DR. PETER VINCENT PRY
STATEMENT FOR THE RECORD
JOINT HEARING BEFORE THE
SUBCOMMITTEE ON NATIONAL SECURITY
SUBCOMMITTEE ON THE INTERIOR
HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
Rayburn HOB Room 2247
May 13, 2015

The EMP Threat: The State of Preparedness Against the Threat of a Electromagnetic Pulse (EMP) Event

Natural EMP from a geomagnetic super-storm, like the 1859 Carrington Event or 1921 Railroad Storm, or nuclear EMP attack from terrorists or rogue states, as apparently practiced by North Korea during the nuclear crisis of 2013, are both existential threats that could kill up to 9 of 10 Americans through starvation, disease, and societal collapse. A natural EMP catastrophe or nuclear EMP attack could blackout the national electric grid for months or years and collapse all the other critical infrastructures--communications, transportation, banking and finance, food and water--necessary to sustain modern society and the lives of 310 million Americans.

Most the general public and most State governments are unaware of the EMP threat and that:

- **Political gridlock in Washington has prevented the Federal government from implementing any of the several cost-effective plans for protecting the national electric grid;**
- **Most State governments are unaware that they can protect that portion of the grid within their State and so protect their citizens from the catastrophic consequences of a national blackout;**
- **The electric grid is the keystone critical infrastructure necessary to recover all other critical infrastructures;**
- **Protection of the grid from EMP, which is the worst threat, will also enhance overall grid security against all other threats, including cyber attack, sabotage, and severe weather.**

All Hazards Strategy--EMP Protection Key

The Congressional EMP Commission warned that an "all hazards" strategy should be pursued to protect the electric grid and other critical infrastructures. An "all hazards" strategy means trying to find common solutions that protect against more than one threat--ideally against all threats.

The "all hazards" strategy is the most practical and most cost-effective solution to protecting the electric grid and other critical infrastructures. Electric grid operation and vulnerability is critically dependent upon two key technologies--Extra-High Voltage (EHV) transformers and Supervisory Control and Data Acquisition Systems (SCADAS).

EHV Transformers
EHV transformers are the technological foundation of our modern electronic civilization as they make it possible to transmit electric power over great distances. An EHV transformer typically is as large as a house, weighs hundreds of tons, costs millions of dollars, and cannot be mass produced but must be custom-made by hand. Making a single EHV transformer takes about 18 months. Annual worldwide production of EHV transformers is about 200 per year.

Unfortunately, although Nikolai Tesla invented the EHV transformer and the electric grid in the U.S., EHV transformers are no longer manufactured in the United States. Because of their great size and cost, U.S. electric utilities have very few spare EHV transformers. The U.S. must import EHV transformers made in Germany or South Korea, the only two nations in the world that make them for export.

An event that damages hundreds--or even as few as 9--of the 2,000 EHV transformers in the United States could plunge the nation into a protracted blackout lasting months or even years.

SCADAS
SCADAS are basically small computers that run the electric grid and all the critical infrastructures. For example, SCADAS regulate the flow of electric current through EHV transformers, the flow of natural gas or of water through pipelines, the flow of data through communications and financial systems, and operate everything from traffic control lights to the refrigerators in regional food warehouses.

SCADAS are ubiquitous in the civilian critical infrastructures, number in the millions, and are as indispensable as EHV transformers to running our modern electronic civilization.

An event that damages large numbers of SCADAS would put that civilization at risk.

Nuclear EMP--The Worst Threat
High-altitude nuclear EMP attack is the greatest single threat that could be posed to EHV transformers, SCADAS and other components of the national electric grid and other critical infrastructures. Nuclear EMP includes a high-frequency electromagnetic shockwave called E1 EMP that can potentially damage or destroy virtually any electronic system having a dimension of 18 inches or greater.

E1 EMP is unique to nuclear weapons.

Consequently, a high-altitude nuclear EMP event could cause broad damage of electronics and critical infrastructures across continental North America, while also causing deep damage to industrial and personal property, including to automobiles and personal computers.

Nuclear EMP can also produce E2 EMP, comparable to lightning.

In contrast, natural EMP from a geomagnetic super-storm generates no E1 EMP, only E3 EMP (technically called magneto-hydrodynamic EMP, or E3 for short). E3 EMP has such long wavelengths that it requires a large "antennae" of about 1 kilometer or more in length, such as

power lines, telephone lines, pipelines, and railroad tracks. E3 EMP cannot enter directly relatively small targets such as automobiles or personal computers.

However, while a geomagnetic super-storm would not directly damage relatively small electronic systems, a protracted nationwide blackout resulting from such a storm would within days stop everything. Personal computers cannot run for long on batteries, nor can automobiles run without gasoline.

Nuclear EMP can also produce E3 EMP comparable to or greater than a geomagnetic super-storm. Even a relatively low-yield nuclear weapon, like the 10-kiloton Hiroshima bomb, can generate an E3 EMP field powerful enough to damage EHV transformers.

The Congressional EMP Commission recommended protecting the electric grid and other critical infrastructures against nuclear EMP as the best basis for an "all hazards" strategy. Nuclear EMP may not be as likely as other threats, but it is by far the worst, the most severe, threat.

The EMP Commission found that if the electric grid can be protected and quickly recovered from nuclear EMP, the other critical infrastructures can also be recovered, with good planning, quickly enough to prevent mass starvation and restore society to normalcy. If EHV transformers, SCADAS and other critical components are protected from the worst threat--nuclear EMP--then they will survive, or damage will be greatly mitigated, from all lesser threats, including natural EMP from geomagnetic storms, severe weather, sabotage, and cyber attack.

The New "Lightning War"

The "all hazards" strategy recommended by the EMP Commission is not only the most cost-effective strategy--it is a necessary strategy. U.S. emergency planners tend to think of EMP, cyber, sabotage, severe weather, and geo-storms in isolation, as unrelated threats

However, potential foreign adversaries in their military doctrines and actual military operations appear to be planning an offensive "all hazards" strategy that would throw at the U.S. electric grid and civilian critical infrastructures--every possible threat simultaneously

Iran, North Korea, China and Russia appear to be perfecting what Moscow calls a "Revolution in Military Affairs" that is potentially more decisive than Nazi Germany's Blitzkrieg ("Lightning War") strategy that nearly conquered the western democracies during World War II. The New Lightning War would attack the electric grid and other critical infrastructures--the technological and societal Achilles Heel of electronic civilization--with coordinated employment of cyber, sabotage, and EMP attacks, possibly timed to leverage severe space or terrestrial weather.

While gridlock in Washington has prevented the Federal Government from protecting the national electric power infrastructure, threats to the grid--and to the survival of the American people--from EMP and other hazards are looming ever larger. Grid vulnerability to EMP and other threats is now a clear and present danger.

Geomagnetic Storms

Natural EMP from geomagnetic storms, caused when a coronal mass ejection from the Sun collides with the Earth's magnetosphere, poses a significant threat to the electric grid and the critical infrastructures, that all depend directly or indirectly upon electricity. Normal geomagnetic storms occur every year causing problems with communications and electric grids for nations located at high northern latitudes, such as Norway, Sweden, Finland and Canada.

For example, the 1989 Hydro-Quebec Storm blacked-out the eastern half of Canada in 92 seconds, melted an EHV transformer at the Salem, New Jersey nuclear power plant, and caused billions of dollars in economic losses.

In 1921 a geomagnetic storm ten times more powerful, the Railroad Storm, afflicted the whole of North America. It did not have catastrophic consequences because electrification of the U.S. and Canada was still in its infancy. The National Academy of Sciences estimates that if the 1921 Railroad Storm recurs today, it would cause a catastrophic nationwide blackout lasting 4-10 years and costing trillions of dollars.

The Carrington Event

The most powerful geomagnetic storm ever recorded is the 1859 Carrington Event, estimated to be ten times more powerful than the 1921 Railroad Storm and classed as a geomagnetic super-storm.

Natural EMP from the Carrington Event penetrated miles deep into the Atlantic Ocean and destroyed the just laid intercontinental telegraph cable. The Carrington Event was a worldwide phenomenon, causing fires in telegraph stations and forest fires from telegraph lines bursting into flames on several continents. Fortunately, in the horse and buggy days of 1859, civilization did not depend upon electrical systems.

Recurrence of a Carrington Event today would collapse electric grids and critical infrastructures all over the planet, putting at risk billions of lives. Scientists estimate that geomagnetic super-storms occur about every 100-150 years. The Earth is probably overdue to encounter another Carrington Event.

NASA warns that on July 22, 2012, a powerful solar flare narrowly missed the Earth that would have generated a geomagnetic super-storm, like the 1859 Carrington Event, and collapsed electric grids and life sustaining critical infrastructures worldwide.

The National Intelligence Council (NIC), that speaks for the entire U.S. Intelligence Community, published a major unclassified report in December 2012 *Global Trends 2030* that warns a geomagnetic super-storm, like recurrence of the 1859 Carrington Event, is one of only eight "Black Swans" that could by or before 2030 change the course of global civilization. The NIC concurs with the consensus view that another Carrington Event could recur at any time, possibly before 2030, and that, if it did, electric grids and critical infrastructures that support modern civilization could collapse worldwide.

NASA estimates that the likelihood of a geomagnetic super-storm is 12 percent per decade. This virtually guarantees that Earth will experience a natural EMP catastrophe in our lifetimes or that of our children.

NERC "Operational Procedures" Non-Solution

The North American Electric Reliability Corporation (NERC), the lobby for the electric power industry that is also supposed to set industry standards for grid security, claims it can protect the grid from geomagnetic super-storms by "operational procedures." Operational procedures would rely on satellite early warning of an impending Carrington Event to allow grid operators to shift around electric loads, perhaps deliberately brownout or blackout part or all of the grid in order to save it. NERC estimates operational procedures would cost the electric utilities almost nothing, about $200,000 dollars annually.

Critics rightly argue that NERC's proposed operational procedures is a non-solution designed as an excuse to avoid the expense of the only real solution--physically hardening the electric grid to withstand EMP.

The ACE satellite is aged and sometimes gives false warnings that are not a reliable basis for implementing operational procedures. While coronal mass ejections can be seen approaching Earth typically about three days before impact, the Carrington Event reached Earth in only 11 hours, and the Ace satellite cannot warn whether a geo-storm will hit the Earth until merely 20-30 minutes before impact.

Most recently, on September 19-20, 2014, the National Oceanic and Atmospheric Administration and NERC demonstrated again that they are unable to ascertain until shortly before impact whether a coronal mass ejection will cause a threatening geomagnetic storm on Earth.

There is no command and control system for coordinating operational procedures among the 3,000 independent electric utilities in the United States. Operational procedures routinely fail to prevent blackouts from normal terrestrial weather, like snowstorms and hurricanes. There is no credible basis for thinking that operational procedures alone would be able to cope with a geomagnetic super-storm--a threat unprecedented in the experience of NERC and the electric power industry.

NERC has not helped its case by being caught red handed peddling "junk science" that grossly underestimates the threat from another Carrington Event.

States Should EMP Harden Their Grids

NERC rejects the recommendation of the Congressional EMP Commission to physically protect the national electric grid from nuclear EMP attack by installing blocking devices, surge arrestors, faraday cages and other proven technologies. These measures would also protect the grid from the worst natural EMP from a geomagnetic super-storm like another Carrington Event. The estimated one time cost--$2 billion dollars--is what the United States gives away every year in foreign aid to Pakistan.

Yet Washington remains gridlocked between lobbying by NERC and the wealthy electric power industry on the one hand, and the recommendations of the Congressional EMP Commission and other independent scientific and strategic experts on the other hand. The States should not wait for Washington to act, but should act now to protect themselves.

Catastrophe from a geomagnetic super-storm may well happen sooner rather than later--and perhaps in combination with a nuclear EMP attack.

Paul Stockton, President Obama's former Assistant Secretary of Defense for Homeland Defense, on June 30, 2014, at the Electric Infrastructure Security Summit in London, warned an international audience that an adversary might coordinate nuclear EMP attack with an impending or ongoing geomagnetic storm to confuse the victim and maximize damage. Stockton notes that, historically, generals have often coordinated their military operations with the weather. For example, during World War II, General Dwight Eisenhower deliberately launched the D-Day invasion following a storm in the English Channel, correctly calculating that this daring act would surprise Nazi Germany.

Future military planners of the New Lightning War may well coordinate a nuclear EMP attack and other operations aimed at the electric grid and critical infrastructures with the ultimate space weather threat--a geomagnetic storm.

Severe Weather

Hurricanes, snow storms, heat waves and other severe weather poses an increasing threat to the increasingly overtaxed, aged and fragile national electric grid. So far, the largest and most protracted blackouts in the United States have been caused by severe weather.

For example, Hurricane Katrina (August 29, 2005), the worst natural disaster in U.S. history, blacked out New Orleans and much of Louisiana, the blackout seriously impeding rescue and recovery efforts. Lawlessness swept the city. Electric power was not restored to parts of New Orleans for months, making some neighborhoods a criminal no man's land too dangerous to live in. New Orleans has still not fully recovered its pre-Katrina population. Economic losses to the Gulf States region totaled $108 billion dollars.

Hurricane Sandy on October 29, 2012, caused blackouts in parts of New York and New Jersey that in some places lasted weeks. Again, as in Katrina, the blackout gave rise to lawlessness and seriously impeded rescue and recovery. Thousands were rendered homeless in whole or in part because of the protracted blackout in some neighborhoods. Partial and temporary blackouts were experienced in 24 States. Total economic losses were $68 billion dollars.

A heat-wave on August 14, 2003, caused a power line to sag into a tree branch, which seemingly minor incident began a series of cascading failures that resulted in the Great Northeast Blackout of 2003. Some 50 million Americans were without electric power--including New York City. Although the grid largely recovered after a day, disruption of the nation's financial capital was costly, resulting in estimated economic losses of about $6 billion dollars.

On September 18, 2014, a heat wave caused rolling brownouts and blackouts in northern California so severe that some radio commentators speculated that a terrorist attack on the grid might be underway.

NERC and Electric Utilities Underperform

Ironically, about one week earlier, on September 8-10, 2014, there was a security conference on threats to the national electric grid meeting in San Francisco. There executives from the electric power industry credited themselves with building robust resilience into the electric power grid. They even congratulated themselves and their industry with exemplary performance coping with and recovering from blackouts caused by hurricanes and other natural disasters.

The thousands of Americans left homeless due to Hurricanes Katrina and Sandy, the hundreds of businesses lost or impoverished in New Orleans and New York City, would no doubt disagree.

The U.S. Government Accountability Office (GAO), if it had jurisdiction to grade electric grid reliability during hurricanes, would almost certainly give the utilities a failing grade. Ever since Hurricane Andrew in 1992, the U.S. GAO has found serious fault with efforts by the Federal Emergency Management Agency, the Department of Homeland Security, and the Department of Defense to rescue and recover the American people from every major hurricane. Blackout of the electric grid, of course, seriously impedes the capability of FEMA, DHS, and DOD to do anything.

Since the utilities regulate themselves through the North American Electric Reliability Corporation, their uncritical view of their own performance reinforces a "do nothing" attitude in the electric power industry.

For example, after the Great Northeast Blackout of 2003, it took NERC a decade to propose a new "vegetation management plan" to protect the national grid from tree branches. NERC has been even more resistant and slow to respond to other much more serious threats, including cyber attack, sabotage, and natural EMP from geomagnetic storms.

As noted earlier, NERC flatly rejects responsibility to protect the grid from nuclear EMP attack.

New York and Massachusetts Protect Their Grids

New York Governor Andrew Cuomo and Massachusetts Governor Deval Patrick would not agree that NERC's performance during Hurricane Sandy was exemplary. Under the leadership of Governor Patrick, Massachusetts is spending $500 million to upgrade the security of its electric grid from severe weather. New York is spending a billion dollars to protect its grid from severe weather.

Unfortunately, both States are probably spending a lot more than they have to by focusing on severe weather, instead of an "all hazards" strategy to protect their electric grids.

The biggest impediment to recovering an electric grid from hurricanes is not fallen electric poles and downed power lines. When part of the grid physically collapses, an overvoltage can result that can damage all kinds of transformers, including EHV transformers, SCADAS and other vital

grid components. Video footage shown on national television during Hurricane Sandy showed spectacular explosions and fires erupting from transformers and other grid vital components caused by overvoltage.

If the grid is hardened to survive a nuclear EMP attack by installation of surge arrestors, it would easily survive overvoltage induced by hurricanes and other severe weather. This would cost a lot less than burying power lines underground and other measures being undertaken by New York and Massachusetts to fortify their grids against hurricanes--all of which will be futile if transformers and SCADAS are not protected against overvoltage.

According to a senior executive of New York's Consolidated Edison, briefing at the Electric Infrastructure Security Summit in London on July 1, 2014--Con Ed is taking some modest steps to protect part of the New York electric grid from nuclear EMP attack. This good news has not been reported anywhere in the press.

I asked the Con Ed executive why New York is silent about beginning to protect its grid from nuclear EMP? Loudly advertising this prudent step could have a deterrent effect on potential adversaries planning an EMP attack.

The Con Ed executive could offer no explanation.

New York City because of its symbolism as the financial and cultural capitol of the Free World, and perhaps because of its large Jewish population, has been the repeated target of terrorist attacks with weapons of mass destruction. A nuclear EMP attack centered over New York City, the warhead detonated at an altitude of 30 kilometers, would cover all the northeastern United States with an EMP field, including Massachusetts.

A practitioner of the New Lightning War may be more likely to exploit a hurricane, blizzard, or heat wave than a geomagnetic storm, when launching a coordinated cyber, sabotage, and EMP attack. Terrestrial bad weather is more commonplace than bad space weather.

New York and Massachusetts have both been frontline States in the war on terrorism. Nuclear EMP attack could potentially put in the frontlines--and in the crosshairs of a New Lightning War--all the States.

All the States should prepare themselves for all hazards in this age of the Electronic Blitzkrieg.

Sabotage--Kinetic Attacks

Kinetic attacks are a serious threat to the electric grid and are clearly part of the game plan for terrorists and rogue states. Sabotage of the electric grid is perhaps the easiest operation for a terrorist group to execute and would be perhaps the most cost-effective means, requiring only high-powered rifles, for a very small number of bad actors to wage asymmetric warfare--perhaps against all 310 million Americans.

Terrorists have figured out that the electric grid is a major societal vulnerability.

Terror Blackout in Mexico
On the morning of October 27, 2013, the Knights Templars, a terrorist drug cartel in Mexico, attacked a big part of the Mexican grid, using small arms and bombs to blast electric substations. They blacked-out the entire Mexican state of Mihoacan, plunging 420,000 people into the dark, isolating them from help from the Federales. The Knights went into towns and villages and publicly executed local leaders opposed to the drug trade.

Ironically, that evening in the United States, the National Geographic aired a television docudrama "American Blackout" that accurately portrayed the catastrophic consequences of a cyber attack that blacks-out the U.S. grid for ten days. The North American Electric Reliability Corporation and some utilities criticized "American Blackout" for being alarmist and unrealistic, apparently unaware that life had already anticipated art just across the porous border in Mexico.

Life had already anticipated art months earlier than "American Blackout", and not in Mexico, but in the United States.

The Metcalf Attack
On April 16, 2013, apparently terrorists or professional saboteurs practiced making an attack on the Metcalf transformer substation outside San Jose, California, that services a 450 megawatt power plant providing electricity to the Silicon Valley and the San Francisco area. NERC and the utility Pacific Gas and Electric (PG&E), that owns Metcalf, claimed that the incident was merely an act of vandalism, and discouraged press interest.

Consequently, the national press paid nearly no attention to the Metcalf affair for nine months.

Jon Wellinghoff, Chairman of the U.S. Federal Energy Regulatory Commission, conducted an independent investigation of Metcalf. He brought in the best of the best of U.S. special forces--the instructors who train the U.S. Navy SEALS. They concluded that the attack on Metcalf was a highly professional military operation, comparable to what the SEALS themselves would do when attacking a power grid.

Footprints suggested that a team of perhaps as many as six men executed the Metcalf operation. They knew about an underground communications tunnel at Metcalf and knew how to access it by removing a manhole cover (which required at least two men). They cut communications cables and the 911 cable to isolate the site. They had pre-surveyed firing positions. They used AK-47s, the favorite assault rifle of terrorists and rogue states. They knew precisely where to shoot to maximize damage to the 17 transformers at Metcalf. They escaped into the night just as the police arrived and have not been apprehended or even identified. They left no fingerprints anywhere, not even on the expended shell casings.

The Metcalf assailants only damaged but did not destroy the transformers--apparently deliberately. The Navy SEALS and U.S. FERC Chairman Wellinghoff concluded that the Metcalf operation was a "dry run", like a military exercise, practice for a larger and more ambitious attack on the grid to be executed in the future.

Military exercises never try to destroy the enemy, and try to keep a low profile so that the potential victim is not moved to reinforce his defenses. For example, Russian strategic bomber exercises only send a few aircraft to probe U.S. air defenses in Alaska, and never actually launch nuclear-armed cruise missiles. They want to probe and test our air defenses--not scare us into strengthening those defenses.

Chairman Wellinghoff was aware of an internal study by U.S. FERC that concluded saboteurs could blackout the national electric grid for weeks or months by destroying just nine crucial transformer substations.

Much to his credit, Jon Wellinghoff became so alarmed by his knowledge of U.S. grid vulnerability, and the apparent NERC cover-up of the Metcalf affair, that he resigned his chairmanship to warn the American people in a story published by the Wall Street Journal in February 2014. The Metcalf story sparked a firestorm of interest in the press and investigations by Congress.

Consequently, NERC passed, on an emergency basis, a new standard for immediately upgrading physical security for the national electric grid. PG&E promised to spend over $100 million over the next three years to upgrade physical security.

Terror Blackout of Yemen

On June 9, 2014, while world media attention was focused on the terror group Islamic State in Iraq and Syria (ISIS) overrunning northern Iraq, Al Qaeda in the Arabian Peninsula (AQAP) used mortars and rockets to destroy electric transmission towers to blackout all of Yemen, a nation of 16 cities and 24 million people.

AQAP's operation against the Yemen electric grid is the first time in history that terrorists have sunk an entire nation into blackout. The blackout went virtually unreported by the world press.

Metcalf Again--NERC and Utilities Negligent

Two months later, amid growing fears that ISIS may somehow act on its threats to attack America, on August 27, 2014, parties unknown again broke into the Metcalf transformer substation and escaped PG&E security guards and the police. PG&E claims that the second Metcalf affair is, again, merely vandalism.

Yet after NERC's emergency new physical security standards and PG&E's alleged massive investment in improved security--Metcalf should have been the Rock of Gibraltar of the North American electric grid. If terrorists or someone is planning an attack on the U.S. electric grid, Metcalf would be the perfect place to test the supposedly strengthened security of the national grid.

Does stolen equipment prove that Metcalf-2 was a burglary? In the world of spies and saboteurs, mock burglary is a commonplace device for covering-up an intelligence operation, and hopefully quelling fears and keeping the victim unprepared.

If PG&E is telling the truth, and the second successful operation against Metcalf is merely by vandals--this is an engraved invitation by ISIS or Al Qaeda or rogue states to attack the U.S. electric grid. It means that all of PG&E and NERC's vaunted security improvements cannot protect Metcalf from the stupidest of criminals, let alone from terrorists.

About one month later, on September 23, 2014, another investigation of PG&E security at transformer substations, including Metcalf, reported that the transformer substations are still not secure. Indeed, at one site a gate was left wide open. Former CIA Director R. James Woolsey, after reviewing the investigation results, concluded, "Overall, it looks like there is essentially no security."

States Should EMP Harden Their Grids

State governments and their Public Utility Commissions should exercise aggressive oversight to ensure that the transformer substations and electric grids in their States are safe and secure. The record of NERC and the electric utilities indicates they cannot be trusted to provide for the security of the grid.

State governments can protect their grid from sabotage by the "all hazards" strategy that protects against the worst threat--nuclear EMP attack.

For example, faraday cages to protect EHV transformers and SCADAS colonies from EMP would also screen from view these vital assets so they could not be accurately targeted by high-powered rifles, as is necessary in order to destroy them by small arms fire. The faraday cages could be made of heavy metal or otherwise fortified for more robust protection against more powerful weapons, like rocket propelled grenades.

Surge arrestors to protect EHV transformers and SCADAS from nuclear EMP would also protect the national grid from collapse due to sabotage. The U.S. FERC scenario where terrorists succeed in collapsing the whole national grid by destroying merely nine transformer substations works only because of cascading overvoltage. When the nine key substations are destroyed, megawatts of electric power gets suddenly dumped onto other transformers, which in their turn get overloaded and fail, dumping yet more megawatts onto the grid. Cascading failures of more and more transformers ultimately causes a protracted national blackout.

This worst case scenario for sabotage could not happen if the transformers and SCADAS are protected against nuclear EMP--which is a more severe threat than any possible system-generated overvoltage.

Cyber Attack

Cyber attacks, the use of computer viruses and hacking to invade and manipulate information systems and SCADAS, is almost universally described by U.S. political and military leaders as the greatest threat 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.

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 (Claudette

Roulo, *DoD News*, Armed Force Press Service): "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."

Cyber Hype?

Skeptics claim that the catastrophic scenarios envisioned for cyber warfare are grossly exaggerated, in part to justify costly cyber programs wanted by both the Pentagon and industry at a time of scarce defense dollars. Many of the skeptical arguments about the limitations of hacking and computer viruses are technically correct.

However, it is not widely understood that foreign military doctrines define "information warfare" and "cyber warfare" as encompassing kinetic attacks and EMP attack--which is an existential threat to the United States.

Thomas Rid's book *Cyber War Will Not Take Place* (Oxford University Press, 2013) exemplifies the viewpoint of a growing minority of highly talented cyber security experts and scholars who think there is a conspiracy of governments and industry to hype the cyber threat. Rid's bottom line is that hackers and computer bugs are capable of causing inconvenience--not apocalypse. Cyber attacks can deny services, damage computers selectively but probably not wholesale, and steal information, according to Rid. He does not rule out that future hackers and viruses could collapse the electric grid, concluding such a feat would be, not impossible, but nearly so.

In a 2012 BBC interview, Rid chastised then Secretary of Defense Leon Panetta for claiming that Iran's Shamoon Virus, used against the U.S. banking system and Saudi Arabia's ARAMCO, could foreshadow a "Cyber Pearl Harbor" and for threatening military retaliation against Iran. Rid told the BBC that the world has, "Never seen a cyber attack kill a single human being or destroy a building."

Cyber security expert Bruce Schneier claims, "The threat of cyberwar has been hugely hyped" to keep growing cyber security programs at the Pentagon's Cyber Command, the Department of Homeland Security, and new funding streams to Lockheed Martin, Raytheon, Century Link, and AT&T, who are all part of the new cyber defense industry. The Brookings Institute's Peter Singer wrote in November 2012, "Zero. That is the number of people who have been hurt or killed by cyber terrorism." Ronald J. Delbert, author of *Black Code: Inside the Battle for Cyberspace*, a lab director and professor at the University of Toronto, accuses RAND and the U.S. Air Force of exaggerating the threat from cyber warfare.

Peter Sommer of the London School of Economics and Ian Brown of Oxford University, in *Reducing Systemic Cybersecurity Risk*, a study for Europe's Organization for Economic Cooperation and Development, are far more worried about natural EMP from the Sun than computer viruses: "a catastrophic cyber incident, such as a solar flare that could knock out satellites, base stations and net hardware" makes computer viruses and hacking "trivial in comparison."

Aurora Experiment
The now declassified Aurora experiment is the empirical basis for the claim that a computer virus might be able to collapse the national electric grid. In Aurora, a virus was inserted into the SCADAS running a generator, causing the generator to malfunction and eventually destroy itself.

However, using a computer virus to destroy a single generator does not prove it is possible or likely that an adversary could destroy all or most of the generators in the United States. Aurora took a protracted time to burn out a generator--and no intervention by technicians attempting to save the generator was allowed, as would happen in a nationwide attack, if one could be engineered.

Nor is there a single documented case of a even a local blackout being caused in the United States by a computer virus or hacking--which surely would have happened by now, if vandals, terrorists, or rogue states could attack U.S. critical infrastructures easily by hacking.

Stuxnet Worm and Gaza Cyber War
Even the Stuxnet Worm, the most successful computer virus so far, reportedly according to White House sources jointly engineered by the U.S. and Israel to attack Iran's nuclear weapons program, proved a disappointment. Stuxnet succeeded in damaging only 10 percent of Iran's centrifuges for enriching uranium, and did not stop or even significantly delay Tehran's march towards the bomb.

During the recently concluded Gaza War between Israel and Hamas, a major cyber campaign using computer bugs and hacking was launched against Israel by Hamas, the Syrian Electronic Army, Iran, and by sympathetic hackers worldwide. The Gaza War was a Cyber World War against Israel.

The Institute for National Security Studies, at Tel Aviv University, in "The Iranian Cyber Offensive during Operation Protective Edge" (August 26, 2014) reports that the cyber attacks caused inconvenience and in the worst case some alarm, over a false report that the Dimona nuclear reactor was leaking radiation: "...the focus of the cyber offensive...was the civilian internet. Iranian elements participated in what the C4I officer described as an attack unprecedented in its proportions and the quality of its targets....The attackers had some success when they managed to spread a false message via the IDF's official Twitter account saying that the Dimona reactor had been hit by rocket fire and that there was a risk of a radioactive leak."

However, the combined hacking efforts of Hamas, SEA, Iran and hackers worldwide did not blackout Israel or significantly impede Israel's war effort.

Dragonfly
But tomorrow is always another day. Cyber warriors are right to worry that perhaps someday someone will develop the cyber bug version of an atomic bomb. Perhaps such a computer virus already exists in a foreign laboratory, awaiting use in a future surprise attack.

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 knows 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 SCADAS that can disrupt the operation of electric power plants in a future crisis.

States Should EMP Harden Their Grids

Cyber warfare is an existential threat to the United States, not because of computer viruses and hacking alone, but as envisioned in the military doctrines of potential adversaries whose plans for an all-out Cyber Warfare Operation include the full spectrum of military capabilities--including EMP attack. In 2011, a U.S. Army War College study *In The Dark: Planning for a Catastrophic Critical Infrastructure Event* 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 by Maxim Shepovalenko (*Military-Industrial Courier* July 3, 2013), 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."

Cyber warriors who think narrowly in terms of computer hacking and viruses invariably propose anti-hacking and anti-viruses as solutions. Such a solution will result in an endless virus versus anti-virus software arms race that may ultimately prove unaffordable and futile.

States can protect themselves from the worst case cyber scenario by following the "all hazards" strategy recommended by the Congressional EMP Commission. The worst case scenario envisions a computer virus infecting the SCADAS that regulate the flow of electricity into EHV transformers, damaging the transformers with overvoltage, and causing a protracted national blackout.

But if the transformers are protected with surge arrestors against the worst threat--nuclear EMP attack--they would be unharmed by the worst possible overvoltage that might be system generated by any computer virus. This EMP hardware solution would provide a permanent and relatively inexpensive fix to what is the extremely expensive and apparently endless virus versus anti-virus software arms race that is ongoing in the new cyber defense industry.

EMP Attack

High-altitude nuclear electromagnetic pulse attack is the most severe threat to the electric grid and other critical infrastructures. A nuclear EMP attack would likely be more damaging than a geomagnetic super-storm, the worst case of severe weather, sabotage by kinetic attacks, or cyber attack.

Contrary to non-experts sometimes cited in the press, there is more empirical data on nuclear EMP and more analysis and a better understanding of EMP effects on electronic systems and infrastructures than almost any other threat, except severe weather. In addition to the 1962 STARFISH PRIME high-altitude nuclear test that generated EMP that damaged electronic systems in Hawaii and elsewhere, the Department of Defense has decades of atmospheric and

underground nuclear test data relevant to EMP. And defense scientists have for over 50 years studied EMP effects on electronics in simulators. Most recently, the Congressional EMP Commission made its threat assessment by testing a wide range of modern electronics crucial to critical infrastructures in EMP simulators.

There is a scientific and strategic consensus behind the Congressional EMP Commission's assessment that a nuclear EMP attack would have catastrophic consequences for the United States, but that "correction is feasible and well within the Nation's means and resources to accomplish." Every major U.S. Government study to examine the EMP threat and solutions concurs with the EMP Commission, including the Congressional Strategic Posture Commission (2009), the U.S. Department of Energy and North American Electric Reliability Corporation (2010), and the U.S. Federal Energy Regulatory Commission interagency report, coordinated with the White House, Department of Defense, and Oak Ridge National Laboratory (2010).

Not one major U.S. Government study dissents from the consensus that nuclear EMP attack would be catastrophic, and that protection is achievable and necessary.

Russian Nuclear EMP Tests

STARFISH PRIME is not the only high-altitude nuclear EMP test.

The Soviet Union (1961-1962) conducted a series of high-altitude nuclear EMP tests over what was then its own territory--not once but seven times--using a variety of warheads of different designs. The EMP fields from six tests covered Kazakhstan, an industrialized area larger than Western Europe. In 1994, during a thaw in the Cold War, Russia shared the results from one of its nuclear EMP tests, that used their least efficient warhead design for EMP--it collapsed the Kazakhstan electric grid, damaging transformers, generators and all other critical components.

The USSR during the Kazakhstan high-altitude EMP experiments tested some low-yield warheads, at least one probably an Enhanced Radiation Warhead that emitted large quantities of gamma rays, that generate the E1 EMP electromagnetic shockwave. It is possible that the USSR developed their Super-EMP Warhead early in the Cold War as a secret super-weapon.

Perhaps the most important lesson to be learned from the USSR's unconscionable and evil nuclear EMP tests against their own people is that there is no excuse to be vulnerable to EMP. The Soviets apparently quickly repaired the damage to Kazakhstan's electric grid and other critical infrastructures, thereby proving definitively that with smart planning and good preparedness it is possible to survive and recover from an EMP catastrophe.

Nuclear EMP Attacks by Missile, Aircraft and Balloon

A nuclear weapon detonated at an altitude of 200 kilometers over the geographic center of the United States would create an EMP field potentially damaging to electronics over all the 48 contiguous States. The Congressional EMP Commission concluded that virtually any nuclear weapon, even a crude first generation atomic bomb having a low yield, could potentially inflict an EMP catastrophe.

However, the EMP Commission also found that Russia, China, and probably North Korea have nuclear weapons specially designed to generate extraordinarily powerful EMP fields-- called by the Russians Super-EMP weapons--and this design information may be widely proliferated: "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."

Nor is a sophisticated long-range missile required to make an EMP attack.

Any short-range missile or other delivery vehicle that can deliver a nuclear weapon to an altitude of 30 kilometers or higher can make a potentially catastrophic EMP attack on the United States. Although a nuclear weapon detonated at 30 kilometers altitude could not cover the entire continental U.S. with an EMP field, the field would still cover a very large multi-state region--and be more intense. Lowering the height-of-burst (HOB) for an EMP attack decreases field radius, but increases field strength.

An EMP attack at 30 kilometers HOB anywhere over the eastern half of the U.S. would cause cascading failures far beyond the EMP field and collapse the Eastern Grid, that generates 75 percent of U.S. electricity. The nation could not survive without the Eastern Grid.

A Scud missile launched from a freighter could perform such an EMP attack. Over 30 nations have Scuds, as do some terrorist groups and private collectors. Scuds are available for sale on the world and black markets.

Any aircraft capable of flying Mach 1 could probably do a zoom climb to 30 kilometers altitude to make an EMP attack, if the pilot is willing to commit suicide.

Even a meteorological balloon could be used to loft a nuclear weapon 30 kilometers high to make an EMP attack. During the period of atmospheric nuclear testing in the 1950s and early 1960s, more nuclear weapons were tested at altitude by balloon than by bombers or missiles.

Nuclear EMP Effects on Critical Infrastructures

Nuclear EMP is like super-lightning. The electromagnetic shockwave unique to nuclear weapons, called E1 EMP, travels at the speed of light, potentially injecting into electrical systems thousands of volts in a nanosecond--literally a million times faster than lightning, and much more powerful. Russian open source military writings describe their Super-EMP Warhead as generating 200,000 volts/meter, which means that the target receives 200,000 volts for every meter of its length. So, for example, if the cord on a PC is two meters long, it receives 400,000 volts. An automobile 4 meters long could receive 800,000 volts, unless it is parked underground or protected in some other way.

No other threat can cause such broad and deep damage to all the critical infrastructures as a nuclear EMP attack. A nuclear EMP attack would collapse the electric grid, blackout and directly damage transportation systems, industry and manufacturing, telecommunications and computers, banking and finance, and the infrastructures for food and water.

Jetliners carry about 500,000 passengers on over 1,000 aircraft in the skies over the U.S. at any given moment. Many, most or virtually all of these would crash, depending upon the strength of the EMP field. Satellite navigation and communication systems would be knocked out, as would ground and air traffic control systems, necessitating that any surviving aircraft land "blind."

Cars, trucks, trains and traffic control systems would be damaged. In the best case, even if only a few percent of ground transportation vehicles are rendered inoperable, massive traffic jams would result. In the worst case, virtually all vehicles of all kinds would be rendered inoperable. In any case, all vehicles would stop operating when they run out of gasoline. The blackout would render gas stations inoperable and paralyze the infrastructure for synthesizing and delivering petroleum products and fuels of all kinds.

Industry and manufacturing would be paralyzed by collapse of the electric grid. Damage to SCADAS and safety control systems would likely result in widespread industrial accidents, including gas line explosions, chemical spills, fires at refineries and chemical plants producing toxic clouds.

Seven days after the commencement of blackout, emergency generators at nuclear reactors would run out of fuel. The reactors and nuclear fuel rods in cooling ponds would meltdown and catch fire, as happened in the nuclear disaster at Fukushima, Japan. The 104 U.S. nuclear reactors, located mostly among the populous eastern half of the United States, could cover vast swaths of the nation with dangerous plumes of radioactivity.

Cell phones, personal computers, the internet, and the modern electronic economy that supports personal and big business cash, credit, debit, stock market and other transactions and record keeping would cease operations. The Congressional EMP Commission warns that society could revert to a barter economy.

Worst of all, about 72 hours after the commencement of blackout, when emergency generators at the big regional food warehouses cease to operate, the nation's food supply will begin to spoil. Supermarkets are resupplied by these large regional food warehouses that are, in effect, the national larder, collectively having enough food to sustain the lives of 310 million Americans for about one month, at normal rates of consumption. The Congressional EMP Commission warns that as a consequence of the collapse of the electric grid and other critical infrastructures, "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."

The EMP Commission estimates that a nationwide blackout lasting one year could kill up to 9 of 10 Americans through starvation, disease, and societal collapse.

Nuclear EMP Threat Is Real

The nuclear EMP threat is not merely theoretical, but real.

"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," according to the Congressional EMP

Commission, "Indeed, as recently as May 1999, during the NATO bombing of the former Yugoslavia, high-ranking members of the Russian Duma, meeting with a U.S. congressional delegation to discuss the Balkans conflict, raised the specter of a Russian EMP attack that would paralyze the United States."

Russia has made many nuclear threats against the U.S. since 1999, which are reported in the western press only rarely. On December 15, 2011, Pravda, the official mouthpiece of the Kremlin, gave this advice to the United States in "A Nightmare Scenario For America":

> *No missile defense could prevent...EMP...No one seriously believes that U.S. troops overseas are defending "freedom" or defending their country.... Perhaps they ought to close the bases, dismantle NATO and bring the troops home where they belong before they have nothing to come home to and no way to get there.*

On June 1, 2014, Russia Today, a Russian television news show, also broadcast to the West in English, predicted that the United States and Russia would be in a nuclear war by 2016.

Iran, the world's leading sponsor of international terrorism, openly writes about making a nuclear EMP attack to eliminate the United States. Iran has practiced missile launches that appear to be training and testing warhead fusing for a high-altitude EMP attack--including missile launching for an EMP attack from a freighter. An EMP attack launched from a freighter could be performed anonymously, leaving no fingerprints, to foil deterrence and escape retaliation.

"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," cautions the EMP Commission in its 2004 report, "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."

On April 16, 2013, North Korea apparently simulated a nuclear EMP attack against the United States, orbiting its KSM-3 satellite over the U.S. at the optimum trajectory and altitude to place a peak EMP field over Washington and New York and blackout the Eastern Grid, that generates 75 percent of U.S. electricity. On the very same day, as described earlier, parties unknown executed a highly professional commando-style sniper attack on the Metcalf transformer substation that is a key component of the Western Grid.

A few months later, in July 2013, North Korean freighter *Chon Chong Gang* transited the Gulf of Mexico carrying nuclear-capable SA-2 missiles in its hold on their launchers. The missiles had no warheads, but the event demonstrated North Korea's capability to execute a ship-launched nuclear EMP attack from U.S. coastal waters anonymously, to escape U.S. retaliation. The missiles were only discovered, hidden under bags of sugar, because the freighter tried returning to North Korea through the Panama Canal and past inspectors.

What does all this signify?

Connect these dots: North Korea's apparent practice EMP attack with its KSM-3 satellite; the simultaneous "dry run" sabotage attack at Metcalf; North Korea's possible practice for a ship-launched EMP attack a few months later; and cyber attacks from various sources were happening all the time, and are happening every day. These suggest the possibility that in 2013 at least North Korea may have exercised against the United States an all-out combined arms operation aimed at targeting U.S. critical infrastructures--the New Lightning War.

Or are these coincidences merely accidental?

Is it also mere happenstance that Metcalf services the Silicon Valley, that reportedly developed the Stuxnet Worm that attacked Iran's nuclear program, for which transgression the Iranian Revolutionary Guard swore revenge? Iran and North Korea are by treaty strategic partners and closely cooperate in their scientific and military programs. With North Korean help, Iran too has orbited satellites on trajectories consistent with practicing a surprise nuclear EMP attack on the United States.

Non-Nuclear EMP Weapons

Radio-Frequency Weapons (RFWs) are non-nuclear weapons that use a variety of means, including explosively driven generators, to emit an electromagnetic pulse similar to the E1 EMP from a nuclear weapon, except less energetic and of much shorter radius. The range of RF Weapons is rarely more than one kilometer.

RF Weapons can be built relatively inexpensively using commercially available parts and design information available on the internet. In 2000 the Terrorism Panel of the House Armed Services Committee conducted an experiment, hiring an electrical engineer and some students to try building an RFW on a modest budget, using design information available on the internet, made from parts purchased at Radio Shack.

They built two RF Weapons in one year, both successfully tested at the U.S. Army proving grounds at Aberdeen. One was built into a Volkswagen bus, designed to be driven down Wall Street to disrupt stock market computers and information systems and bring on a financial crisis. The other was designed to fit in the crate for a Xerox machine so it could be shipped to the Pentagon, sit in the mailroom, and burn-out Defense Department computers.

EMP simulators that can be carried and operated by one man, and used as an RF Weapon, are available commercially. For example, one U.S. company advertises for sale an "EMP Suitcase" that looks exactly like a metal suitcase, can be carried and operated by one man, and generates 100,000 volts/meter over a short distance. The EMP Suitcase is not intended to be used as a weapon, but as an aid for designing factories that use heavy duty electronic equipment that emit electromagnetic transients, so the factory does not self-destruct.

But a terrorist, criminal, or madman, armed with the EMP Suitcase, could potentially destroy electric grid SCADAS or an EHV transformer and blackout a city. Thanks to RF Weapons, we have arrived at a place where the technological pillars of civilization for a major metropolitan area could be toppled by a single individual.

The EMP Suitcase can be purchased without a license by anyone.

Terrorists armed with RF Weapons might use unclassified computer models to duplicate the U.S. FERC study and figure out which nine crucial transformer substations need to be attacked in order to blackout the entire national grid for weeks or months. RFWs would offer significant operational advantages over assault rifles and bombs. Something like the EMP Suitcase could be put in the trunk of a car, parked and left outside the fence of an EHV transformer or SCADA colony, or hidden in nearby brush or a garbage can, while the bad guys make a leisurely getaway. If the EMP fields are strong enough, it would be just as effective as, and far less conspicuous than, dropping a big bomb to destroy the whole transformer substation. Maximum effect could be achieved by penetrating the security fence and hiding the RF Weapon somewhere even closer to the target.

Some documented examples of successful attacks using Radio Frequency Weapons, and accidents involving electromagnetic transients, are described in the 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):

--"In the Netherlands, an individual disrupted a local bank's computer network because he was turned down for a loan. He constructed a Radio Frequency Weapon the size of a briefcase, which he learned how to build from the Internet. Bank officials did not even realize that they had been attacked or what had happened until long after the event."
--"In St. Petersburg, Russia, a criminal robbed a jewelry store by defeating the alarm system with a repetitive RF generator. Its manufacture was no more complicated than assembling a home microwave oven."
--"In Kzlyar, Dagestan, Russia, Chechen rebel commander Salman Raduyev disabled police radio communications using RF transmitters during a raid."
--"In Russia, Chechen rebels used a Radio Frequency Weapon to defeat a Russian security system and gain access to a controlled area."
-- "Radio Frequency Weapons were used in separate incidents against the U.S. Embassy in Moscow to falsely set off alarms and to induce a fire in a sensitive area."
--"March 21-26, 2001, there was a mass failure of keyless remote entry devices on thousands of vehicles in the Bremerton, Washington, area...The failures ended abruptly as federal investigators had nearly isolated the source. The Federal Communications Commission (FCC) concluded that a U.S. Navy presence in the area probably caused the incident, although the Navy disagreed."
--"In 1999, a Robinson R-44 news helicopter nearly crashed when it flew by a high frequency broadcast antenna."
--"In the late 1980s, a large explosion occurred at a 36-inch diameter natural gas pipeline in the Netherlands. A SCADA system, located about one mile from the naval port of Den Helder, was affected by a naval radar. The RF energy from the radar caused the SCADA system to open and close a large gas flow-control valve at the radar scan frequency, resulting in pressure waves that traveled down the pipe and eventually caused the pipeline to explode."

--"In June 1999 in Bellingham, Washington, RF energy from a radar induced a SCADA malfunction that caused a gas pipeline to rupture and explode."
--"In 1967, the *USS Forrestal* was located at Yankee Station off Vietnam. An A4 Skyhawk launched a Zuni rocket across the deck. The subsequent fire took 13 hours to extinguish. 134 people died in the worst U.S. Navy accident since World War II. EMI [Electro-Magnetic Interference, Pry] was identified as the probable cause of the Zuni launch."
--North Korea used an 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 as reported in "Massive GPS Jamming Attack By North Korea" (*GPSWORLD.COM*, May 8, 2012).

Protecting the electric grid and other critical infrastructures from nuclear EMP attack will also protect them from the lesser threat posed by Radio Frequency Weapons.

States Should EMP Harden Their Grids

States should harden their electric grids against nuclear EMP attack because there is a clear and present danger, because protecting against nuclear EMP will mitigate all lesser threats, and because both the federal government in Washington and the electric power industry have failed to protect the people from the existential peril that is an EMP catastrophe.

In the U.S. Congress, bipartisan bills with strong support, such as the GRID Act and the SHIELD Act, that would protect the electric grid from nuclear and natural EMP, have been stalled for a half-decade, blocked by corruption and lobbying by powerful utilities.

The U.S. Federal Energy Regulatory Commission has published interagency reports acknowledging that nuclear EMP attack is an existential threat against which the electric grid must be protected. But U.S. FERC claims to lack legal authority to require the North American Electric Reliability Corporation and the electric utilities to protect the grid.

"Given the national security dimensions to this threat, there may be a need to act quickly to act in a manner where action is mandatory rather than voluntary and to protect certain information from public disclosure," said Joseph McClelland, Director of FERC's Office of Energy Projects, testifying in May 2011 before the Senate Energy and Natural Resources Committee. "The commission's legal authority is inadequate for such action."

Others think U.S. FERC has sufficient legal authority to protect the grid, but lacks the will to do so because of an incestuous relationship with the NERC.

NERC and the electric power industry deny that it is their responsibility to protect the grid from nuclear EMP attack. NERC thinks it is not their job, but the job of the Department of Defense, to protect the United States from nuclear EMP attack, so argued NERC President and CEO, Gerry Cauley, in his May 2011 testimony before the Senate Energy and Natural Resources Committee. Mark Lauby, NERC's reliability manager, is quoted by Peter Behr in his *EENEWS* article (August 26, 2011) that "...the terrorist scenario--foreseen as the launch of a crude nuclear

weapon on a version of a SCUD missile from a ship off the U.S. coast--is the government's responsibility, not industry's."

But DOD can protect the grid only by waging preventive wars against countries like Iran, North Korea, China and Russia, or by vast expansion and improvement of missile defenses costing tens of billions of dollars--none of which may stop the EMP threat.

Preventive wars would make an EMP attack more likely, perhaps inevitable. It is not worth spending thousands of lives and trillions of dollars on wars, just so NERC and the utilities can avoid a small increase in electric bills for EMP hardening the grid. U.S. FERC estimates EMP hardening would cost the average ratepayer an increase in their electric bill of 20 cents annually.

The Department of Defense has no legal authority to EMP harden the privately owned electric grid. Such protection is supposed to be the job of NERC and the utilities.

Most alarming, NERC and the utilities do not appear to know their jobs, and are already in panic and despair over the challenges posed by severe weather, cyber threats, and geomagnetic storms. Peter Behr in an article published in *Energy Wire* (September 12, 2014) reports that at an electric grid security summit, Gary Leidich, Board Chairman of the Western Electricity Coordinating Council--which oversees reliability and security for the Western Grid--appears overwhelmed, as if he wants to escape his job, crying: "Who is really responsible for reliability? And who has the authority to do something about it?"

"The biggest cyber threat is from an electromagnetic pulse, which in the military doctrines of our potential adversaries would be part of an all-out cyber war.", writes former Speaker of the House, Newt Gingrich, in his article "The Gathering Cyber Storm" (*CNN*, August 12, 2013). Gingrich warns that NERC "should lead, follow or get out of the way of those who are trying to protect our nation from a cyber catastrophe. Otherwise, the Congress that certified it as the electric reliability organization can also decertify it."

Much to their credit, a few in the electric power industry understand the necessity of protecting the grid from nuclear EMP attack, have broken ranks with NERC, and are trying to meet the crisis. John Houston of Centerpoint Energy in Texas; Terry Boston of PJM, the largest grid in North America (located in the midwest); and Con Ed in New York--all are trying to protect their grids from nuclear EMP.

State Governors and State Legislatures need to come to the rescue. States have a duty to their citizens to fill the gap in homeland security and public safety when the federal government, and the utilities, fail.

State governments and their Public Utility Commissions have the legal authority and the moral obligation to, where necessary, compel the utilities to secure the grid against all hazards. State governments have an obligation to help and oversee and ensure that grid security is being done right by those utilities that act voluntarily.

Failing to protect the grid from nuclear EMP attack is failing to protect the nation from all hazards.

Regulatory Malfeasance

As noted repeatedly elsewhere, Washington's process for regulating the electric power industry has never worked well, in fact has always been broken. The electric power industry is the only civilian critical infrastructure that is allowed to regulate itself.

The North American Electric Reliability Corporation is the industry's former trade association, which continues to act as an industry lobby. NERC is not a U.S. government agency. It does not represent the interests of the people. NERC in its charter answers to its "stakeholders"--the electric utilities that pay for NERC, including NERC's highly salaried executives and staff.

The U.S. Federal Energy Regulatory Commission, the U.S. government agency that is supposed to partner with NERC in protecting the national electric grid, has publicly testified before Congress that 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. Federal Aviation Administration (FAA), the U.S. Department of Transportation (DOT), or the U.S. Food and Drug Administration (FDA):

--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 airline passengers.
--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.
--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 FAA, DOT, FDA or any other U.S. government regulatory agency, the Federal Energy Regulatory Commission does not have legal authority to compel the industry it is supposed to regulate to act in the public interest. For example, U.S. FERC lacks legal power to direct NERC and the electric utilities to install blocking devices, surge arrestors, faraday cages or other protective devices to save the grid, and the lives of millions of Americans, from a natural or nuclear EMP catastrophe. Or so the FERC has testified to the Congress.

Congress has responded to this dilemma by introducing bipartisan bills, the SHIELD Act and the GRID Act, to empower U.S. FERC to protect the grid from an EMP catastrophe. Lobbying by NERC has stalled both bills for years.

Currently, 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 the electric power industry.

Historically, NERC typically takes years to develop standards to protect the grid that will pass industry approval. For example, NERC took a decade to propose a "vegetation management"

standard to protect the grid from tree branches in 2012. This after ruminating for ten years over the tree branch induced Great Northeast Blackout of 2003, that plunged 50 million Americans into the dark.

Once NERC proposes a standard to U.S. FERC, FERC cannot modify the standard, but must accept or reject the proposed standard. If U.S. FERC rejects the proposed standard, NERC gets to go back to the drawing board, and the process starts all over again.

The NERC-FERC arrangement is a formula for thwarting effective U..S. government regulation of the electric power industry. Fortunately, Governors, State Legislatures and their Public Utility Commissions have legal power to compel utilities to protect the grid from natural and nuclear EMP and other threats.

Critics argue that the U.S. Federal Energy Regulatory Commission is corrupt--because of a too cozy relationship with NERC and a rotating door between FERC and the electric power industry--and cannot be trusted to secure the grid, even if given legal powers to do so. U.S. FERC's approval of NERC's hollow standard for geomagnetic storms appears proof positive that Washington is too corrupt to be trusted.

NERC's Hollow GMD Protection Standard

Observers serving on NERC's Geo-Magnetic Disturbance Task Force, that developed the NERC standard for grid protection against geomagnetic storms, have denounced the NERC GMD Standard and published papers exposing, not merely that the Standard is inadequate, but that it is hollow, a pretended or fake Standard. These experts opposed to the NERC GMD Standard include the foremost authorities on geomagnetic storms and electric grid vulnerability in the Free World. See:

--John G. Kappenman and Dr. William A. Radasky, *Examination of NERC GMD Standards and Validation of Ground Models and Geo-Electric Fields Proposed in this NERC GMD Standard*, Storm Analysis Consultants and Metatech Corporation, July 30, 2014 (Executive Summary appended to this chapter).
--*EIS Council Comments on Benchmark GMD Event for NERC GMD Task Force Consideration*, Electric Infrastructure Security Council, May 21, 2014.
--Thomas Popik and William Harris for The Foundation for Resilient Societies, *Reliability Standard for Geomagnetic Disturbance Operations*, Docket No. RM14-1-000, critiques submitted to U.S. FERC on March 24, July 21, and August 18, 2014.

Kappenman and Radasky, who served on the Congressional EMP Commission and are among the world's foremost scientific and technical experts on geomagnetic storms and grid vulnerability, warn that NERC's GMD Standard consistently underestimates the threat from geo-storms: "When comparing...actual geo-electric fields with NERC model derived geo-electric fields, the comparisons show a systematic under-prediction in all cases of the geo-electric field by the NERC model."

The Foundation for Resilient Societies, that includes on its Board of Advisors a brain trust of world class scientific experts--including Dr. William Graham who served as President Reagan's

Science Advisor, director of NASA, and Chairman of the Congressional EMP Commission--concludes from their participation on the NERC GMD Task Force that NERC "cooked the books" to produce a hollow GMD Standard:

> *The electric utility industry clearly recognized in this instance how to design a so-called "reliability standard" that, though foreseeably ineffective in a severe solar storm, would avert financial liability to the electric utility industry even while civil society and its courts might collapse from longer-term outages. In this instance and others, a key feature of the NERC standard-setting process was to progressively water down requirements until the proposed standard obviously benefitted the ballot participants and therefore could pass. In the process, any remaining public benefit was diluted beyond perceptibility...*

The several Foundation critiques identify numerous profound and obvious holes in what it describes as NERC's "hollow" GMD Standard, and rightly castigates U.S. FERC for approving what is, in reality, a paper mache GMD Standard that would not protect the grid from a geomagnetic super-storm:

--"FERC erred by approving a standard that exempts transmission networks with no transformers with a high side (wye-grounded) voltage at or above 200 kV when actual data and lessons learned from past operating incidents show significant adverse impacts of solar storms on equipment operating below 200 kV."
--"The exclusion of networks operating at 200kV and below is inconsistent with the prior bright-line definition of the Bulk Electric System" as defined by U.S. FERC.
--"FERC erred by approving a standard that does not require instrumentation of electric utility networks during solar storm conditions when installation of GIC [Ground Induced Current--Pry] monitors would be cost-effective and in the public interest."
--"FERC erred by approving a standard that does not require utilities to perform the most rudimentary planning for solar storms, i.e., mathematical comparison of megawatt capacity of assets at risk during solar storms to power reserves."
--"FERC erred by concluding that sixteen Reliability Coordinators could directly communicate with up to 1,500 Transmission and Generator Operators during severe GMD events with a warning time of as little as 15 minutes and that Balancing Authorities and Generator Operators should not take action on their own because of possible lack of GIC data."
--"FERC erred by assuming that there would be reliable and prompt two-way communications between Reliability Coordinators and Generator Operators immediately before and during severe solar storms."

The Foundation is also critical of U.S. FERC for approving a NERC GMD Standard that lacks transparency and accountability. The utilities are allowed to assess their own vulnerability to geomagnetic storms, to devise their own preparations, to invest as much or as little as they like in those preparations, and all without public scrutiny or review of utility plans by independent experts.

Dr. William Radasky, who holds the Lord Kelvin Medal for setting standards for protecting European electronics from natural and nuclear EMP, and John Kappenman, who helped design the ACE satellite upon which industry relies for early warning of geomagnetic storms, conclude that the NERC GMD Standard so badly underestimates the threat that "its resulting directives are not valid and need to be corrected." Kappenman and Radasky:

> *These enormous model errors also call into question many of the foundation findings of the NERC GMD draft standard. The flawed geo-electric field model was used to develop the peak geo-electric field levels of the Benchmark model proposed in the standard. Since this model understates the actual geo-electric field intensity for small storms by a factor of 2 to 5, it would also understate the maximum geo-electric field by similar or perhaps even larger levels. Therefore, the flaw is entirely integrated into the NERC Draft Standard and its resulting directives are not valid and need to be corrected.*

The excellent Kappenman-Radasky critique of the NERC GMD Standard represents the consensus view of all the independent observers who participated in the NERC GMD Task Force, including the author. The Kappenman-Radasky critique warns NERC and U.S. FERC that, "Nature cannot be fooled!"

Perhaps most revelatory of U.S. FERC's untrustworthiness, by approving the NERC GMD Standard that grossly underestimates the threat from geo-storms--U.S. FERC abandoned its own much more realistic estimate of the geo-storm threat. It is incomprehensible why U.S. FERC would ignore the findings of its own excellent interagency study, one of the most in depth and meticulous studies of the EMP threat ever performed, that was coordinated with Oak Ridge National Laboratory, the Department of Defense, and the White House.

U.S. FERC's preference for NERC's "junk science" over U.S. FERC's own excellent scientific assessment of the geo-storm threat can only be explained as incompetence or corruption or both.

The bottom line is that the people and the States cannot trust NERC and U.S. FERC to protect the national electric grid from natural EMP. They probably cannot trust NERC and the U.S. FERC to protect the grid from anything.

States should protect their own electric grids, and their people who depend upon the grid for survival, from the worst threat--nuclear EMP attack--so they will be ready for everything.