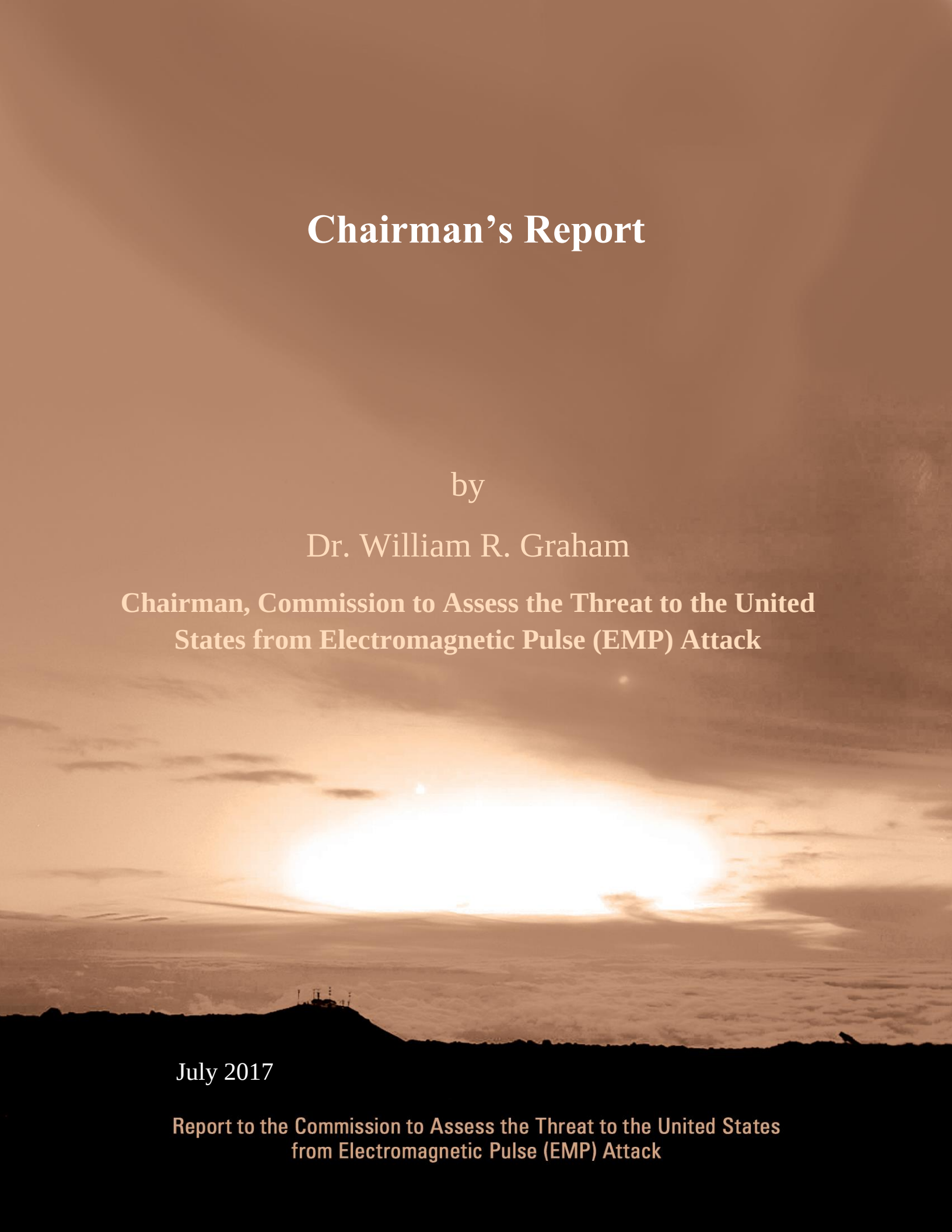


Chairman's Report

by

Dr. William R. Graham

Chairman, Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

July 2017

Report to the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

REPORT TO THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE (EMP) ATTACK

Chairman's Report

by
Dr. William R. Graham, Chairman
Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

July 2017

The cover photo depicts Fishbowl Starfish Prime at 0 to 15 seconds from Maui Station in July 1962, courtesy of Los Alamos National Laboratory.

This report was produced to support the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. The Commission was established by Congress in the FY2001 National Defense Authorization Act, Title XIV, and was continued per the FY2016 National Defense Authorization Act, Section 1089.

The Commission completed its information-gathering in June 2017. The amended report was cleared for open publication by the Department of Defense Office of Prepublication and Security Review on July 27, 2018.

This report is unclassified and cleared for public release.

Acknowledgements

The author would like to thank Dr. Peter Pry for conducting the research and preparing most of the material in the section on EMP Attack and Combined-Arms Cyber Warfare.

Acronyms and Abbreviations

AQAP	Al Qaeda in The Arabian Peninsula
BMEWS	Ballistic Missile Early Warning System
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
EEI	Edison Electric Institute
EHV	extra high voltage
EMP	electromagnetic pulse
EPRI	Electric Power Research Institute
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
FERC	Federal Energy Regulatory Commission
FOBS	Fractional Orbital Bombardment System
GAO	Government Accountability Office
GMD	geomagnetic disturbances
HEMP	high-altitude electromagnetic pulse
JAEIC	Joint Atomic Energy Intelligence Committee
MNA	Mehr News Agency
NATO	North Atlantic Treaty Organization
NERC	North American Electric Reliability Corporation
PLA	People's Liberation Army
PRC	People's Republic of China
RFW	radio frequency weapon
RMA	revolution in military affairs
SCADA	supervisory control and data acquisition
SHSGA	Homeland Security and Government Affairs Committee

Table of Contents

Abstract 4

Background and Recommendations 6

- Immediately 9
- Mid-Term 10
- Long-Term 10

The EMP Commission History 12

EMP Attack and Combined-Arms Cyber Warfare 17

- Russia 18
- China 19
- Iran 21
- North Korea 23

Non-Nuclear EMP Weapons 26

Physical Attacks on Power Grids 27

Cyber-Attacks on Power Grids 28

Misinformation about EMP and the North Korean Threat 31

North Korea Nuclear EMP Attack: An Existential Threat 35

The Fragility of Complex Systems 37

Regulatory Failures by the U.S. Federal Energy Regulatory Commission, the North American Energy Regulatory Corporation, and the Electric Power Industry 39

The 2014 Intelligence Report 43

Conclusions 44

Abstract

The United States critical national infrastructure faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, and natural EMP from a solar superstorm. During the Cold War, the U.S. was primarily concerned about a high altitude nuclear-weapon generated EMP attack as a tactic by which the Soviet Union could suppress the U.S. national command authority and U.S. strategic forces' ability to respond to a nuclear attack, and thus destroy the U.S. deterrence value of assured nuclear retaliation. Within the last decade, newly-nuclear armed adversaries, including North Korea, have been developing the ability to deploy and threatening to carry out an EMP attack against the U.S. Such an attack would give North Korea and countries that have only a small number of nuclear weapons the ability to cause widespread, long-lasting damage to critical national infrastructures of the United States itself as a viable country and to the survival of a majority of its population.

While during the Cold War major efforts were undertaken by the Department of Defense (DoD) to assure that the U.S. national command authority and U.S. strategic forces could survive and operate after an EMP attack, no major efforts were then thought necessary by the national leadership to protect critical national infrastructures, provided that nuclear deterrence was successful. With the development of small nuclear arsenals and long-range missiles by small, hostile, potentially irrational countries, including North Korea, the threat of a nuclear EMP attack against the U.S. becomes one of the few ways that such a country could inflict devastating damage to the U.S. Therefore, it is critical that the U.S. national leadership address the EMP threat as an immediate, existential issue, and give a high priority to assuring the necessary leadership is engaged and the necessary steps are taken to protect the country from EMP. Otherwise, foreign adversaries may reasonably consider such an attack as one that can gravely damage the U.S. by striking at its technological Achilles' heel, without having to overcome the U.S. military.

Protecting and defending the national electric grid and other critical infrastructures from EMP can be accomplished at reasonable cost and minimal disruption to the present systems that comprise our critical infrastructure; all commensurate with Trump Administration plans to repair and improve U.S. infrastructures, increase their reliability, and strengthen our homeland defense and military capability.

I highly commend President Trump's new executive order "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" signed on May 11, 2017. I strongly recommend that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection, since all-out cyber warfare as planned by Russia, China, North Korea, and Iran includes nuclear EMP attack, and integrating EMP and cyber-protection will be both the least expensive and most technically sound approach. Protecting against nuclear EMP will also protect

against natural EMP from solar super storms. The United States should not remain in our current state of existential vulnerability to well-known natural and manmade EMP threats. Such vulnerability invites attack.

The single most important action that must be taken immediately to advance national strength and survivability is:

> **Establish an Executive Agent, with the authority, accountability, and resources, to manage U.S. national infrastructure protection and defense against the existential EMP threat.** Current institutional authorities and responsibilities—government, industry, regulatory agencies—are fragmented, incomplete, inexperienced, under-resourced, and unable to protect and defend against foreign hostile EMP threats and solar super-storms.

Background and Recommendations

WE CAN PREVENT AN EMP CATASTROPHE

The United States—and modern electric power- and electronic-based civilization more generally—face present and continuing existential threats from naturally occurring and manmade EMP and Combined-Arms Cyber Warfare on our military and on our critical national infrastructures.

Protecting the national electric grid and other critical infrastructures from the most severe of these threats—nuclear EMP attack—could be done in a manner that protects against other electromagnetic threats, including geomagnetic storms. Extensively tested, performance-proven technologies for EMP hardening have been developed and implemented by the DoD to protect critical military systems for over 50 years, and can be ***affordably*** adapted to protect electric grids and other critical infrastructures, at a remarkably low cost relative to that of an EMP catastrophe. Such hardening should be applied in a prioritized manner, with the most important and difficult to replace assets being addressed first. For example, the nuclear reactors providing electric power in the U.S., along with their spent fuel storage facilities, should be given high priority.

President Trump's plan to repair and strengthen our national infrastructure, cyber security, homeland defense, and military capability presents an excellent opportunity to include measures for EMP protection that would mitigate the existential threats from solar super-storms *and* Combined-Arms Cyber Warfare.

A plausible long term nationwide blackout of the electric power grid and grid-dependent critical infrastructures—e.g., communications, public health, transportation, food-and-water supply—could disable most of our critical supply chains, leaving the U.S. in its condition prior to the advent of electric power in the 19th Century, when the national population was less than 60 million, but today without many of the past skills and assets necessary for our population to survive in those conditions. The result could be the death of a large fraction of the American people through the effects of starvation, disease, and societal collapse.

While national planning and preparation for such events could help mitigate the damage, outside the DoD few such actions are currently underway or even being contemplated. The United States, as the most technologically advanced nation in the world, is also the society most dependent upon electricity and electronics for survival and well-being. An extended national-scale blackout and loss of most electricity-dependent infrastructure could be induced by any of several threats:

Solar super-storms, like the 1859 Carrington Event, generate natural EMP that could blackout electric grids and other life-sustaining critical infrastructures over remarkably wide areas, putting

at risk the lives of many millions. Recurrence of another Carrington Event is inevitable. The National Aeronautics and Space Administration (NASA) reports the Earth was nearly impacted by a solar super-storm on July 23, 2012. NASA estimates the likelihood of such an event to be 12 percent per decade, virtually guaranteeing Earth will be impacted by a solar super-storm within the lifetimes of our grandchildren—and perhaps ourselves as well.

Nuclear EMP attack can be conducted with only a single nuclear weapon detonated at high altitude (a few dozen to several hundred kilometers) delivered either by satellite, a wide variety of long- and short-range missiles including some cruise and anti-ship missiles, a jet doing a zoom-climb, or even a high-altitude balloon. Some modes of such attacks could be executed relatively anonymously, thereby impairing attribution and therefore deterrence. Russia and China now have the capability to conduct a nuclear EMP attack against the U.S., and if not already at hand North Korea will soon have that capability. All have practiced or described contingency plans to do so. Terrorists or other less-sophisticated actors also might mount a nuclear EMP attack if they have access to a suitable nuclear explosive. Missile or other weapon delivery for EMP attack does not require a nuclear weapon re-entry system or accurate missile guidance.

Sabotage of the national grid by damaging extra-high-voltage (EHV) transformers using rifles, explosives, or non-nuclear EMP weapons could produce protracted and widespread blackouts by attacking less than a dozen major grid substations, according to the public statements of a past Chairman of the U.S. Federal Energy Regulatory Commission (FERC). At least one substantive rehearsal of such an attack may have already taken place: the sophisticated, damaging attack of the Metcalf electric substation in the San Francisco Bay Area.

Combined-Arms Cyber Warfare, as planned by Russia, China, North Korea, and Iran may use combinations of cyber-, sabotage-, and ultimately nuclear EMP-attack to impair the United States quickly and decisively by blacking-out large portions of its electric grid and other critical infrastructures. Foreign adversaries may also consider nuclear EMP attack as the ultimate cyber "denial of service" weapon, one which can gravely damage the U.S. by striking at its technological Achilles' heel, without having to engage the U.S. military. The synergism of such combined-arms is described in the military doctrines of all these potential adversaries as the greatest Revolution in Military Affairs (RMA) in history—one which anticipates rendering obsolete many, if not all, traditional instruments of military power.

While I highly commend President Trump's new Executive Order "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" signed on May 11, 2017, I strongly recommend that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection, since all-out cyber warfare as planned by Russia, China, North Korea, and Iran includes nuclear EMP attack. However, current institutional arrangements for protecting and improving the reliability of the electric grids and other critical infrastructures through the U.S. FERC and the North American Electric Reliability

Corporation (NERC) are not designed to address major national security threats to the electric power grids and other national critical infrastructures. Using the U.S. FERC and NERC to achieve this level of national security is beyond the purpose for which those organizations were created and has proven to be fundamentally unworkable; new institutional arrangements are needed to advance preparedness to survive EMP and related threats to our critical national infrastructures.

I continue to recommend that U.S. critical national infrastructures be protected from EMP as outlined in our unclassified reports provided in 2004 and 2008, and elsewhere. Additional recommendations are provided in the present report. The single most important action that must be taken urgently to advance national strength and survivability is:

> **Establish an Executive Agent—a Cabinet Secretary designated by the President—with the authority, accountability, and resources, to manage U.S. national infrastructure protection and defense against EMP and the other existential threats described above.** Current institutional authorities and responsibilities—government, industry, regulatory agencies—are fragmented, incomplete, and unable to protect and defend against foreign hostile EMP threats and solar super-storms.

Additionally:

I encourage the President to work with Congressional leaders to stand-up a Joint Presidential-Congressional Commission, with its members charged with supporting the Nation's leadership and providing expertise, experience, and oversight to achieve, on an accelerated basis, the protection of critical national infrastructures. The U.S. FERC and NERC have for nearly a decade been unable or unwilling to implement the EMP Commission's recommendations. A Presidential-Congressional Commission on Critical Infrastructure Protection could engage the Free World's preeminent experts on EMP and Combined-Arms Cyber Warfare to serve the entire Government in a manner akin to the Atomic Energy Commission of the 1947-74 period, advising the Administration regarding actions to attain most quickly and most cost-effectively the protection essential to long-term national survival and wellbeing. The United States should not remain in our current state of fatal vulnerability to well-known natural and man-made threats.

I recommend, given the proximity and enormity of the threat from EMP and Combined-Arms Cyber Warfare, the President exercise leadership to implement immediate, mid-term, and long-term steps to deter and defeat this existential threat.

Immediately

I recommend that the President declare that EMP or cyber-attacks that blackout or threaten to blackout the national electric grid constitute the use of weapons of mass destruction that justify preemptive and retaliatory responses by the United States using all possible means, including nuclear weapons. Some potential adversaries have the capability to produce a protracted nationwide blackout induced by EMP and other elements of Combined-Arms Cyber Warfare. A Defense Science Board study *Resilient Military Systems and the Advanced Cyber Threat* (January 2013) equates an all-out cyber-attack on the United States with the consequences of a nuclear attack, and concludes that a nuclear response is justified to deter or retaliate for cyber warfare that threatens the life of the nation: "While the manifestations of a nuclear and cyber-attack are very different, in the end, the existential impact to the United States is the same."

I recommend that the President issue an Executive Order titled "Protecting the United States from Electromagnetic Pulse (EMP) Attack." Among many other provisions to protect the nation from EMP on an emergency basis, the Executive Order would instantly mobilize a much needed "whole of government solution" to the EMP and combined-arms cyber threat: "All U.S. Government Departments, Agencies, Offices, Councils, Boards, Commissions and other U.S. Government entities…shall take full and complete account of the EMP threat in forming policies and plans to protect United States critical infrastructures…" Protecting the electric grid and other critical infrastructures from the worst threat—nuclear EMP attack—can, if carried out in a system-wide, integrated approach, help mitigate all lesser threats, including natural EMP, man-made non-nuclear EMP, and cyber-attack, physical sabotage, and severe solar and terrestrial weather.

I recommend that the President direct the Secretary of Defense to include a Limited Nuclear Option for EMP attack among the U.S. nuclear strike plans, and immediately assure targeting and fusing capabilities for some of the nuclear forces to implement a nuclear EMP attack capability.

[redacted] If either or both of these satellites are nuclear-armed, they should be intercepted and destroyed over a broad ocean area where an EMP resulting from possible salvage-fusing will do the least damage.

I recommend that the President direct the Secretary of Defense to post Aegis ships in the Gulf of Mexico and near the east and west coasts, and the Secretary in turn should direct them to be prepared to intercept missiles from freighters, submarines, or other platforms that might launch a nuclear EMP attack on the United States. Ground-based U.S. National Missile Defenses (NMD) are primarily located in Alaska and California and oriented for a missile attack coming at

the U.S. from the north, and are not deployed to intercept a missile attack launched near the U.S. coasts or from the south.

I recommend that the President direct the Secretary of Homeland Security to harden the FirstNet emergency communications system against EMP.

I recommend that the President initiate Training, evaluating, and "Red Teaming" efforts to prepare the U.S., and in the event of an EMP attack to respond, and periodically report the results of these efforts and the state or national readiness to the Congress.

Mid-Term

I recommend that the President direct the Secretary of Defense to deploy Aegis-ashore missile interceptors along the Gulf of Mexico coast to fill the gap in U.S. missile defenses. [redacted]

I recommend that the President direct the Secretary of Defense to develop a space-surveillance program to determine if any satellites orbited over the United States are nuclear-armed, and develop space-interception capabilities to defend against nuclear-armed satellites that might make an EMP or other attack.

I recommend that the President direct the Nuclear Regulatory Commission to launch a crash program to harden the active nuclear power reactors and all spent fuel storage facilities against nuclear EMP attack. Even if the reactors and storage facilities survive an initial EMP attack, they currently are not able to restart generating power if there is no electric power available on its grid, and they typically only have enough emergency power to cool reactors and spent fuel facilities for several days, after which they would "go Fukushima," spreading radioactivity over adjacent areas.

Long-Term

The Commission recommends that the President through his Executive Agent protect elements of the national electric grid, the keystone critical infrastructure upon which all other critical infrastructures depend. Priority should be given to elements that are difficult and time-consuming to replace. Such elements can be protected from EMP at very low cost relative to the cost of an EMP catastrophe, and paid for without federal dollars by a slight increase in electric rates.

I recommend that a similar approach be taken to key elements of the national telecommunications infrastructure and other national critical infrastructures.

Progress Made by the Department of Defense

The statute re-establishing the EMP Commission directs it to evaluate and report on:

(1) The vulnerability of electric-dependent military systems in the United States to a manmade or natural EMP event, giving special attention to the progress made by the Department of Defense, other Government departments and agencies of the United States, and entities of the private sector in taking steps to protect such systems from such an event.

The DoD has been the primary federally funded organization to analyze, develop models, simulate, develop hardening technology, and using resources provided to it, to strengthen U.S. national security. The DoD has in the past sponsored much excellent work in these areas; however, even though it is the most knowledgeable federal agency in the field of EMP, it has:

1. Failed to transfer much of its technical capabilities and accomplishments to other agencies of the federal government;
2. Failed to use its knowledge to assist and critique activities of other federal agencies, including the intelligence community;
3. Failed to declassify EMP environment and effects data and predictions that, while known to U.S. adversaries, are not available to the U.S. public, U.S. infrastructure organizations, and U.S. professional societies that develop specifications and standards for protecting critical national infrastructure;
4. Failed to obtain the complete archive of Russian nuclear weapons effects data when offered for sale to the U.S. at modest cost in 1996;
5. Failed to inform the Congress and the public of the present and continuing existential EMP threat to the nation; and
6. Failed to develop and pursue plans to protect the U.S. from EMP threats.

Overall, for more than a decade, the DoD has been derelict in its duties to lead the country in providing for national defense and security from EMP attack. This dereliction of duty should not be allowed by the leadership of the Administration and the Congress to continue.

I recommend the development and deployment of enhanced-EMP nuclear weapons and other means to deter adversary attack on the United States. Enhanced-EMP nuclear weapons, called by the Russians Super-EMP weapons, can be developed without nuclear testing.

I recommend strengthening U.S. ballistic missile defense, deploying it to protect the U.S. from attack from near-by oceans as well as from longer distances, including by development and deployment of space-based defenses.

The EMP Commission History

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack was first established by Congress in the FY2001 Floyd D. Spence National Defense Authorization Act, Title XIV, following 5 years of classified and unclassified hearings by Congress to ascertain if Russia, China, rogue states or terrorists had plans and capabilities to make an EMP attack. The final impetus to establish the EMP Commission was provided in April 1999, during the bombing of former Yugoslavia by the North Atlantic Treaty Organization (NATO), when a congressional delegation meeting in Vienna to discuss the Balkans crisis with senior members of the Russian Duma were threatened with a "hypothetical" nuclear EMP attack against the United States.

Under the Congressional EMP Commission's original statutory charter, Public Law 106-398, Title XIV, Section 1402 Duties of Commission:

> ***(a) Review of EMP Threat. The Commission shall assess:***
>
> *(1) the nature and magnitude of potential high-altitude EMP threats to the United States from all potentially hostile states or non-state actors that have or could acquire nuclear weapons and ballistic missiles enabling them to perform a high-altitude EMP attack against the United States within the next 15 years;*
>
> *(2) the vulnerability of United States military and especially civilian systems to an EMP attack, giving special attention to vulnerability of the civilian infrastructure as a matter of emergency preparedness;*
>
> *(3) the capability of the United States to repair and recover from damage inflicted on United States military and civilian systems by an EMP attack; and*
>
> *(4) the feasibility and cost of hardening select military and civilian systems against EMP attack.*
>
> *(b) Recommendation. The Commission shall recommend any steps it believes should be taken by the United States to better protect its military and civilian systems from EMP attack.*

Between 2001 and 2008, the Congressional EMP Commission produced several reports addressing the EMP threat to U.S. military systems and making recommendations. The EMP Commission produced two unclassified reports addressing EMP threats to critical national infrastructures:

Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume I: Executive Report (2004)

Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures (2008)

The above unclassified reports on civilian critical infrastructures addressed EMP threats to:

- infrastructure commonalities, including Supervisory Control And Data Acquisition (SCADA) systems,
- electric power, identified as the "keystone critical infrastructure" upon which all others depend,
- telecommunications,
- banking and finance,
- petroleum and natural gas,
- transportation,
- food,
- water,
- emergency services,
- space systems, and
- government.

The EMP Commission *Executive Report* summarized the problem as below:

Several potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated EMP. A determined adversary can achieve an EMP attack capability without having a high level of sophistication.

EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences. EMP will cover the wide geographic region within line of sight to the nuclear weapon. It has the capability to produce significant damage to critical infrastructures and thus to the very fabric of U.S. society, as well as to the ability of the United States and Western nations to project influence and military power.

The common element that can produce such an impact from EMP is primarily electronics, so pervasive in all aspects of our society and military, coupled through critical infrastructures. Our vulnerability is increasing daily as our use of and dependence on electronics continues to grow. The impact of EMP is asymmetric in relation to potential protagonists who are not as dependent on modern electronics.

The current vulnerability of our critical infrastructures can both invite and reward attack if not corrected. Correction is feasible and well within the Nation's means and resources to accomplish.

The Congressional EMP Commission 2004 *Executive Summary* stated in "Overview: EMP Is Capable of Causing Catastrophe for The Nation" several additional salient points about the nuclear EMP threat:

- *The recovery of any one of the key national infrastructures is dependent on the recovery of others. The longer the outage, the more problematic and uncertain the recovery will be. It is possible for the functional outages to become mutually reinforcing until at some point the degradation of infrastructure could have irreversible effects on the country's ability to support its population.*
- *EMP effects from nuclear bursts are not new threats to our nation…What is different now is that some potential sources of EMP threats are difficult to deter—they can be terrorist groups that have no state identity, have only one or a few weapons, and are motivated to attack the U.S. without regard for their own safety.*
- *Rogue states, such as North Korea and Iran, may also be developing the capability to pose an EMP threat to the United States, and may also be unpredictable and difficult to deter.*
- *Certain types of relatively low-yield nuclear weapons can be employed to generate potentially catastrophic EMP effects over wide geographic areas, and designs for variants of such weapons may have been illicitly trafficked for a quarter-century.*
- *China and Russia have considered limited nuclear attack options that, unlike their Cold War plans, employ EMP as the primary or sole means of attack.*
- *Another key difference from the past is that the U.S. has developed more than most other nations as a modern society heavily dependent on electronics, telecommunications, energy, information networks, and a rich set of financial and transportation systems that leverage modern technology.*
- *Therefore, terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or military base, they may obtain the greatest political-military utility from one or a few such weapons by using them—or threatening their use—in an EMP attack.*

The Congressional EMP Commission 2008 report *Critical National Infrastructures* made over 100 recommendations to protect the civilian critical infrastructures from nuclear EMP attack and other hazards. The EMP Commission endorsed an "all hazards" strategy as the most cost-effective approach to protecting the critical infrastructures, wherever possible using measures that would safeguard against multiple threats—including nuclear EMP, natural EMP or geomagnetic disturbance (GMD) from solar storms, intentional and accidental electromagnetic interference, cyber-attack, sabotage, and severe weather.

While the Congressional EMP Commission accurately described nuclear EMP attack as an existential threat to the United States, the thrust of the Commission's 2004 and 2008 reports was to recommend how to protect the nation cost-effectively, noting that protection is possible "and well within the Nation's means and resources to accomplish."

Congressional efforts to re-authorize the EMP Commission became more urgent because of misleading and inaccurate reports that are impeding implementation of the EMP Commission recommendations and are making the nation more vulnerable. For example:

- The NERC and the Edison Electric Institute (EEI) in 2012 and subsequently published a series of reports underestimating EMP threats from nuclear attack and from solar storms. These resulted in approval by the U.S. FERC of an inadequate natural EMP and GMD Standard for protecting electric grids, and impeded initiatives by several States to protect their grids from EMP.
- The Joint Atomic Energy Intelligence Committee in 2014 published a report on the EMP threat that is factually inaccurate and deeply flawed analytically, and has impeded implementation of EMP Commission recommendations.
- In 2016, the Electric Power Research Institute (EPRI), which is funded by the electric power industry, published an erroneous report that significantly underestimates the nuclear E3 EMP threat to electric grids. EPRI and others have used the report to lobby against Federal and State initiatives to protect the electric grid against nuclear EMP attack.
- In 2016, a report by the U.S. Government Accountability Office (GAO) concluded, "[U.S. Department of Homeland Security] DHS and [U.S. Department of Energy] DOE, in conjunction with industry, have not established a coordinated approach to identifying and implementing key risk management activities to address EMP risks." Congressional hearings subsequently confirmed that little or nothing has been done to implement EMP Commission recommendations to protect the electric grid.

Moreover, since the EMP Commission terminated in 2008, growing geopolitical instability, increased risk of war in the Middle East, Asia, and Europe, increasing threats from global terrorism, and increased awareness of natural EMP threats from the Sun—all have heightened congressional concerns about dangers to the electric grid from EMP and other threats. For example:

- North Korea in 2012 and 2016, amidst threats to annihilate the United States and a rapidly advancing nuclear missile program, orbited two satellites in polar orbits that cross over the U.S. on trajectories consistent with practice or preparation for a surprise nuclear EMP attack.
- On June 9, 2014, Al Qaeda in the Arabian Peninsula sabotaged the Yemen electric grid, inducing a temporary nationwide blackout of 19 cities and 24 million people. It is the first time in history that a terror attack has blacked-out an entire nation.

- On March 31, 2015, Turkey experienced a temporary nationwide blackout, allegedly from a cyber-attack by Iran, later denied by the Turkish government. On December 23, 2015, Western Ukraine was blacked-out temporarily by a cyber-attack from Russia. One of these is the first time in history that a large-scale blackout has been induced by cyber-attack.
- On July 23, 2012, the Earth was narrowly missed by a large coronal mass ejection from the Sun that NASA assessed could have caused a protracted worldwide blackout with potentially catastrophic consequences. NASA estimates the likelihood of a potentially catastrophic worldwide natural EMP event from a solar super-storm is 12 percent per decade.

In response to these events and others, Congress re-established the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack in the FY2016 National Defense Authorization Act, Section 1089. The renewed EMP Commission has a broader agenda, to assess threats to the U.S. military and civilian critical infrastructures from nuclear EMP, non-nuclear EMP weapons, cyber-attack, sabotage, and solar storms:

(d) Expanded PURPOSE. —Section 1401(b) of the Commission charter (114 Stat. 1654A–345) is amended by inserting before the period at the end the following: ", from non-nuclear EMP weapons, from natural EMP generated by geomagnetic storms, and from proposed uses in the military doctrines of potential adversaries of using EMP weapons in combination with other attack vectors."

(e) DUTIES OF COMMISSION. —*Section 1402 of the Commission charter (114 Stat. 1654A–346) is amended to read as follows:*

SEC. 1402. **DUTIES OF COMMISSION**.

The Commission shall assess the following:

(1) The vulnerability of electric-dependent military systems in the United States to a manmade or natural EMP event, giving special attention to the progress made by the Department of Defense, other Government departments and agencies of the United States, and entities of the private sector in taking steps to protect such systems from such an event.

(2) The evolving current and future threat from state and non-state actors of a manmade EMP attack employing nuclear or non-nuclear weapons.

(3) New technologies, operational procedures, and contingency planning that can protect electronics and military systems from the effects of a manmade or natural EMP event.

(4) Among the States, if State grids are protected against manmade or natural EMP, which States should receive highest priority for protecting critical defense assets.

(5) The degree to which vulnerabilities of critical infrastructure systems create cascading vulnerabilities for military systems.

EMP Attack and Combined-Arms Cyber Warfare

Nuclear EMP attack is part of the military doctrines, plans and exercises of Russia, China, North Korea, and Iran for a revolutionary new way of warfare against military forces and civilian critical infrastructures by cyber, sabotage, and EMP. This new way of warfare is called many things by many nations. In Russia, China, and Iran it is called Sixth Generation Warfare, Non-Contact Warfare, Electronic Warfare, Total Information Warfare, and Cyber Warfare. Some U.S. analysts—the very small number paying attention—call it Cybergeddon, Blackout War, or Combined-Arms Cyber Warfare.[1]

Significantly, EMP attack entails detonating a nuclear weapon at such high altitude that no blast or other prompt effects injurious to humans are delivered other than possible eye burn to those looking near the burst point. Since EMP immediately damages only electrical and electronics components and systems, potential adversaries do not appear to regard nuclear EMP attack as an act of nuclear warfare.

Potential adversaries understand that millions could die from the long-term collateral effects of EMP and cyber-attacks that cause protracted black-out of national electric grids and other life-sustaining critical infrastructures. At least some regard this relatively easy, potentially anonymous, method of inflicting mass destruction as an attractive feature of what they describe as a Revolution in Military Affairs.

Ignorance of the military doctrines of potential adversaries and a failure of U.S. strategic imagination, as noted in military writings of potentially hostile powers, is setting America up for an EMP Pearl Harbor.[2] Russia, China, North Korea and Iran appear to regard nuclear EMP attack as the ultimate weapon in an all-out cyber operation aimed at defeating U.S. and allied military forces on the battlefield and in a theater of operations. They also see EMP and Combined-Arms Cyber Warfare as a means of defeating entire nations by blacking-out their electric grids and other critical infrastructures for longer periods of time than technologically developed societies, including the U.S., can tolerate without major disruption and loss of life.[3]

---

1 While many analysts are paying attention to cyber warfare, narrowly defined as the use of computer viruses and hacking and other such techniques, relatively few conceive of "cyber warfare" as potential adversaries do— as Combined-Arms Cyber Warfare entailing coordinated use of computer viruses etc., sabotage and kinetic attack, non-nuclear and nuclear EMP weapons. Dr. Peter Vincent Pry, *Blackout Wars* (Task Force on National and Homeland Security, 2015), Chapter II "The Blackout War".

2 For Example: Zhang Shouqi and Sun Xuegui, "Be Vigilant Against 'Pearl Harbor' Incident in The Information Age" Jiefangjun Bao (Official newspaper of the PRC People's Liberation Army, May 14, 1996).

3 Ambassador R. James Woolsey, "Heading Toward An EMP Catastrophe" Statement for the Record before the Senate Homeland Security and Governmental Affairs Committee, July 22, 2015.

Russia

For example, Russian General Vladimir Slipchenko in his military textbook *Non-Contact Wars* describes the combined use of cyber viruses and hacking, physical attacks, non-nuclear EMP weapons, and ultimately nuclear EMP attack against electric grids and critical infrastructures as a new way of warfare that is the greatest Revolution in Military Affairs in history. Like Nazi Germany's Blitzkrieg ("Lightning War") Strategy that coordinated airpower, armor, and mobile infantry to achieve strategic and technological surprise that nearly defeated the Allies in World War II, the New Blitzkrieg is, literally and figuratively, an electronic "Lightning War" so potentially decisive in its effects that an entire civilization could be overthrown in hours.[4]

According to General Slipchenko, EMP and the new RMA renders obsolete modern armies, navies and air forces. For the first time in history, small nations or even non-state actors can humble the most advanced nations on Earth.

An article in ***Military Thought***, the flagship journal of the Russian General Staff, "Weak Points of the U.S. Concept of Network-Centric Warfare" points to nuclear EMP attack as a means of defeating the United States: "American forces may be vulnerable to electronic warfare attacks, in particular, an electromagnetic pulse that is a brief powerful electromagnetic field capable of overloading or destroying numerous electronic systems and high-tech microcircuits that are very sensitive to the electromagnetic field, even if transmitted from a distance. A single low-yield nuclear weapon exploded for this purpose high above the area of combat operations can generate an electromagnetic pulse covering a large area and destroying electronic equipment without loss of life that is caused by the blast or radiation."[5]

Moreover: "Today, too, a considerable body of administrative information in the U.S. armed forces goes through the civilian Internet. Many commercial communication satellites, particularly satellites in low orbits, can have their functions impaired or they can be disabled by electromagnetic shocks from high altitudes."[6]

A 2015 article from Russia's A.A. Maksimov Scientific Research Institute for Space Systems, alludes to low-yield nuclear enhanced-EMP as the most effective cyber weapon: "Even more effective are remote-controlled cyber weapons in the nuclear variant, but in this case a warhead

---

4 Major General Vladimir Ivanovich Slipchencko, *Non-Contact Wars* (Moscow: 2000). See also Slipchenko, *Future War* (Moscow Public Science Foundation, 1999).

5 Colonel A.V. Kopylov, "Weak Points of the U.S. Concept of Network-Centric Warfare" Military Thought (Moscow: Volume 3, 2011).

6 Ibid.

is required with a capacity many times smaller by comparison with the charges of the typical strategic missiles."[7]

Russia's then First Deputy Minister of Defense, Andrey Kokoshin, in a 1997 interview, claimed Russia was developing nuclear weapons "that have no counterparts in the world," including something that sounds suspiciously like a Super-EMP weapon: "ultra-small nuclear warheads weighing less than 90 kilograms, which are already being manufactured…and radiofrequency weapons."[8] In Russian military writings, the phrase "radiofrequency weapons" is used to describe nuclear or non-nuclear weapons designed to destroy enemy electronics by means of EMP.

China

China's military doctrine sounds an identical theme. According to People's Liberation Army Textbook *World War, the Third World War—Total Information Warfare*, written by Shen Weiguang (allegedly, according to the People's Republic of China (PRC), the inventor of Information Warfare), "Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies...":

> *With their massive destructiveness, long-range nuclear weapons have combined with highly sophisticated information technology and information warfare under nuclear deterrence....Information war and traditional war have one thing in common, namely that the country which possesses the critical weapons such as atomic bombs will have "first strike" and "second strike retaliation" capabilities....As soon as its computer networks come under attack and are destroyed, the country will slip into a state of paralysis and the lives of its people will ground to a halt. Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies in order to equip China without delay with equivalent deterrence that will enable it to stand up to the military powers in the information age and neutralize and check the deterrence of Western powers, including the United States.*

An article "Overview of Electromagnetic Pulse Weapons and Protection Techniques Against Them" from the People's Republic of China Air Force Engineering University describes nuclear EMP weapons as the most powerful and effective variant of electronic warfare weapons for waging Information Warfare. Nuclear and non-nuclear EMP weapons in the context of

---

7 Dr. Grigoriy Vokin, Department Chief, "Remote Custodian. Warheads with Artificial Intelligence for Reconnaissance, Guaranteed Destruction of Targets, and Human Rescue" A.A. Maksimov Scientific Research Institute for Space Systems (2015).

8 Denis Baranets, Komsomolskaya Pravda (7 August 1997), p. 1.

Information Warfare are the crucial instruments for implementing this Revolution in Military Affairs:

> *In future high-tech warfare under informatized conditions, information warfare will span multiple dimensions, including ground, sea, air, and the EM spectrum. Information superiority has already become central and crucial to achieving victory in warfare…If the communications equipment used for the transmission of battlefield information were attacked and damaged by an opponent's EMP weapons, then the one attacked would face the danger of disruption in battlefield information transmission. EMP severely restricts the tactical performance and battlefield survivability of informatized equipment.*[9]

Moreover, the article clearly makes a distinction between nuclear weapons and nuclear EMP weapons, describing the latter as "a new type of weapon" like non-nuclear EMP weapons for waging Information Warfare:

> *As opposed to conventional and nuclear weapons, EMP weapons are a new type of weapon capable of causing mass destruction by instantly releasing high-intensity EMP…They can interfere, damage, and overheat electronics, resulting in logic circuit dysfunctions, control malfunctions, or total failure. The unique destructive effect that EMP have on electronic equipment was unintentionally discovered by the United States in the 1960s during a nuclear test. In July 1962, the United States conducted a high-altitude nuclear explosion in the Pacific Ocean. This…unexpectedly overloaded the Honolulu power grid in Hawaii, 1,400 km away, even overheating lightning protection devices on powerlines. On a battlefield, this new-type weapon will cause devastating damage to electronic systems, including computers, communications and control systems, and radars, resulting in immeasurable losses.*[10]

Furthermore, according to the article: "There are 3 types of military EMP based on pulse sources: the first is the high-altitude electromagnetic pulse (HEMP) produced by the detonation of a low yield nuclear bomb in the atmosphere at high-altitude; the second is…produced by high explosives and related devices; the third is the HPM…produced by HPM devices such as magnetrons and vircators." Nuclear EMP weapons are, or include, Enhanced-EMP or so-called Super-EMP weapons designed to produce gamma rays and high-frequency E1 EMP: "HEMP weapons are a type of weak nuclear explosive EMP bomb that produces EMP through the detonation of low-yield nuclear bombs at high-altitudes (70 to 100 km above ground)." The E1

---

9 Zhao Meng, Da Xinyu, and Zhang Yapu, "Overview of Electromagnetic Pulse Weapons and Protection Techniques Against Them" Winged Missiles (PRC Air Force Engineering University: May 1, 2014).

10 Ibid.

EMP field "produced by nuclear EMP is about 10 to 100 kV/m and can penetrate and melt any electronic components."[11]

A January 2016 article "General Trend of the Worldwide Revolution in Military Affairs and the Form of Future War" by China's National Security Policy Committee sees "electromagnetic pulse bombs" among the new "disruptive technologies" that "can change the 'rules of the game'" by disrupting U.S. military "precision warfare capabilities centered on information technology" thereby sounding "the horn of a new round of revolution in military affairs."[12]

Iran

A recently translated military textbook ironically titled *Passive Defense* by the Army of the Islamic Republic of Iran (Martyr Lt. General Sayed Shirazi Center for Education and Research, 2010) endorses the theories of Russian General Slipchenko (who is acknowledged on page one of the first chapter).[13] The military manual notes the potentially decisive effects of nuclear EMP attack to defeat an adversary in more than 20 passages. Ambassador R. James Woolsey, former Director of Central Intelligence, writes:

> *"Death to America" is more than merely an Iranian chant—Tehran's military is planning to be able to make a nuclear EMP attack....Rep. Trent Franks quoted from an Iranian military textbook recently translated by the Defense Intelligence Agency's National Intelligence University...The official Iranian military textbook advocates a revolutionary new way of warfare that combines coordinated attacks by nuclear and non-nuclear EMP weapons, physical and cyber-attacks against electric grids to blackout and collapse entire nations. Iranian military doctrine makes no distinction between nuclear EMP weapons, non-nuclear radio-frequency weapons and cyber-operations—it regards nuclear EMP attack as the ultimate cyber weapon.*[14]

EMP is most effective at blacking-out critical infrastructures, while it does not directly damage the environment or harm human life, according to Iran's Passive Defense:

> *As a result of not having the other destructive effects that nuclear weapons possess, among them the loss of human life, weapons derived from electromagnetic pulses have attracted attention with regard to their use in future wars...The superficiality of secondary damage sustained as well as the*

---

11 Ibid.

12 Li Bingyan, "General Trend of the Worldwide Revolution in Military Affairs and the Form of Future War" Guangming Ribao Online (January 27, 2016).

13 Army of the Islamic Republic of Iran, *Passive Defense: Approach to the Threat Center* (Tehran: Martyr Lt. General Sayad Shirazi Center for Education and Research, Spring 2010).

14 "A Shariah-Approved Nuclear Attack" Washington Times, September 15, 2015.

avoidance of human casualties serves as a motivation to transform this technology into an advanced and useful weapon in modern warfare.[15]

Former CIA Director Woolsey notes: "Because EMP destroys electronics directly, but people indirectly, it is regarded by some as Shariah-compliant use of a nuclear weapon. *Passive Defense* and other Iranian military writings are well aware that nuclear EMP attack is the most efficient way of killing people, through secondary effects, over the long run. The rationale appears to be that people starve to death, not because of EMP, but because they live in materialistic societies dependent upon modern technology."[16]

An Iranian political-military journal, in an article entitled "Electronics To Determine Fate Of Future Wars," states that the key to defeating the United States is EMP attack and that, "If the world's industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years…":

Advanced information technology equipment exists which has a very high degree of efficiency in warfare. Among these we can refer to communication and information gathering satellites, pilotless planes, and the digital system.... Once you confuse the enemy communication network you can also disrupt the work of the enemy command and decision-making center. Even worse, today when you disable a country's military high command through disruption of communications you will, in effect, disrupt all the affairs of that country.... If the world's industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years.... American soldiers would not be able to find food to eat nor would they be able to fire a single shot.[17]

Ironically, while electric power lobbyists are resisting EMP protection of the U.S. grid in Washington, the Iranian Mehr News Agency reported that Iran is violating international sanctions and going full bore to protect itself from a nuclear EMP attack:

Iranian researchers...have built an Electromagnetic Pulse (EMP) filter that protects country's vital organizations against cyber attack. Director of Kosar Information and Communication Technology Institute Saeid Rahimi told [Mehr News Agency] MNA correspondent that the EMP (Electromagnetic Pulse) filter is one of the country's boycotted products and until now procuring it required considerable costs and various strategies. "*But recently Kosar ICT...has managed to domestically manufacture the EMP filter for the very first time in*

---

15 Ibid.
16 Ibid
17 Tehran, Nashriyeh-e Siasi Nezami, December 1998 -January 1999.

this country," said Rahimi. Noting that the domestic EMP filter has been approved by security authorities, Rahimi added "the EMP filter protects sensitive devices and organizations against electromagnetic pulse and electromagnetic terrorism." He also said the domestic EMP filter has been implemented in a number of vital centers in Iran.[18]

North Korea

North Korea appears to have practiced the military doctrines described above against the United States—including possibly by simulating a nuclear EMP attack and Combined-Arms Cyber Warfare operation against the U.S. mainland.[19]

Following North Korea's third illegal nuclear test in February 2013, North Korean dictator Kim Jong-Un repeatedly threatened to make nuclear missile strikes against the U.S. and its allies. In what was then the worst ever nuclear crisis with North Korea, that lasted months, the U.S. responded by beefing-up National Missile Defenses and flying B-2 bombers in exercises just outside the Demilitarized Zone to deter North Korea.[20]

On April 16, 2013, North Korea's KMS-3 satellite orbited over the U.S. from a south polar trajectory, over-flying the Washington, DC-New York City corridor, the nation's political and economic capitals, from the south. [redacted] On April 16, KMS-3's trajectory was near optimal to make an EMP attack that could blackout the Eastern Grid that services half of the United States—if the satellite is nuclear-armed. On that same day, parties unknown used AK-47s to make a sophisticated commando-style attack on the Metcalf transformer substation, which services San Francisco and the Silicon Valley, an important part of the Western grid. Cyber-attacks on U.S. critical infrastructures continued throughout the crisis.[21]

On January 6, 2016, North Korea provoked another nuclear crisis with its fourth illegal nuclear test of what it claimed was an H-Bomb. On February 7th, again amidst threats to make a nuclear

---

18 "Iran Builds EMP Filter For 1st Time" Mehr News Agency, June 13, 2015.

19 "EMP Threat from North Korea, 2013" Family Security Matters, April 27, 2014.

20 "U.S. Warns North Korea With Stealth Bomber Flights" Wall Street Journal, March 29, 2013.

21 "EMP Threat from North Korea, 2013" op. cit.; KMS-3 is NORAD's acronym for North Korea's satellite Kwangmyongsong-3 (Lodestar-3 or Guiding Star-3), a name richly symbolic for Korean mythology and the deification of Kim Jong-Un who according to official propaganda was born on Mt. Paeku under a newly appeared bright guiding star, signifying the birth of a great general. KMS-3 was launched on December 12, 2013, exactly two months before, and probably in anticipation of, North Korea's illegal nuclear test on February 12, 2013.

Are North Korea's Satellites an EMP Threat?

North Korea's KMS-3 and KMS-4 satellites orbit over the U.S. daily. [redacted] Their trajectory is similar to that planned for a Soviet-era secret weapon called the Fractional Orbital Bombardment System (FOBS) deployed by the USSR to make a surprise nuclear attack on the United States. In 2004, two retired Russian generals, then teaching at Russia's Voroshilov General Staff Academy, told the EMP Commission that the design for Russia's Super-EMP nuclear weapon was accidentally transferred by Russian scientists and engineers working on North Korea's missile and nuclear weapons program. They said North Korea could test a Super-EMP weapon "in a few years." The 2006 and subsequent low-yield tests do not appear to have been failures because North Korea proceeded with weaponization. In 1997, Andrey Kokoshin, then Russia's First Deputy Defense Minister, stated Russia was deploying a new generation of advanced nuclear weapons "that have no counterparts in the world" including EMP weapons and "ultra-small warheads weighing less than 90 kilograms." Such weapons would be small enough for North Korea's satellites. General Vladimir Slipchenko and General Vladimir Belous, who warned the EMP Commission about North Korean development of Super-EMP weapons, are among Russia's most prominent military scientists and experts on EMP and advanced technology warfare. General Slipchenko's advocacy of EMP and Combined-Arms Cyber Warfare is recognized in Iran's military textbook *Passive Defense* that advocates development of capabilities for nuclear EMP attack.

missile strike on the United States, Pyongyang orbited another satellite, the KMS-4, on the same polar trajectory as the KMS-3.[22]

Kim Jong-Un has threatened to reduce the United States to "ashes" with "nuclear thunderbolts" and threatened to retaliate for U.S. diplomatic and military pressure by "ordering officials and scientists to complete preparations for a satellite launch as soon as possible" amid "the enemies' harsh sanctions and moves to stifle" the North.[23] North Korean press asserts readiness for "any form of war" and includes their satellite with "strengthening of the nuclear deterrent and legitimate artificial satellite launch, which are our fair and square self-defensive choice." Moreover: "The nuclear [weapons] we possess are, precisely, the country's sovereignty, right to live, and dignity. Our satellite that cleaves through space is the proud sign that unfolds the future of the most powerful state in the world." The same article, like many others, warns North Korea

[22] "North Korea May Have Tested Components of A Hydrogen Bomb" CNN, January 29, 2016; "North Korea Launches 'Satellite," Sparks Fears About Long-Range Missile Program" Washington Post, February 6, 2016.

[23] Alex Lockie, "North Korea Threatens 'Nuclear Thunderbolts' as U.S. And China Finally Work Together" American Military News (April 14, 2017); Fox News, "U.S. General: North Korea 'Will' Develop Nuclear Capabilities to Hit America" (September 20, 2016) www.foxnews.com/world/2016/09/20/north-korea-says-successfully-ground-tests-new-rocket-engine.html

makes "constant preparations so that we can fire the nuclear warheads, which have been deployed for actual warfare for the sake of national defense, at any moment!"[24]

On April 30, 2017, South Korean officials told The Korea Times and YTN TV that North Korea's test of a medium-range missile on April 29 was not a failure, as widely reported in the world press, because it was deliberately detonated at 72 kilometers altitude. [redacted] According to South Korean officials, "It's believed the explosion was a test to develop a nuclear weapon different from existing ones." Japan's Tetsuro Kosaka wrote in Nikkei, "Pyongyang could be saying, 'We could launch an electromagnetic pulse (EMP) attack if things get really ugly.'"[25]

On September 3, 2017, North Korea conducted its sixth underground nuclear test. The test produced a seismic signal of 6.3 on the Richter scale, indicating a yield of over 100 kilotons. Shortly after that test, North Korea released an article titled "Kim Jong Un Gives Guidance to Nuclear Weaponization," which contained the following paragraph: **"The H-bomb, the explosive power of which is adjustable from tens kiloton to hundreds kiloton, is a multifunctional thermonuclear nuke with great destructive power which can be detonated even at high altitudes for super-powerful EMP attack according to strategic goals."** On September 4, 2017, Pyongyang published a technical report "The EMP Might of Nuclear Weapons" accurately describing what the Russians and Chinese call a Super-EMP nuclear weapon. These warnings leave little room for wishful thinking by the U.S. leadership.[26]

[24] Rodong Sinmun (March 7, 2016).
[25] Tetsuro Kosaka, "North Korea's 'Failed' Missile Test May Have Been a Thinly Disguised Threat," Nikkei (May 2, 2017).
[26] Kim Song-won, "The EMP Might of Nuclear Weapons," Rodong Sinmun, Pyongyang, (September 4, 2017).

Non-Nuclear EMP Weapons

Terrorists, criminals, and even disgruntled individuals have already made localized EMP attacks using radio frequency weapons (RFWs) in Europe and Asia. Probably sooner rather than later, the RFW threat will come to America.

RFWs typically are much less powerful than nuclear weapons and much more localized in their effects, usually having a range of one kilometer or less. And unlike damage from guns and bombs, an attack by RFWs is much less conspicuous, and may even be misconstrued as an unusual accident arising from faulty components and systemic failure.

Some documented examples of successful attacks using Radio Frequency Weapons, and accidents involving electromagnetic transients, are described in the DoD *Pocket Guide for Security Procedures and Protocols for Mitigating Radio Frequency Threats*.[27]

For example, North Korea used a Radio Frequency Weapon, purchased from Russia, to attack airliners and impose an "electromagnetic blockade" on air traffic to Seoul, South Korea's capitol. The repeated attacks by RFW also disrupted communications and the operation of automobiles in several South Korean cities in December 2010; March 9, 2011; and April-May 2012.[28]

---

27 U.S. Department of Defense, "*Pocket Guide for Security Procedures and Protocols for Mitigating Radio Frequency Threats* (Technical Support Working Group, Directed Energy Technical Office, Dahlgren Naval Surface Warfare Center).

28 "Massive GPS Jamming Attack by North Korea" GPSWORLD.COM (May 8, 2012).

Physical Attacks on Power Grids

On April 16, 2013, parties unknown used AK-47s to attack the Metcalf transformer substation that services San Jose, the Silicon Valley, and is an important part of the Western Grid. Blackout of the Western Grid could impede U.S. power projection capabilities against North Korea.

Cases of physical sabotage of electric power grids include the following:

- On October 27, 2013, the Knights Templars, a terrorist drug cartel, used explosives and small arms to blackout Mexico's Michoacan State, putting 420,000 people into the dark, isolating them from federal police, so they could publicly assassinate town and village leaders opposed to the drug trade.
- On June 9, 2014, Al Qaeda in The Arabian Peninsula (AQAP) used rocket-propelled grenade launchers to attack powerline towers, blacking-out all of Yemen, a nation of 16 cities and 24 million people. It is the first time in history terrorists have blacked-out an entire nation.
- On January 25, 2015, the Taliban blacked-out most of the electric grid in Pakistan, a nuclear weapons state.

All of these blackouts were temporary, caused by sabotage of powerlines or small substations. A coordinated attack on a relatively small number of the most important transformer substations could cause a protracted blackout lasting months. The Wall Street Journal has reported that a study by the U.S. FERC concluded that a terrorist attack that destroys just 9 key transformer substations could cause a protracted nationwide blackout.[29]

[29] Pry, *Blackout* Wars, op. cit.; Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism" Wall Street Journal, February 5, 2014.

Cyber-Attacks on Power Grids

Suspected and known cases of cyber-attacks causing blackouts of power grids include the following:

- On March 31, 2015, Turkey's national electric grid was temporarily blacked-out, briefly causing widespread chaos to businesses and society in a NATO member and crucial U.S. Middle Eastern ally. Reportedly, Iran caused the blackout by a cyber-attack. Weeks later, amidst a confrontation with Russia over shooting down a Russian jet that violated Turkish airspace, Turkey denied being victimized by an Iranian cyber-blackout. If Iran was the culprit, it would be the first time in history that a nationwide blackout resulted from cyber warfare.
- On December 23, 2015, a partial blackout of Ukraine's electric grid that lasted 1 to 6 hours, affecting 230,000 people, is widely regarded as the first confirmed case of a successful cyber-attack on an electric grid. The cyber-blackout is attributed to Russia.
- A year later, on December 17, 2016, Ukraine was again victimized, allegedly by Russians disrupting power grid control systems to temporarily blackout over 100 cities and towns.

Cyber-attacks, the use of computer viruses and hacking to invade and manipulate information and SCADA systems, is described by some U.S. political and military leaders as one of the greatest threats facing the United States. Every day, literally thousands of cyber-attacks are made on U.S. civilian and military systems, most of them designed to steal information.

Then Joint Chiefs Chairman, General Martin Dempsey, warned on June 27, 2013, that the United States must be prepared for the revolutionary threat represented by cyber warfare: "One thing is clear. Cyber has escalated from an issue of moderate concern to one of the most serious threats to our national security," cautioned Chairman Dempsey, "We now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of a mouse."[30]

On July 6, 2014, reports surfaced that Russian intelligence services allegedly infected 1,000 power plants in Western Europe and the United States with a new computer virus called Dragonfly. No one has stated what Dragonfly is supposed to do. Some analysts think it was just probing the defenses of western electric grids. Others think Dragonfly may have inserted logic bombs into SCADA systems that can disrupt the operation of electric power plants in a future crisis.

Tomorrow's cyber super-threat, that with computer viruses and hacking alone can blackout the national electric grid for a year or more, may already be upon us today.

---

30 Claudette Roulo, *DoD News*, Armed Force Press Service, June 27, 2013.

Admiral Michael Rogers on November 20, 2014, warned the House Permanent Select Committee on Intelligence that sophisticated great powers like China and Russia have the capability to blackout the entire U.S. national electric grid for months or years by means of cyber-attack, according to press reports. Admiral Rogers, as Chief of U.S. Cyber Command and Director of the National Security Agency, is officially the foremost U.S. authority on the cyber threat. "It is only a matter of the when, not if, that we are going to see something traumatic," Admiral Rogers testified to Congress.[31]

In June 2015, congressional hearings revealed the discovery, about a year earlier, that China, probably the Chinese People's Liberation Army (PLA), hacked into computer files at the U.S. Office of Personnel Management and stole sensitive information on 30 million federal employees and U.S. citizens.

Russia apparently made a cyber-attack on the U.S. Joint Chiefs of Staff in July 2015 that crippled an unclassified e-mail communications network used by the Joint Chiefs. "The U.S. military believes hackers connected to Russia are behind the recent intrusion into a key, unclassified e-mail server used by the office of the Joint Chiefs," according to press reports, "Military officials assessed the attack had a sophistication that indicates it came from a state-associated actor." The widely reported Russian cyber-attack on the Joint Chiefs disrupted e-mail communications for 4,000 users at the Defense Department for over 10 days.[32]

In April 2015, another Russian cyber-attack reportedly penetrated "sensitive parts of the White House computer system."[33]

Few Americans make any connection between cyber-thefts and intrusions, such as those described above, and EMP attacks on the grid that could threaten the existence of society. But in the context of foreign military doctrine on Information Warfare, these cyber-thefts and intrusions look less like isolated cases of hacking and more like systematic probing of U.S. defenses and gauging Washington's reactions—perhaps in preparation for an all-out cyber offensive that would include physical sabotage, radiofrequency weapons, and nuclear EMP attack. In Nazi Germany's blitzkrieg strategy, the massed onslaught of heavy armored divisions was preceded by scouting and probing by their motorcycle corps. The same principle may be at work here in cyber space with probing attacks on the U.S. from China, Russia, North Korea and Iran.

---

31 CNN November 21, 2014. However, Jonathan Pollett, a cyber-security expert, in an article challenged Admiral Rogers' warning as wrong, or misunderstood and exaggerated by the press: "No, hackers can't take down the entire, or even a widespread portion of the U.S. electric grid. From a logistical standpoint, this would be far too difficult to realistically pull off," writes Pollett in "What Hackers Can Do To Our Power Grid," Business Insider (November 23, 2014).

32 CNN, "Official: Russia Suspected In Joint Chiefs E-mail Server Intrusion," August 7, 2015.

33 Ibid.

All Hazards Strategy

We recommend an "all hazards" strategy to protect the nation by addressing the worst threat—nuclear EMP attack. Nuclear EMP is worse than natural EMP because it combines several threats in one. Nuclear EMP has a long-wavelength component like a geomagnetic super-storm, a short-wavelength component like Radio-Frequency Weapons, a mid-wavelength component like lightning—and is potentially more widespread and can do more damage than all three. Measures to protect electric grids and other critical infrastructures from EMP can also be designed to make these systems more resilient against cyber-attacks, sabotage, and severe weather.

A U.S. Army War College Study, *"In The Dark: Planning for a Catastrophic Critical Infrastructure Event,"* (2011) warned U.S. Cyber Command that U.S. doctrine should not overly focus on computer viruses to the exclusion of EMP attack and the full spectrum of other threats, as planned by potential adversaries.

Reinforcing the above, a Russian technical article on cyber warfare notes that a cyber-attack can collapse "the system of state and military control...its military and economic infrastructure" because of "electromagnetic weapons...an electromagnetic pulse acts on an object through wire leads on infrastructure, including telephone lines, cables, external power supply and output of information."[34]

Resilient Military Systems and the Advanced Cyber Threat, a January 2013 study by the Defense Science Board, recommends that it may be necessary for the U.S. to respond to an all-out cyber warfare operation with nuclear deterrence—or nuclear war. The Defense Science Board warns that while operationally "a nuclear and cyber-attack are very different" in terms of the consequences "the existential impact to the United States is the same."

The Defense Science Board likewise warns that cyber warfare is not only about computer viruses and hacking, but becomes an existential threat "from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities (a "full spectrum" adversary)."

[34] Maxim Shepovalenko, Military-Industrial Courier (July 3, 2013).

Misinformation about EMP and the North Korean Threat

EMP non-experts often dismiss the possibility of a nuclear EMP attack from North Korea as "science fiction" and "unlikely" because either they lack knowledge of the effects of the Soviet and U.S. high altitude nuclear tests in the early 1960s, do not have access to or understand the extensive body of testing and analysis carried out by the DoD over the last fifty-five years, or they mistakenly believe the nuclear weapons currently possessed by North Korea are incapable of making an effective EMP attack.

One EMP skeptic correctly implies in his article that it is analytically risky to draw conclusions about the EMP threat when so much of the data is classified. It is riskier still for analysts with no technical training on EMP and without working professionally in the defense or intelligence communities on the EMP threat, to conclude the EMP threat is not real—dismissing the consensus view of EMP experts who have advanced degrees in physics and electrical engineering, have worked on EMP generation and effects for several decades, have throughout that time had access to classified data, and have conducted simulated EMP tests on a wide variety of electronic systems, beginning in 1963.

I offer this commentary to correct errors of fact, analysis, and myths about EMP and the threat from North Korea:

- Even primitive, low-yield nuclear weapons are such a significant EMP threat that rogue states or terrorists may well prefer using a nuclear weapon for EMP attack, instead of destroying a city: "Therefore, terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or military base, they may obtain the greatest political-military utility from one or a few such weapons by using them—or threatening their use—in an EMP attack."[35]
- North Korea may either now or in the future be armed with what the Russians call "Super-EMP" weapons, that can generate extraordinarily high-intensity EMP fields, according to unclassified Russian sources up to 200,000 volts per meter.[36] In 2004, two Russian generals, both EMP experts, warned the EMP Commission that the design for Russia's Super-EMP warhead was "accidentally" transferred to North Korea, and that due to "brain drain" Russian scientists were in North Korea, helping with their missile and nuclear weapon programs. South Korean military intelligence told their press that Russian scientists are in North Korea helping develop an EMP nuclear weapon. In 2013, a People's Republic of China military commentator stated North Korea has Super-EMP nuclear weapons. The EMP Commission 2004 Report warns: "Certain types of relatively

[35] EMP Commission *Executive Report 2004*, p. 2.

[36] "Russia: Nuclear Response To America Is Possible Using Super-EMP Factor," Aleksey Vaschenko, "A Nuclear Response To America Is Possible" Zavtra (November 1, 2006).

low-yield nuclear weapons can be employed to generate potentially catastrophic EMP effects over wide geographic areas, and designs for variants of such weapons may have been illicitly trafficked for a quarter-century."[37]

- Super-EMP weapons are low-yield and designed to produce not a big kinetic explosion, but rather a high level of gamma rays, which is what generates the high-frequency E1 EMP most damaging to the broadest range of electronics. North Korean nuclear tests, including the first in 2006, whose occurrence was predicted to the EMP Commission two years in advance and by the two Russian EMP experts, are consistent with testing of a Super-EMP weapon.
- The design of a Super-EMP weapon could be relatively small and lightweight. Such a device could fit inside North Korea's satellites that can orbit over the United States. [redacted], resembling a Russian secret weapon developed during the Cold War that could have used a nuclear-armed satellite to make a surprise EMP attack on the United States.
- One popular myth is that during the 1962 STARFISH PRIME high-altitude nuclear test "just one string of street lights failed in Honolulu" and that the test proves EMP is no threat. In fact, the EMP knocked-out thirty-six strings of street lights, caused a telecommunications microwave relay station to fail, burned out high-frequency radio links, set off burglar alarms, and caused other damage. The Hawaiian Islands did not experience a catastrophic protracted blackout because they were on the far edge of the EMP field contour, where effects are weakest, and were still in an age dominated by vacuum tube electronics. In addition, the slow pulse (E3) component of the EMP waveform couples most effectively to very long electric power transmission lines present on large land masses but not present in Hawaii. A 1983 twelve-page report, formerly classified Confidential Restricted Data, summarizing the observed EMP effects of the Fishbowl U.S. exo-atmospheric tests, has recently been reviewed at the request of the EMP Commission and found to be unclassified, but has been placed under a distribution restriction by the Department of Defense that makes it unavailable to analysts and others concerned about the viability of U.S. critical national infrastructure. No justification for the distribution restriction has been given.
- Russia in 1961-62 conducted a series of high-altitude EMP tests over Kazakhstan, an industrialized area nearly as large as Western Europe, that damaged the Kazakh electric grid. Modern electronics are much more vulnerable to EMP than the electronics of 1962 exposed to STARFISH PRIME and the Kazakh nuclear tests. A similar EMP event over the U.S. today would be an existential threat to our society, due to our dependence on the

[37] EMP Commission *Executive Report 2004,* p. 2. Kim Min-sek and Yoo Jee-ho, "Military Source Warns of North's EMP Bomb" JoonAng Daily (September 2, 2009). Li Daguang, "North Korea Electromagnetic Attack Threatens South Korea's Information Warfare Capabilities" Tzu Chin, No. 260 (Hong Kong: June 1, 2012), in "PRC Owned HK Journal Says DPRK May Build EMP Bombs To Paralyze ROK Weapons System."

electric power grid and other lifeline infrastructures, all the more susceptible due to the vulnerability of advanced electronic controls and communications.

- One popular but poorly informed author mistakenly inferred from a single simulated EMP test series on vehicles that, because only 6 of 55 vehicles were shut down, vehicle transportation would continue after an EMP event. During that test one of the vehicles was damaged and could not be operated until repaired, indicating that at least 2 percent of vehicles would be at risk of EMP damage. Even a 2 percent failure rate of vehicles would cause traffic jams, crippling transportation in urban areas. Moreover, the EMP test protocol limited testing vehicles only to upset, not to damage, because the EMP Commission could not afford to repair damaged cars; however, one vehicle was damaged by EMP despite best efforts to limit the effects to upset. Several of the vehicles tested stopped operating but could be restarted. Over 50 years of EMP testing indicates that full field damage to vehicles would probably be much higher than was observed on the limited tests. Today's vehicles depend on a much larger complement of electronics than the vehicles tested by the Commission more than a decade ago. Furthermore, vehicles cannot run without fuel, which cannot be pumped in a protracted electrical blackout.
- Another poorly informed analyst wondered why EMP from atmospheric nuclear tests in Nevada did not blackout Las Vegas. The nuclear tests he describes were all endo-atmospheric tests that do not generate appreciable EMP fields beyond a range of about 5 miles. The HEMP threat of interest requires exo-atmospheric detonation, at 30 kilometers altitude or above, and produces EMP out to ranges of hundreds to thousands of miles, depending on the height of detonation. Las Vegas was not affected by EMP because those endo-atmospheric nuclear tests generated much lower level fields outside the Nevada Test Site.
- Another poorly informed author miscalculates that "a 20-kiloton bomb detonated at optimum height would have a maximum EMP damage distance of 20 kilometers" in part because he mistakenly assumes "15,000 volts/meter or higher" in the E1 EMP extends only a short distance from the detonation point and that field strength is necessary for damage. These figures are extreme underestimates of the EMP field range and an extreme overestimate of system damage field thresholds. A one meter wire connected to a semiconductor device, such as a mouse cord or interconnection cable, would place hundreds to thousands of volts on microelectronic devices out to ranges of hundreds of miles for low-yield exo-atmospheric detonations. Semiconductor junctions operate at a few volts, and will experience breakdown at a few volts over their operating point, then allowing their power supply to destroy junctions experiencing reverse bias breakdown, as has been our experience in many EMP tests.
- The North Korean missile test on April 29, 2017, that apparently either failed or deliberately detonated at an altitude of 72 kilometers [redacted] could have been a test for creating a potentially damaging EMP field to a distance, not of one ill-informed author's miscalculated 20

kilometers, but of about 930 kilometers [Kilometers Radius = 110 (Kilometers Burst Height to the 0.5 Power)].

- Ill-informed authors often mistakenly ignore system upset as a vulnerability. Digital electronics can be upset by extraneous pulses of a few volts. For unmanned control systems present within the electric power grid, long-haul communication repeater stations, and gas pipelines, an electronic upset can be tantamount to permanent damage. Temporary upset of electronics can also have catastrophic consequences for military operations. No electronics should be considered invulnerable to EMP unless hardened or tested to certify survivability. Some highly critical unprotected electronics have been upset or damaged in simulated EMP tests, not at one author's alleged "15,000 volts/meter or higher" but at threat levels far below 1,000 volts/meter.

Therefore, even for a low-yield 10 to 20 kiloton weapon, the EMP field should be considered dangerous for unprotected U.S. systems. The EMP Commission 2004 Report warned against the U.S. military's increasing use of commercial-off-the-shelf-technology that is not protected against EMP: "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."[38]

[38] EMP Commission *Executive Report 2004*, p. 47.

North Korea Nuclear EMP Attack: An Existential Threat

While most military and other analysts are fixated on when in the future North Korea will develop highly reliable intercontinental missiles, guidance systems, and reentry vehicles capable of striking a U.S. city, the present and continuing threat from EMP is largely ignored. EMP attack does not require an accurate guidance system because the area of effect, having a radius of hundreds or thousands of kilometers, is so large. No reentry vehicle is needed because the warhead is detonated at high-altitude, above the atmosphere. Missile reliability matters little because only one missile has to work to make an EMP attack against an entire nation.

North Korea could make an EMP attack against the United States by ICBM, or by launching a short-range missile off a freighter or submarine or by lofting a warhead to 30 kilometers burst height by balloon. While such lower-altitude EMP attacks would not cover the whole U.S. mainland, as would an attack at higher-altitude (300 kilometers), even a balloon-lofted warhead detonated at 30 kilometers altitude could blackout the Eastern Grid that supports most of the population and generates 75 percent of U.S. electricity.

An EMP attack could also be made by a North Korean satellite.

North Korea's KMS-3 and KMS-4 satellites were launched to the south on polar trajectories and passed over the United States on their first orbit. Pyongyang launched KMS-4 on February 7, 2017, shortly after its fourth illegal nuclear test on January 6, 2017, that began the present protracted nuclear crisis with Pyongyang.

[redacted], resembling a Russian secret weapon developed during the Cold War, called the Fractional Orbital Bombardment System (FOBS) that would have used a nuclear-armed satellite to make a surprise EMP attack on the United States.[39]

Ambassador Henry Cooper, former Director of the U.S. Strategic Defense Initiative, and a preeminent expert on missile defenses and space weapons, has written numerous articles warning about the potential North Korean EMP threat from their satellites. For example, on September 20, 2016 Ambassador Cooper wrote:

> *U.S. ballistic missile defense (BMD) interceptors are designed to intercept a few North Korean ICBMs that approach the United States over the North Polar region. But current U.S. BMD systems are not arranged to defend against even a single ICBM that approaches the United States from over the South Polar region, which is the direction toward which North Korea launches its*

[39] Miroslav Gyurosi, *The Soviet Fractional Orbital Bombardment System Program*, (January 2010) Technical Report APA-TR-2010-010.

satellites…This is not a new idea. The Soviets pioneered and tested just such a specific capability decades ago—we call it a Fractional Orbital Bombardment System (FOBS)…So, North Korea doesn't need an ICBM to create this existential threat. It could use its demonstrated satellite launcher to carry a nuclear weapon over the South Polar region and detonate it…over the United States to create a high-altitude electromagnetic pulse (HEMP)…The result could be to shut down the U.S. electric power grid for an indefinite period, leading to the death within a year of up to 90 percent of all Americans—as the EMP Commission testified over eight years ago.[40]

Former NASA rocket scientist James Oberg visited North Korea's Sohae space launch base, witnessed elaborate measures undertaken to conceal space launch payloads, and concludes in a 2017 article that the EMP threat from North Korea's satellites should be taken seriously:

…there have been fears expressed that North Korea might use a satellite to carry a small nuclear warhead into orbit and then detonate it over the United States for an EMP strike. These concerns seem extreme and require an astronomical scale of irrationality on the part of the regime. The most frightening aspect, I've come to realize, is that exactly such a scale of insanity is now evident in the rest of their "space program." That doomsday scenario, it now seems, has been plausible enough to compel the United States to take active measures to ensure that no North Korean satellite, unless thoroughly inspected before launch, be allowed to reach orbit and ever overfly the United States.[41]

An earlier generation immediately understood the alarming strategic significance of Sputnik in 1957, yet few today understand the strategic significance of North Korea's satellites, perhaps because of widespread ignorance about EMP.

---

40 Ambassador Henry F. Cooper, "Whistling Past The Graveyard…" High Frontier (September 20, 2016) highfrontier.org/sept-20-2016-whistling-past-the-graveyard. See also: highfrontier.org/category/fobs. On up to 90 percent U.S. fatalities from an EMP attack, see: U.S. House of Representatives, Hearing, "Threat Posed by Electromagnetic Pulse (EMP) Attack" Committee on Armed Services (Washington, D.C.: July 10, 2008), p. 9.

41 Jim Oberg, Space Review (February 6, 2017) www.thespacereview.com/article/3164/1in

The Fragility of Complex Systems

When assessing the potential vulnerability of U.S. military forces and civilian critical infrastructures to EMP, it is necessary to be mindful of the complex interdependencies of these highly-networked systems, such that EMP upset and damage of a very small fraction of the total system can cause total system failure.

Real world failures of electric grids from various causes indicate that a nuclear EMP attack would have catastrophic consequences. Significant and highly disruptive blackouts have been caused by single-point failures cascading into system-wide failures, originating from damage comprising far less than 1 percent of the total system. For example:

- The Great Northeast Blackout of 2003—that put 50 million people in the dark for a day, contributed to at least 11 deaths, and cost an estimated $6 billion—originated from a single failure point when a powerline contacted a tree branch, damaging less than 0.0000001 (0.00001 percent) of the system.
- The New York City Blackout of 1977, that resulted in the arrest of 4,500 looters and injury of 550 police officers, was caused by a lightning strike on a substation that tripped two circuit breakers.
- The Great Northeast Blackout of 1965, that affected 30 million people, happened because a protective relay on a transmission line was improperly set.
- India's nationwide blackout of July 30-31, 2012—the largest blackout in history, affecting 670 million people, 9 percent of the world population—was caused by overload of a single high-voltage powerline.
- India's blackout of January 2, 2001—affecting 226 million people—was caused by equipment failure at the Uttar Pradesh substation.
- Indonesia's blackout of August 18, 2005—affecting 100 million people—was caused by overload of a high-voltage powerline.
- Brazil's blackout of March 11, 1999—affecting 97 million people—was caused by a lightning strike on an EHV transformer substation.
- Italy's blackout of September 28, 2003—affecting 55 million people—was caused by overload of two high-voltage powerlines.
- Germany, France, Italy, and Spain experienced partial blackouts on November 4, 2006—affecting 10 to 15 million people—from accidental shutdown of a high-voltage powerline.
- The San Francisco blackout in April 2017 was caused by the failure of a single high voltage breaker at a substation.

In contrast to the above blackouts caused by single-point or small-scale failures, a nuclear EMP attack would inflict massive widespread damage to the electric grid causing a large number of

failure points. With few exceptions, the U.S. national electric grid is unhardened and untested against nuclear EMP attack.

In the event of a nuclear EMP attack on the United States, a widespread protracted blackout is inevitable. This commonsense assessment is also supported by the nation's best computer modeling:

Modeling by the U.S. FERC reportedly assesses that a terrorist attack that destroys just 9 EHV transformer substations would produce catastrophic damage, causing a protracted nationwide blackout.

Modeling by the EMP Commission assesses that a terrorist nuclear EMP attack, using a primitive 10-kiloton nuclear weapon, could destroy many EHV transformers and thousands of SCADA and electronic systems, causing catastrophic collapse and protracted blackout of the U.S. power grids, putting at risk the lives of millions.

For the best unclassified modeling assessments of likely damage to the U.S. national electric grid from nuclear EMP attack see the following: U.S. FERC Interagency Report, coordinated with the DoD and Oak Ridge National Laboratory: *Electromagnetic Pulse: Effects on the U.S. Power Grid, Executive Summary* (2010); U.S. FERC Interagency Report by Edward Savage, James Gilbert and William Radasky, *The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid* (Meta-R-320) Metatech Corporation (January 2010); U.S. FERC Interagency Report by James Gilbert, John Kappenman, William Radasky, and Edward Savage, *The Late-Time (E3) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid* (Meta-R-321) Metatech Corporation (January 2010).

Regulatory Failures by the U.S. Federal Energy Regulatory Commission, the North American Energy Regulatory Corporation, and the Electric Power Industry

The current largely self-regulatory structure of the U.S. Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and the electric power industry was not designed to address U.S. survival under nuclear EMP or other hostile attack. The Commission assesses that the existing regulatory framework for safeguarding the security and reliability of the electric power grid, which is based upon a partnership between the U.S. FERC and the private NERC representing the utilities, is not able to protect the U.S. against hostile attack. The U.S. FERC and NERC standards for protecting the power grids from geomagnetic disturbances caused by solar storms are also inadequate to address storms of historical record.[42]

The U.S. FERC, the U.S. government agency that is supposed to partner with NERC in protecting the national electric grid, has publicly testified before Congress that the U.S. FERC lacks regulatory power to compel NERC and the electric power industry to protect the grid from natural and nuclear EMP and other threats.

Consider the contrast in regulatory authority between the U.S. FERC and, as examples, the U.S Nuclear Regulatory Commission (NRC), the U.S. Federal Aviation Administration (FAA), the U.S. Department of Transportation (DOT), or the U.S. Food and Drug Administration (FDA):

- The NRC has regulatory power to compel the nuclear power industry to incorporate nuclear reactor design features to make nuclear power safe. (To date, however, the NRC has not incorporated EMP survival criteria into its regulations. By the NRC's failure to use its authority to mandate protection from EMP of U.S. nuclear reactor control, safe shutdown, cooling, and other reactor systems and spent fuel storage systems, the NRC continues to place at risk the safety and survivability of the 99 U.S. commercial power reactors in operation and the safety of the people living in the vicinity of these reactors.)
- The FAA has regulatory power to compel the airlines industry to ground aircraft considered unsafe, to change aircraft operating procedures considered unsafe, and to make repairs or improvements to aircraft in order to protect the lives of passengers.
- The DOT has regulatory power to compel the automobile industry to install on cars safety glass, seatbelts, and airbags in order to protect the lives of the driving public.

[42] John G. Kappenman and Dr. William Radasky, *Examination of NERC GMD Standards and Validation of Ground Models and Geo-Electric Fields* (Storm Analysis Consultants and Metatech Corporation, July 30, 2014) adopted as an EMP Commission Staff Paper. See also Foundation for Resilient Societies, Comments Submitted on Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events, U.S. FERC Docket No. RM15-11-000, July 27, 2015; supplementary comments submitted August 10, 2015.

Underestimating the EMP Threat to Transformers

The most recent example of industry inadequacy as a champion for EMP preparedness is a study by EPRI that purports to prove a nuclear EMP attack would destroy few, if any EHV transformers. I have reviewed this study and find many flaws in the EPRI assessment. Contrary to EPRI, many EHV transformers would be at risk from the same nuclear EMP attack postulated by EPRI. The EMP Commission has produced a report providing a more realistic assessment of the E3 EMP field strengths likely to be generated by a nuclear EMP attack. The Commission's unclassified assessment of the E3 EMP threat should better inform the electric power industry and other private sector critical infrastructures so they can better protect themselves. See the EMP Commission Report by Dr. Edward B. Savage and Dr. William A. Radasky, *Development of Estimates of Peak Values of the Late-Time (E3) HEMP Heave Electric Fields Using Measured Data from High Altitude Nuclear Testing* (Metatech: Meta-R-440, July 10, 2017).

- The FDA has power to regulate the quality of food and drugs, and can ban under criminal penalty the sale of products deemed by the FDA to be unsafe to the public.

Unlike the NRC, FAA, DOT, FDA or any other U.S. government regulatory agency, the U.S. FERC does not have legal authority to compel the industry it is supposed to regulate to act in the public interest. For example, the U.S. FERC lacks legal power to direct NERC and the electric utilities to install devices to protect the grid.

Currently, the U.S. FERC only has the power to ask NERC to propose a Standard to protect the grid. NERC standards are approved, or rejected, by its membership, which is largely made up of representatives from the electric power industry. Once NERC proposes a Standard to the U.S. FERC, the FERC cannot modify the Standard, but must accept or reject the proposed Standard. If the U.S. FERC rejects the proposed Standard, NERC goes back to the drawing board, and the process starts all over again.

The geomagnetic disturbance standards proposed by the NERC that the U.S. FERC has adopted to date substantially underestimate the problem, and no standards for protecting the grid against nuclear or non-nuclear EMP weapons have been proposed or adopted.

Regulatory inadequacy over the electric power industry for national security is demonstrated, not only in the failure of industry to protect the grid, but in lobbying by NERC, EPRI, EEI and other industry groups to oppose initiatives by federal and state officials and private citizens to protect the grid from EMP over the past 9 years by implementing the recommendations of the EMP Commission made in 2008. Texas State Senator Bob Hall speaks for many Americans frustrated by the electric power industry's active, and frequently misleading, opposition:

> *As a Texas State Senator who tried in the 2015 legislative session to get a bill passed to harden the Texas grid against an EMP attack or nature's GMD, I*

learned first-hand the strong control the electric power company lobby has on elected officials. We did manage to get a weak bill passed in the Senate but the power companies had it killed in the House. A very deceitful document which was carefully designed to mislead legislators was provided by the power company lobbyist to legislators at a critical moment in the process. The document was not just misleading, it actually contained false statements. The EMP/GMD threat is real and it is not "if" but WHEN it will happen. The responsibility for the catastrophic destruction and wide spread death of Americans which will occur will be on the hands of the executives of the power companies because they know what needs to be done and are refusing to do it. In my opinion power company executives, by refusing to work with the legislature to protect the electrical grid infrastructure are committing an egregious act that is equivalent to treason. I know and understand what I am saying. As a young U.S. Air Force captain, with a degree in electrical engineering from The Citadel, I was the project officer who lead the Air Force/contractor team which designed, developed and installed the modification to "harden" the Minuteman strategic missile to protect it from an EMP attack. The American people must demand that the power company executives that are hiding the truth stop deceiving the people and immediately begin protecting our electrical grid so that life as we know it today will not end when the terrorist EMP attack comes.

In March 2016, the U.S. GAO published a report with the (misleading) title *Critical Infrastructure Protection: Federal Agencies Have Taken Actions to Address Electromagnetic Risks, But Opportunities Exist to Further Assess Risks and Strengthen Collaboration* (GAO-16-243). Appendices in the U.S. GAO report reveal that none of the essential measures recommended by the EMP Commission to protect the national electric grid have been undertaken:

Recommendation	**Action**
Expand and extend emergency power supplies	None
Extend black start capability	None
Prioritize and protect critical nodes	None
Expand and assure intelligent islanding capability	None
Assure protection of high-value generation assets	None
Assure protection of high-value transmission assets	None
Assure sufficient numbers of adequately trained recovery personnel	None

In the U.S. GAO report, the "actions" undertaken by federal agencies to address EMP are almost entirely studies and a few experimental programs.

During a hearing before the Senate Homeland Security and Government Affairs Committee (SHSGA) on July 22, 2015, under questioning by the Chairman, Senator Ron Johnson, the U.S.

GAO acknowledged that none of the recommendations of the EMP Commission to protect the national grid from EMP have been implemented by the U.S. Department of Homeland Security, U.S. Department of Energy, U.S. FERC, or NERC.

The U.S. GAO report explained lack of progress in protecting the national electric grid from EMP as due to a lack of leadership, because no one was in charge of solving the EMP problem: "DHS and DOE, in conjunction with industry, have not established a coordinated approach to identifying and implementing key risk management activities to address EMP risks."

The 2014 Intelligence Report

The report by the Joint Atomic Energy Intelligence Committee (JAEIC) on EMP issued in 2014 is factually erroneous and analytically unsound. I recommend that the Director of National Intelligence withdraw the JAEIC EMP Report and direct that the EMP Commission critique of the JAEIC EMP Report be circulated to all the recipients of the 2014 JAEIC EMP Report, which is a threat to national security by impeding progress on EMP understanding and protection.

Conclusions

The United States critical national infrastructure faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade EMP attack, and natural EMP from a solar superstorm. During the Cold War, the U.S. was primarily concerned about a high altitude nuclear-weapon generated EMP attack as a tactic by which the Soviet Union could suppress the ability of the U.S. national command authority and U.S. strategic forces to respond to a nuclear attack, and thus destroy the U.S. deterrence provided by assured nuclear retaliation. Within the last decade, newly nuclear-armed adversaries, including North Korea, have been developing the ability and threatening to carry out an EMP attack against the U.S. Such an attack would give countries that have only a small number of nuclear weapons the ability to cause widespread, long-lasting damage to U.S. critical national infrastructures, to the United States itself as a viable country, and to the survival of a majority of its population.

While during the Cold War major efforts were undertaken by the DoD to assure that the U.S. national command authority and U.S. strategic forces could survive and operate after an EMP attack, no major efforts were then thought necessary by the national leadership to protect critical national infrastructures, provided that nuclear deterrence was successful. With the development of small nuclear arsenals and long-range missiles by small, hostile, potentially unstable and irrational countries, including North Korea, the threat of a nuclear EMP attack against the U.S. becomes one of the few ways that such a country could inflict devastating damage to the U.S. Therefore, it is urgent that the U.S. national leadership address the EMP threat as a critical, existential issue, and give a high priority to assuring the necessary leadership is engaged and the necessary steps are taken to protect the country from EMP. Otherwise, foreign adversaries may reasonably consider such an attack as one which can gravely damage the U.S. by striking at its technological Achilles' heel, without having to overcome the U.S. military.

Protecting and defending the national electric grid and other critical infrastructures from EMP attack could be accomplished at reasonable cost and minimal disruption to the present systems that comprise our critical infrastructure; all commensurate with Trump Administration plans to repair and improve U.S. infrastructures, increase their reliability, and strengthen our homeland defense and military capability. Continued failure to address our country's vulnerability to high altitude nuclear weapon-generated EMP invites attack.