TESTIMONY OF

CYNTHIA E. AYERS,
DEPUTY TO THE EXECUTIVE DIRECTOR
TASK FORCE ON NATIONAL AND HOMELAND SECURITY

BEFORE THE

ENERGY POLICY COMMITTEE,
MICHIGAN HOUSE OF REPRESENTATIVES

on
March 7, 2017

Note: The views expressed in this product are those of the author and the Task Force on National and Homeland Security, and do not necessarily reflect the official policy or position of the U.S. Army War College or any Intelligence Agency within the United States Government.

The Cyber/Smart Grid Tech Threat to the Integrated North American Critical Electric Infrastructure

Honorable Chairman Glenn and Distinguished Representatives –

Thank you for this opportunity to discuss a topic that I believe is of primary importance to the security of the people of Michigan and the entire United States.

I am a threat/warning analyst with 44 years of experience, mostly as an employee of the National Security Agency (NSA), at times attached to other organizations to include:

- the Central Intelligence Agency's Counterterrorism Center during the attacks on the USS Cole and 9/11, as well as
- the U.S. Army War College (USAWC) where, for 8 ½ years as the NSA Visiting Professor, I taught Cyberwarfare, Current Strategic Threats to National Security, and Military Applications of Artificial Intelligence. I am currently employed at the USAWC as a strategic cyberwarfare consultant.

It is also my honor to serve as Deputy to the Executive Director of the Congressionally-sponsored Task Force on National and Homeland Security, as well as on the advisory board of Canada's Mackenzie Institute.

My testimony will concentrate on the possibility of a catastrophic cyber attack to the systems we depend on for the delivery of electricity – the lifeblood of our modern civilization.

The Threat

In this modern, networked world, our country's strategic center of gravity ("the hub of all power and movement, on which everything depends"[1]) for both military and civilian sectors is the electric grid. Our critical electric infrastructure is therefore exactly where belligerents aim their weapons, both cyber and kinetic.

A successful military operation against an enemy's center of gravity will effectively remove that entity's ability to act or react, instantaneously and long-term. Such an attack against the electric grid of a country could easily win an entire war – and it can be done with relatively little effort as a strategic "first strike." Because a great deal of coordination is generally needed for a cyber-only endeavor of that magnitude, and cyber effects may not be long-lasting, it is probable that a first-strike option would begin with a major cyber distraction followed by a devastating kinetic blow to the strategic center of gravity – the grid.

Cyber threats to our electric infrastructure, from a variety of sources, have increased at an astounding rate. The aggregate attack statistics are overwhelming. For example, a small Midwestern utility consortium "recently detected nearly 4 million hacking attempts in one eight-week period."[2] But much like the growth of the Internet, the development of smart grid technology has been paramount, while security designed for components and networks remains deficient.

As our electric grid becomes "smarter" and more networked, it also becomes more vulnerable, making it a very inviting – perhaps *the most* inviting – target for adversaries. Threats specific to smart grid technology range from the tactical (e.g. house-to-house, building-to-building) to the national strategic level. As with cyber activities world-wide, operational attacks against small, inconspicuous elements (smart meters, for example) could ultimately have a much larger, truly catastrophic impact to the grid and to the society it sustains.

Smart Meters and Open Backdoors

Although security can always be improved, all networks, all systems – virtually anything computerized – can be hacked. As systems become more highly networked, it becomes easier for attackers to locate "backdoors." Multiple "smart" appliances and other home or business devices are being developed and sold on the market, with the assumption that IoT (Internet of Things) networking and metering will soon be (if not already) commonly available. Demand for full optimization of smart meters will ultimately rule out limited, billing-only usage (e.g. Meter

to Cash or M2C). The number of gaps in security will multiply per person, per household; and a successful ingress of any "backdoor" could have detrimental effects on neighbors, communities, regions, states, the nation and beyond (e.g. Canada and Mexico). Passive cyber defenses will be of prime importance, yet ubiquitous usage of large numbers of components will only serve to increase gaps in security, regardless of the options given to consumers.

Smart meters can provide digital backdoors to facilities (e.g. the home, office, building, etc.) via the items within (e.g. televisions, refrigerators, thermostats, etc.). They can also allow access to multiple components of external electric infrastructure.[3] Therefore, the use of smart meters must be carefully evaluated in the context of threats to personal safety as well as the safety of the grid.

Physical Security

A trip to Johns Hopkins Applied Physics Lab to speak with the young students who work on IoT networks will reveal the extent to which hackers can gain access to metered appliances, which – even individually – can reveal dynamic information such as whether a building is occupied, who the occupants are, and where they are located within the building. This information alone gives kidnappers, terrorists, or other types of attackers previously unimagined advantages.

Another physical safety aspect of smart meters was raised by a Fire Chief Duane Roddy during your hearing of February 21, 2017. In a discussion of electrical arching and a fire that began only 36 hours after the installation of a smart meter on his own home, the Chief stated that there is no surge protection associated with the new meters (older analog meters do have surge protection). It should be noted that massive surges (with much greater effects than weather related or other types of flow interruptions) are associated with severe space weather (geomagnetic storms caused by coronal mass ejections from the sun) and electromagnetic pulse (EMP) associated with high-altitude nuclear explosions – both of which have been known to cause arching and fires.[4]

Hackers are also figuring out how to cause surges, using smart meters to access air conditioning systems. "If an attacker were to turn the air conditioners on and off repeatedly, the [infiltrator] could create disturbances and imbalances in the grid that could trip breakers beyond the neighborhood they're targeting and cause an even more widespread blackout."[5]

Grid Security

Interestingly, hacker access to appliances within a networked building doesn't seem improbable these days; and the general idea of a need for increased grid security is gaining ground from public and private sector perspectives. "In a January 2016 poll, 84 percent of cybersecurity professionals believed there was a high or medium likelihood of a cybersecurity attack occurring this year that would be serious enough to disrupt critical U.S. infrastructure such as the electric grid."[6]

Nevertheless, it remains difficult to explain the potentially *lethal* aspect of adversarial intent in the cyber realm. We've grown used to so much inconvenience on the net, caused largely by hactivists and criminals, that thinking in terms of cyberwarfare (where cyber attacks may turn kinetic) is a difficult cognitive leap for some to make. It is, however, extremely important that all who are tasked with or otherwise concerned with the well-being of the grid understand the potentially devastating consequences of what has become the most plausible conflict scenario – a strategic cyber "first strike."

Strategic "First Strike"

Cyber analysts have relatively recently proposed that nations around the world are currently engaged in a "cyber cold war." If indeed that has been the case, the year 2015 might, in retrospect, be classified as the point at which the cyber cold war escalated to the very edge of a global "hot war." It began with revelations of system infiltration and data theft on a massive scale. It ended with a successful "show of force:" a message in the form of what could be considered a "proof-of-concept" display of a strategic cyber "first strike" strategy against an opponent's military and civilian center of gravity – the Ukrainian electric infrastructure.

The electric grid is a requirement, paramount for the continued functioning of modern society. Without it, there is no banking, no water sanitation, marginal health care, limited transportation, communications, food production, and (equally important) food distribution. Within a period of weeks to months without electricity, supplies of food, water, and medicines will be gone, and social order will spiral out of control. The result of a prolonged outage could ultimately be millions of deaths.[7] A successful "first strike" against an opponent's electric infrastructure could effectively – and possibly instantaneously – decide the outcome of a war.

The electric grid is the one essential element upon which all other critical infrastructures rely. Our adversaries (specifically Russia, China, Iran and North Korea) know this. They have written about it. They have warned us and threatened us. At least one actor – allegedly Russia – has now provided evidence of a cyber capability to disrupt civil society, with an operational component that portends full-scale war.

Proof-of-Concept

On December 23rd, 2015, "multiple regional power companies"[8] in Ukraine were identified as targets of a major cyber attack which resulted in a power outage to 225,000 customers (households, businesses, etc). A few months later, the United States Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) convened briefing sessions across the U.S. for public utility asset owners, Industrial Control System (ICS) vendors, and government personnel, to deliberate the implications of the attack against the Ukraine's power infrastructure. These briefings represented a sea change, by both utilities and governing bodies, in public acknowledgement that cyber intrusions, previously believed to be merely benign (albeit with malicious intent), have evolved into dormant weapons that, when triggered, could be considered "acts of war."[9]

The cyber attack on the Ukrainian electric grid was a demonstration of power by the attackers. Although cyber and military conflict between Russia and Ukraine has been simmering since early 2014, this event was, in essence, a proof-of-concept for a larger application – a "first strike" that could neutralize and potentially destroy the center of gravity for virtually any opponent dependent on the continued availability of electricity. For Ukraine, this proof-of-concept was indeed an act of war. For the rest of the world, it was a message – an omen of what is yet to come.[10]

Dr. Adam Segal, writing for the Council on Foreign Relations, labeled a period beginning June 2012 as "Year Zero:"

- Cyber activities prior to Year Zero consisted mostly of espionage and criminal acts, as well as a continual low-to-mid-level digital clash among a wide variety of cyber actors.
- Events within Year Zero (to include the introduction of Stuxnet and Shamoon malware) proved that nation-states could, and would, inflict damage to the maximum

> extent possible on public or privately owned targets, within their capabilities and means, in order to achieve their objectives.[11]

The question of whether the escalation evident with the Ukrainian grid attack is considered a "Year Zero" event is better left to analysts such as Dr. Segal. What is clear, is that objectives have expanded and intent has shifted. The victims of Stuxnet and Shamoon were computer systems. The main target of the 23 December cyber attack was the Ukrainian center of gravity. The end-users of the systems targeted were the citizens of Ukraine – their National Security depended upon electricity and their grid had been compromised.

No Longer Theoretical

The Ukrainian power outage, as the first (officially acknowledged)[12] successful cyber attack against a power grid, has "marked a major cybersecurity escalation global governments have long feared."[13] A digital "first strike," delivered remotely and stealthily as a devastating blow across the networks and against systems that are both critical to military operations and crucial to the maintenance of modern society, is no longer theoretical.

Based on analysis of the known operational aspects and malware associated with the event – a variant of BlackEnergy was identified as present – the Ukrainian attack is believed to have originated from within Russia. Originally intended for espionage, adaptations of BlackEnergy may now pose a threat to energy, water distribution and filtration, and financial systems worldwide.[14] In fact, similar attacks against a mining company and part of the national railway in Ukraine may have been part of the same attack scenario.[15]

This is the type of threat that American officials (to include former Defense Secretary Leon Panetta,[16] former DHS Secretary Janet Napolitano,[17] United States Cyber Command (USCYBERCOM) Commander and National Security Agency (NSA) Director Admiral Michael Rogers,[18] and the Director of National Intelligence (DNI) James Clapper[19]) have been warning the public about since 2012. It's interesting to note that the U.S. Industrial Control Systems Cyber Emergency Response Teams (ICS-CERT) have identified BlackEnergy malware within U.S. systems. Published warnings have surmised that the U.S. malware "campaign" may have begun as early as 2011.[20]

Arguably, the devastation resulting from a massive cyber attack may be more limited in scope than that expected of a high-altitude nuclear attack or a direct hit from a great geomagnetic

storm; but the abilities of attackers are growing as vulnerabilities lie unaddressed. Certainly, *at this point in time*, a more highly-coordinated effort would be necessary to initiate a continental-wide collapse and maintain it for a long period of time, but capabilities are ever-increasing and will undoubtedly remain relatively inexpensive to implement, with the additional benefit of limited or no attribution for the attackers. For example, KillDisk malware (seen in conjunction with BlackEnergy), which effectively "wipes" infected systems, adds to the disruption and can effectively limit attribution.[21] On-site spares could become difficult to maintain as "clean" replacements, due to the pervasive nature of systemic infections.

A U.S. team of cyber experts sent to Ukraine to investigate the event not only noted the physical damage caused by KillDisk malware associated with the attack, but also described actions associated with the monitoring of event response as well as continued disruptions intended to slow down the process of restoring power. The attackers were apparently performing surveillance, developing battle-damage assessments, and performing tactical maneuver in cyberspace, while adapting to conditions "on the ground." [22]

Peer and near-peer adversaries now have the resources to retain large numbers of cyber operators ("militias") to infiltrate, hide, conduct intelligence preparation of the battlespace, change data, disrupt system integrity, probe, prod, strike, and inflict damage conducive to further, incremental collapse[23] using valuable "zero-day" exploits.[24] Russia, China, Iran and North Korea are the main culprits at this level. Semi-state and non-state actors, such as those connected with the "so-called Islamic State,"[25] the hacktivist group Anonymous,[26] and the Syrian Electronic Army[27] are of somewhat lesser concern, although Ransomware attacks (which are gaining in popularity and sophistication) remain a threat to virtually all critical infrastructures.[28]

In testimony before the U.S. Senate Armed Services Committee on the 5th of April (2016), Admiral Rogers (in his capacity as Commander, USCYBERCOM), stated: "we have seen cyber actors from more than one nation exploring the networks of our nation's critical infrastructure—and can potentially return at a time of their choosing."[29]

Post Cyber Event Kinetic Attack

A cyber "first strike" to critical electric infrastructure could severely damage the military's ability to respond. Admiral Rogers warned that "if directed at the critical infrastructure that supports our nation's military, cyber attacks could hamper our forces, interfering with

deployments, command and control, and supply functions, in addition to the broader impact such events could have across our society."[30]

Furthermore, the distraction and disruption caused by an unexpected digital assault paves the way for post-cyber event kinetic action. In fact, the progress of digital "first strike" can be seen in the following aggressions involving Russia:

- "The first major cyber conflict" was in April of 2007,[31] when Russia expressed displeasure with the Estonian government over the movement of a World War II memorial in the capital city Tallinn. Estonia fell under cyber attack (mostly described as Distributed Denial of Service or DDOS) for a period of almost three weeks. (Moscow denied involvement.)
- In 2008, Russia used proxy cyber forces (or "third-party hackers") to assist with DDOS attacks against Georgia in order to disrupt communications prior to a Russian invasion. (Again, Moscow denied involvement with the cyber activities.) This was seen as a prototype for a "hybrid war."
- Cyber and military activities have been ongoing within Ukraine since early 2014, without yet reaching a climax associated with complete invasion, yet Ukrainian analysts believe there to be notable similarities between the "build-up" in the Ukraine and the earlier (pre-2008) conflict between Russia and Georgia.[32] The Ukrainian power outage ended within hours, and there was no reported military follow-on. The lack of action at the point of a grid-down scenario could, however, be explained as:
    - The intent to merely display capability and send a message; and/or
    - The need to obtain more information – in other words, the action was taken for the specific purpose of compiling intelligence on mitigation / recovery of data as "lessons learned" for a subsequent, larger effort.

The possibility of a cyber "first strike" against the electric infrastructure of a much larger opponent may not be far off. The use of cyber weapons for the purpose of power disruption does not rule out subsequent attack with weapons that have lasting effects (e.g. a high-altitude nuclear device). In fact, there are benefits to the utilization of cyber weapons for a "first strike:"

- Flexibility with regard to operation initialization (e.g. "zero hour");
- The ability to use the same deployed cyber weapon for intelligence surveillance and weapons activation, as well as other functions;
- The ability to monitor and modify deployed cyber weapons as deemed necessary;

- If deployment is successful, a cyber assault can mask (by virtue of data corruption or distraction) other activities associated with a conflict, to include the arrival of kinetic weapons, military forces, or pre-positioned proxy cells.

Passive Cyber Defense is not a Reliable Sole Defense

Industrial Control Systems and their Supervisory Control and Data Acquisition networks (ICS/SCADA) – essentially all computerized systems that attach to and/or interface with transmission and distribution equipment, whether or not they individually interface with the Internet – are highly vulnerable to attack. This is true of communications links and all equipment (transformers, generators, capacitors, etc) that could be manipulated, altered, denied access to, and otherwise damaged or destroyed via instructions from hackers and/or malware.

Malicious code can be introduced to the system via the internet, via wireless devices, and from external storage devices[33] (e.g. those used during system maintenance). There are a multitude of ways that malware can be injected into a system. Once system infiltration has been accomplished, equipment settings can be changed, effects can be modified, and attacks masked. The most widely known example is the Aurora generator test;[34] but the Stuxnet virus[35] brought major attention to the problem, as did the destruction of Aramco's 30,000 computers in August of 2012.[36]

In March of 2013, Trend Micro researcher Kyle Wilhoit released a report on his effort to discover the types and extent of cyber attacks on control systems. Having set up "honeypots" where hackers would believe that they were able to control "fake gauges" of a water plant, Wilhoit found a surprising number of attacks that were amazingly advanced and successful ("roughly 17 would have been considered 'catastrophic' to the water pressure pumping system" that was used as a honeypot). The attacks notably came from both international and domestic sources.

Protection against cyber attacks via usual methods (passive defense) is not enough to thwart major adversarial cyber operations. A 2013 Verizon report noted that "finding specific vulnerabilities and blocking specific exploits is a losing battle."[37] In a similar vein, Secretary of

Defense Panetta had earlier noted that the U.S. "won't succeed in preventing a cyberattack through improved [cyber] defenses alone." [38]

One reason that passive defense is not always the best defense is the time lag between attack and identification of attack-related activity, let alone the time needed to generate a software "fix." A major cyber intrusion and compromise of the US Army Corps of Engineers' National Inventory of Dams, attributed to Chinese military/government cyber actors in open source reporting, is one example that raised alarm over the possibility of a future cyber attack by China on the U.S. power grid.[39] The attacks occurred over a period of months, beginning in January (2013), only to be discovered in April – a delay that could be costly, if not deadly, in a cyberwar "first strike" scenario.

Passive defense is reactive and slow, as well as "patchy" in terms of efficiency. Because passive cyber defense will not always work, nor will it ever be enough, we need to look at other options for defense. An all-hazards approach is necessary to ensure protection of the grid.

Physical protections against electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) will enhance protection against cyber attacks. Blocking devices and transient voltage surge suppression devices that are specifically designed to eliminate the threat from GMD and EMP effects will go a long way toward eliminating the cyber threat. This is because many cyber attacks utilize data manipulation to cause damage to transformers, generators, etc. Obviously, passive defense practices in the way of software upgrades, protection programs, and firewalls must not be discounted; but they need to be supplemented by physical mitigation measures.

Risk Management Practices and Grid Security Are Not Compatible

"Worst case" does happen. In war, strategies designed to successfully employ worst case scenarios against an enemy are intentional. "Experienced practitioners . . . aim to identify the enemy's center of gravity and its critical vulnerabilities, then concentrate superior combat power to exploit those critical vulnerabilities, thereby forcing the enemy's culmination and so achieve decisive success."[40]

Consider the possibility that in one decisive action, critical vulnerabilities existing within our electric infrastructure could be exploited so successfully ***that the first and last battle in the next war occur simultaneously.***

In 2013, in response to a recent Executive Order (*Improving Critical Infrastructure Cybersecurity*[41]), a Brookings paper entitled *Bound to Fail: Why Cyber Security Risk Cannot Simply be 'Managed' Away*, was published. As the title would suggest, the authors criticized the Executive Order as insufficient because of its reliance on risk management and voluntary participation. ***"Business logic," which the authors note as inherent in the risk management framework, "ultimately gives the private sector every reason to argue the always hypothetical risk away, rather than solving the factual problem of insanely vulnerable cyber systems that control the nation's most critical installations*** **[italics added]."**[42]
Indeed, this has been the experience of those who have taken stances on grid protection against other types of attacks (e.g. high-altitude nuclear and radio frequency weapons) and natural disasters (e.g. great geo-magnetic storms caused by coronal mass ejections).[43] The North American Electric Reliability Corporation (NERC) is specifically cited by Langner and Pederson in the Brookings report as having difficulties with critical infrastructure protection (CIP) standards with regard to cyber security.

Risk-based models, as noted by the Brookings study,[44] effectively cause the user to ignore the outliers and engage only in the "most likely" threat. The complete, unquestioning acceptance of such has led us to a point where "worst case" is dismissed as "never going to happen," even when experience tells us otherwise. Our vulnerabilities are exposed by the over-reliance on risk management practices, and these vulnerabilities literally point our adversaries directly to the most effective strategic targets, tactics and procedures. While we, as nations, think "mutually assured destruction" (MAD) will keep catastrophic attacks from being attempted, our enemies think in terms of catastrophic first-strike scenarios to remove the United States and its neighbors as actors on the world stage – they know they can, because vulnerabilities are allowed to persist.

Reality

The Aramco attack (the Shamoon virus) in August of 2012 which destroyed over 30,000 computers was thought to be a counter-attack by Iran in retribution for the release of Stuxnet,[45] as were subsequent multiple and sustained attacks against U.S. banks. To the public's knowledge, little (if anything) was done in response. This has not yet seemed to have raised the ire of the grassroots. In fact, although Secretary of Defense Panetta raised the specter of a "Cyber Pearl Harbor" (as have others in the past), there is a great deal of published debate over the true capabilities of even the best cyber attackers. The discussion has led some to contend that a cyberwar would never cross the line into "physical space" or the kinetic realm,[46] in spite of the fact that operations associated with the 2008 Russian invasion of Georgia did just that.[47]

The substance of this open-source media debate on cyber capabilities is weakened by the fact that the public has not been made aware of the true extent to which actual cyber attacks have already been successful. The reasons for secrecy are myriad, and include not only classification of the data, but also an absolute need by business to exhibit trustworthiness as well as a fear of fallout related to insurance. (It may be a toss-up as to what business is more afraid of—cyber attacks, a loss of public confidence, or insurance "blowback.")

Cyber attacks, large or small, are most often thought of simply as excursions or provocations — without the kinetic attack/response assumptions associated with the event. Thus, to this point, even those resulting in substantial damage (e.g. leakage of classified data, loss of system functionality, or economic loss) – have not instigated a full-scale war, of either the cyber or kinetic varieties. Unless, that is, you count the current "cyber standoff" (multiple instances of cyber theft, vandalism, activism, intelligence gathering, and sabotage by a variety of actors)[48] as a type of long-term cold war enacted mainly by proxy.

Regardless, unpredictability in adversarial attack and response modes is something that must always be considered. There are occasionally unintended consequences of adversarial activities, especially if attacks have been sequential and cumulative. One such consequence is the possibility of a "trigger event" for a larger, less controlled cyber conflict leading up to full-scale kinetic war. The attack on the Ukrainian electric grid, as a proof-of-concept "first strike" weapon, may be the kind of cyber trigger that would initiate warfare in the other domains (Land, Sea, Air, and Space).

To the public's knowledge, however, there has been no definitive "red line" in regard to how much damage or loss a victim should accept before responding. It is to this point that a so-called "secret legal review," as reported by the *New York Times* (2013), speaks. The *Times* claimed that the President now "has the broad power to order a pre-emptive strike if the United States detects credible evidence of a major digital attack looming from abroad." The rules are said to be "highly classified."[49] This would seem to indicate concern of an adversarial catastrophic "first strike."

It has long been understood that one of the risks associated with initiating a cyber attack against a target is that the software involved can be turned around and used against the originator. Stuxnet, for instance, targeted a specific type and brand of industrial controllers which operated nuclear power plants in Iran. Although focused as an initial attack, once identified, nothing

prevented the malicious software from being revamped and redirected — making it more generic and/or focused on other types of systems.

It is advisable, of course, for the originator to harden vulnerable systems against blowback prior to unleashing damaging malware; but much depends on security classification, timing, and comprehensive identification of possible damage. Perhaps the well-publicized angst over attacks on U.S. critical infrastructure is indicative of a lack of adversarial intent on the part of the United States. Regardless, given the extent of the warnings issued since October of 2012, it seems that the United States is ill-prepared for a major attack against the electric grid. Such an attack, if well-coordinated as well as sufficiently staffed and resourced, could have catastrophic effects on the U.S. – and potentially the Canadian – population. If the grid were down for a year or more, over two-thirds of our population could be lost to malnutrition, disease, and chaos.[50] ***The "Pearl Harbor" analogy would be nowhere near sufficient to describe the extent of damage that would result.***

Furthermore, the analogy of a "Pearl Harbor event" could be short-sighted, by virtue of a subsequent lack of capability to respond. This would most probably be the intended result of any attack scenario against a bigger, more militarily equipped enemy, especially if a power grid attack had been previously and publicly cited as one of the few "trigger events" that would be considered an "act of war." It should be noted that Panetta's description was essentially that – "if a cyber attack . . . crippled our power grid in this country, took down our financial systems, took down our government systems, that would constitute an act of war."[51]

The Congressional EMP commission report on critical infrastructure stressed that everything (including banking and government) hinges on the success or failure of the power grid.[52] If the U.S. is ever hit with a catastrophic, long-term "grid-down" scenario, no matter what the exact cause, any response might be too late (and therefore irrelevant) for those within the affected area. ***It's hard to consider how to respond to a "cyber trigger" that is, in itself, a "civilization-ending event."***

If, as the *Times* reported, a pre-emptive authority has been given to the President, it is no doubt due to an understanding that ***we have yet to see "worst case."*** Those who prefer to advise the government to wait until "a safety issue is pervasive"[53] or until evidence of the effects present themselves *en masse*,[54] may not be expecting a "worst case" trigger event – a catastrophic attack against our center of gravity.

Why the Rush?

If recent history is any example, the North American Electric Reliability Corporation could take 10 to 15 years (or longer) to adopt standards necessary for an all-hazards approach to mitigation. By then, it could (and probably will) be too late. Our adversaries are "at the door," knowing that we are currently vulnerable. Some have already threatened use of high-altitude nuclear EMP attacks, others are building weapons to ensure catastrophic grid collapse, and still others have been attacking us incrementally within the cyber realm. They have more recently displayed the capability of a "first strike" against a nation's electric grid.

A continental crisis is already upon us, in the form of an extremely vulnerable power generation and distribution system existing within an increasingly threatening environment. As a threat/warning analyst with over 40 years of experience working national security issues, I regard the potential loss of our country's electric infrastructure as the number one threat we currently face. The facts have been presented in a number of reports – they speak for themselves.

Due to the manner in which cyber attacks are propagated, cybersecurity is everyone's business. It is ultimately up to individuals and the companies who employee them, to do what is necessary to meet this looming crisis. Leaders, in both the public and private spheres, must provide an environment conducive to the preservation of national security. The destruction of our critical infrastructure is not simply a "worst case scenario" that will probably never happen. It is a "weapon of choice" that will ensure victory to the attacker.

Our enemies are already protected against critical infrastructure collapse. We cannot and must not wait to protect our own center of gravity against inevitable attack.

ANNEX

Recommendations:

- Use an "all-hazards" approach for grid mitigation. **Retain analog systems to the extent possible.**
- Remove barriers to (or incentivize) cyber event reporting. Refrain from "punishing" utilities for reporting cyber intrusions or other grid deficiencies. Punishment (with or without fines) encourages a lack of reporting.[55]
- Establish clarity of authorities, roles, and responsibilities.[56]
- Maintain training standards that include the potential for manual operations (if possible) as well as constant questioning of data displayed (corruption/manipulation of data has been noted in cyberattacks).[57]
- Utilize best cybersecurity practices. ICS-CERT has posted Department of Homeland Security, Department of Justice, and National Security Agency document entitled *Seven Steps to Effectively Defend Industrial Control Systems*. Contact information for all three organizations is included.[58] (See: https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems)
- Retain "clean" and/or analog spares (e.g. uninfected control systems) and other resources to the extent possible.
- Secure and maintain all physical grid components, as damage can be exacerbated and amplified by weak links, even if the initiation of an event is cyber specific.[59]
- Do not depend on risk management for any aspect of grid security.[60]

Endnotes

[1] Strange, Joe and Iron, Richard (n.d.). "Understanding Centers of Gravity and Critical Vulnerabilities," http://www.au.af.mil/au/awc/awcgate/usmc/cog1.pdf (accessed March 5, 2017).
[2] Begos, Kevin (2016, November 11). *Protecting the Power Grid.* CQPress http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2016111100 (accessed March 5, 2017).
[3] Downing, Louise and Polson Jim (2014, July 2). "Hackers Find Open Back Door to Power Grid With Renewables," *Bloomberg*.
[4] Foster, J. S. Jr.; Gjelde, E; Graham, W. R.; Hermann, R. J.; Kluepfel, H. M.; Lawson, R. L.; Soper, G. K.; Wood, L. L. Jr.; and Woodard, J. B. (2008, April). *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*, Washington, DC;
[5] Zetter, Kim (2016, February 9). "How to Hack the Power Grid Through Home Air Conditionings," Wired https://www.wired.com/2016/02/how-to-hack-the-power-grid-through-home-air-conditioners/ (accessed March 5, 2017).
[6] Begos, Kevin (2016, November 11). *Protecting the Power Grid.* CQPress http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2016111100 (accessed March 5, 2017).
[7] Foster, J. S. Jr.; Gjelde, E; Graham, W. R.; Hermann, R. J.; Kluepfel, H. M.; Lawson, R. L.; Soper, G. K.; Wood, L. L. Jr.; and Woodard, J. B. (2008, April). *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*, Washington, DC;
[8] Radiflow (2016, January 21). "The Ukrainian Outage," *Radiflow*.
[9] Tapper, Jake (2012, May 27). "Leon Panetta: A Crippling Cyber Attack Would be 'Act of War," *ABC News*.
[10] Defazio, Congressman Peter (2016, April 14). *Blackout! Are We Prepared to Manager the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?* U.S. House of Representatives Committee on Transportation and Infrastructure.
AFP (2016, March 2). "NSA Chief Worries About Cyber Attack on US Infrastructure," *Security Week*.
[11] Segal, Adam (2016). *The Hacked World Order*, New York: Council on Foreign Relations, p. 1-16.
[12] See Harris, Shane (2014). *@War: The Rise of the Military-Internet Complex*. New York: Houghton Mifflin Harcourt. See also Brenner Joel (2011). *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: The Penguin Press, p. 105 for reports of apparently successful grid attacks against other nations.
[13] Tomkiw, Lydia. (2016, January 6). "Did Russia Kill Ukraine's Electricity? Cyberattack Linked to Power Outage Has Global Implications," *International Business Times*.
[14] Segal, Adam (2016). *The Hacked World Order*, New York: Council on Foreign Relations, p. 13; See also, ICS-CERT Alert (ICS-ALERT-14-281-01E), (2016, March 2). *Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)*.
[15] Wilhoit, Kyle (2016, February 11). "KillDisk and BlackEnergy Are Not Just Energy Sector Threats," *Trendlabs Security Intelligence Blog*. TrendMicro.
[16] Bumiller, Elisabeth and Shanker, Thom (2012, October 11). "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times.*
[17] Levine, Mike (2013, August 27). "Outgoing DHS Secretary Janet Napolitano Warns of 'Serious' Cyber Attack, Unprecedented Natural Disaster," *ABC News*.
[18] Lyngaas, Sean (2014, November 20). "NSA Director Predicts Major Cyberattack by 2025," *FCW*.
[19] Gertz, Bill (2015, September 16). "DNI: Russians Hacked U.S. Industrial Control Nets," *The Washington Free Beacon*.
[20] ICS-CERT Alert (ICS-ALERT-14-281-01E), (2016, March 2). *Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)*.
[21] Tucker, Patrick (2016, March 9). "The Ukrainian Blackout and the Future of War," *Defense One*.
[22] Abdollah, Tami (2016, February 27). "Sophisticated Attackers Hacked Ukrainian Electric Grid," *Military.com*; See also Gertz, Bill (2016, March 9). "CYBERCOM Says Cyberattacks on Infrastructure Coming," *The Washington Tiimes.*
[23] Burke, Garrance and Fahey, Jonathan (2015, December 22). "Iranian Hackers Breached US Power Grid to Engineer Blackouts: Investigation Finds Outdated Cyberdefense for America's Key Infrastructure, With Attackers Lurking, Waiting to Strike," *The Times of Israel*. See also: Clayton, Mark (2013, February 27). "Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage," *Christian Science Monitor*.

[24] Tucker, Patrick, (2016, March 9). "The Ukrainian Blackout and the Future of War," *Defense One*. For more on "Zero Day exploits," see Zetter, Kim (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.
[25] Rogers, Admiral Michael S. (2016, April 5). *Statement Before the Senate Armed Services Committee*. Washington, DC: U.S. Senate.
[26] Liebowitz, Matt (2012, February 21). Could Anonymous Really Knock Out the Power Grid? *NBC News*.
[27] Department of Justice (2016, March 22). *Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army*. Washington, DC: Department of Justice Office of Public Affairs.
[28] Storm, Darlene (2016, January 27). "No, Israel's Power Grid Wasn't Hacked, but Ransomware Hit Israel's Electric Authority," *Computer World.*
[29] Rogers, Admiral Michael S. (2016, April 5). *Statement Before the Senate Armed Services Committee*. Washington, DC: U.S. Senate.
[30] Rogers, Admiral Michael S. (2016, April 5). *Statement Before the Senate Armed Services Committee*. Washington, DC: U.S. Senate.
[31] Segal, Adam (2016). *The Hacked World Order*, New York: Council on Foreign Relations, p. 60-66.
[32] Euromaidan Press (2015, September 5). Kremlin Hybrid War Tactics in Georgia, 2008, and Ukraine, 2014-2015: Different Countries, Same Playbook. Euromaidan Press.
[33] ICS-CERT (2012). Industrial Control Systems Cyber Emergency Response Team Monthly Monitor (ICS-MM201210) October/November/December 2012: http://ics-cert.us-cert.gov/monitors/ICS-MM201210 (accessed 30 September 2013).
[34] Burkhart, Lori A. (2008, January), "Cyber Attack! – Lessons Learned: Aurora Attack," *Fortnightly Magazine*.
[35] Kushner, David (2013, February 26). "The Real Story of Stuxnet: How Kapersky Lab tracked down the malware that stymied Iran's nuclear fuel enrichment program," *IEEE Spectrum*.
[36] Infosecurity Magazine (2012, August 24) "Shamoon likely the malware used against Saudi oil giant Aramco," *Infosecurity Magazine.*
[37] Chuvakin, Anton (2013, April 29) "Verizon DBIR 2013 Highlights and Favorites;" Verizon (2013) *2013 Data Breach Investigations Report*.
[38] Bumiller and Shanker, "Panetta warns of Dire Threat of Cyberattack on U.S."
[39] ICS-CERT (2013). Industrial Control Systems Cyber Emergency Response Team Monthly Monitor (ICS-MM201306) April/May/June 2013: http://ics-cert.us-cert.gov/monitors/ICS-MM201306 (accessed September 30, 2013).
[40] Strange, Joe and Iron, Colonel Richard (n.d.). "Part 2: *The CG-CC-CR-CV Construct: A Useful Tool to Understand and Analyze the Relationship between Centers of Gravity and their Critical Vulnerabilities."*
[41] Obama, President Barak H. (2013, February 12) *Executive Order: Improving Critical Infrastructure Cybersecurity*.
[42] Langner, Ralph and Pederson, P. (2013, February) "Bound to Fail: Why Cyber Security Risk Cannot Simply Be 'Managed' Away," February 2013, *Center for 21st Century Security and Intelligence.*
[43] Kappenman, John. G. (2012, April 30) *Prepared Testimony of John G. Kappenman Before the U.S. Federal Energy Regulatory Commission Technical Conference on Geomagnetic Disturbances on the Bulk Power System*; and Pry, Peter Vincent (2012, April 30) *Testimony of Dr. Peter Vincent Pry, Executive Director, Task Force on National and Homeland Security, Before the U.S. Federal Energy Regulatory Commission Technical Conference on Geomagnetic Disturbances to the Bulk Power System*.
[44] Langner and Pederson, "Bound to Fail: Why Cyber Security Risk Cannot Simply Be 'Managed' Away."
[45] Shanker, Thom and Sanger, David E. (2012, October 13) "U.S. Suspects Iran Was Behind a Wave of Cyberattacks," *The New York Times*.
[46] Clayton, Mark (2012, December 7) "'Cyber Pearl Harbor': Could future cyberattack really be that devastating?" *Christian Science Monitor*.
[47] Masters, Jonathan (2011, May 23) "Confronting the Cyber Threat," *Council on Foreign Relations.*
[48] Ibid.
[49] Sanger, David. E. and Shanker, Thom (2013, February 3) "Broad Powers Seen for Obama in Cyberstrikes," *The New York Times*.
[50] Foster, et al. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*.
[51] Tapper, " Leon Panetta: A Crippling Cyber Attack Would Be 'Act of War.'"
[52] Foster, et al. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*.

[53] Sternstein, Aliya (2013, February 1). "Carhacking," *Government Executive*.
[54] Langner and Pederson, "Bound to Fail: Why Cyber Security Risk Cannot Simply Be 'Managed' Away."
[55] Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, p. 106-107.
[56] Government Accountability Office (2016, April 4). *DOD Needs to Clarify Its Roles and Responsibilities for Defense Support to Civil Authorities During Cyber Incidents* (GAO-16-332). Washington, DC: U.S. Government Accountability Office.
[57] Tadjdeh, Yasmin (2013, July). "Cyberspies Can Destroy, Corrupt Data as Easily as They Snoop," *National Defense*.
[58] ICS-CERT (2015, December). *Seven Steps to Effectively Defend Industrial Control Systems.* Washington, DC: DHS, DOJ, NSA.
[59] Faza, Ayman, Sedigh, Sahra, and McMillin, Bruce (2010, April 21). "Integrated Cyber-Physical Fault Injection for Reliability Analysis of the Smart Grid," *Proceedings of the 4th Annual ISC Research Symposium*, Rolla, MO.
[60] Langner and Pederson, "Bound to Fail: Why Cyber Security Risk Cannot Simply Be 'Managed' Away."