paralyzing confusion if not planned for and practiced. In the near term, training should emphasize response options for current fielded forces, expanding on mitigation techniques proposed by Marine Major John CaJohn. Maj CaJohn recommends forces develop standard procedures to immediately restore communications (using messengers or pyrotechnics if necessary), use UHF instead of VHF radios, shut down and protect unneeded radios for later use as backups, use small antennas, keep cable runs short, run cables on the ground, shield critical components, ground all equipment, and avoid use of commercial power to decrease vulnerability to EMP.[79] In addition to practicing sound EMP protective measures, combat and civil disaster response units should start incorporating EMP scenarios in major training exercises. Red teams should identify portions of forces notionally taken out by EMP and deem them ineffective for portions of the exercise, forcing blue forces to adapt.

Development of EMP-Resistant Manufacturing Standards

Legislated industry standards for EMP protection of critical systems could be the best way to address the long-term EMP threat. Although the U.S. military has long known the potential effects of EMP and the small procurement costs to mitigate against it, few systems have been hardened. The civil sector is even less inclined to spend extra money hardening against what is characteristically a military threat. Therefore, Congress should consider establishing and enforcing EMP protection standards to compel compliance. For example, major electrical power and telecommunications infrastructure components should be required to be "EMP compliant," as should most components of future military systems. Such legislation would levy a small burden on industry today but could make a huge contribution to America's survival in the future.

Conclusion

Electromagnetic pulse weapons represent one of the most ominous threats to U.S. national security in the near term and offer potential adversaries an attractive asymmetric attack option to stymie U.S.

expeditionary operations. Both nuclear and non-nuclear EMP technologies are proliferating and threaten U.S. operations in different ways and at different levels. In light of the emerging threats, it is clear that the United States should respond with a coordinated diplomatic, military, and civilian effort that addresses the most likely and most catastrophic EMP scenarios. The response should include a formal mandate classifying high-power nuclear EMP weapons as WMD, recursive hardening of critical expeditionary capabilities, near-term establishment of a credible EMP-hardened strike force, hardening critical components of the civilian infrastructure, large-scale military and civilian EMP response training, and legislated EMP hardness requirements for future military and civilian systems. A coordinated response can protect America's electronic Achilles' heel from EMP, ensure effectiveness of its military forces, and help guarantee viability of U.S. society for years to come.

Notes

[1] George W. Bush, *National Security Strategy of the United States* (Washington DC: White House, 2002), 1.

[2] Ibid, 15.

[3] Joint Chiefs of Staff, *Joint Vision 2010* (Washington D.C.: Joint Chiefs of Staff, 1995), 17-18.

[4] Donald H. Rumsfeld, *Transformation Planning Guidance* (Washington D.C.: Department of Defense, 2003), 1.

[5] A.K. Cebrowski, *The Implementation of Network-centric Warfare* (Washington DC: Department of Defense, 2005), 4.

[6] Richard D. Winters, "Power Supply Voltage Transient Analysis & Protection" (paper presented at the Powercon III, Power Conversion Conference, Tempe AZ, 1976). Available from http://ieeexplore.org.

[7] Dennis Bodson, "Electromagnetic Pulse and the Radio Amateur," *QST* 70, no. 8 (August 1986), 19.

[8] Winters, "Power Supply Voltage Transient Analysis & Protection.'" Available from http://ieeexplore.org .

[9] Eileen M. Walling, "High Power Microwaves: Strategic and Operational Implications for Warfare," (Maxwell AFB AL: Air University, 2000), 4.

[10] Carlo Kopp, "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction," (Fairbairn, Australia: RAAF Air Power Studies Centre, 1996), 2. Available from http://www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html.

[11] House Military Research & Development Subcommittee, *Threats Posed by Electromagnetic Pulse to U.S. Military Systems and Civilian Infrastructure*, Statement of Dr. Lowell Wood, July 16, 1997, 63. Available from http://commdocs.house.gove/committees/security/has197010.000/has197010_Of.htm.

[12] Major M. CaJohn, "Electromagnetic Pulse: From Chaos to a Manageable Solution," (Quantico VA: Marine Corps Command and Staff College, 1988), 6. Available from http://www.globalsecurity.org/wmd/library/report/1988/CM2.htm.

[13] Kopp, "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction," 9.

[14] *Threats Posed by Electromagnetic Pulse to U.S. Military Systems and Civilian Infrastructure*, 14.

[15] Walling, "High Power Microwaves," 4-8.

[16] Jack Spencer, "America's Vulnerability to a Different Nuclear Threat: An Electromagnetic Pulse," *Backgrounder 1372* (Washington DC: Heritage Foundation, 26 May 2000), 1. Available from http://www.heritage.org/Research/MissileDefense/bg1372.htm.

[17] Dr. J. S. Foster et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, (Washington DC: U.S. Congress, 2004), 4. Available from http://www.globalsecurity.org/wmd/library/congress/2004_r/04-07-22emp.pdf.

[18] Office of the Under Secretary of Defense for Acquisition and Technology, *The Military Critical Technologies List Part II: Weapons of Mass Destruction Technologies* (Washington D.C.: Department of Defense, 1998), II-6-28. Available from http://www.wetp.org/Wetp/public/dwlds/HASL_271dnlfile.PDF.

[19] Foster et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, 5.

[20] Ibid., 5-6.

[21] Ibid., 6.

[22] *Threats Posed by Electromagnetic Pulse to U.S. Military Systems and Civilian Infrastructure*, Statement of Dr. George W. Ullrich, 21.

[23] Dr. Bruce C. Gabrielson, "An Introduction to the EMP and Lightning Threat," in *EMC Expo 87* (San Diego, CA: Sachs/Freeman Associates, Inc., 1987). Available from http://molasar.blackmagic.com/ses/bruceg/EMC/EMP-Light.html.

[24] *The Military Critical Technologies List Part II: Weapons of Mass Destruction Technologies*, II-6-4.

[25] CDI, "Nuclear Facts at a Glance," (Center for Defense Information, 4 February 2003). Available from http://www.cdi.org/nuclear/facts-at-a-glance.cfm.

[26] Dr. Jane Orient, "The Really Big Threats," *Civil Defense Perspectives* 18, no. 6 (September 2002), 1. Available from http://www.oism.org/cdp/sept2002.htm.

[27] Walling, "High Power Microwaves," 1.

[28] Ibid.

[29] AFRL, "High Power Microwave Fact Sheet," (Kirtland AFB: Air Force Research Laboratory, 2002).

[30] Ibid.

[31] Walling, "High Power Microwaves," 4. Field strength calculated using free air impedance of 377 ohms, [V/m = Sqr(377*W/m^2)]

[32] *Threats Posed by Electromagnetic Pulse to U.S. Military Systems and Civilian Infrastructure*, 63.

[33] Walling, "High Power Microwaves," 4.

[34] Ibid., 22.

[35] Kopp, "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction," 3.

[36] Ibid., 5. Field strength calculated assuming an energy output of 20 MegaJoules, pulse width of 200 microseconds, isotropic antenna pattern, and free air impedance of 377 ohms.

[37] D. V. Giri, "Electromagnetic Sources and Threats to Civilian Systems," *IEEE*, 2003. Available from http://www.geml.uni-hannover.de/ieee/events/emv2003/Aushang_Giri_ro.pdf.

[38] Kopp, "The Electromagnetic Bomb: A Weapon of Mass Destruction," 6.

[39] Jim Wilson, "E-Bombs and Terrorists," *Popular Mechanics* 178, no. 9 (September 2001), 51.

[40] Kopp, "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction," 18.

[41] Joint Economic Committee, United States Congress, Statement of Dr. Ira W. Merritt, 25 February 1998, 3. Available from http://www.iwar.org.uk/iwar/resources/senate/merritt.htm.

[42] Walling, "High Power Microwaves, " 4; *Threats Posed by Electromagnetic Pulse to U.S. Military Systems and Civilian Infrastructure*, 63.

[43] David Isenberg, "Taiwan Defense: Finger on the 'Enter' Key," *Asia Times Online*, 14 August 2002. Available from http://www.atimes.com/atimes/china/DH14Ad04.html.

[44] Ibid.

[45] *Taiwan Relations Act.* US Code Title 22, Chapter 48, Section 3301, subsection (b) (6), 10 April 1979. Available from http://www.taiwandocuments.org/tra01.htm.

[46] Thomas B. Fargo, "Operationalizing the Asia-Pacific Defense Strategy," *Joint Force Quarterly*, Autumn 2002, Issue 32, 12.

[47] Monterey Institute of International Studies, "Chinese Ballistic Missiles," 1999. Available from http://cns.miis.edu/research/China/coxrep/wbmdat.htm.

[48] CIA, *CIA World Fact Book* (Washington DC: Central Intelligence Agency, 2005). Available from http://www.odci.gov/cia/publicatons/factbook/geos/ks.html-p.

[49] Han Ho Suk, "North Korea's War Strategy of Massive Retaliations against US Attacks," Center for Korean Affairs, 24 April 2003, entire article but especially 5-7, 9-10. Available from http://resistance.chiffonrouge.org/article.php3?id_article=189.

[50] John Pike, "Republic of Korea Military Guide," 2002. Available from http://www.globalsecurity.org/military/world/rok/index.html.

[51] Suk, "North Korea's War Strategy of Massive Retaliations," 1.

[52] Ibid., 7.

[53] *Threats Posed by Electromagnetic Pulse to U.S. Military Systems and Civilian Infrastructure*, Statement of Dr. Lowell Wood, 63, 74.

[54] Foster et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, 27.

[55] Spencer, "America's Vulnerability to a Different Nuclear Threat: An Electromagnetic Pulse," 5.

[56] Foster et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, v (abstract).

[57] Paul M. Weyrick, "Electromagnetic Pulse: An Avoidable Disaster," *Free Congress Research and Education Foundation*, 3 January 2005. Available from http://www.renewamerica.us/columns/weyrich/050103.

[58] *Threats Posed by Electromagnetic Pulse to U.S. Military Systems and Civilian Infrastructure*, 84.

[59] Foster et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, 1, 8.

[60] New York Independent System Operator, *Interim Report on the August 14, 2003 Blackout*, (New York, NY: New York Independent System Operator, 2004), 4. Available from http://www.ksg.harvard.edu/hepg/Papers/NYISO.blackout.report.8.Jan.04.pdf.

[61] J. Peter Lark, "Report on August 14th Blackout," Michigan Public Service Commission, 2003, 1. Available from http://www.michigan.gove/mpsc/0,1607,7-159-16370_17060-80766--,00.html.

[62] Foster et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, 6.

[63] Ibid., 24.

[64] Ibid., 25.

[65] Ibid., 25-27.

[66] Ibid., 35.

[67] Ibid., 36.

[68] Ibid., 37.

[69] Ibid., 31.

[70] "Federal Reserve Board Sponsorship for Priority Telecommunications Services of Organizations That Are Important to National Security/Emergency Preparedness," *Federal Register* 67, no. 236 (9 December 2002), 72958. Available from http://www.occ.treas.gov/fr/federalreister/67fr72958.pdf.

[71] Foster et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, 43.

[72] *Threats Posed by Electromagnetic Pulse to U.S. Military Systems and Civilian Infrastructure*, 23.

[73] CaJohn, "Electromagnetic Pulse-from Chaos to a Manageable Solution," 8.

[74] Foster et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, 48.

[75] Ibid., 11.

[76] Ibid., 20.

[77] Ibid., 21-22.

[78] Ibid., 29.

[79] CaJohn, "Electromagnetic Pulse-from Chaos to a Manageable Solution," 15-16.