Order Code RL32544

CRS Report for Congress

High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments

Updated July 21, 2008

Clay Wilson
Specialist in Technology and National Security
Foreign Affairs, Defense, and Trade Division

Congressional Research Service

Prepared for Members and Committees of Congress

High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments

Summary

Electromagnetic Pulse (EMP) is an instantaneous, intense energy field that can overload or disrupt at a distance numerous electrical systems and high technology microcircuits, which are especially sensitive to power surges. A large scale EMP effect can be produced by a single nuclear explosion detonated high in the atmosphere. This method is referred to as High-Altitude EMP (HEMP). A similar, smaller-scale EMP effect can be created using non-nuclear devices with powerful batteries or reactive chemicals. This method is called High Power Microwave (HPM). Several nations, including reported sponsors of terrorism, may currently have a capability to use EMP as a weapon for cyber warfare or cyber terrorism to disrupt communications and other parts of the U.S. critical infrastructure. Also, some equipment and weapons used by the U.S. military may be vulnerable to the effects of EMP.

The threat of an EMP attack against the United States is hard to assess, but some observers indicate that it is growing along with worldwide access to newer technologies and the proliferation of nuclear weapons. In the past, the threat of mutually assured destruction provided a lasting deterrent against the exchange of multiple high-yield nuclear warheads. However, now even a single, low-yield nuclear explosion high above the United States, or over a battlefield, can produce a large-scale EMP effect that could result in a widespread loss of electronics, but no direct fatalities, and may not necessarily evoke a large nuclear retaliatory strike by the U.S. military. This, coupled with published articles discussing the vulnerability of U.S. critical infrastructure control systems, and some U.S. military battlefield systems to the effects of EMP, may create a new incentive for other countries to rapidly develop or acquire a nuclear capability.

Policy issues raised by this threat include (1) what is the United States doing to protect civilian critical infrastructure systems against the threat of EMP, (2) could the U.S. military be affected if an EMP attack is directed against the U.S. civilian infrastructure, (3) are other nations now encouraged by U.S. vulnerabilities to develop or acquire nuclear weapons, and (4) how likely are terrorist organizations to launch a smaller-scale EMP attack against the United States?

This report will be updated as events warrant.

Contents

Background 1
The EMP Commission 2
2008 Report on Critical Infrastructure Vulnerabilities 4
Private Sector and State Government Poorly Prepared 4
Inaction May Increase EMP Threat to the United States 5
Electromagnetic Pulse Overview 6
Description of High-Altitude Electromagnetic Pulse 6
Description of High-Power Microwaves 8
Disruptive Effects of EMP 9
Recovery After Attack 10
Economic Damage Estimates after Attack on Washington, D.C., Region . 11
Portable Data Centers and Hardening Against EMP 13
DOD Vulnerabilities and Research 14
Ground Wave Emergency Network 16
EMP Capabilities of Other Nations 16

Policy Analysis 18
Preparedness 18
Department of Homeland Security 20
Nuclear Incentive 20
Terrorists 21
Human Rights 22

Legislative Activity 22

CRS Products 22

List of Figures

Figure 1. Estimated Area Affected by High-Altitude EMP 7

List of Tables

Table 1. Estimates of Damage and Recovery Times After HEMP Attack on Washington, D.C., Regional Area 12

High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments

Background

A Commission to Assess the Threat from High Altitude Electromagnetic Pulse (EMP commission) was established by Congress in FY2001 after several experts expressed concern that the U.S. critical infrastructure and military were vulnerable to EMP attack.[1] On July 20, 2008, the Commission presented a report to the House Armed Services Committee (HASC) assessing the effects of an EMP attack on U.S. critical national infrastructures. The 2008 report contained analysis of results of tests for modern electronics and telecommunications equipment for public networks supported by the power grid and by temporary isolated power supplies, including cell phones, computer servers, and Internet routers and switches. The report also made recommendations for preparation, protection, and recovery of U.S. critical infrastructures from EMP attack.

The Commission reported that the ubiquitous dependency of society on the electrical power system, coupled with the EMP's particular damage mechanisms, creates the possibility of long-term, catastrophic consequences for national security. Comparison was made to hurricane Katrina in 2005, where the protracted power blackout exhausted the limited fuel supplies for emergency generators. However, in the case of an EMP attack, a widespread collapse of the electric power grid could lead to cascading effects on interdependent infrastructures, possibly lasting weeks or months. The Commission stated, "Should significant parts of the electrical power infrastructure be lost for any substantial period of time ... many people may ultimately die for lack of the basic elements necessary to sustain life in dense urban and suburban communities ... [and] the Federal Government does not today have sufficiently robust capabilities for reliably assessing and managing EMP threats."[2]

At a prior hearing, on July 22, 2004, panel members from the EMP commission stated that as U.S. military weapons and control systems become more complex, and as portions of the military's administrative communications systems continue to rely on the U.S. civilian infrastructure for support, they may be increasingly vulnerable to the effects of EMP. The consensus of the Commission in 2004 was that a large-

---

[1] Michael Sirak, "U.S. vulnerable to EMP Attack," *Jane's Defence Weekly*, July 26, 2004, [http://www.janes.com/defence/news/jdw/jdw040726_1_n.shtml].

[2] Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack; Critical National Infrastructures, Apr 2008, p.vi-viii, and p.79.

scale, high-altitude EMP attack could possibly cause widespread damage to unprotected civilian and military electronic equipment for an extended period.[3]

However, the consensus of the EMP commission in 2008 was that the United States need not remain vulnerable to catastrophic consequences of an EMP attack, and that the nation's vulnerability can be reasonably reduced by coordinated and focused effort between the private and public sectors. The Committee stated that the cost for improved security in the next three to five years would be modest, especially when compared with the costs associated with the war on terror and the value of the national infrastructures threatened.[4]

The EMP commission's reports in both 2004 and 2008 focused only on the effects of High Altitude EMP (HEMP), and not necessarily the effects High Power Microwave (HPM) devices, which are non-nuclear Radio-Frequency (RF) weapons that can also produce damaging EMP, but with different characteristics and covering a smaller geographic area. Both types of EMP are discussed below.

The widely published vulnerability of U.S. civilian and some military electronics to EMP, along with technical accessibility and lower cost, could make smaller-scale HPM weapons attractive in the future as weapons for terrorist groups. Also, some observers argue that unless the United States openly describes how it is taking action to reduce EMP vulnerabilities within critical infrastructures, perceived inaction will increase the likelihood that a rogue nation will seek to employ the asymmetric effects of HEMP against our computer systems.

The EMP Commission

The EMP commission was reestablished by P.L. 109-163, the National Defense Authorization Act for FY2006. The new Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack (note that the new title no longer includes the phrase "High Altitude", and adds the new word "Attack") continues with the same membership, and the Secretary of Defense is authorized to appoint a new member in the event of a vacancy.[5] The EMP commission is tasked to monitor, investigate, and make recommendations about the vulnerability of electric-dependent systems of the Department of Defense, government agencies, and the private sector.

On July 22, 2004, members of the EMP commission testified before the House Armed Services Committee and presented a report consisting of the following five volumes:

Volume 1 is an unclassified Executive Summary.
Volume 2 is a classified Threat Assessment.
Volume 3 is an unclassified Assessment of the U.S. Critical Infrastructure.

---

[3] Daniel G. Dupont, "Panel Says Society At Great Risk From Electomagnetic Pulse Attack," *Inside the Pentagon*, July 15, 2004, p.1.

[4] William Graham, Testimony before the House Armed Services Committee, Jul 10, 2008.

[5] P.L. 109-163, Section 1052, reestablishes the EMP commission.

Volume 4 is a classified discussion of Military Topics.
Volume 5 is a classified Assessment of Potential Threats.

The report stated that High Altitude EMP is capable of causing catastrophic consequences for the nation, and that the current vulnerability of our critical infrastructures, which depend so heavily on computers and electronics, can both invite and reward attack if not corrected.[6]

Specifically referring to the U.S. military, the report states:

> ... EMP test facilities have been mothballed or dismantled, and research concerning EMP phenomena, hardening design, testing, and maintenance has been substantially decreased. However, the emerging threat environment, characterized by a wide spectrum of actors that include near-peers, established nuclear powers, rogue nations, sub-national groups, and terrorist organizations that either now have access to nuclear weapons and ballistic missiles or may have such access over the next 15 years have [sic] combined to place the risk of EMP attack and adverse consequences on the U.S. to a level that is not acceptable.... Our increasing dependence on advanced electronics systems results in the potential for an increased EMP vulnerability of our technologically advanced forces, and if unaddressed makes EMP employment by an adversary an attractive asymmetric option."[7]

The EMP commission's 2004 report proposed a five-year plan for protecting critical infrastructures from EMP and from other large-scale terrorist attacks. The five-year plan is briefly summarized in Volume 3 of the report. However, some portions of the five-year plan that are related to military equipment may remain classified. The Commission is currently preparing a review of the DOD response to recommendations made in 2004.[8]

Testimony at the 2004 hearing included questions such as (1) how would the United States respond to a limited HEMP attack against the U.S. homeland or against U.S. forces, where there is loss of technology, but no directly caused loss of life; (2) does the current lack of U.S. preparedness invite adversaries to plan and attempt a HEMP attack; and (3) are the long-term effects of a successful HEMP attack, leading to possible widespread starvation and population reduction, potentially more devastating to the U.S. homeland than an attack by surface nuclear weapons?

---

[6] William Graham, et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, Volume 1: Executive Report 2004*, [http://www.house.gov/hasc/openingstatementsandpressreleases/108thcongress/04-07-22emp.pdf].

[7] William Graham, et. al., Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, Volume 1: Executive Report 2004, [http://www.house.gov/hasc/openingstatementsandpressreleases/108thcongress/04-07-22emp.pdf], p.47.

[8] Personal communication with EMP Commission staff, Mar 26, 2008.

2008 Report on Critical Infrastructure Vulnerabilities

The 2008 EMP Commission report discussed vulnerabilities and interdependencies among 10 U.S. critical infrastructures. Findings showed that only limited EMP vulnerability testing had previously been done for modern electronic systems that help support these infrastructures. In addition, the Commission expressed concern that widespread use of automated supervisory and control data acquisition (SCADA) systems for the critical infrastructure had allowed companies and agencies to systematically reduce the size of their work forces having the necessary technical knowledge needed to support manual operations of these infrastructure control systems, as might be needed during a prolonged emergency. The Commission concluded, after reviewing national capabilities to manage the effects of nuclear weapons (and EMP) on modern systems, that "the Country is rapidly losing the technical competence in this area that it needs in the Government, National Laboratories, and Industrial Community."[9]

Private Sector and State Government Poorly Prepared

Experts on the Commission have asserted that little has been done by the private sector to protect against the threat from electromagnetic pulse, and that commercial electronic systems in the United States could be severely damaged by EMP attack.[10] Commercial electronic surge arresters commonly used for lightning strikes reportedly cannot be relied on because most do not clamp fast enough to protect against the near-instantaneous effects of EMP (see section below on "Electromagnetic Pulse Overview").[11]

In March 2007, a survey of state Adjutants General who oversee National Guard units throughout the country found that most state-based emergency responders are not actively preparing against an attack on the United States by electromagnetic pulse. The survey, entitled "Missile Defense and the Role of the States", was conducted jointly by the Anchorage-based Institute of the North and the Claremont Institute of Claremont, California. Survey questions were sent to Adjutants General of all 50 states, with more than half responding. Although 96% of state Adjutants General indicated significant concern over an EMP attack, the majority had done little or no analysis of the effects of an overhead EMP attack, and little or no training, or preparation to harden electronic equipment. None of the

---

[9] Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack; Critical National Infrastructures, Apr 2008, p.viii.

[10] House Armed Services Committee, *Committee Hearing on Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack*, July 22, 2004.

[11] Army Training Manual 5-692-2, "Maintenance of Mechanical and Electrical Equipment at Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities, *HEMP Protection Systems*, April 15, 2001, Chapter 27, [http://www.usace.army.mil/publications/armytm/tm5-692-2/chap27VOL-2.pdf].

Adjutants General surveyed indicated that they were actively involved in a formal planning process for response to an EMP attack.[12]

Inaction May Increase EMP Threat to the United States

Some analysts discount the likelihood of a large-scale EMP attack against the United States in the near term, and the extent of possible damage, stating that the critical infrastructure reportedly would survive, and that military communications would continue to operate and a high percentage of civilian phone calls would continue to connect. The argument is that limited testing has shown that modern commercial equipment may be surprisingly resistant to the effects of electromagnetic pulse, and that some military systems using commercial equipment are also retrofitted to be made more EMP resistant before they are fielded.[13]

However, other analysts maintain that some past testing done by the U.S. military may have been flawed, or incomplete, leading to faulty conclusions about the level of resistance of commercial equipment to the effects of EMP. These analysts also point out that EMP technology has been explored by several other nations, and as circuitry becomes more miniaturized, modern electronics become increasingly vulnerable to disruption. They argue that, depending on the targeted area and power of an EMP attack, it could possibly take years for the United States to recover fully from the resulting widespread damage to electronics and the power grid.[14]

Commission members have stated at hearings that, as time passes without a visible effort to show the world that we are protecting our computer systems and critical infrastructures, the perceived inaction may actually invite a possible EMP attack.[15] In the past, the threat of mutually assured destruction provided a lasting deterrent against the exchange of multiple high-yield nuclear warheads. However, a single, low-yield nuclear explosion high above the United States, or over a battlefield, can produce a large-scale, high-altitude EMP effect resulting in widespread loss of electronics, but possibly without direct fatalities. Therefore, an

---

[12] Press release, *Survey Finds Nation Vulnerable to EMP Attack: States Not Preparing*, Institute of the North and The Claremont Institute, March 7, 2007, [http://www.institutenorth.org/servlet/download?id=261].

[13] Stanley Jakubiak, statement before the House Military Research and Development Subcommittee, hearing on *EMP Threats to the U.S. Military and Civilian Infrastructure*, October 7, 1999.

[14] Lowell Wood, Statement before the House Military Research and Development Subcommittee, hearing on *EMP Threats to the U.S. Military and Civilian Infrastructure*, October 7, 1999; Jack Spencer, "America's Vulnerability to a Different Nuclear Threat: An Electromagnetic Pulse," *The Heritage Foundation Backgrounder*, No.1372, May 26, 2000, p.6.; and Carlo Kopp, "The Electromagnetic Bomb — A Weapon of Electrical Mass Destruction," *Air and Space Power*, 1993, [http://www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html].

[15] U.S. Congress, House Armed Services Committee, *Committee Hearing on Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack*, Jul 22, 2004 and on Jul 10, 2008.

EMP attack directed against the United States involving no violent destruction, nor instant death for large numbers of U.S. citizens, may not necessarily evoke massive nuclear retaliation by the U.S. military, where, for example, large numbers of innocent civilians of a nation with a rogue leader might be killed. Such a perceived lower risk of assured destruction by the United States, and widespread knowledge about the vulnerability of U.S. civilian and military computers to the effects of an EMP attack, could actually create a new incentive for other countries or terrorist groups to develop, or perhaps purchase, a nuclear capability.

Electromagnetic Pulse Overview

Electromagnetic energy, characterized as weapon potentially threatening to national security, can be created as a pulse traditionally by two methods: overhead nuclear burst and microwave emission. High-Altitude Electromagnetic Pulse (HEMP) is a near-instantaneous electromagnetic energy field that is produced in the atmosphere by the power and radiation of a nuclear explosion, and that is damaging to electronic equipment over a very wide area, depending on power of the nuclear device and altitude of the burst. High-Power Microwave (HPM) electromagnetic energy can be produced as a near-instantaneous pulse created through special electrical equipment that transforms battery power, or powerful chemical reaction or explosion, into intense microwaves that are also very damaging to electronics, but within a much smaller area. In addition, while HEMP weapons are large in scale and require a nuclear capability along with technology to launch high altitude missiles, HPM weapons are smaller in scale, and can involve a much lower level of technology that may be more easily within the capability of some extremist groups. HPM can cause damage to computers similar to HEMP, although the effects are limited to a much smaller area.

Description of High-Altitude Electromagnetic Pulse

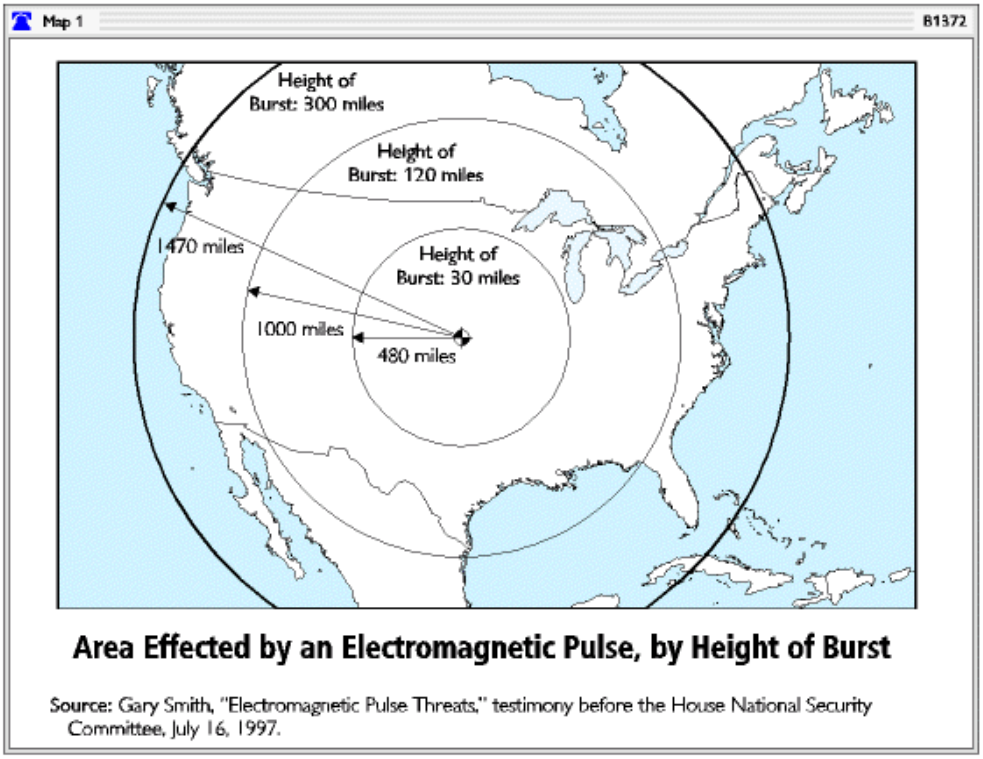
HEMP is produced when a nuclear weapon is detonated high above the Earth's surface, creating gamma-radiation that interacts with the atmosphere to create an instantaneous intense electromagnetic energy field that is harmless to people as it radiates outward, but which can overload computer circuitry with effects similar to, but causing damage much more swiftly than, a lightning strike.[16] The effects of HEMP became fully known to the United States in 1962 during a high-altitude nuclear test (code named "Starfish Prime") over the Pacific Ocean, when radio stations and electronic equipment were disrupted 800 miles away throughout parts of Hawaii. The HEMP effect can span thousands of miles, depending on the altitude and the design and power of the nuclear burst (a single device detonated at an appropriate altitude over Kansas reportedly could affect all of the continental United

---

[16] A nuclear explosion produces gamma rays, which interact with air molecules in a process called the Compton effect. Electrons are scattered at high energies, which ionizes the atmosphere, generating a powerful electrical field. This EMP effect is strongest at altitudes above 30,000m, and lasts so briefly that current cannot start flowing through a human body to cause harm to people. [http://www.physics.northwestern.edu/classes/2001Fall/Phyx135-2/19/emp.htm].

States)[17], and can be picked up by metallic conductors such as wires, or overhead power lines, acting as antennas that conduct the energy shockwave into the electronic systems of cars, airplanes, or communications equipment.

Figure 1. Estimated Area Affected by High-Altitude EMP



Source: Heritage Foundation, Jack Spencer, *America's Vulnerability to a Different Nuclear Threat: An Electromagnetic Pulse*, Backgrounder #1372, May 26, 2000, [http://www.heritage.org/Research/MissileDefense/bg1372.cfm].

A high altitude nuclear explosion (that creates HEMP) produces three major energy components that arrive in sequence, and which have measurably different effects that can be cumulatively damaging to electronic equipment. The first energy component is the initial energy shockwave, which lasts up to 1 microsecond, and is similar to extremely intense static electricity that can overload circuitry for every electronic device that is within line of sight of the burst. A secondary energy component then arrives, which has characteristics that are similar to a lightning strike. By itself, this second energy component might not be an issue for some critical infrastructure equipment, if anti-lightning protective measures are already in place. However, the rise time of the first component is so rapid and intense that it can destroy many protective measures, allowing the second component to further disrupt the electronic equipment.

The third energy component is a longer-lasting magnetohydrodynamic (MHD) signal, about 1 microsecond up to many seconds in duration. This late time pulse,

---

[17] The Federation of American Scientists, "Nuclear Weapons EMP Effects," [http://www.fas.org/nuke/intro/nuke/emp.htm].

or geomagnetic signal, causes an effect that is damaging primarily to long-lines electronic equipment.

There are two components to this third late time energy pulse, which experts call "blast" and "heave." The "blast" results from a distortion of the earth's magnetic field lines by the expanding, fully conductive fireball. The "heave" comes from the heating and ionization of a patch of atmosphere directly below the bomb that rises and, being conductive, also distorts the earth's magnetic field. Both of these are considered MHD signals and are termed "slow" because they depend on the dynamics of cloud or fireball expansion.

As the fireball expands, a localized magnetic effect builds up on the ground throughout the length of long transmission lines and then quickly collapses, producing the MHD "late-time" power surge, which can overload equipment connected to the power grid and telecommunications infrastructure. This late-time effect can add to the initial HEMP effect, and systems connected to long-lines power and communications systems may be further disrupted by the combined effects. Smaller isolated systems do not collect so much of this third energy component, and are usually disrupted only by the first energy component of HEMP.[18]

It is also important to note that this third, late-time pulse depends on the total energy of the nuclear detonation and therefore is usually associated only with larger yield nuclear weapons. However, the first energy pulse is a saturation-limited effect and is produced by all nuclear weapons, both small and large yield.

Description of High-Power Microwaves

Microwaves are characterized by electromagnetic energy with wavelengths as small as centimeters or millimeters, and can be used at moderate power levels for radio frequency communications or for radar.[19] High-power microwaves can be created as an instantaneous electromagnetic pulse, for example, when a powerful chemical detonation is transformed through a special coil device, called a flux compression generator, into an intense electromagnetic field.[20] Other methods can also be used to create a reusable HPM weapon, such as combining reactive chemicals or using powerful batteries and capacitors to create EMP. HPM energy can be

---

[18] The Federation of American Scientists, "Nuclear Weapons EMP Effects," [http://www.fas.org/nuke/intro/nuke/emp.htm], and Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Vol.1: Executive Report 2004, p.5.

[19] For example, microwaves with wavelengths about 5.7 cm long (C-band), or 20 cm long (L-band), or 3 cm long (X-band) are often used for radar or communications.

[20] A Flux Compression Generator consists of explosives packed inside a cylinder, all of which is contained within a cylindrical copper coil structure. The explosive is detonated from rear to front, causing the tube to flare in a wave that touches the copper coil, which produces a moving short circuit. This compresses the magnetic field and creates an electromagnetic pulse that is emitted from the front end, which is then directed by a special focusing antenna. [http://www.physics.northwestern.edu/classes/2001Fall/Phyx135-2/19/emp.htm].

focused using a specially-shaped antenna, or emitter, to produce effects similar to HEMP within a confined area, or over a limited distance. Unlike HEMP, however, HPM radiation uses shorter wave forms at higher-frequencies which make it highly effective against electronic equipment and more difficult to harden against. A mechanically simple, suitcase-sized device, using a chemical explosive and special focusing antenna, might theoretically produce a one-time, instantaneous HPM shockwave that could disrupt many computers within a 1-mile range.[21] Also, HPM energy at higher power levels (megawatts), and powered for a longer time interval, reportedly could cause physical harm to persons near the source emitter, or possibly in the path of a narrowly focused energy beam.[22]

Disruptive Effects of EMP

Studies related to the effects of electromagnetic energy used as weapons have been published infrequently, or remain classified.[23] Nevertheless, it is known that a powerful HEMP field as it radiates outward can interfere with radio frequency links and instantly produce damaging voltage and currents in electronic devices thousands of miles from the nuclear explosion. Effectiveness is increased if the electronic devices are connected to any other metal that could also act as an antenna. Because infrastructure computer systems are interconnected, a widespread HEMP effect could lead to possible long-term disruption of the power grid, fuel distribution, transportation systems, food and water supplies, and communications and equipment for hospitals and first responders, as well as military communications systems which utilize the civilian infrastructure.

An HPM weapon has a shorter possible range than HEMP, but it can induce currents large enough to melt circuitry, or it can cause equipment to gradually fail over a period of minutes, days, or even weeks. In 2001, a U.S. Comanche helicopter, flying in New York while performing a radar test involving HPM weapons, generated a low-level energy pulse that reportedly disrupted for two weeks the global positioning systems (GPS) being used to land commercial aircraft at a nearby airport in Albany, New York.[24]

A HEMP attack directed against the Unites States continent might involve a one-megaton nuclear warhead, or a smaller one, using a burst several hundred miles

---

[21] Dr. Robert C. Harney, Naval Postgraduate School, April 12, 2004, personal communication.

[22] Victorino Matus, "Dropping the E-bomb," *The Weekly Standard*, February 2, 2003, [http://theweeklystandard.com/Utilities/printer_preview.asp?idArticle=2209&R=9F0C225C3].

[23] William Graham, *Electromagnetic Pulse Threats to U.S. Military and Civilian Infrastructure*, hearing before the Military Research and Development Subcommittee, House Armed Services Committee, October 7, 1999; and Carlo Kopp, "The Electromagnetic Bomb — A Weapon of Electrical Mass Destruction," *Air and Space Power*, 1993, at [http://www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html].

[24] Kenneth R. Timmerman, "U.S. Threatened with EMP Attack," *Insight on the News*, May 28, 2001, [http://www.insightmag.com/news/2001/05/28/InvestigativeReport/U.Threatened.With.Emp.Attack-210973.shtml].

above the mid-western states to affect computers on both coasts.[25] However, creating a HEMP effect over an area 250 miles in diameter, an example size for a battlefield, might only require a rocket with a modest altitude and payload capability that could loft a relatively small nuclear device. If a medium or higher range missile with a nuclear payload were launched from the deck of a freighter at sea, the resulting HEMP could reportedly disable computers over a wide area of the coastal United States.

The disruptive effects of both HEMP and HPM reportedly diminish with distance, and electronic equipment that is turned off is only less likely to be damaged.[26] To produce maximum coverage for the HEMP effect, a nuclear device must explode very high in the atmosphere, too far away from the earth's surface to cause injury or damage directly from heat or blast. Also, HEMP produced by the nuclear explosion is instantaneous — too brief to start current flowing within a human body — so there is no effect on people. However, microwave energy weapons (HPM) are smaller-scale, are delivered at a closer range to the intended target, and can sometimes be emitted for a long duration. These characteristics of HPM can sometimes cause a painful burning sensation or other injury to a person directly in the path of the focused power beam, or can even be fatal if a person is too close to the microwave emitter.[27]

Both HEMP and HPM can permanently immobilize vehicles with modern electronic ignition and control systems. However, older electrical components, such as vacuum tubes and induction coils for spark ignition, are generally built more massively, and are more tolerant of EMP. As modern electronics shrink in size, circuitry is becoming increasingly tiny and more vulnerable to electromagnetic interference. Therefore, countries with infrastructure that relies on older technology may be less vulnerable to the disabling effects of HEMP or HPM than countries that rely on a higher level of technology.[28]

Recovery After Attack

The simultaneous loss of communications and power that would likely result from an EMP attack would also complicate the restoration of systems. Without

---

[25] [http://www.physics.northwestern.edu/classes/2001Fall/Phyx135-2/19/emp.htm].

[26] Experts may disagree on whether the damaging effects of HPM actually diminish following the familiar inverse-square-of-the-distance rule. Michael Abrams, "The Dawn of the E-Bomb," *IEEE Spectrum*, November 2003, [http://www.spectrum.ieee.org/WEBONLY/publicfeature/nov03/1103ebom.html]. Some experts state that the severity of HEMP effect depends largely on the bomb design, so a specially-designed low yield bomb may pose a larger HEMP threat than a high yield bomb. Lowell Wood, statement before the House Research and Development Subcommittee, hearing on *EMP Threats to the U.S. Military and Civilian Infrastructure*, October 7, 1999.

[27] Victorino Matus, "Dropping the E-bomb," *The Weekly Standard*, February 2, 2003, [http://theweeklystandard.com/Utilities/printer_preview.asp?idArticle=2209&R=9F0C225C3].

[28] Lowell Wood, statement before the House Research and Development Subcommittee, hearing on.*EMP Threats to the U.S. Military and Civilian Infrastructure*, October 7, 1999.

communications, it would be difficult to ascertain the nature and location of damage, or to order personnel out to make repairs. The estimated recovery times for various elements of the electrical system are provided in a list that appears on pages 50-51 of the 2008 Commission report.

The report states that the continuing business need to improve and expand the electric power system provides an opportunity to improve both the security and reliability of the entire system in an economically acceptable manner.[29] The Commission reported that the seriousness of loss of the electric power grid could be reduced through focused coordination between industry and government. The Commission recommended that the federal government, according to standards it determines, should validate proposed enhancements to protect systems against damage from EMP attack, and fund those security related elements.

Economic Damage Estimates after Attack on Washington, D.C., Region

In September 2007, the Sage Policy Group of Baltimore and Instant Access Networks (IAN) published a study of the potential economic impact of a HEMP attack on the Baltimore-Washington-Richmond area. The study focuses on the economic effects of EMP experienced by a region after a high-altitude EMP pulse generated by a nuclear device detonated between 30-80 miles above ground impacting an area at least 500 miles in radius. In these instances of high-altitude EMP, no one would feel the heat or blast but merely experience the effects of the disruption or damage to the electronic and power infrastructure. The Baltimore-Washington-Richmond area likely comprises only one-tenth of the economic loss that would occur for the total geographic area affected by a regional EMP event.

The report was presents a range of low, medium, and high estimates of economic damage, all within bounds accepted by a broad range of EMP experts. The methodology relied on assumptions about disruption and damage to the regional electrical power system, communications systems, system control and data acquisition (SCADA) devices, and other critical infrastructure that might occur as a result of an EMP, and on the time required to repair that damage and fully restore economic activity. These assumptions were used in combination to estimate the ultimate effects of an EMP on the region's economy. The cumulative effect of an EMP on critical infrastructure was assumed to be largely determined by effects on the electrical grid and communications systems. Cumulative damage was then determined by multiplying the remaining capacity of the electrical grid by the remaining capacity of communication systems under three scenarios. For example, under the high case, an EMP damages 50% of the capacity of the electric grid and 50% of the capacity of communication systems. The analysis assumed that the economy was then able to operate at only 25% of capacity (i.e., 50% multiplied by 50%).

---

[29] Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack; Critical National Infrastructures, Apr 2008, p.52.

The study concluded that an EMP attack affecting the Baltimore-Washington-Richmond region could result in economic output loss potentially exceeding $770 billion, or 7% of the nation's annual gross domestic product. Even under the most favorable assumptions, including both shielded and unshielded critical infrastructure, an EMP might still result in damage that would require one month of recovery and economic loss of $9 billion and $34 billion respectively.

Table 1. Estimates of Damage and Recovery Times After HEMP Attack on Washington, D.C., Regional Area

Infrastructure	Percentage of Capacity Damaged			Midpoint of Replacement Times (months)		
	Low Case	Mid Case	High Case	Low Case	Mid Case	High Case
Electric grid						
Transformers	10%	40%	70%	2.5	13.5	33.0
Other	30%	40%	50%	1.5	5.0	10.0
Communications systems						
Large	10%	20%	50%	4.0	18.0	27.0
Small	5%	20%	50%	2.0	12.0	17.0
SCADA						
All types	5%	20%	50%	1.5	5.0	10.0
Electronics						
Large	20%	45%	70%	4.0	12.0	17.0
Small	1%	2%	3%	1.5	5.0	10.0

Source: Instant Access Networks and Sage Policy Group, "Initial Economic Assessment of Electromagnetic Pulse (EMP) Impact upon the Baltimore-Washington-Richmond Region," September 10, 2007, Exhibit 2, p. 5, at [http://www.pti.org/docs-safety/EMPecon_9-07.pdf].

In the worst case, according to the study, not only is the damage from EMP widespread, but the duration of disrepair lasts for years. In such cases, there are numerous complicating factors that could slow the recovery process. The quantity of replacement equipment needed to restore the economy may quickly exhaust readily available supplies and, in extreme cases, existing manufacturing capacity. In such cases, the availability of skilled labor to replace and restore key infrastructure elements may also be in extraordinarily short supply. High-altitude EMP would also affect much larger parts of the region than the immediate Baltimore-Washington-Richmond area, further complicating recovery efforts. It is unlikely that restoration would occur in an orderly, linear fashion. More likely, restoration efforts would start slowly and gather speed as basic infrastructure is gradually brought on line.

Portable Data Centers and Hardening Against EMP

Electronic equipment may be made more resistant to EMP by surrounding it with protective metallic shielding, which routes damaging electromagnetic surges away from highly sensitive electrical components. This method, commonly known as Faraday cage protection, is often used to protect electronic equipment from a lightning strike. However, these devices must be constructed carefully. Any wires running into the protected area could act as antennae and conduct the electromagnetic shockwave into the equipment. These points of entry into a shielded area must be protected from EMP by using specially designed surge protectors, special wire termination procedures, screened isolated transformers, spark gaps, or other types of specially designed electrical filters.[30] Additionally, an EMP surge from a very powerful nuclear blast, possibly involving a 200 Kilovolts/meter electric field, could pass through some protective shielding.[31]

Microsoft, Sun Microsystems, and other vendors have recently marketed a new product commonly called a "Portable Data Center" (PDC) where computer equipment is placed on racks that are pre-grouped inside a modular room, which can be moved and connected to other portable computer room modules, as needed.[32] For example, a portable module can hold as many as 1,200 servers along with power supply and a cooling system. All this computer equipment fits into a box that can be placed inside a 40-foot standard freight shipping container, which can also be mounted on a truck for portability.[33] This new method for housing computers is intended to reduce the cost for computer facility installation.

However, additional features may also transform a PDC into an effective method for making U.S. computer equipment less vulnerable to EMP attack. For

---

[30] Electrical systems connected to any wire or line that can act as an antenna may be disrupted. [http://www.physics.northwestern.edu/classes/2001Fall/Phyx135-2/19/emp.htm]. Army Training Manual 5-692-2, April 15, 2001, "Maintenance of Mechanical and Electrical Equipment at Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities, *HEMP Protection Systems*, Chapter 27, [http://www.usace.army.mil/publications/armytm/tm5-692-2/chap27VOL-2.pdf].

[31] Recent Russian military writings claim that they have a Super-EMP weapon that can generate more than 200 KVs per meter, which is 4 times greater than the level of EMP hardening tested by the United States. Kilovolts per meter is the standard measure for describing the strength of an EMP field. In layman's terms, the statement that a Russian Super-EMP weapon could generate 200 kilovolts per meter means that a conductive object exposed to the EMP field will experience a surge of 200,000 volts for every meter of its length. So if the object is 2 meters long, it gets 400,000 volts. If 3 meters long, it gets 600,000 volts, and so on. Testimony from the EMP Commission before the House Armed Services Committee, Jul 10, 2008.

[32] Rich Miller, Microsoft Mulling Portable Data Centers, [http://www.datacenterknowledge.com/archives/2007/Apr/05/microsoft_mulling_portable_data_centers.html].

[33] Stephen Shankland, Rackable's portable data center goes on sale, CnetNews.com, Mar 26, 2007, [http://news.cnet.com/Rackables-portable-data-center-goes-on-sale/2100-1010_3-6170495.html].

example, Instant Access Networks (IAN), a specialized technology vendor, now offers a portable modular equipment room that reportedly can meet military specifications for EMP protection.[34] The IAN product uses welded metal enclosures of precise composition and thickness. A recently filed patent application involves a unique construction method to block different EMP frequencies and also reduce weight for easier portability. This type of portable module, built and tested according to strict specifications, could possibly be mass-produced and deployed as an effective way to protect existing and future U.S. computer systems from EMP attack.[35] For example, a single module placed at a remote critical location could possibly operate as an EMP-protected SCADA system, or multiple shielded modules could be connected together at a central headquarters location for a high-capacity protected computing.

DOD has also published Mil-Standard 188-125, which describes methods for protecting against High-Altitude Electromagnetic Pulse for ground-based command and control facilities.[36] However, not all military systems are currently hardened against EMP. In addition, some DOD systems rely on commercial facilities, such as communications satellites and ground-based stations, for support of military operations. Hardening most military systems, and mass-produced commercial equipment including PCs and communications equipment, against HEMP or HPM reportedly would add from 2% to 3% to the total cost, if the hardening is engineered into the original design. To retro-fit existing military electrical equipment with hardening would add about 3%-10% to the total cost.[37]

DOD Vulnerabilities and Research

In 2004, the EMP Commission held the collective the opinion that DOD had not engaged in any tabletop exercises and simulations that anticipate and EMP attack. In fact, an EMP commissioner observed that over the past 40 years, DOD has tended to "not introduce EMP attack into exercise scenarios or game scenarios because it tends to end the game, and that is not a good sign."[38]

In April, 2005, the Defense Science Board (DSB) Task Force on Nuclear Weapon Effects (NWE) Test, Evaluation and Simulation published a report for DOD describing current and emerging threat environments. This included a

---

[34] Instant Access Networks, LLC, provides a commercial off-the-shelf, portable data center that meets or exceeds military specifications for EMP protection. [http://www.safe9-1-1.com/].

[35] Charles Manto, et. al., Pending U.S. Patent number 20070105445, "System and Method for Providing Certifiable Electromagnetic Pulse and RFI Protection Through Mass-Produced Shielded Containers and Rooms", published May 10, 2007.

[36] MIL-STD-188-125-1, Apr 2005, [http://www.wbdg.org/ccb/FEDMIL/std188_125_1.pdf].

[37] Lowell Wood, statement before the House Research and Development Subcommittee, hearing on *EMP Threats to the U.S. Military and Civilian Infrastructure*, October 7, 1999. Personal communication with EMP Commission members, July 2008.

[38] Dr. Lowell Wood, testimony before the House Committee on Armed Services, H.A.S.C No. 108-37, July 22, 2004, p.23.

comprehensive evaluation of future DOD capabilities for successful operation in nuclear environments. The DSB findings were independent, "but are highly consistent with, the findings and recommendations of the Congressionally mandated Electromagnetic Pulse (EMP) Commission." The DSB findings include the following:

> Despite the reduction of the threat of strategic nuclear exchange, it is becoming more, not less, likely that U.S. forces will have to operate in a nuclear environment in regional operations. This is driven by the proliferation of nuclear weapon capabilities and the attractiveness of nuclear weapons as an offset to U.S. conventional superiority and as a counter to U.S. preemptive doctrine.
>
> ... factors that should make decision makers concerned about the survivability of critical warfighting elements in a nuclear environment. These include the shift to commercial-off-the-shelf (COTS) based electronics, aging of key systems, the growing reliance on historically "soft" C4ISR2 assets, the general neglect of nuclear hardening as a requirement, and the general neglect of nuclear environments as a factor in gaming and exercises. The bottom line is that commanders and planners cannot be assured that today's weapons platforms, command and control (C2), intelligence, surveillance and reconnaissance (ISR), and associated support systems will be available should a nuclear detonation occur.[39]

Underground testing of nuclear devices done in 1992 at the Nevada Test Site were designed to research protection techniques to harden military systems against HEMP effects resulting from a nuclear exchange.[40] The Limited Test Ban Treaty of 1963 prohibits nuclear explosions in the atmosphere, in space, and under water. Since then, testing to calibrate the effects of large-scale HEMP on the critical infrastructure has been restricted. The design of new simulators to help measure these effects would call for complex computations to represent the large number of possible interactions between components found in the circuit boards, network connections, wireless systems, hardware modules, and operating environments of modern electronic systems that support the critical infrastructure.

DOD research on pulsed-power HPM electromagnetic weapons is currently being done at Kirtland Air Force Base, in Albuquerque, New Mexico. Weapons now being developed by the U.S. military for electronic warfare can disrupt the trajectory of missiles while in flight, and can overpower or degrade enemy communications, telemetry, and circuitry. Other HPM weapons being tested by the military are portable and re-usable through battery-power, and many are effective when fired miles away from a target. These weapons can also be focused like a laser beam and tuned to an appropriate frequency in order to penetrate electronics that are heavily shielded against a nuclear attack. The deepest bunkers with the thickest concrete

---

[39] Report of the Defense Science Board Task Force on Nuclear Weapon Effects Test, Evaluation, and Simulation, April 2005, at [http://www.acq.osd.mil/dsb/reports/2005-04-NWE_Report%20_Final.pdf].

[40] Associated Press, "Experts Cite Electromagnetic Pulse as Terrorist Threat," *Las Vegas Review-Journal*, October 3, 2001.

walls reportedly are not safe from such a beam if they have even a single unprotected wire reaching the surface.[41]

Because instantaneous HPM energy can reflect off the ground and possibly affect piloted aircraft above, much testing currently involves HPM devices on Unmanned Aerial Vehicles (UAVs), and on the Air Force Conventional Air-Launched Cruise Missile system. By 2010, DOD reportedly will field several air-launched UAVs using disposable and reusable HPM weapons designed to disrupt enemy computers.[42]

Ground Wave Emergency Network

During the Cold War, the US Military designed an innovative communications system to relay emergency messages between strategic military areas in the continental United States, using signals that travel by means of low frequency ground waves — electromagnetic fields that hug the ground — rather than by radiating into the atmosphere. The Ground Wave Emergency Network, or GWEN system, was intended to allow continuous communications despite EMP disruptions. However, the hardware was reportedly transistor based, leaving the system with some level of vulnerability to EMP. In addition, the fixed locations of GWEN sites were known to adversaries, and thus vulnerable to direct attack.[43]

As the Cold War ended, the U.S. military took steps to reduce its nuclear arsenal and associated infrastructure.[44] After 1998, the USAF decommissioned GWEN assets and replaced the entire system with the Single Channel Anti-Jam Man-Portable (SCAMP) Terminal. SCAMP uses extremely high frequency (EHF) technology, is resistant to EMP, and offers more flexibility than GWEN because the equipment is lightweight, transportable, and interoperable with DOD satellite networks.[45]

EMP Capabilities of Other Nations

Reportedly, several potential U.S. adversaries, such as Russia or China, are now capable of launching a crippling HEMP strike against the United States with a

---

[41] Michael Abrams, The Dawn of the E-Bomb, *IEEE Spectrum Online*, November 2003, [http://www.spectrum.ieee.org/WEBONLY/publicfeature/nov03/1103ebom.html].

[42] David Fulghum and Douglas Barrie Farnboruogh, "Directed-Energy Weapon for UAV, cruise and air-to-ground missile payloads nears production," *Aviation Week & Space Technology*, July 26, 2004, p. 34.

[43] Rosalie Bertell, "Background on the HAARP Project," *Global Policy Forum*, November 5, 1996, [http://www.globalpolicy.org/socecon/envronmt/weapons.htm].

[44] Admiral Richard W. Mies, Commander in Chief, United States Strategic Command, statement before the Senate Armed Services Committee Strategic Subcommittee on Command Posture, July 11, 2001, p.11, [http://www.defenselink.mil/dodgc/lrs/-docs/test01-07-11Mies.rtf].

[45] Federation of American Scientists, *AN/PSC-11 Single Channel Anti-Jam Man-Portable (SCAMP)Terminal*, March 2000 [http://www.fas.org/spp/military/program/com/an-psc-11.htm].

nuclear-tipped ballistic missile, and other nations, such as North Korea, could possibly have the capability by 2015.[46] Other nations that could possibly develop a capability for HEMP operations over the next few years include United Kingdom, France, India, Israel, and Pakistan.

In 2005, Iran reportedly acquired several medium and intermediate-range ballistic missiles from North Korea, with a range of 2,500 miles.[47] In 2006, Iran tested several of their Shahab-3 nuclear-warhead-capable ballistic missiles, which were exploded in mid-flight. While these explosions could have been the result of a missile self-destruct mechanism, Iran has officially described the tests in 2006 as fully successful. It was noted by witnesses at a 2005 hearing of the Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology and Homeland Security, that this event could indicate that Iran may be practicing for the execution of an HEMP attack.[48] In July 2008, Iran test-launched several more long-range ballistic missiles. However, other observers caution that these and similar actions might simply be a scare tactic used by Iran, but without much substance.[49]

A discussion of asymmetric warfare and anti-satellite weapons, at a June 25, 2008, hearing by the House Armed Services Committee, included the possible example of the United States being targeted for attack by China using EMP.[50] According to a 1999 DOD report, China has been actively pursuing the development of electromagnetic pulse weapons, and has devoted significant resources to development of other electronic warfare systems and laser weapons. The report also noted that China's leaders view offensive counter space weapons and other space-based defense systems as part of inevitable scenarios for future warfare. The report noted that China could have as many as 60 ICBMs capable of striking the

---

[46] Michael Sirak, "U.S. vulnerable to EMP Attack," *Jane's Defence Weekly*, July 26, 2004, [http://www.janes.com/defence/news/jdw/jdw040726_1_n.shtml], and House Armed Services Committee, hearing on *Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack*, July 22, 2004.

[47] Alon Ben-David, *Iran Acquires Ballistic Missiles from DPRK*, Jane's Intelligence and Oversight, December 29, 2005.

[48] Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology and Homeland Security, March 8, 2005. Jane's Information Group, *Shahab break-ups suggest possible EMP trial* , May 1, 2005, Jane's Rockets and Missiles. Joseph Farah, *Iran plans to knock out U.S. with 1 nuclear bomb*, April 25, 2005, WorldNewsDaily.com, [http://wnd.com/news/article.asp?ARTICLE_ID=43956].

[49] Officials in Iran have also reported that in March 2006, they successfully tested their "Fajr-3" long-range missile, which they claim has a range of 2000 miles, and which is invisible to radar. However, other intelligence sources reportedly argue that the "Fajr-3" is merely an upgraded artillery shell with a very short range. *"Iran Claims Test of Fajr-3 Missile 'Invisible' to Radar, Interceptors"*, April 3, 2006, MissileThreat.com, [http://www.missilethreat.com/news/200604030826.html].

[50] Testimony of James Shinn, Assistant Secretary of Defense, Security Developments in China, hearing before the House Armed Services Committee, June 25, 2008.

United States by 2010. Also, China may replace 20 of its current ICBMs with a longer-range missile by the end of this decade, or sooner.[51]

Vladimir Lukin, the former Soviet Ambassador to the United States, and former Chairman of the International Affairs Committee for the Russian Parliament, reportedly has stated that Russia currently has a capability to create a HEMP effect over the United States.[52] During 1962, the then Soviet Union conducted a series of atmospheric nuclear tests and observed HEMP effects that included surge protector burnouts, power supply breakdowns, and damage to overhead and underground buried cables at distances of 600 kilometers. Since then, Russia has reportedly made extensive preparations to protect their infrastructure against HEMP by hardening both civilian and military electronic equipment, and by providing continuous training for personnel operating these protected systems.[53] Other sources have reportedly stated that Russia may also have some of the leading physicists in the world currently doing research on electronic warfare weapons and electromagnetic pulse effects.[54]

Policy Analysis

Preparedness

What is the United States doing to protect critical infrastructure systems against the threat of electromagnetic pulse? What is the appropriate response from the United States to a nuclear HEMP attack, where there may be widespread damage to electronics, but relatively little, or possibly no loss of life as a direct result? How could the United States determine which nation or group launched a HEMP attack? After experiencing a HEMP effect, the United States may retain its capability to use strategic weapons for nuclear retaliation, but will the U.S. industrial base and critical infrastructure be crippled or incapable of supporting a sustained military campaign? During such time, would the United States be capable of a making an effective

---

[51] FY04 Report to Congress on PRC Military Power, Annual Report on The Military Power of the People's Republic of China, [http://www.defenselink.mil/pubs/d20040528PRC.pdf].

[52] The statement was reportedly made on April 30, 1999, to a U.S. Congressional delegation that traveled to Vienna to meet with officials from the Russian Duma to discuss a framework for a peaceful solution of the then crisis in Kosovo. Hearing before the Military Research and Development Subcommittee of the Committee on Armed Services House of Representatives, October 7, 1999, [http://commdocs.house.gov/committees/security/-has280010.000/has280010_0.HTM].

[53] Lowell Wood, statement before the House Research and Development Subcommittee, hearing on *EMP Threats to the U.S. Military and Civilian Infrastructure*, October 7, 1999.

[54] Barry Crane, a physicist and former F-4 pilot now working at the Institute for Defense Analysis, has visited Russia's top electromagnetic pulse laboratories and design bureaus, and has stated that many Russian electromagnetic pulse specialists may also be now working on contract in China. Kenneth R. Timmerman, May 28, 2001, "U.S. Threatened with EMP Attack," *Insight on the News*, [http://www.insightmag.com/news/2001/05/28/InvestigativeReport/U.Threatened.With.Emp.Attack-210973.shtml].

response should other nations chose to make military advances in other parts of the world?

A large percentage of U.S. military communications during Operation Iraqi Freedom was reportedly carried over commercial satellites, and much military administrative information is currently routed through equipment that comprises the civilian Internet.[55] Many commercial communications satellites, particularly those in low earth orbit, reportedly may degrade or cease to function shortly after a high altitude nuclear explosion.[56] Many commercial satellite control stations on the ground may also degrade after an EMP attack. However, some observers believe that possible HEMP and HPM vulnerabilities of military information systems are outweighed by the benefits gained through access to innovative technology and increased communications flexibility that come from using state-of-the-art electronics and from maintaining connections to the civilian Internet and satellite systems.

The effects of large-scale HEMP have been studied over several years by the Defense Atomic Support Agency, the Defense Nuclear Agency, and the Defense Special Weapons Agency, and are currently being studied by the Defense Threat Reduction Agency (DTRA). However, the application of the results of these studies has been uneven across military weapons and communications systems. Some analysts argue that U.S. strategic military systems (intercontinental ballistic missiles and long-range bombers) may have strong protection against HEMP, while many other U.S. weapons systems used for the battlefield have less protection, and that this is undoubtedly known to our potential adversaries.[57]

Some analysts reportedly state that limited testing has shown modern commercial equipment may be surprisingly resistant to the effects of electromagnetic pulse, and some military systems using commercial equipment have been retrofitted to increase resistance to EMP.[58] However, there is disagreement among observers about whether the procedures used by the U.S. military to test EMP survivability may

---

[55] Jefferson Morris, "DISA Chief Outlines Wartime Successes," *Federal Computer Week*, June 6, 2003; and "GAO: DOD Needs New Approach to Buying Bandwidth," *Aerospace Daily*, December 12, 2003.

[56] U.S. Congress, House Armed Services Committee, *Hearing on Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack*, July 22, 2004.

[57] Because of the very specialized nature, strategic weapons use essentially no commercial equipment. However, DOD increasingly uses commercial equipment in other tactical weapons. Stanley Jakubiak and Lowell Wood, statements before the House Military Research and Development Subcommittee, hearing on *EMP Threats to the U.S. Military and Civilian Infrastructure*, October 7, 1999.

[58] Stanley Jakubiak, statement before the House Military Research and Development Subcommittee, Hearing on *EMP Threats to the U.S. Military and Civilian Infrastructure*, October 7, 1999.

have been flawed, leading to erroneous conclusions about the effects of electromagnetic pulse on commercial electronics.[59]

Department of Homeland Security

As part of its risk analysis mission, the Department of Homeland Security (DHS) has developed a set of 15 National Planning Scenarios, which depict a diverse set of high-consequence threat scenarios of both potential terrorist attacks and natural disasters. These 15 scenarios are designed to focus contingency planning for homeland security preparedness work, at all levels of government, and with the private sector. These scenarios form the basis for coordinated federal planning, training, exercises, and grant investments needed to prepare for emergencies of all types.[60] However, EMP Commission members stated at the 2008 HASC hearing that they have been unable to convince DHS to add EMP attack to its list of National Planning Scenarios.[61]

Nuclear Incentive

A single nuclear device exploded at an appropriate altitude above the continental United States could possibly affect our industrial capacity, economic stability, and military effectiveness. Does knowledge of this vulnerability, combined with the proliferation of nuclear technology, provide a new incentive for potential adversaries to develop or acquire a nuclear weapons capability? Will countries now view the development and acquisition of nuclear weapons, even a small arsenal, as a strategy for cyber warfare?

During the Cold War, a HEMP attack was viewed as the first step of a nuclear exchange involving many warheads, but the threat of mutually assured destruction provided a lasting deterrent. Today, the proliferation of nuclear technology makes the threat of HEMP attack more difficult to assess. Would the leader of a rogue state be motivated to use a small nuclear arsenal to launch a crippling HEMP strike against the United States, with no resulting fatalities, if it believed the U.S. likely would not retaliate with a nuclear salvo, destroying thousands, or millions of innocent people? Would a HEMP strike over a disputed area during a regional conflict be seen as a way to defeat the communications links and network centric capability of the U.S.

---

[59] Lowell Wood, statement before the House Military Research and Development Subcommittee, hearing on *EMP Threats to the U.S. Military and Civilian Infrastructure*, October 7, 1999; and Jack Spencer, "America's Vulnerability to a Different Nuclear Threat: An Electromagnetic Pulse," *The Heritage Foundation Backgrounder*, No.1372, May 26, 2000, p.6.; and Carlo Kopp, "The Electromagnetic Bomb — A Weapon of Electrical Mass Destruction," *Air and Space Power* 1993, [http://www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html].

[60] Department of Homeland Security, National Preparedness Guidelines, September 2007, Fig. B-1, p.31, [http://www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf].

[61] ,William Graham, testimony before the House Armed Services Committee, Jul 10, 2008.

military, and gain battlefield advantage from an existing supply of smaller nuclear warheads?[62]

Terrorists

A smaller-scale HPM weapon requires a relatively simple design, and can be built using electrical materials and chemical explosives that are easy to obtain. It is estimated that a limited-range suitcase-sized HPM weapon could be constructed for much less than $2,000, and is within the capability of almost any nation, and perhaps many terrorist organizations.[63] In 2001, DOD recruited a scientist to create two small HPM weapons for testing using only commercially available electrical components, such as ordinary spark plugs and coils. One device was developed that could be broken down into two parcels so it could be shipped by regular mail, for example, from one terrorist to another. The second HPM device was constructed to fit inside a small vehicle.[64] Currently, HPM devices, including suitcase-sized devices powerful enough to jam or destroy electronic facilities, are reportedly also available through catalog sales from commercial vendors.[65]

It is difficult to assess the threat of a terrorist organization possibly using a smaller-scale HPM weapon against the United States critical infrastructure. It could be argued that an HPM bomb by itself, may not be attractive to terrorists, because its smaller explosion would not be violent enough, and the visible effect would not be as dramatic as a larger, conventional bomb. Observers have reported that the leadership of some terrorist organizations may increasingly become aware of the growing advantages from an EMP attack launched against U.S. critical information systems. In addition, the use of a new weapon directed at U.S. information systems would attract widespread media attention, and may motivate other rival groups to follow along a new pathway.[66]

---

[62] Jack Spencer, "America's Vulnerability to a Different Nuclear Threat: An Electromagnetic Pulse," *The Heritage Foundation Backgrounder*, No.1372, May 26, 2000, p.3.

[63] Some experts may disagree about whether most terrorist organizations are capable of building an inexpensive HPM weapon powered by a flux-compression generator. Michael Abrams, "The Dawn of the E-Bomb," *IEEE Spectrum Online*, November 2003, [http://www.spectrum.ieee.org/WEBONLY/publicfeature/nov03/1103ebom.html], and Carlo Kopp, "The Electromagnetic Bomb — A Weapon of Electrical Mass Destruction," *Air and Space Power*, 1993, [http://www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html].

[64] Kenneth R. Timmerman, "U.S. Threatened with EMP Attack," *Insight on the News*, May 28, 2001, [http://www.insightmag.com/news/2001/05/28/InvestigativeReport/U.Threatened.With.Emp.Attack-210973.shtml].

[65] Personal communication with EMP Commission. Diehl BGT Defense, High Power Microwaves, [http://www.diehl-bgt-defence.de/index.php?id=547&L=1].

[66] Jerrold M. Post, Kevin G. Ruby, and Eric D. Shaw, "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism," *Terrorism and Political Violence*, vol. 12, no. 2 (summer 2000), pp.97-122.

Human Rights

HEMP and HPM energy weapons primarily damage electronic systems, with little or no direct effect on humans, however, these effects may be difficult to limit or control. As HEMP or HPM energy fields instantly spread outward, they may also affect nearby hospital equipment or personal medical devices, such as pace-makers, or other parts of the surrounding civilian infrastructure. For this reason, some international human rights organizations may object to the development or testing of HEMP or HPM weapons.

Legislative Activity

P.L. 110-181, The National Defense Authorization Act for Fiscal Year 2008, requires the Department of Homeland Security to coordinate efforts with the Commission for work related to electromagnetic pulse attack on electricity infrastructure, and protection against such attack. Funding by provided by the Department of Defense to the Commission for preparation and submission of the final report is limited to $5,600,000. The deadline for the submission of the final report of the Commission has been extended to November 30, 2008.

CRS Products

CRS Report RL32114. *Botnets, Computer Attack, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*.

CRS Report RL32411. *Network Centric Warfare: Background and Oversight Issues for Congress*.

CRS Report RS21528. *Terrorist "Dirty Bombs": A Brief Primer*.

CRS Report IB92099. *Nuclear Weapons: Comprehensive Test Ban Treaty*.