Backgrounder

Published by The Heritage Foundation

No. 2199
October 20, 2008

Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe

Jena Baker McNeill and Richard Weitz, Ph.D.

A major threat to America has been largely ignored by those who could prevent it. An electromagnetic pulse (EMP) attack could wreak havoc on the nation's electronic systems—shutting down power grids, sources, and supply mechanisms. An EMP attack on the United States could irreparably cripple the country. It could simultaneously inflict large-scale damage and critically limit our recovery abilities. Congress and the new Administration must recognize the significance of the EMP threat and take the necessary steps to protect against it.

Systems Gone Haywire

An EMP is a high-intensity burst of electromagnetic energy caused by the rapid acceleration of charged particles. In an attack, these particles interact and send electrical systems into chaos in three ways: First, the electromagnetic shock disrupts electronics, such as sensors, communications systems, protective systems, computers, and other similar devices. The second component has a slightly smaller range and is similar in effect to lightning. Although protective measures have long been established for lightning strikes, the potential for damage to critical infrastructure from this component exists because it rapidly follows and compounds the first component. The final component is slower than the previous two, but has a longer duration. It is a pulse that flows through electricity transmission lines—damaging distribution centers and fusing power lines. The combination of the three components can easily cause irreversible damage to many electronic systems.[1]

Talking Points

- A major threat to America has been largely ignored by those who could prevent it—the U.S. Congress and the President. An electromagnetic pulse (EMP) attack on the United States could irreparably cripple the country, wreaking havoc on the nation's electronic systems—shutting down power grids, sources, and supply mechanisms.
- Congress and the new Administration cannot continue to ignore the EMP threat. Next steps include research on the nature of the EMP threat, planning for such an attack within the National Planning Scenarios, the deployment of a comprehensive missile defense system, and the development of a National Recovery Plan.
- America's very existence depends on the U.S. government's ability to understand the very real possibility and the devastating consequences of an EMP attack—and to take the actions necessary to prevent them.

This paper, in its entirety, can be found at:
www.heritage.org/Research/HomelandSecurity/bg2199.cfm

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies of the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

An EMP attack on the United States could materialize in two forms: nuclear and non-nuclear. The most devastating form, and most difficult to achieve, is an EMP that results from a nuclear weapon. This form destroys any "unhardened" electronic equipment and electric power system—which means virtually any civilian infrastructure in the United States. The pulse occurs when a nuclear weapon explodes above the visual horizon line at an altitude between 40 and 400 kilometers. The detonation of the nuclear warhead releases photons in the form of gamma radiation and x-rays. These energetic particles scatter in every direction away from the blast. Many of the particles descend and interact with the magnetic field lines of the Earth, where they become trapped. The trapped electrons then create an oscillating electric current within the field, which rapidly produces a large electromagnetic field in the form of a pulse. Once the pulse reaches electronic equipment, it negatively interacts with them and either disables, damages, or destroys them. An EMP generated by a nuclear weapon could affect all critical infrastructures that depend on electricity and electronics within the vicinity of the nuclear warhead blast radius. A nuclear weapon with a burst height of approximately 100 kilometers could expose objects located within an area 725 miles in diameter to the effects of EMP.[2]

A non-nuclear, or improvised, EMP is a radio-frequency (rather than gamma or x-ray frequency) weapon. While easier to conceal and not requiring a missile, a non-nuclear EMP must be detonated close to the target and does not produce as much damage as the nuclear version, affecting largely localized areas.[3] But such a weapon could be harnessed as an "E-Bomb" (electromagnetic bomb), a stand-alone weapon that is easier to hide and maneuver. It is difficult to estimate the exact damage of an improvised attack, but in 1993 EMP testing by the U.S. military shut down engine controls 300 meters away at a contractor site.[4] Not large-scale by any means, but damaging enough to cause concern.

It was not until the United States began high-altitude testing of nuclear weapons over the Pacific in the early 1960s that the potentially devastating effects of EMP on even distant ground targets attracted widespread attention within the U.S. defense community. In the 1962 Starfish Prime test, during which a nuclear weapon was detonated 400 kilometers (250 miles) above Johnston Island in the Pacific, electrical equipment more than 1,400 kilometers (870 miles) away in Hawaii was affected. Street lights, alarms, circuit breakers, and communications equipment all showed signs of distortions and damage.[5]

In 1997 and 1999, the House National Security Committee and the House Military Research and Development Subcommittee held hearings on the potential threats to civilian systems in America from an EMP attack. Congress subsequently established the Commission to Assess the Threat to the United States from an Electromagnetic Pulse (EMP) Attack, also known as the Graham Commission after its chairman, William Graham (former science advisor to President Ronald Reagan). The Commission issued a report in 2004 that evaluated the threat to the U.S. from an EMP attack, assessed vulnerabilities in both military and civilian systems, and offered recommendations for overcoming these weaknesses. The Commission recommended hard-

1. John S. Foster, Jr., *et al.*, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," The Graham Commission, Vol. 1 (2004), p. 3, at *http://www.globalsecurity.org/wmd/library/congress/2004_r/04-07-22emp.pdf* (September 13, 2008).
2. *Independent Working Group on Missile Defense, the Space Relationship, and the Twenty-First Century, 2007 Report*, The Institute for Foreign Policy Analysis, 2007, p. 10, at *http://missilethreat.com/repository/doclib/IWGreport.pdf* (October 9, 2008).
3. Statement of William R. Graham, Ph.D., "Electromagnetic Weapons and their Effects on Electronics Systems," 1999, at *http://www.globalsecurity.org/wmd/library/congress/1999_h/99-10-07graham.htm* (October 8, 2008).
4. Major Scott W. Merkle, USAF, "Non-Nuclear EMP: Automating the Military May Prove a Real Threat," *Military Intelligence Professional Bulletin*, January–March 1997, at *http://www.fas.org/irp/agency/army/mipb/1997-1/merkle.htm* (October 8, 2008).
5. William R. Graham, "Electromagnetic Pulse Attack: Statement of Dr. William R. Graham," testimony before the House Armed Services Committee, U.S. House of Representatives, July 10, 2008, at *http://www.empcommission.org/docs/GRAHAMtestimony10JULY2008.pdf* (October 8, 2008).

ening key power nodes as well as storing spares of essential but hard-to-build components of the U.S. electric grid and other critical infrastructure for communications, finance, and emergency public services.[6] Congress held hearings the same year to evaluate the Commission's recommendations, but little tangible progress followed.[7] The Commission was re-established in 2006 to continue monitoring the EMP threat.

A few select sites have been hardened against an EMP attack since the threat was identified. Air Force One, the airplane that carries the U.S. President, is designed to withstand an EMP attack. During the Cold War, the U.S. military hardened its most important military systems, such as U.S. nuclear weapons systems, against EMP threats. These efforts have decreased since the end of the Cold War, despite the continued vulnerability of these systems. Presently, most efforts to counter the EMP threat are focused on initiatives to stop the proliferation of nuclear weapons and ballistic missiles. These efforts include programs like the Proliferation Security Initiative, the Cooperative Threat Reduction Program, and the Global Initiative to Combat Nuclear Terrorism.

Comprehensive threat assessment and scenario planning for EMP attacks remain underdeveloped. This inaction is in the face of warnings, such as the one in the 2006 Quadrennial Defense Review (QDR) which stated clearly that the "expanded reliance on sophisticated electronic technologies by the United States, its allies and partners increases their vulnerability to the destructive effects of electromagnetic pulse (EMP)."[8] Yet, the Department of Defense has not implemented the QDR's proposed EMP Action Plan.[9] Meanwhile, the Department of Homeland Security (DHS) has focused on other urgent threats, such as from conventional explosive devices or chlorine bombs, concluding that EMP is simply not a large enough threat for its attention. Even the National Infrastructure Protection Plan (NIPP), the plan dedicated to ensuring that U.S. critical infrastructure is protected from terrorist attack, does not directly address the EMP threat. Congress has recently reassumed its leadership role on EMP by holding hearings on the issue in July 2008, but its ability to compel executive branch action in this area is limited.

While many non-federal homeland security authorities in many U.S. states express concern about an EMP attack, a comprehensive survey found that state-based emergency responders and National Guard units have done little to prepare for such an incident.[10] Alaska, perhaps because of its relative isolation from most federal emergency response assets and the state's vulnerability due to its reliance on satellite-based communications, is a notable exception. In May 2007, the Alaskan state government announced it would include EMP when it next revises its emergency response plan. The state's homeland security officials plan to address the vulnerability of the state's electric and telecommunications infrastructures as well as related integration, implementation, and survivability issues.[11] Alaska's efforts are considerable in comparison to other states; most have not even touched the issue. Limited state preparedness for an EMP attack is especially dangerous given the inability of the U.S. government, itself mostly unprepared for an EMP strike, to render much if any immediate assistance.

6. Foster, Jr., *et al.*, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," pp. 17–23.
7. Clay Wilson, "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments," Congressional Research Service *Report for Congress*, March 26, 2008, at *http://www.fas.org/sgp/crs/natsec/RL32544.pdf* (July 3, 2008).
8. U.S. Department of Defense, *Quadrennial Defense Review Report*, February 6, 2006, p. 33, at *http://www.defenselink.mil/qdr/report/Report20060203.pdf* (October 8, 2008).
9. Wilson, "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave Devices," p. 2.
10. Institute of the North and The Claremont Institute, "Project Report: Missile Defense and the Role of the States," 2007, at *http://www.missilethreat.com/repository/docLib/20070306_MissileDefenseandtheStates.pdf* (June 30, 2008).
11. Press Release, "Alaska to Revise Emergency Response Plan to Include Preparation for EMP Attack," Institute of the North, May 29, 2007, at *http://www.missilethreat.com/repository/doclib/20070614_SERC.pdf* (October 8, 2008).

Americans remain gravely ill prepared for an EMP attack. In fact, the average U.S. city has only three days worth of food and health care provisions.[12] Most Americans do not have enough batteries to keep flashlights working for any period of time, much less generator capabilities. And many of the country's most vulnerable citizens rely on the electricity grid for medical equipment, such as dialysis machines. Even standard medication will be difficult or impossible to come by if EMP disables pharmacies and transportation networks.

A Weapon of Mass Disruption

EMP has been dubbed a "weapon of mass disruption" because of its ability to devastate its target by disrupting electronic infrastructure. The August 2003 Northeast Blackout that affected Ohio, New York, Maryland, Pennsylvania, Michigan, and parts of Canada demonstrated the potential effects of a wide-area EMP attack. During that incident, more than 200 power plants, including several nuclear plants, were shut down as a result of the electricity cutoff. Loss of water pressure led local authorities to advise affected communities to boil water before drinking due to contamination from the failure of sewage systems. Many backup generators proved unable to manage the crisis.

The day of the blackout brought massive traffic jams and gridlock when people tried to drive home without the aid of traffic lights. Additional transportation problems arose when railways, airlines, gas stations, and oil refineries also halted operations. Phone lines were overwhelmed due to the high volume of calls, while many radio and television stations went off the air. Overall, the blackout—which lasted only one day—cost $7 billion to $10 billion in spoiled food, lost production, overtime wages, and other related expenses inflicted on more than one-seventh of the U.S. population.[13]

In the case of an EMP attack, depending on whether it is nuclear or improvised, the damage could easily prove more severe. An EMP detonation could affect car and truck engines, aircraft ignition systems, hospital equipment, pacemakers, communications systems, and electrical appliances. Road and rail signaling, industrial control applications, and other electronic systems are all susceptible to EMP. Electromagnetic energy on a radio frequency will travel through any conductive matter with which it comes into contact—from electrical wires to telephone wires, even water mains—which can spread the effects to areas far beyond ground zero.

A successful EMP attack could result in airplanes literally falling from the sky; vehicles could stop functioning, and water, sewer, and electrical networks could all fail—all at once.[14] Food would rot, health care would be reduced to its most rudimentary level, and there would not be any transportation. Rule of law would become impossible to sustain; police departments would be overwhelmed.

Communication abilities would be limited, preventing federal, state, and local governments from communicating with one another—severely limiting abilities to shift needed resources around the country. During the 2003 blackout, some communications systems remained intact. Cars and aircraft were not directly affected and rapidly resumed operation after the electrical system recovered a few days later. In an EMP attack, however, the damage to power lines, supervisory control and data acquisition (SCADA) control systems (for utility systems infrastructure), and commercial computers would very likely be *permanent* due to fused power lines and lost data—which would require replacing the entire electric system in the affected area. One estimate warns that the likely costs from the detonation of an EMP weapon over the Washington, D.C., metropolitan area could exceed $770 billion.[15] Millions

12. Graham, "Electromagnetic Pulse Attack," p. 2.
13. CNN, "Major Power Outage Hits New York, Other Large Cities," August 14, 2003, at *http://www.cnn.com/2003/US/08/14/power.outage* (October 8, 2008). See also The Electricity Consumers Resource Council, "The Economic Impacts of the August 2003 Blackout," February 9, 2004, pp. 1–3, at *http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf* (October 8, 2008).
14. Marshall A. Hanson, "Ultimate Weapon: A High-Energy Electromagnetic Pulse Could Cause Mass Destruction to America's Infrastructure," *The Officer*, November 1, 2006, p. 19.

of Americans could suffer death or injury, and social chaos could ensue.

Besides the domestic consequences of an EMP attack, it would also be difficult for the U.S. to organize a coherent retaliatory strike against the aggressor. America's armed forces may simply be unprepared for an attack, or our national devastation could prove too distracting. Furthermore, it may be too difficult to rapidly determine the perpetrator of the attack, for instance, if a compact E-Bomb were smuggled into the U.S. If a nuclear warhead is detonated in orbit, there is a strong potential for substantial damage to U.S. and other satellites as well as any spacecraft in use at the time of the explosion. The military applications of such satellites are critical for defense systems that rely on GPS guidance, such as ballistic missiles and many conventional military strike weapons. The adverse impact on U.S. space-based communications, early-warning assets, fire-control systems, overhead sensors and imagery, and geospatial intelligence would be substantial as well.

Near-term recovery could prove impossible because of America's dependence on extensive transportation networks and other electricity-powered infrastructures. America's infrastructure is highly interconnected, as was demonstrated during the blackout. A problem in one part of the country can translate into problems across the United States, contributing immensely to lives lost and property destroyed during an EMP attack.

Potential U.S. Adversaries Have the Knowledge—and the Capability

The range of actors that might attempt an EMP attack against the United States is obviously—and distressingly—large and includes conventional military regimes, rogue states with limited conventional military capabilities, and terrorist groups that seek to inflict catastrophic damage on America. Both Russia and China have dabbled in EMP technology for decades.

There is evidence that suggests that certain Russian nuclear weapons have already been optimized to generate enhanced EMP effects.[16] Just this year, Russian scientists claimed to have developed a compact apparatus that can fit on a dining table. The electromagnetic pulse associated with this device could amount to billions of watts of power in a single platform.[17] Analysts have also identified Chinese military writings that discuss using EMP weapons in international conflicts.[18]

For countries less dependent on modern technologies and electronics, including both rogue states like Iran and North Korea as well as stateless terrorist groups, EMP provides a potential way to attack the United States through asymmetric means. EMPs could be used to circumvent America's superior conventional military power while reducing vulnerability to retaliation in kind. It would certainly not be impossible for a terrorist organization, especially if state-sponsored, to acquire or construct an unsophisticated ballistic missile (non-working Scuds are reportedly available on the open market for $100,000) and use it in an EMP attack against America.[19] Such a missile could be launched from a freighter in international waters and detonated in the atmosphere over the United States without warning.

The materials used to build non-nuclear EMP weapons can be easily acquired or manufactured by moderately developed terrorist groups with even limited financial resources. Although the potential impact is less, an improvised EMP could still inflict major damage. The construction of a nuclear weapon is much more difficult and requires a good understanding of physics, electrical engineering,

15. James G. Zumwalt, "Not a Movie Made for T.V." *The Washington Times*, October 2, 2007, p. A16.
16. Dr. Mark Schneider, *The Emerging EMP Threat to the United States* (Fairfax, Virginia: National Institute Press, 2007), p. 4, at *http://www.nipp.org/Adobe/EMP%20Paper%20Final%20November07.pdf* (October 8, 2008).
17. Pravda.ru, "Russia to Create Electromagnetic Superweapon," *Pravda.ru*, April 9, 2008, at *http://english.pravda.ru/science/tech/04-09-2008/106296-electromagnetic_super_weapon-0* (October 8, 2008).
18. Schneider, *The Emerging EMP Threat to the United States,* pp. 6–9.
19. Senator Jon Kyl, "Unready for this Attack," *The Washington Post*, April 16, 2005, p. A19, at *http://www.washingtonpost.com/wp-dyn/articles/A57774-2005Apr15.html* (October 8, 2008).

and explosives; but these terror groups are actively seeking to gain this knowledge, and rogue states could see opportunity in collaborating with these groups to accelerate the process.

The Time for Action Is Now

The U.S. cannot continue to ignore the EMP threat. While some progress has been made in hardening potential U.S. targets against attack, including critical military and government systems, the vast majority of electrical systems are unshielded and unprotected, especially in the civilian sector. If properly shielded, electrical devices and systems can generally survive even the strongest EMPs.[20] Congress and the new Administration must:

- **Perform More Research on the Threat.** Further research is needed in order to ensure that America can respond to the EMP threat appropriately without wasting government resources on flimsy or useless security measures. Although there are numerous methods to harness EMPs capable of affecting electronic systems, there is still a theoretical limit to what damage they can produce in terms of both geographic size and intensity.

  Some EMP weapons release just enough energy to disable small electrical devices while others can destroy all the electronic devices and systems within a city block. Altitude plays a major role in whether an EMP attack will be successful; lower heights typically expose a smaller surface area to EMP damage. Some systems are simply more vulnerable to EMP attack than others, such as devices plugged into power grids and commercial computer equipment. The U.S. government must gain knowledge of the attributes and capabilities of EMP and understand the amount of money, time, and effort that will be required for meaningful prevention. EMP research should also include actions by Congress to simulate the effects of an EMP attack on Washington and other high-value targets and re-examine the Graham Report recommendations.

- **Build a Comprehensive Missile Defense System.** The most likely method of EMP attack would be a ballistic missile armed with a nuclear warhead. Building a comprehensive missile defense system would allow the U.S. to intercept and destroy a missile bound for the United States. The mere implementation of such a system would go a long way to prevent an attack by dissuading those who wish to carry out such actions and sending a clear message that the U.S. takes this threat seriously.

  Those opposed to missile defense in Congress and elsewhere have attempted to paint such an endeavor as a waste of resources that does nothing to further American security. *33 Minutes: Protecting America in the New Missile Age, A Reader*, a collection of essays by pre-eminent defense scholars, emphasized the need for such measures, and recent missile testing by Iran demonstrates that other countries are actively involved in developing missile programs—which could be used against the U.S.[21]

- **Incorporate EMP Attacks into National Planning Scenarios.** The National Planning Scenarios are 15 all-hazards planning scenarios used by federal, state, and local officials in disaster response exercises. The exercises can determine capabilities and needs and address problems before a disaster instead of after the fact. Given an EMP attack's unique nature and its ability to paralyze the U.S., individualized preparation is necessary. EMP must be added to the list.

- **Develop a National Recovery Plan.** The U.S. must identify the key power grid and telecommunications infrastructure that is critical to preserving our nation's core capabilities and create a National Recovery Plan. This risk-based approach recognizes that certain infrastructure is key to recovery after an EMP attack. By taking measures to protect this infrastructure, we can lessen the recovery time from an attack.

20. United States Army, "Electromagnetic Pulse (EMP) Protection," Grounding and Bonding in Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities TM 5-690, February 15, 2002, at *http://www.usace.army.mil/publications/armytm/tm5-690/c-5.pdf* (October 8, 2008).
21. *33 Minutes: Protecting America in the New Missile Age, A Reader* (Washington, D.C.: The Heritage Foundation, 2008), forthcoming.

According to the National Fire Protection Association's (NFPA) "Standard on Disaster/Emergency Management and Business Continuity Programs," a private company should prepare to function without electricity for a short period in order to maintain uninterrupted operations.[22] While this time period will certainly vary by industry, encouraging the private sector to prepare in this manner and to develop company recovery plans will allow the government to focus on bringing key infrastructure back online. The private sector can move toward this goal by investing in more adequate infrastructure now.

A Threat too Big to Be Ignored

Although many in Congress and the White House tend to ignore the EMP threat, America's potential adversaries will not. To these adversaries, EMP technology represents the opportunity to inflict—with relative ease—catastrophic and lasting damage on the United States that could threaten our very existence. Preventing such an attack depends on the U.S. government's ability to understand the very real chance and the devastating consequences of an EMP attack—and to take the actions necessary to prevent them.

—Jena Baker McNeill is Policy Analyst for Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation and Richard Weitz, Ph.D., is Senior Fellow and Director of Program Management at the Hudson Institute.

22. National Fire Protection Association, "Standard on Disaster/Emergency Management and Business Continuity Programs," 2007, at *http://www.nfpa.org/assets/files//PDF/CodesStandards/1600-2007.pdf* (October 8, 2008).