North Carolina Grid Security Task Force

Presentation to

NC Joint Legislative Emergency Management Oversight Committee

March 13, 2014

Sid Morris:

Welcome and report "State of the Union" for NC grid status.

Dr. William Forstchen:

A Timeline to Disaster

Ambassadors Henry Cooper and R. James Woolsey:

Discuss Real and Present Danger Assessment.

Dr. Peter Pry:

Overview of the Washington Gridlock and How NC can Lead the Nation to Harden the Power Grid.

Sid Morris:

NOAH Foundation Proposal for Research and Development of Grid Hardening Plan for State of NC.

THE NOAH FOUNDATION

March 13, 2014

Dear Honorable Members of the Joint Commission,

Thank you for allowing us the opportunity to sit down with you and have a real conversation about these uncertain times we now find ourselves in.

While I don't have a Crystal ball capable of predicting the future, I do know how to recognize trends and the trends I am seeing are troubling. There are several real threats gathering around us that, some of which, if they materialize, have the potential to be "game changers" capable of breaking down society.

The sole purpose of creating the NOAH Project was to provide my family and myself the reassurance in knowing that I am providing for them a solid plan of action should the national security of our country be compromised due to one of many real threats congregating around us. Having a 100% self-reliant, self-sustainable, off-the-grid alternative home based solution seems fitting. However, if we are able to harden the electrical grid in North Carolina we will lead the country in protecting all of our families from the devastating effects of an EMP event.

I am convinced that the gridlock in Washington will continue and the only real answer for the security of our families is to take charge at the local and State level. If we lead the way other States will follow rapidly.

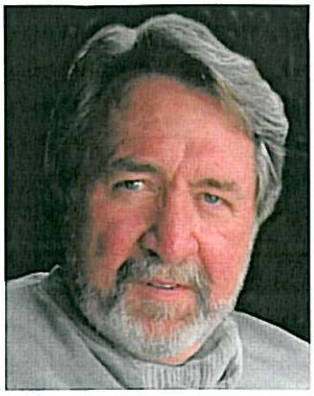
With your help we can make it happen!

Thank you for your time today,

Sid Morris
704-516-1689

www.morrisinternational.com
www.thenoahfoundations.com

The NOAH Foundation is a non-government organization dedicated to the protection and security of our power grid against acts of nature, solar EMP, and cyber or terrorist attack.



Sid Morris

Morris International Inc

The NOAH Foundation

There is a relatively small segment of leaders in the business world; individuals who are able to build relationships, and rapport with almost anyone, and then are able to broker those relationships and make connections between people, creating partnerships and alliances, and motivating forward momentum to "get things done." A high energy, fiscally conscious, and goal-driven entrepreneur, Sid Morris approaches each new business challenge with his intrinsic flair for innovation, creative problem-solving and measured risk-taking.

Sid Morris founded Morris International in 1971 and became the first and only AAAA advertising agency specializing in Sports Marketing with his major focus on motorsports. In 1978 Charlotte Motor Speedway retained Morris International as their Agency of Record. In 1984, when Bill France Jr. wanted a new image for Daytona, Darlington and Talladega motor speedways and the famed Daytona 500, NASCAR called on Morris. So began an impressive, results-driven tenure with Morris bringing Proctor & Gamble's Crisco and Tide brands to the sport, along with developing one of the first "Official" NASCAR sponsorships with AC Delco, Western Auto, Wrangler and Sears Craftsman.

Morris made world sports history in April 1988 by organizing the first professional sailboat racing series in the world, The Salem ProSail Series. In their first year of competition, the ProSail regattas were featured in three ESPN sports television programs. Privately owned and operated by Morris International, of Davidson, NC, Morris designed ProSail to be the NASCAR of water sports.

In 1991 Morris acquired The Lake Norman Company, a commercial property management and real estate development company. Morris provide the leadership and general management needed to accomplish a complete turnaround of the struggling company; growing and expanding operations to feature the only waterfront office space offerings on Lake Norman, along with five marinas, Davidson Mini-Storage, and The North Harbor Club restaurant.

In March 2011, Sid embarked on a daunting new journey, one that will have a profound effect on our community and in fact our very way of life. The NOAH Foundation.

Dr. William R. Forstchen

Military Historian

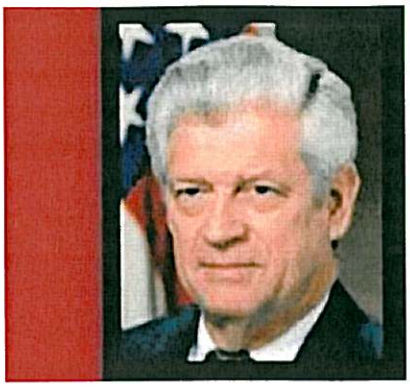
NY Times Best Selling Author

William R. Forstchen has a Ph.D. from Purdue University with specializations in Military History and the History of Technology. He is a Faculty Fellow and Professor of History at Montreat College.

He is the author of over forty books, including the New York Times bestselling series *Gettysburg* and *Pearl Harbor* (coauthored with Newt Gingrich), as well as the award-winning young adult novel *We Look Like Men of War*. He has also authored numerous short stories and articles about military history and military technology.

In March 2009, Dr. Forstchen's latest work, *One Second After*, (Forge/St. Martin's books) was released. Based on intensive research and interviews, it examines what might happen to the social order in a "typical" American town in the wake of an EMP attack on the United States. The book was cited by Congressman Roscoe Bartlett (R.-MD) on the floor of Congress and before the House Armed Services Committee, as a realistic portrayal of the damage of an EMP attack on the continental United States.

Dr. Forstchen's interests include archaeological research on sites in Mongolia, and as a pilot he owns and flies an original World War II "recon bird." Dr. Forstchen resides near Asheville, North Carolina with his teenage daughter Meghan and their small pack of golden retrievers and yellow labs.



Ambassador Henry F. Cooper

Hank serves as a Director of NICOR Global, LLC. Ambassador Cooper served as Director of the Strategic Defense Initiative Organization, Department of Defense, Washington, D.C. He was appointed to this position by President Bush on July 10, 1990, and is the first Civilian Director.

After his stint at Bell Labs in 1964, Ambassador Cooper served as 1st Lieutenant in the U.S. Air Force and then as Scientific Adviser to the Air Force Weapons Laboratory until 1972. From 1972 to 1980, he served as a Member of the Senior Technical Staff and Program Manager (Current as of April 1992) at R&D Associates.

In 1980, he served as Deputy to the Assistant Secretary of the Air Force with programmatic oversight responsibilities for all Air Force strategic and space systems, a position he held until 1982. From 1982 to 1983, Ambassador Cooper returned to Research & Development Associates, serving as the Deputy Director of the Nuclear Effects Division. In November 1983, Ambassador Cooper was appointed by President Reagan to serve as an Assistant Director of the Arms Control and Disarmament Agency. In that capacity, he was responsible for backstopping all bilateral negotiations with the Soviet Union related to strategic and theater nuclear matters and chaired the Assistant Secretary- level interagency group responsible for developing U.S. Space Arms Control policy options. In March 1985, he was appointed by President Reagan as Ambassador and Deputy U.S. Negotiator at the Defense and Space Talks with the Soviet Union. In 1987, he was named Chief United States Negotiator at the Defense and Space Talks with the Soviet Union. From December 11, 1989, until being named Director of SDIO, Ambassador Cooper served as Senior Vice President for Strategic Planning at JAYCOR.

Ambassador Cooper is a nationally recognized expert on nuclear weapon effects, strategic systems, and policy and arms control matters. He has served as Chairman, Member, or Consultant for numerous national-level committees, panels, and working groups in these areas. Ambassador Cooper is the author of over one hundred publications on applied systems analysis, targeting analysis, strategic policy, intelligence, and arms control. He was awarded a Bachelor of Science degree from Clemson University in 1958, and a Master of Science in 1960. He received his Doctorate from New York University in 1964. Ambassador Cooper taught Engineering Mechanics at Clemson University from 1958 to 1960, while doing his Master's Degree there. From 1960 to 1964, he conducted Independent Research as a Member of the Technical Staff of the world-renowned Bell Telephone Laboratories.

R. JAMES WOOLSEY

U.S. Ambassador

Former Director of Central Intelligence

Ambassador R. James Woolsey, a former Director of Central Intelligence, chairs the board of the Foundation for Defense of Democracies and is a Venture Partner with Lux Capital Management.

Woolsey also currently chairs the Strategic Advisory Group of the Washington, D.C. private equity fund, Paladin Capital Group, and the Advisory Board of the Opportunities Development Group, and he is Of Counsel to the Washington, D.C. office of the Boston-based law firm, Goodwin Procter. In the above capacities he specializes in a range of alternative energy and security issues.

Mr. Woolsey previously served in the U.S. Government on five different occasions, where he held Presidential appointments in two Republican and two Democratic administrations. From July 2002 to March 2008 Mr. Woolsey was a Vice President and officer of Booz Allen Hamilton, and then a Venture Partner with VantagePoint Venture Partners until January 2011. He was also previously a partner at the law firm of Shea & Gardner in Washington, DC, now Goodwin Procter, where he practiced for 22 years in the fields of civil litigation, arbitration, and mediation.

During his 12 years of government service, in addition to heading the CIA and the Intelligence Community, Mr. Woolsey was: Ambassador to the Negotiation on Conventional Armed Forces in Europe (CFE), Vienna, 1989– 1991; Under Secretary of the Navy, 1977–1979; and General Counsel to the U.S. Senate Committee on Armed Services, 1970–1973. He was also appointed by the President to serve on a part-time basis in Geneva, Switzerland, 1983–1986, as Delegate at Large to the U.S.–Soviet Strategic Arms Reduction Talks (START) and Nuclear and Space Arms Talks (NST). As an officer in the U.S. Army, he was an adviser on the U.S. Delegation to the Strategic Arms Limitation Talks (SALT I), Helsinki and Vienna, 1969–1970.

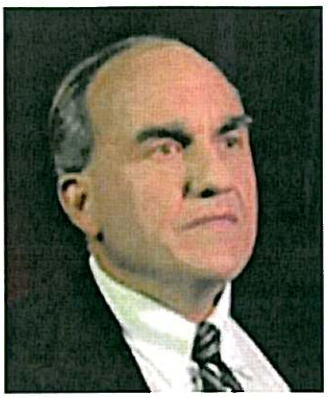
Ambassador Woolsey currently serves on a range of government, corporate, and non-profit advisory boards and chairs several, including the Advisory Boards of the Clean Fuels Foundation and the New Uses Council, and he is a Trustee of the Center for Strategic & Budgetary Assessments. Previously he was Chairman of the Executive Committee of the Board of Regents of The Smithsonian Institution, and a trustee of Stanford University. He has also been a member of The National Commission on Terrorism, 1999–2000; The Commission to Assess the Ballistic Missile Threat to the U.S. (Rumsfeld Commission), 1998; The President's

Commission on Federal Ethics Law Reform, 1989; The President's Blue Ribbon Commission on Defense Management (Packard Commission), 1985–1986; and The President's Commission on Strategic Forces (Scowcroft Commission), 1983.

Ambassador Woolsey has served in the past as a member of boards of directors of a number of publicly and privately held companies, generally in fields related to technology and security, including Martin Marietta; British Aerospace, Inc.; Fairchild Industries; and Yurie Systems, Inc. In 2009, he was the Annenberg Distinguished Visiting Fellow at the Hoover Institution at Stanford University and in 2010-11 he was a Senior Fellow at Yale University's Jackson Institute for Global Affairs.

Ambassador Woolsey was born in Tulsa, Oklahoma, and attended Tulsa public schools, graduating from Tulsa Central High School. He received his B.A. degree from Stanford University (1963, With Great Distinction, Phi Beta Kappa), an M.A. from Oxford University (Rhodes Scholar 1963–1965), and an LL.B from Yale Law School (1968, Managing Editor of the Yale Law Journal).

Ambassador Woolsey is a frequent contributor of articles to major publications, and from time to time gives public speeches and media interviews on the subjects of energy, foreign affairs, defense, and intelligence. He is married to Suzanne Haley Woolsey and they have three sons, Robert, Daniel, and Benjamin.



Dr. Peter Vincent Pry

Task Force on National and Homeland Security

Dr. Peter Vincent Pry is Executive Director of the Task Force on National and Homeland Security, a congressional advisory board dedicated to achieving protection of the United States from electromagnetic pulse (EMP) and other threats on an accelerated basis. Dr. Pry also is Director of the United States Nuclear Strategy Forum, an advisory body to Congress on policies to counter Weapons of Mass Destruction.

Dr. Pry has served on the staffs of the Congressional Commission on the Strategic Posture of the United States (2008-2009);); the Commission on the New Strategic Posture of the United States (2006-2008); the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (2001-2008); as Professional Staff on the House Armed Services Committee of the U.S. Congress, with portfolios in nuclear strategy, WMD, Russia, China, NATO, the Middle East, intelligence, and terrorism (1995-2001); as an Intelligence Officer with the Central Intelligence Agency responsible for analyzing Soviet and Russian nuclear strategy and operational plans, including EMP threats (1985-1995); and as a Verification Analyst at the U.S. Arms Control and Disarmament Agency responsible for assessing Soviet compliance with nuclear and strategic forces arms control treaties (1984-1985).

Dr. Pry played a key role: running hearings in Congress that warned terrorists and rogue states could pose an EMP threat, establishing the Congressional EMP Commission, helping the Commission develop plans to protect the United States from EMP, and working closely with senior scientists who first discovered the nuclear EMP phenomenon. Dr. Pry has written numerous books on national security issues, including *Civil-Military Preparedness For An Electromagnetic Pulse Catastrophe, War Scare: Russia and America on the Nuclear Brink, Nuclear Wars: Exchanges and Outcomes, The Strategic Nuclear Balance: And Why It Matters,* and *Israel's Nuclear Arsenal.*

Dr. William Forstchen
STATEMENT
"A TIMELINE TO DISASTER"
TO
NORTH CAROLINA JOINT
LEGISLATIVE EMERGENCY
MANAGEMENT OVERSIGHT COMMITTEE
December 3, 2013

An evaluation of nearly any disaster scenario in the past will reveal certain common points in terms of how individuals, groups and from there large crowds will react, either as a team to help each other, or disintegrate into panic.

The primary ingredient in nearly every scenario is the understanding, by citizens, of what has happened, and combined with that, information from trusted sources to explain in honest detail what has occurred, what is being done to bring aid to a stricken area, and clear instructions as to what every citizen should do during the emergency situation.

It cannot be emphasized enough that knowledge and communications are the crucial ingredients to reduce casualties, maintain calm, bring about community organization and neighbor helping neighbor until outside relief arrives, and a communal sense that leadership that can be trusted has a grasp of the situation, is telling the truth, and moving aggressively.

But a few examples:

On 9/11 the citizens of New York City reacted with calmness, compassion, nearly instant cheering and respect for emergency responders, and there was no social breakdown. Much can be attributed to Mayor Giuliani's appearance on national television, having obviously just come out of the hell of ground zero, covered in grit, and passing along clear, calm orders and reassurance. It worked.

There is some mythology with how Londoners responded during the Blitz of 1940, but in general there was a "we can do it,' spirit, acts of incredible heroism by ordinary citizens, and throughout it all, the defiant reassuring voice of Winston Churchill.

In contrast. A comparison of New Orleans and Houston just several years past. In the one city wide spread looting, elderly abandoned to die horrific deaths in nursing homes, outright panic, (this author will never forget Geraldo Rivera's hysterical broadcast from the main emergency shelter screaming there was mass rioting, rape and murder), as compared to Houston, in which there were only a handful of casualties, the withdraw and return of the citizens handled professionally and calmly.

THE DIFFERENCE IS PLANNING BEFORE AN '"EVENT" NOT AFTERWARDS.

New York City's leadership has repeatedly drilled and evaluated nearly any kind of scenario from infectious disease breakout to a full scale nuclear strike. Months before the Blitz hit London, training was taking place, non-essential citizens, especially children and the elderly evacuated, emergency supplies and repair equipment already in place.

WITHOUT DOUBT, AN EMP OR CME EVENT WILL BE ONE OF THE MOST CATASTROPHIC EVENTS TO EVER STRIKE OUR NATION, OR PERHAPS THE ENTIRE PLANET IF THE CME IS OF THE LEVEL OF THE "CARRINGTON EVENT" OF 1859.

With that statement in mind, it would be helpful to consider a "timeline" of what will transpire with a society, post EMP/CME that is ill prepared or not prepared.

DAY #1.

The mere simple fact of being able to recognize an EMP is known by only a small percentage of the population. And yet it is so easy to teach that to every citizen, and especially emergency responders, from local to national.

With a sudden shut down of power, we are all conditioned to just sit back and wait for the power company to arrive. In the same way, up until a tragic day in September, all airline travelers were conditioned that in a hijacking situation, to just sit back, be calm, follow orders and all will be well. For some years, when the hijacking of planes to Cuba was in full swing, there are reports that passengers actually laughed, declaring they were getting a free vacation and compensation afterwards.

In the seconds after an EMP, no one will be laughing aboard the approximately 2,000 commercial aircraft crisscrossing the United States at mid-day. Most will be within a few minutes of dying, or if there is some semblance of control left aboard our computer driven aircraft, they will be in for the most harrowing flight of their lives. Most if not nearly all will be beyond saving, with additional casualties on the ground.

For the rest of us, learning if an EMP event has occurred is easy enough. No power, high percentage of cars no longer functioning, all communications systems, especially cell phones are down equals EMP. A trained community, citizens and first responders will then know what to do. An untrained community will, without doubt, now face the following:

Within hours, with absolutely no communications to explain what is happening, panic will begin to set in. For most civilians, as they hear rumors, often garbled that some sort of attack with an EMP nuclear weapon has transpired, but little else as to explaining it, will trigger an exodus to try and snatch as much food and safe liquids as possible, along with a rush on essential medications, and panic rushes for survival supplies such as weapons, ammunition, cold weather gear in winter.

Ignorance of the reality of the event, and for the first time in generations, a nation suffering from absolute total silence and removal from trusted leadership explaining what is happening and measures to be taken, will fuel this panic.

For those among us who have no regard for law and order, it will be a signal that all restraint is down, such as we witnessed in the post Rodney King riots in Los Angeles, and again, post Katrina, New Orleans.

With the onset of darkness, either in freezing cold, or boiling summer heat, (we are only a couple of generations removed from a world without air conditioning and buildings designed for summer heat without AC) social order will begin to break down. It will be a terrifying night for tens, perhaps hundreds of millions.

DAY #2

This will be a day of trying, in some organized way, either as individuals, families or perhaps even small community groups banding together to secure whatever supplies still might be out there. The scale of social order and social breakdown, in a clinical scientific sense is a fascinating subject to observe. London was able to maintain a wide spread sense of "we are all in this together and let's work together," due to preparation and training beforehand. But in the mysterious and frightening post EMP world, one can expect, at best, perhaps just a neighborhood, or apartment building in a large city to organize itself in some fashion. Everyone else becomes an "outsider" a threat. In rural settings, perhaps an entire town if population is low enough and there is a recognized leader of the town who can rally that community together will be able to maintain control.

Adding significantly to the panic is the simple fact that our entire financial system is in total collapse. Only a few generations ago banks actually did have significant amounts of cash on hand. When was the last time any of us went to a bank clutching our "bank book" in order to deposit or withdraw money? We are an ATM generation and over 90% of what we think is money, is in fact, nothing but electronically stored data.

How to purchase food from your local store when they say cash only, when there is no longer any cash? One can easily imagine crowds flooding into markets, pharmacies, "big box" stores, clamoring at first to "just take a check" to increasing frustration, to a collapse into looting. And without communications, "command and control" in place and trained for prior to the event, wide spread looting, and the violence spinning off from that, will become the norm, those doing it, never imagining but three days earlier they would act in such a manner, but with a terrified and hungry family, or elderly parents waiting back at home, what alternative is now left. . .especially when "everyone else" is now doing it.

DAY #5

This will be the beginning of the true onset of ugliness. With the shutdown of safe water supplies on day one, any reserves will be gone, and the beginning of gastro-intestinal illnesses, which in a normal setting would mean just a day or two of discomfort but solved by proper medication, will be wide spread, and for the very young, the elderly, and those weakened by other illnesses, oftentimes fatal. In the "Maslow Hierarchy of Needs" of survival, clean pure water, at least a gallon a day, and in hot climates two to three gallons a day are essential, along with proper waste disposal. That is gone, people will sicken, begin to die, and feed a sense of frustration, helplessness and panic. For those requiring major medications, ranging from heart disease to psychiatric disorders, the onset of serious symptoms will begin. The million dollar condo on the twenty fifth floor is now a tower of exhaustion that will actually kill more than a few of their owners as they try and lug supplies that they can scrounge up and down the two hundred and fifty foot climb.

Moral questions will now abound. Millions of our citizens are in retirement communities, dependent on significant support structures and personal, nursing homes with even more intense support structures, and on the other end of the spectrum, well over a million in jail, ranging from minor offenders to psychotic murderers. Hardly any personnel will be showing up for work, concerned with protecting their own families, or simply just too far away to walk in. The moral questions of how to respond have become staggering by this point.

Entire cities, with the collapse of safe drinking water supplies are now uninhabitable and a mass exodus will begin, fueled by a near mythical belief that surely, out in the "countryside" people are "nicer" and will be willing to help. But those out in the countryside, if anything, will look at their own dwindling supplies and be terrified by this "swarm of locusts" heading their way.

Wide spread violence will already have become the norm, as the several percent of our population, without any sense of moral guidance and compassion, will prey upon the weakest for what they want, which in turn will trigger even more fear, violence and finally pre-emptive violent response from citizens who were law abiding but ten days earlier who never dreamed they might "shoot first and ask questions later.".

Day #10

True panic now. Any who have successfully organized, be they a block, an apartment building, a small town will have sealed up, all else are "outsiders" that if not barred will consume the dwindling supplies. Some groups will have, by this point, realized the extent of the catastrophe and crossed the moral line that it is "them or us" and without remorse take what they desire from any unable to defend themselves. Disease will now be wide spread, in those areas without any safe drinking water; illness might strike down half, or more of the population, debilitating, infecting care givers, fueling the panic. Food stocks within homes will be short or even depleted.

Day #25

According to studies dating back to the Cold War era, the average American community has approximately twenty five days of food on hand, ranging from what is in a family's fridge and pantry, to stocks in convenience stores, supermarkets or in transit to that community via truck or train. Chances are, that in our high tech "just in time" delivery systems which are set up to reduce inventory to just the required minimum, be it food, fuel, or medication, the supply is now actually far less.

In a "postindustrial" high tech society we created an elaborate but highly delicate web of information flow which in turn triggers "supply flow.' That is gone. On the day a community food supply drops to zero, without any pre-planning as to how to sustain and rebuild from an EMP/CME event, any concept of social order has gone into the ash bin of history.

A hundred and fifty years ago, as the industrial revolution took hold, well over half our population still lived on farms. In the region from the Mississippi to the Atlantic coast, thirty million people were able to live in relative surplus of food, and had even begun to transport that food from significant distances thanks to railroads, steam ships and improved road ways. The average farm, in its fields, orchards, and barn, had on average over a year's worth of food directly on hand, except for a few essentials such as salt and what were thought to be medications. In that same area of land today there are nearly two hundred million people.

Today less than two percent of our population live and work on farms. Of course there are the "local farmers" now so popular with those who proclaim we should support local organic farm supplies, but that is only a few percentage points of our total food supply and still absolutely tied to seasonal production. Nearly all our food comes from outside where we live, how else do we have fresh vegetables in Chicago in the winter, meat that is stamped safe to consume in 110 degree heat in Arizona in the summer, and aisle after aisle of frozen foods to choose from at any time of year.

On Day #25, the pantry is empty for nearly every major urban center in the country. There might be a vast surplus of cattle and pigs by the millions in the Midwest or on factory like pig farms in eastern North Carolina, but how to get them to where they are needed? People will literally begin to starve to death only a few score miles from such sources. And even if ordinary citizens can fall upon such a supply, how many today know how to not just slaughter, but to also preserve such food for the long term. There is a horrifying film clip of Berliners' at the end of WWII, hacking off meat from a blotted and decaying horse. If they survived eating that. . .what of the following day?

DAY #365

According to the Congressional study of a post EMP America issued in 2004, upwards of 90% of our population will be dead and 80% of our generating capacity will still be off line.

The numbers sound absurd when first presented. But when considered in light of the few basic facts presented above, the estimate seems terrifying realistic.

It will be realistic unless we prepare before it happens.

Amb. Henry F. Cooper, Chairman

STATEMENT
TO
NORTH CAROLINA JOINT
LEGISLATIVE EMERGENCY
MANAGEMENT OVERSIGHT COMMITTEE
March 13, 2014

As the mainstream media's awareness of threats to the electric power grid grows and recent weather reminds us of even worse events that will happen, the powers that be need to develop ways to shield against them. These threats extend from physical attacks, to cyber attacks, to natural and manmade electromagnetic pulse events that could take down the grid for an indefinite period of time, during which several hundred million Americans could perish.

NERC, FERC and All That.

Wellinghoff was Chairman of the Federal Energy Regulatory commission (FERC) at the time of the physical attack on a large substation in Jan Jose, California in the early morning hours of April 16, 2013 and, since leaving that post, has been conveying to all who will listen his concerns about the vulnerability of the grid to physical attack—and his message went viral on the mainstream media last week and even provoked action by senior Democrat senators, as reported last week. It will be interesting to see if anything comes of that initiative other than yet another study.

Notably, the News Hour also featured Mark Weatherford of the Chertoff Group, a former Department of Homeland Security Deputy Undersecretary for Cyber Security, and Vice President and Chief Security Officer of the North American Electric Reliability Corporation (NERC) where he directed the organization's critical infrastructure and cybersecurity program. This exchange illustrates the dysfunctional nature of the congressionally-mandated FERC-NERC relationship which so far has not formally acknowledged the general vulnerability of the grid, let alone taken any serious interest in rectifying that condition. Notably, Weatherford observed that perhaps it had been shortsighted to focus on the cyber threat while paying too little attention to the physical attack threat. But, even though Weatherford stated he was less informed on the threat than Wellinghoff, he carried NERC's water in downplaying it.

This dysfunctionality is why Congress should pass the Shield Act, bottled up in the House Energy and Commerce Committee for the past three years, no doubt because of NERC's lobbying efforts—even though, reportedly, it has strong bipartisan support. Wellinghoff stated that we need a single regulatory commission, like the Nuclear Regulatory Commission, which oversee our nuclear power infrastructure with authority and resources to act. The Shield Act would give FERC that capability. NERC is trying to block its passage.

The powers that be need to rectify this situation, for reasons including those illustrated below.

Stormy Weather.

I was a first-hand witness to the East Coast storm that caused shutdowns throughout the eastern seaboard. Due to flight cancelations, we were stalled on our South Carolina farm where the ice storm caused such damage that Governor Niki Haley compared it to Hurricane Hugo—some 350,000 people were without power for days. Georgia had a similar experience. As the storm headed north the ice turned to snow and things also shut down around our Virginia residence, where the national capital region was covered with 1-2 feet of snow.

Interestingly, some of Sunday's news reports connected these east coast difficulties with the west coast drought to claim this was evidence of manmade (or to be more politically correct, human-made) Global Warming—or at least Climate Change. This, in my view, was absurdly arrogant, since climate is always changing—has been for millennia and it's been warmer and it's been colder.

Perhaps the most ludicrous recent related event was Secretary of State John Kerry's inclusion of alleged climate change in his discussion of international terrorism—calling it "the world's largest weapon of mass destruction." Was this just another bumbling attempt to divert attention from the administration's obviously failing diplomacy, particularly in the Middle East and in his negotiations with Syria and Iran?

In fact, the climate has sometimes has been dramatically altered by Mother Nature, like the 1883 Krakatoa volcanic eruption, which created unseasonably cool weather, brilliant sunsets, and prolonged twilights due to the spread of aerosols throughout the stratosphere. A repetition of such—or worse—was the concern that was raised in the 1970s by the "Nuclear Winter" advocates seeking policies of nuclear abolition—when "Global Cooling" was in vogue.

A lesson from last week's weather that did occur to me is that we are now much less prepared to deal with extreme variations. For example, I recall worse ice storms in Georgia and South Carolina during the 1940s that slowed us down less than the recent vigil. Some of our wells had hand pumps, we heated and cooked on wood, coal and kerosene stoves; the cows were fed and watered as usual (including in our pond)—producing plenty of milk, cream and butter; and we had salt cured pork in the smoke house and lots of canned goods from the past summer. Last week was very different for many who now depend on electricity and the just in time economy for comfort and sustenance.

And I recall the winter of 1960 and my introduction to northern weather at Bell Laboratories in New Jersey. It was then alleged to be the worst winter since the 1880s. First snow fell around Thanksgiving and was still on the ground in March after several other snows of 18 inches or more. I don't recall school stopping—and I never missed a day of work. A youthful President Kennedy seemingly ignored the cold in taking his oath of office and delivering his inaugural address, when everyone else seemed to be bundled up.

And so far as droughts go, remember the "dustbowl" of the 1930s that prompted a mass migration to the West Coast—a la John Steinbeck's The Grapes of Wrath—and many of those folks, like many in my wife's family, moved from Oklahoma to contribute to California's aerospace boom—including "Rosie the Riveter" roles supporting our World War II effort and beyond? Was this weather manmade—pardon, human-made?

Then there is, in fact, much more deadly stormy weather beyond our control and headed our way—solar storms that go on all the time. One day, one will hit us!

Solar Storms.

Recently, the Earth passed within about a week of when the emission from such a storm intersected the Earth's orbit and could have produced a catastrophic "so-called Carrington event." As we have discussed for many months, particularly last December 18th , the powers that be have so far not hardened the electric power grid to counter this electromagnetic pulse (EMP) threat—the loss of which could, indeed, have effects much worse than most terrorist, but not all, weapons of mass destruction—leading to the death of several hundred million Americans if we continue to ignore it. And I am not talking about climate change or environmental impact issues.

These massive solar emissions are real, happen frequently, and should not be—but are being—ignored by the powers that be. The National Weather Service Space Weather Prediction Center of the National Oceanic and Atmospheric Administration in Boulder, Colorado maintain a watch on these events. When they detect such events, they provide formal warning to those who have an interest in the consequences. For example, the Federal Aviation Agency (FAA) uses their warning to redirect flights that might be exposed to effects that might create risks to aircraft and passengers. But regrettably those responsible for the electric power grid have not yet taken steps to assure its survival to this existential threat.

One of the Center's specialists, Mr. William Murtagh, discussed these events at the recent DuPont Summit in Washington, DC (cosponsored by the Policy Studies Organization and the InfraGard National EMP Special Interest Group). Key observations were:

- Such events go on all the time—not just during a solar maximum; and very consequential events can occur during the dwell period between solar maxima that occur on an 11-year cycle.
- The 1859 Carrington Event, often taken as a "worst case" event for planning purposes, occurred during such a dwell period—and it actually was not near the magnitude of the largest emissions that have been observed.
- A 1921 solar storm event that, among other things, put the entire signal and switching system of the New York Central Railroad below 125th Street out of operation and induced currents causing a fire in the control tower. (Systems depending on today's electronics would have fared far worse.)
- In 2012, a much larger event than either of these barely missed enveloping planet earth with a lethal cloud of charges from a Coronal Mass Ejection (CME)—slightly different timing and it could have enveloped the earth and shut down the electric power grid in the U.S. as well as throughout the world.
- October 2013 "Halloween storms" should serve as another "wake-up call"—it illustrated the damaging effects of solar storms on the Global Positioning System (GPS) upon which navigation and numerous other applications depend—as well as other applications, such as communications and the electric power grid.
- The FAA pays particular attention to the National Weather Service assessments—and all flights have been diverted from major regions of the globe because of that warning—which normally is a day or so in advance, there was about 18 hours of warning in last year's major CME.

While we would have 18 or so hours of warning of the arrival of solar wind particles from the sun's surface, we would not know the cloud's composition until it is identified by the Advanced Composition Explorer (ACE) satellite at the L1 libration point between the earth and the sun. Until that composition is known, the power companies would not take action because of a possible false alarm, depending on the polarization of the particles' associated magnetic field relative to the Earth's magnetic field. About 30 minutes after determination of actionable warning those particles will interact with the earth's geomagnetic field and possibly produce the EMP of concern.

Ironically, this is approximately the same time of flight of an intercontinental ballistic missile (ICBM) from Iran to the U.S. In that case, we have prepared for a rapid response . . . that is why the President always has with him an individual carrying the "football" with the launch codes for our retaliatory response to a nuclear attack. But in the case of the solar induced EMP, there will likely be insufficient time for the power companies to shut down and protect the grid.

So, alternative hardening measures are required—and possible. But the powers that be are not taking needed actions to protect the American people from this existential threat.

This incredibly dangerous condition was recently lamented at the DuPont Summit by Dr. Daniel Baker, a solar scientist and director of the University of Colorado-Boulder's Laboratory for Atmospheric and Space Physics, while relating our good fortune in avoiding the largest-on-record, June 2012 CME. It occurred on the far side of the rotating sun just a week after that source area was pointed directly toward Earth. NASA's STEREO-A satellite was flying ahead of Earth as the planet orbited the sun and recorded the event, including the intensity of the solar wind, the interplanetary magnetic field and a rain of solar energetic particles into space.

In commenting on lack of attention paid to the near miss, Dr. Baker has in sorrow observed:

"My space weather colleagues believe that until we have an event that slams Earth and causes complete mayhem, policymakers are not going to pay attention . . . The message we are trying to convey is that we made direct measurements of the 2012 event and saw the full consequences without going through a direct hit on our planet."

So, is he wrong? Will we pay attention to this important threat??? Or just wait for disaster to strike.

Then there's Iran.

I cannot close this reflection on threats without mentioning the looming threat from Iran—also highlighted by recent events, including Iran's increasing bellicosity and obviously failing U.S. diplomacy.

As mentioned above, if Iran were to launch a nuclear armed intercontinental ballistic missile (ICBM) at us "over the North Pole," our ballistic missile defense (BMD) system should be prepared to shoot it down during its 30 minute or so flight time. But if Iran employs a nuclear weapon on a shorter range missile launched from a vessel off our coast, we would have only a few minutes to respond—but we have defenses that, if prepared, could respond.

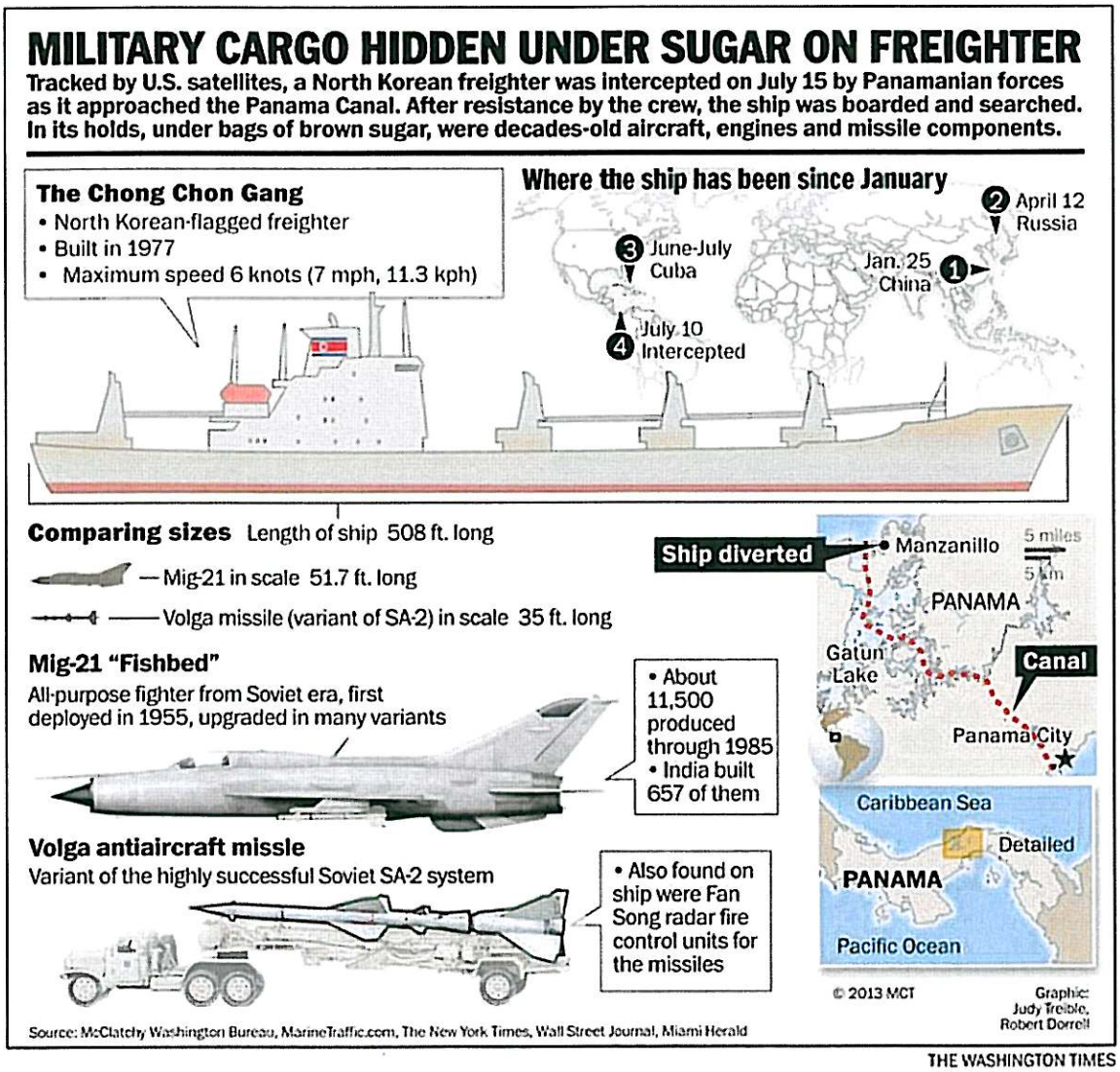
In either case, a nuclear weapon detonated a hundred miles or so above the United States would harm no one immediately. But the consequent EMP would (among other things) shut down indefinitely the unhardened electric power grid by severely damaging its very high voltage (VHF) transformers—the consequences within a year would return the nation to its 18th century existence without the 18th century agrarian support. The resulting chaos would no doubt lead to the death of several hundred million Americans.

These nuclear produced EMP effects actually would be more severe than those caused by solar storms, which are bad enough. And we know how to counter them, if and when the powers that be decide to do so.

We could shoot down these attacking missiles if our Aegis BMD ships along the coast or in port are prepared to do so. As previously reported, on a day chosen at random in 2012 there were 4-6 such ships—all that is needed is training for them to deal with the possibility of an off-coast missile attack. (With an appropriate radar in Maine, they can also help defend against Iranian

ICBMs coming over the North Pole.) But Aegis BMD ships do not normally enter the Gulf of Mexico—so we are vulnerable to attack from there or from other points south.

To illustrate this threat is in fact not hypothetical, note that last July Panamanian officials intercepted a North Korean vessel smuggling through the Canal rockets (originally designed to be) capable of carrying nuclear weapons. Furthermore, as indicated in the figure below, the particular vessel had interacted with charter members of the cacophony of proliferation on this very trip.



To counter this threat, I strongly urge that the Pentagon consider the merits of deploying Aegis Ashore sites at military bases around the Gulf of Mexico. We are building such sites in Romania (by 2015) and Poland (by 2018) to protect our NATO allies from Iranian missiles, and we already have built a site in Hawaii for testing for these European sites. Surely we can afford to protect Americans from Iranian missiles launched at us from the south. You think?

We also need to protect against an Iranian satellite that could carry a nuclear weapon over the South Pole to attack us from the South. Iran and North Korea (Iran's partner which already has nukes) have repeatedly launched satellites into such orbits that can easily be steered over the U.S. Today, this "back door" is wide open because our defenses are deployed against missiles approaching the U.S. from the North.

And we need to harden the electric grid in any case to deal with the electromagnetic pulse if our defenses fail or from a solar storm. The Carrington event happened 155 years ago—and we are due for an encore.

We know how to do this. No additional development is needed to get started—though we might be able to improve on the hardening technology developed and applied to harden our nuclear forces and their command and control systems for decades.

R. JAMES WOOLSEY
TESTIMONY
BEFORE THE
HOUSE COMMITTEE ON ENERGY AND COMMERCE
May 21, 2013

This hearing is about cyber threats and solutions. But I am going to talk about a dimension of the cyber threat that is not usually considered a cyber threat in Western doctrine, but is in the playbooks for an Information Warfare Operation of Russia, China, North Korea, and Iran. These potential adversaries in their military doctrines include as a dimension of cyber warfare a wide spectrum of operations beyond computer viruses, including sabotage and kinetic attacks, up to and including nuclear electromagnetic pulse (EMP) attack.

It is vitally important that we understand that a nuclear EMP attack is part of cyber and information warfare operations as conceived by our potential adversaries. Our cyber doctrine must be designed to deter and defeat the cyber doctrines of our potential adversaries by anticipating how they plan to attack us--but our doctrine currently does not.

Our cyber and information warfare doctrines are dangerously blind to the likelihood that a potential adversary making an all-out information warfare campaign designed to cripple U.S. critical infrastructures would include an EMP attack.

The assessment that nuclear EMP attack is included in the cyber and information warfare doctrine of potential adversaries, and the effects of an EMP attack described here, are based on the work of the Congressional EMP Commission that analyzed this threat for nearly a decade (2001-2008). The Congressional Strategic Posture Commission and several other major U.S. Government studies independently arrived at similar conclusions, and represent collectively a scientific and strategic consensus that nuclear EMP attack upon the United States is an existential threat.

What is EMP? A nuclear weapon detonated at high-altitude, above 30 kilometers, will generate an electromagnetic pulse that can be likened to a super-energetic radio wave, more powerful than lightning, that can destroy and disrupt electronics across a broad geographic area, from the line of sight from the high-altitude detonation to the horizon.

For example, a nuclear weapon detonated at an altitude of 30 kilometers would project an EMP field with a radius on the ground of about 600 kilometers, that could cover all the New England States, New York and Pennsylvania, damaging electronics across this entire region, including electronics on aircraft flying across the region at the time of the EMP attack. The EMP attack would blackout at least the regional electric grid, and probably the entire Eastern Grid that generates 70 percent of U.S. electricity, for a protracted period of weeks, months, possibly years. The blackout and EMP damage beyond the electric grid in other systems would collapse all the other critical infrastructures--communications, transportation, banking and finance, food and water--that sustain modern civilization and the lives of millions.

Such an EMP attack, a nuclear detonation over the U.S. East Coast at an altitude of 30 kilometers, could be achieved by lofting the warhead with a meteorological balloon.

A more ambitious EMP attack could use a freighter to launch a medium-range missile from the Gulf of Mexico, to detonate a nuclear warhead over the geographic center of the United States at an altitude of 400 kilometers. The EMP field would extend to a radius of 2,200 kilometers on the ground, covering all of the contiguous 48 United States, causing a nationwide blackout and collapse of the critical infrastructures everywhere. All of this would result from the high-altitude detonation of a single nuclear warhead.

The Congressional EMP Commission warned that Iran appears to have practiced exactly this scenario. Iran has demonstrated the capability to launch a ballistic missile from a vessel at sea. Iran has also several times practiced and demonstrated the capability to detonate a warhead on its medium-range Shahab III ballistic missile at the high-altitudes necessary for an EMP attack on the entire United States. The Shahab III is a mobile missile, a characteristic that makes it more suitable for launching from the hold of a freighter. Launching an EMP attack from a ship off the U.S. coast could enable the aggressor to remain anonymous and unidentified, and so escape U.S. retaliation.

The Congressional EMP Commission warned that Iran in military doctrinal writings explicitly describes making a nuclear EMP attack to eliminate the United States as an actor on the world stage as part of an Information Warfare Operation. For example, various Iranian doctrinal writings on information and cyber warfare make the following assertions:

- "Nuclear weapons...can be used to determine the outcome of a war...without inflicting serious human damage [by neutralizing] strategic and information networks."

- "Terrorist information warfare [includes]...using the technology of directed energy weapons (DEW) or electromagnetic pulse (EMP)."

- "...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."

China's premier military textbook on information warfare, written by China's foremost expert on cyber and information warfare doctrine, makes unmistakably clear that China's version of an all-out Information Warfare Operation includes both computer viruses and nuclear EMP attack. According to People's Liberation Army textbook *World War, the Third World War--Total Information Warfare*, written by Shen Weiguang, "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.

North Korea appears to be attempting to implement the information warfare doctrine described above by developing a long range missile capable of making a catastrophic nuclear EMP attack on the United States. In December 2012, North Korea demonstrated the capability to launch a satellite on a polar orbit circling the Earth at an altitude of 500 kilometers. An altitude of 500 kilometers would be ideal for making an EMP attack that places the field over the entire contiguous 48 United States, using an inaccurate satellite warhead for delivery, likely to miss its horizontal aimpoint over the geographic center of the U.S. by tens of kilometers. North Korea's satellite did not pass over the United States--but a slight adjustment in its trajectory would have flown it over or near the U.S. bull's eye for a high-altitude EMP burst.

North Korea appears to have borrowed from the Russians their idea for using a so-called Space Launch Vehicle to make a stealthy nuclear attack on the United States. During the Cold War, Moscow developed a secret weapon called a Fractional Orbital Bombardment System (FOBS) that looked like a Space Launch Vehicle, but was designed to launch a nuclear warhead southward, away from the United States initially, but deliver the warhead like a satellite on a south polar orbit, so the nuclear attack comes at the U.S. from the south. The United States has no Ballistic Missile Early Warning (BMEW) radars or missile interceptors facing south. We might not even see the attack coming.

Miroslav Gyurosi in *The Soviet Fractional Orbital Bombardment System* describes Moscow's development of the FOBS:

The Fractional Orbital Bombardment System (FOBS) as it was known in the West, was a Soviet innovation intended to exploit the limitations of U.S. BMEW radar coverage. The idea behind FOBS was that a large thermonuclear warhead would be inserted into a steeply inclined low altitude polar orbit, such that it would approach CONUS from any direction, but primarily from the southern hemisphere, and following a programmed braking maneuver, re-enter from a direction which was not covered by BMEW radars.

"The first warning the U.S. would have of such a strike in progress would be the EMP...," writes Gyurosi.

The trajectory of North Korea's satellite launch of December 12, 2012 looked very much like a Fractional Orbital Bombardment System for EMP attack. The missile launched southward, away

from the United States, sent the satellite over the south polar region, approaching the U.S. from the south, at the optimum altitude for EMP attack--although the test trajectory deliberately avoided flying over the United States.

North Korea appears to have borrowed from Russia more than the FOBS. In 2004, a delegation of Russian generals met with the Congressional EMP Commission to warn that design information for a Super-EMP nuclear warhead had leaked from Russia to North Korea, and that North Korea might be able to develop such a weapon "in a few years." A few years later, in 2006, North Korea conducted its first nuclear test, of a device having a very low yield, about 3 kilotons. All three North Korean nuclear tests have had similarly low yields. A Super-EMP warhead would have a low-yield, like the North Korean device, because it is not designed to create a big explosion, but to produce gamma rays, that generate the EMP effect.

According to several press reports, South Korean military intelligence concluded independently of the EMP Commission that Russian scientists are in North Korea helping develop a Super-EMP nuclear warhead. In 2012, a military commentator for the People's Republic of China stated that North Korea has Super-EMP nuclear warheads.

One design of a Super-EMP warhead would be a modified neutron bomb, more accurately an Enhanced Radiation Warhead (ERW) because it produces not only large amounts of neutrons but large amounts of gamma rays, that cause the EMP effect. One U.S. ERW warhead (the W-82) deployed in NATO during the Cold War weighed less than 50 kilograms. North Korea's so-called Space Launch Vehicle, which orbited a satellite weighing 100 kilograms, could deliver such a warhead against the U.S. mainland--or against any nation on Earth.

Iran may already have a FOBS capability, as it has successfully launched several satellites on polar orbits, assisted by North Korean missile technology and North Korean technicians. Iranian scientists were present at all three North Korean nuclear tests, according to press reports.

What is to be done about the Cyber and EMP threats?

Technically, it is important to understand that surge arrestors and other hardware designed to protect against EMP can also protect against the worst-case cyber scenarios that, for example, envision computer viruses collapsing the national power grid. For example, surge arrestors that protect Extra High Voltage transformers from EMP can also protect transformers from damaging electrical surges caused by a computer virus that manipulates the grid Supervisory Control And Data Acquisition Systems (SCADAS).

Administratively, a coherent and effective answer will not likely arise from uncoordinated decisions made independently by the thousands of individual industries at risk. Because cyber preparedness should encompass EMP preparedness--and since EMP is an existential threat--it is imperative that Government play a supervisory and coordinating role to achieve protection against these threats swiftly.

Guest Column

The Future U.S. Energy Picture?

In March, at a workshop convened by Sandia National Laboratories and the University of California, San Diego, leaders from academia, government, and the private sector gathered to discuss key energy policy issues.

At the workshop, attendees were asked a question about what the future U.S. energy picture might look like.

Below is R. James Woolsey's response to the question. Mr. Woolsey was Director of the Central Intelligence Agency and is Chairman of the Advisory Board of the Clean Fuels Foundation.

"Imagine it is ten years from now. U.S. energy policy has changed dramatically for the better in response to the intersecting priorities of economic security, environmental and climate security, and national security. Describe the underlying principles and long-term goals that drove that change. What does the U.S. and the world energy picture look like as a result?"

Report of March 2019: The 2009 Plan for a "Smart" Electricity Grid

Plans had been completed ten years ago—in March 2009—for hundreds of billions of dollars in investment to make the electricity grid smarter and more capable of carrying the stranded electricity, produced by solar plants in the southwest and wind farms in the Great Plains, to population centers on the coasts. Central control of electricity demand was to be a major aspect of this new grid, and there were to be a great many other "smart" improvements.

By September 2009, however, a series of cyber attacks on the grid during the summer had a devastating effect, creating dozens of serious regional electricity brownouts and blackouts. For some weeks, authorities were certain the sophisticated attacks had come from, at first, China, then Russia, then Hezbollah cyber-cells in Lebanon.

In September, however, an eighth-grader in Burbank, California, confessed that he and a group of friends had grown bored with video games during the summer and had decided to bring down major parts of the grid for various periods of time. Under questioning by authorities, the group protested that it would have been easy for them to have taken the grid down for months, and that "you guys" should feel lucky they had only taken portions down for days.

The eighth-grader added that the Supervisory Control and Data Acquisition (SCADA) systems that control the grid, using commercial off-the-shelf software over the Internet, were so easy to hack that he and his friends soon got bored with that as well, and several new, more challenging video games had temporarily led them to set aside their grid shutdowns.

The young witness said to his astonished interrogators, "If you dorks can't even deal with us, how are you going to deal with Chinese, Russian, or Hezbollah cyber-dudes? You aren't building a smart grid. It's headed towards being an ODAV grid—we normally don't spell that out for the rents and other old peeps, but it stands for 'Ostrich-Designed, Awesomely Vulnerable.'" (Editor's Note: 'rents' is slang for parents and 'peeps' is slang for people.)

An urgent national re-evaluation of the planning for the smart grid project followed.

The administration learned that the combined incentives of electricity deregulation and electricity companies' consequent total focus on the quarterly bottom line—together with utilities' lawyers' warnings that they risked liability if they acknowledged any security problem that they didn't fix immediately—had destroyed most of the incentives to make the grid secure.

It was also a classic tragedy-of-the-commons problem: if any utility spent the money to fix vulnerabilities, chances were that the blackout of a still-vulnerable neighbor utility—if the neighbor were taken down by cyber or other attacks (e.g. on transformers)—would black them out as well.

When the utility executives were asked why they had fought so hard in the summer of 2008 against increased authority for the Federal Energy Regulatory Commission to be enabled to order security improvements that would apply to all utilities, they looked guiltily at one another—and shrugged.

As a result of these events, the administration re-structured the smart grid program to emphasize security as well as renewables and distributed generation, including co-generation. They also adopted a feed-in-tariff. Consequently, over the last decade the rapid growth of clean, distributed, secure electricity and the accelerating move, led by battery improvements, in the electrification of transportation and in electricity storage has brought the U.S. to a position of world leadership in bringing about far greener, and far more resilient, energy systems.

Rumor has it that most of the former Burbank eighth-graders now work for a highly-classified office within the U.S. National Security Agency with two responsibilities: designing U.S. retaliatory steps to deal with any attempted foreign cyber-attacks and periodically functioning as a Red Team to keep U.S. utilities on their toes. e

NORTH CAROLINA--THE HINGE OF HISTORY

DR. PETER VINCENT PRY
STATEMENT ON PROTECTING
THE NORTH CAROLINA ELECTRIC GRID FROM
ELECTROMAGNETIC PULSE (EMP)
TO
NORTH CAROLINA JOINT LEGISLATIVE EMERGENCY
MANAGEMENT OVERSIGHT COMMITTEE
March 13, 2014

Honorable members of the North Carolina State Legislature, thank you for the opportunity to appear before this body and speak in support of NOAH's initiative to protect North Carolina's electric grid from natural and manmade electromagnetic pulse (EMP).

As Executive Director of the Task Force on National and Homeland Security, an advisory board to the U.S. Congress, and as a former member of the Congressional EMP Commission, I unreservedly endorse NOAH' s initiative and urge you to act swiftly to protect North Carolina's electric grid from an EMP catastrophe.

The National Intelligence Council, that writes National Intelligence Estimates for the President and speaks for the entire U.S. Intelligence Community, in a recent study *Global Trends 2030*, warned that natural EMP from a geomagnetic super-storm is one of only eight "Black Swan" events that could--sometime during the next 17 years--change the course of global civilization.

The Congressional EMP Commission estimated that a geomagnetic super-storm occurs about once a century, the last such called the Carrington Event that happened in 1859. In those horse and buggy days, civilization did not depend upon electricity. If a Carrington Event recurred today, given the current state of unpreparedness, the EMP Commission assessed that electric grids could collapse everywhere on Earth, causing a protracted planetary blackout, endangering the lives of billions worldwide.

Scientists are concerned that another Carrington Event may recur soon, that such an event is overdue, because it has been more than a century since the last. Moreover, in December 2012, the Sun entered its solar maximum, and over the next year shall emit more solar flares and coronal mass ejections, increasing the possibility of a geomagnetic super-storm.

The EMP Commission warned that terrorists and rogue states could inflict a protracted EMP catastrophe on the entire United States by launching a primitive nuclear missile off a ship near our shores, and detonating the warhead at high-altitude over the United States. According to the EMP Commission, this could collapse the national electric grid and other critical infrastructures--communications, transportation, banking and finance, food and water--and kill up to 90 percent of the American people by starvation, disease, and societal collapse.

Scientific and strategic consensus exists among every major U.S. Government study that, given the current state of unpreparedness, a natural or nuclear EMP event would have catastrophic

consequences for the nation--and therefore the electric grid must be protected. This consensus includes reports by the Congressional EMP Commission (2004 and 2008); the National Academy of Sciences (2008); the Congressional Strategic Posture Commission (2009); the Department of Energy and North American Electric Reliability Corporation (2010); and an interagency study that included the Department of Defense, Department of Homeland Security, and Oak Ridge National Laboratory by the U.S. Federal Energy Regulatory Commission (2010). Most recently, two new independent reports by the Task Force on National and Homeland Security (2013), a Congressional Advisory Board, also concurs with the consensus that the electric grid must be protected from EMP.

There is no excuse for North Carolina or any of the United States to be vulnerable to a natural or manmade EMP catastrophe. Cost-effective technologies for protecting electronic systems from EMP were developed by the Department of Defense and have been known for fifty years by using such proven technologies as surge arrestors, blocking devices, and faraday cages..

Estimating the cost of protecting an electric grid can vary widely because there are a wide variety of ways to achieve EMP protection. One plan for robust protection of the entire U.S. national electric grid, proposed by the Congressional EMP Commission, would cost a one-time investment of $2 billion dollars, which is what the United States gives every year in foreign aid to Pakistan. Another plan by the U.S. Federal Energy Regulatory Commission estimates that protecting the U.S. national electric grid from EMP would cost the average rate payer an increase in their electric bill of merely 20 cents annually.

Rough preliminary calculations indicate that the North Carolina grid can be protected for less than $10 million--and possibly for substantially less.

The biggest obstacle to achieving national EMP preparedness is not technological or financial--but political.

Unfortunately, despite strong bipartisan support in Congress to advance legislation to protect the national electric grid from EMP, these efforts have not been able to overcome the bureaucratic politics of Washington. For years, both parties have tried to protect the grid, and the lives of the American people, and failed.

The core problem is that the electric power industry is the only critical infrastructure that is allowed to regulate itself. No federal department or agency has legal authority to require the electric utilities to protect the grid from EMP or any threat.

Congressional efforts to pass legislation to require the electric power industry to protect the grid have failed repeatedly because of dysfunction in the congressional committee system and especially because of opposition by the powerful electric power lobby, led by the North American Electric Reliability Corporation (NERC).

For example, in 2009, when Democrats controlled the House, the House Homeland Security Committee tried to pass a bill requiring industry to protect the national electric grid.

Unfortunately, the bill never came to a vote because of jurisdictional squabbles between the House Homeland Security Committee and the House Energy and Commerce Committee.

For example, in 2010, Democrats and Republicans joined forces to pass the GRID Act through the House unanimously. Every Member of the House, liberal democrats and conservative Republicans alike, voted "Aye" in a very rare act of unanimous bipartisanship to send the GRID Act sailing over to the Senate. Unfortunately, a single Senator used committee rules to prevent the GRID Act from a vote in the Senate Energy and Natural Resources Committee.

For example, in 2011, with Republicans in charge of the House, despite the bitterly partisan 2010 elections, both parties again joined forces behind the Republican initiated SHIELD Act that, like the GRID Act, enjoys overwhelming bipartisan support. Unfortunately, lobbying by NERC has kept SHIELD bottled in the House Energy and Commerce Committee, where it has languished without a vote for three years.

The White House has also been stymied in efforts to protect the national electric grid. Presidential Policy Directive 8 "National Preparedness" and other White House initiatives have called upon industry to protect the electric grid from "all hazards" including EMP. Unfortunately, because there is no legal authority to require grid protection, voluntary compliance by NERC with these Presidential Directives has not been forthcoming.

Most recently, on October 30, 2013, Rep. Trent Franks introduced the "Critical Infrastructure Protection Act" to the House Homeland Security Committee. This bill will require the Department of Homeland Security to create a new National Planning Scenario focused on EMP that will become the basis for training and planning by Federal, State and local emergency responders. Unfortunately, because the House Homeland Security Committee lacks jurisdiction over the electric grid, this bill cannot require NERC to protect the grid.

North Carolina has an opportunity with NOAH's grid protection initiative to lead the entire nation toward EMP preparedness. If just one state takes the lead and starts to protect its electric power infrastructure from EMP, others will follow, and this almost certainly will break the logjam in Washington.

Technically, it is possible to protect from EMP that portion of the electric grid within a State, even though the State is part of a larger regional grid. "Islanding" North Carolina's electric grid can be accomplished by protecting the Extra-High Voltage transformers, SCADAS, and other critical assets within the State. Such a strategy will in no way impede North Carolina's ability to receive electric power or to transmit electric power from other States.

Indeed, if the North Carolina grid is protected, this will also enhance the energy security of neighboring states by making it easier for their recovery from a catastrophic blackout.

EMP protection does not protect against EMP alone but against all hazards. Since EMP is the worst-case threat, if the electric grid is protected from EMP, it will also be more secure from lesser threats. EMP protection will also mitigate cyber threats, sabotage, and natural disasters like hurricanes and tornadoes.

Because the electric grid is the keystone critical infrastructure, grid protection will enable the recovery of other critical infrastructures. However, there can be no recovery of other critical infrastructures, nor can society long endure, under conditions of a protracted blackout lasting months or years.

Recently, the State of Maine has received much credit from the press for being the first State to launch an initiative to protect its electric grid from EMP, and deservedly so. While Washington has struggled to protect the nation from EMP for five years unsuccessfully, Maine passed an EMP protection initiative in just three months last year.

Ambassador Woolsey has rightly praised Maine's EMP protection initiative, likening its importance to the Battle of Gettysburg: "Men from the 20th Maine defended the hill Little Round Top in the Battle of Gettysburg, in an action widely regarded by historians as the decisive moment that saved the Union. Now Public Utility Commissions and electricity providers are in the frontlines of the cyber battlefield, where EMP is the heavy artillery of cyber warfare, and Maine by quirk of fate or chance has again become the hinge of history."

However, North Carolina may still be nearer than Maine to achieving EMP protection of a State electric grid, thanks to years of work by Sid Morris and NOAH. NOAH has already prepared and planned to hit the ground running to protect the North Carolina grid, while Maine is still exploring the most cost-effective technical options, even while being lobbied to do nothing by NERC.

And North Carolina, like Maine, has also been the hinge of history.

In 1776, the North Carolina delegation to the Continental Congress was the first to be authorized to declare independence from Great Britain and establish as a free republic the United States of America. In 1903, North Carolina became "first in flight" with the Wright Brothers airplane. Just eleven years later, in 1914, the new technology of aerial reconnaissance saved western democracy from losing World War I to Germany by making possible their victory in the First Battle of the Marne, considered by historians one of the most decisive battles in world history.

Now, civilization is again at risk from the looming threat of cyber warfare, and especially from EMP, that is indeed the heavy artillery of cyber threats coming our way. Now North Carolina, by quirk of fate or chance, is again at the crossroads of history, facing new barbarians armed with an unprecedented technological terror.

So do the right thing. Protect the people of North Carolina and their life sustaining electric grid from an EMP catastrophe, and by this brave example lead your Nation to safety from the ultimate cyber threat.

THE WALL STREET JOURNAL.

Transformers Expose Limits in Securing Power Grid

By Rebecca Smith, The Wall Street Journal
Updated March 4, 2014 4:59 p.m. ET

The U.S. electric grid could take months to recover from a physical attack due to the difficulty in replacing one of its most critical components.

The glue that holds the grid together is a network of transformers, the hulking gray boxes of steel and copper that weigh up to 800,000 pounds and make it possible to move power long distances. Transformers were badly damaged in an attack on a California substation last year, and government reports have warned for years that saboteurs could cause sustained damage to the grid by targeting the massive machines.

Only a handful of companies build transformers in the U.S., and it can take weeks or months to ship transformers in from overseas. The manufacturing process itself can last more than a year, in part because a transformer can't be bought off the shelf but rather must be made to measure for its substation.

If attackers damaged enough of the nation's 2,000 biggest transformers at critical locations, they could cause extended blackouts.

Such worries moved beyond the hypothetical recently after The Wall Street Journal reported details about the attack last April on a substation that funnels electricity to Silicon Valley. Unknown gunmen shot up 17 large transformers, knocking PG&E Corp.'s Metcalf substation out of service until repairs were made.

A 2012 report by the National Research Council, written for the Department of Homeland Security, said that the "greatest vulnerability in the event of a terrorist physical attack on the power system will likely be securing needed replacements of high-voltage transformers." It said restoring power "could take weeks, months, or even longer."

Transformers are critical because they boost voltages of electricity, so it can travel long distances efficiently. As electricity nears users, transformers reduce voltages so it is suitable for consumption.

Buying and installing a giant transformer is time-consuming and labor intensive. Depending on size, the transformers can cost $1 million to $8 million.

When FirstEnergy Corp. added a new substation in Pennsylvania a couple of years ago, a South Korean factory took about a year to make one of the big transformers, which then traveled by ship for 26 days to Newark, N.J.

There, a crane lifted the 400,000-pound box onto a train to Pennsylvania. At the end of its 7,000-mile journey in 2012, the equipment traveled on a centipede-like contraption with 192 wheels called a crawler, used to keep the heavy transformer from cracking axles or the road.

Total elapsed time from purchase order to delivery: about two years.

Bill Westerman, police chief for Adams Township, Pa., provided some of the 30 escorts it took to move the transformer nine very slow miles to its substation. If utilities had to transport lots of transformers to end a blackout, "we'd be in real trouble," he said. "You'd better go buy yourself a portable generator."

Just one U.S. factory, in Memphis, Tenn., has the capacity to build the biggest 765,000-volt transformers, according to its owner, Mitsubishi Electric Power Products Inc. Seven companies make big transformers in the U.S., but only three or four make the largest sizes that most experts think would be the likely targets of terrorists. Some of the companies declined to comment, citing security concerns.

In 2012, the U.S. International Trade Commission found that Korean companies were dumping large transformers in the U.S. market at unfairly low prices, threatening the last few makers and prompting the federal government to impose duties on those imports.

American factories, which were running at only about 40% of capacity at the time, said business improved last year.

Recently, new U.S. factories have started up, partly to build replacements for aging equipment.

ABB Inc. of Zurich, Switzerland, would mobilize its three factories in North America and 10 overseas in the event of an emergency, said Deidre E. Cusack, senior vice president in Raleigh, N.C. Even so, she said, it could take several months to build and deliver units.

The industry isn't organized for speed, said Ravi Rahangdale, who owns Pennsylvania Transformer Technologies Inc. in Pittsburgh. Units often last 40 or 50 years, he said, giving utilities plenty of time to plan for replacements.

"We never have had the situation where someone said, 'we need one tomorrow,'" Mr. Rahangdale said, adding that even if his company added another shift, it only could build 20 units in six months.

Jiangsu Huapeng Co. Ltd. has one of the biggest factories in the world in Jiangsu Province, China. Jim Cai, the company's U.S. representative, said his company would try to fill a rush order, but he figured the shortest time it could take is three or four months.

Efforts to speed delivery run into practical problems. When the Phoenix utility known as the Salt River Project needed to get a transformer to Arizona from Austria, it ended up renting the world's largest cargo plane, a Russian Antonov-225, built to carry the Soviet space shuttle.

Utilities say they are trying to address the transformer problem. About 50 electric companies participate in a program to share spares that is run by the Edison Electric Institute, a trade association. The North American Electric Reliability Corp., another power industry group, keeps a database of spares. Neither will say how many are in inventory. Since transformers are custom-designed, it is unclear how helpful the programs would be.

And there are limits to how much equipment utilities are willing to share. When it comes to transformers, "you're not going to give up one that's critical to you," said Rick O'Callaghan, director of transmission and substation engineering for FirstEnergy in Akron, Ohio.

The utility industry is trying to come up with a universal transformer—or something close to it—but the effort is still in an early stage. It is also reconsidering the common practice of storing spares alongside working transformers, exposing both to attacks.

Some suppliers say that the best solution is the most obvious: protect the transformers. Steve Newman, vice president of Delta Star Inc., of Lynchburg, Va., said the problem is, "we've always known that with a couple dollar bullets, you can take out a transformer worth millions of dollars."

Corrections & Amplifications

The Salt River Project hired the world's largest cargo plane to transport a giant electrical transformer from Austria to Arizona. An earlier version of this article incorrectly said the transformer was airlifted from Texas to Arizona.

Write to Rebecca Smith at rebecca.smith@wsj.com

Time to ditch private oversight of America's electric grid system

By Dr. George Baker, Thomas S. Popik

Published February 26, 2014

In April of 2013, unknown parties used a high-powered rifle to shoot out seventeen transformers at a San Jose substation—but only after cutting the fiber optic cables alerting 911 emergency centers.

A prescient 2007 report by the National Academy of Sciences foresaw this grid attack, but the report's release was suppressed by security classification at the Department of Homeland Security. Only recently has the national media begun to cover the San Jose substation attack and its implications for national security.

Most Americans probably don't know that standards for protection of electric grid facilities against terrorist attack are set not by the federal government, but by an electric power industry consortium located in Atlanta, Georgia -- the North American Electric Reliability Corporation or "NERC," as it is called by industry insiders.

NERC had spent years developing a standard for physical protection of transformer substations, but this effort was cancelled after the San Jose attack. For NERC and the electric utilities that control its governance, avoiding regulation looks to be more important than protecting against terrorists.

Standards for protection of electric grid facilities against terrorist attack are set not by the federal government, but by an electric power industry consortium located in Atlanta, Georgia.

In November of last year, NERC sponsored its second voluntary "GridEx" grid security exercise.

Southern California Edison, Pacific Gas and Electric, and other major utilities nationwide simulated cyber and physical attacks on the electric grid. In the make-believe world of GridEx II,

Internet service and telecommunications among electric utilities and their control centers worked perfectly throughout the simulated three-day exercise.

In the real world, utilities are dependent on commercial telecommunications equipment with on-site backup power that will be depleted within a few hours. GridEx II and other industry "work-around procedures" serve as expedient substitutes for the hard work of developing needed federal grid regulation.

In 1965 and again in 2003, regional blackouts hit the Northeastern United States, causing deaths and severe economic disruption. At the time of the 2003 Northeast Blackout, regulation of electric grid reliability was purely voluntary.

Constituents pressured Congress to act, but electric utilities, concerned about their bottom lines, resisted formation of a federal regulator. In a compromise with industry, Congress converted a pre-existing trade association, the North American Electric Reliability Council, into a self-regulatory organization with the power to both set and enforce grid standards.

NERC remained a private corporation, governed by the vote of its membership. And as before, its membership consists mostly of private electric utility companies. In fact, seventy percent of NERC members are electric utilities.

One would expect that electric utilities would be reluctant to impose grid protection standards on themselves, especially when those standards might reduce profits and increase liability.

The NERC track record since designation as a self-regulatory organization in 2006 has borne this out. Even the simplest standards take years to develop and approve.

For example, an errant tree branch was one cause of the 2003 Northeast Blackout affecting 50 million people, but NERC took ten years to approve a standard for tree-trimming.

On more complicated standards, such as those for cyber security, NERC inserts technical loopholes and questionable self-exemptions. For example, a 2011 NERC survey found that three-quarters of large electric generation plants—those with capacity over 300 megawatts—exempted themselves from cyber security standards. The current tenuous cyber-protection standards took forty-three months to write and approve.

In 2012, the persistent authors of the initially classified National Academy of Sciences report, "Terrorism and the Electric Power Delivery System," succeeded in obtaining its declassification. Page 1 states: "A terrorist attack on the power system would lack the dramatic impact of the attacks in New York, Madrid, or London....But if it were carried out in a carefully planned way, by people who knew what they were doing, it could deny large regions of the country access to bulk system power for weeks or even months."

California is the heart of America's high-tech industry, filled with data centers that need highly reliable grid power. Local businesses and homes cannot tolerate an electricity transmission system vulnerable to outages lasting "weeks or months."

Last April's transformer substation attack in San Jose demonstrates that terrorist threats to the grid are real and that voluntary standards are insufficient.

Californians and the entire country need a federal regulator that will mandate electric grid security, not a private consortium controlled by the interests of its electric utility members.

Dr. George H. Baker is Professor Emeritus, James Madison University and directed the JMU Institute for Infrastructure and Information Assurance.

Thomas S. Popik is chairman of the Foundation for Resilient Societies.

Energy firm cyber-defence is 'too weak', insurers say

By Mark Ward, Technology correspondent, BBC News
26 February 2014 Last updated at 19:26 ET

Power companies are being refused insurance cover for cyber-attacks because their defences are perceived as weak, the BBC has learned.

Underwriters at Lloyd's of London say they have seen a "huge increase" in demand for cover from energy firms.

But surveyor assessments of the cyber-defences in place concluded that protections were inadequate.

Energy industry veterans said they were "not surprised" the companies were being refused cover.

"In the last year or so we have seen a huge increase in demand from energy and utility companies," said Laila Khudari, an underwriter at the Kiln Syndicate, which offers cover via Lloyd's of London.

The market is one of few places in the world where businesses can come to insure such things as container ships, oil tankers, and large development projects and to secure cash that would help them recover after disasters.

'Worried'

For years, said Ms Khudari, Kiln and many other syndicates had offered cover for data breaches, to help companies recover if attackers penetrated networks and stole customer information.

Now, she said, the same firms were seeking multi-million pound policies to help them rebuild if their computers and power-generation networks were damaged in a cyber-attack.

"They are all worried about their reliance on computer systems and how they can offset that with insurance," she said.

Any company that applies for cover has to let experts employed by Kiln and other underwriters look over their systems to see if they are doing enough to keep intruders out.

Assessors look at the steps firms take to keep attackers away, how they ensure software is kept up to date and how they oversee networks of hardware that can span regions or entire countries.

Unfortunately, said Ms Khudari, after such checks were carried out, the majority of applicants were turned away because their cyber-defences were lacking.

"We would not want insurance to be a substitute for security," she said.

What was not clear, she said, was why firms were suddenly seeking cover in large numbers.

Although many governments had sent warnings about the threat from hackers, attackers and hacktivists to utility firms and other organisations running critical infrastructure, none had mandated them to get cover.

"I think what's behind it is the increase in threats and the fact that a lot of these systems were never previously connected to the outside world," she said.

Mike Assante, who helped develop cyber-security standards for US utilities and now helps to teach IT staff how to defend critical infrastructure including power networks, said it was "unfortunately not surprising" that insurers were turning away energy firms.

Power generators and distributors had struggled with the complexity and size of the networks they managed, he said. In addition they had found it hard to find and recruit staff with the specialist skills to defend these systems, he added.

"There have been a number of incidents that have caused company leadership to re-evaluate their risk and develop strategies to mitigate it," he said in an email to the BBC.

Growing threat

Financial pressures and the ability to manage systems remotely was inadvertently giving attackers a loophole they could slip through, said Nathan McNeill, chief strategy officer at remote management firm Bomgar.

Trying to cut costs by linking up plant and machinery to a control centre so they could be managed remotely meant those systems were effectively exposed to the net, he said.

"If something has basic connectivity then it will become internet connectivity through some channel," he said.

This left critical infrastructure exposed, he said, because typically the control systems for such hardware was written long before the web age and had only rudimentary security tools.

Known as Scada (Supervisory Control and Data Acquisition), this software has come under increasing scrutiny by security researchers who have exposed many flaws in it.

In addition, added Mr McNeill, it was often very difficult to update the core code in many Scada systems to close loopholes that attackers had slipped through.

Ed Skoudis, who runs "war games" for IT and security staff at many US utilities, said the numbers of attacks on Scada and other control systems was escalating.

Malware was being written just to get at particular vulnerable elements in the infrastructure run by many utilities and manufacturers, he said.

Some attackers were just curious but others were thought to be carrying out reconnaissance in service of some future event.

US power companies had begun sharing information about attacks so everyone knew about all the threats to them, said Mr Skoudis.

"However," he added, "it's surprising no big incident has happened given how weak the infrastructure is. It's very hackable."

The Washington Times

Was attack on San Jose electric-power substation terrorism?

By Peter Vincent Pry
Thursday, February 6, 2014

Vulnerability of grid demands attention, action

Now making headlines is news that last April unknown parties attacked an electric-power substation outside San Jose, Calif., attempting to black out Silicon Valley.

This underreported story deserved national attention when it happened nearly a year ago owing to major implications for electric-power grid vulnerability to terrorist attack.

The FBI must have read the White House memo that the war on terrorism is over. It says there is "no evidence" the attack was by terrorists. Never mind that a U.S. Navy SEAL team that investigated found it was highly professional, like a military operation.

Never mind that the attackers also knew how to cut telephone cables, understood the importance and vulnerability of transformers, and sprayed them with AK-47 fire, the favorite assault rifle of rogue states and terrorists.

The perpetrators, whoever they were, got away clean, and nearly a year later they have not been apprehended by the FBI.

Whoever attempted to sabotage the San Jose electric substation, whether or not they were terrorists, the incident should be a wake-up call to federal and state governments, and to the electric-power industry, that much more needs to be done to protect the grid.

Six months after the San Jose attack, on Oct. 29, a terrorist drug cartel called the Knights Templar, sabotaged the power grid in Mexico's Michoacan state, plunging 420,000 people into blackout, cutting off communications and help from federal authorities. They took advantage of the isolation to publicly execute town and village leaders opposed to the drug trade.

The bad guys are learning that the electric grid is a key societal vulnerability.

Those of us who want to protect the national grid need to make common cause and not get distracted over whether our efforts should focus primarily on kinetic attacks or cyberattacks, or on an electromagnetic pulse (EMP) from the sun, or from nuclear or non-nuclear weapons. We need to protect the grid from all the above.

R. James Woolsey, a former director of the CIA, in testimony to Congress in May 2013, warned that military plans by Iran, North Korea, China and Russia would not be limited to computer

viruses and hacking in an all-out cyberwarfare operation, but would include grid sabotage, kinetic attacks and nuclear EMP attack.

It is just common sense that if terrorists or rogue states try crashing America with a nationwide blackout, they are going to throw everything at us, including the kitchen sink.

The Congressional EMP Commission advocated an "all hazards" strategy and made recommendations for cost-effective protection of the national grid. By safeguarding the grid from the worst-case threat — nuclear EMP attack — all other threats would be mitigated as well.

The commission estimated the cost of hardening the national grid would be about $2 billion — the amount we give away annually in aid to Pakistan.

In its investigation of the attack on the Silicon Valley grid, perhaps the FBI might want to consider the following: A senior executive at the Electric Power Research Institute was quoted in The Wall Street Journal saying that the San Jose attack "appears to be preparation for an act of war."

The April 16 attack happened amid a major nuclear crisis. On Feb. 12, 2013, North Korea conducted its third nuclear test, and throughout March and April, it was threatening to make nuclear-missile strikes on the United States.

President Obama took these threats so seriously that he beefed up national missile defense and made demonstrations over the Korean demilitarized zone with B-2 bombers to deter the North.

If the attack on the San Jose substation, which services a nearby 470-megawatt power plant, had been successful, it might have triggered a cascading blackout beyond the Silicon Valley, collapsing the grid in California and the West Coast, which is vital to supporting U.S. military operations in the Pacific.

A few months later in July 2013, a North Korean freighter was intercepted attempting to transit the Panama Canal carrying two nuclear-capable SA-2 missiles with their launchers, hidden in its hold.

The missiles had no warheads, but the EMP Commission's nightmare scenario is the execution of an anonymous EMP attack by terrorists or a rogue state launching a missile off a freighter near the U.S. coast, such as in the Gulf of Mexico.

Iran has threatened retaliation on the U.S. grid for the U.S.-Israeli cyberattack known as the "Stuxnet Worm" on Iran's nuclear program. The worm allegedly was developed in the Silicon Valley. Iran and North Korea are strategic allies by treaty.

Maybe all of this is mere coincidence. Maybe not.

Peter Vincent Pry is executive director of the Task Force on National and Homeland Security and served on the Congressional EMP Commission.

The national electric grid system supports all other critical infrastructures, including food and water delivery, banking and financial services, transportation and telecommunications, and hospital and emergency services.