Legal Duties to Avert, Mitigate, and Recover from Cyber Attacks on the Grid[1]

by

Roland L. Trope[2] and Stephen J. Humes[3]

Introduction. In this brief essay, we have two objectives: first, to provide a glimpse at the complexities that will be faced by electric power utilities, wholesale power generators, power grid operators and their customers if the North American electrical grid is the target of a systematic and combined physical and cyberattack that causes cascading outages, damage to hard-to-replace equipment, and results in months of degraded reliability in electricity delivery in one or more regions; and second, to explore some of the existing and emerging legal duties of electrical utility companies and other major enterprises of the bulk power system to avert, mitigate, and recover from damaging cyberattacks on the North American electrical grid.

This discussion is to provide background for a continuing legal education presentation on the subject and for a proposed project for development of a guide for electric bulk power utility and other corporate counsel to assist their clients in addressing their legal obligations to defend against, reasonably respond to, and recover from a damaging cyberattack on the grid, particularly one that could severely degrade the grid for a prolonged period and pose significant potential liability for utility and non-utility enterprises in that event. This essay will therefore attempt to give lawyers, who are experienced in cybersecurity and other cyberspace issues, a short introduction to some of the issues and complexities that we believe may arise if coordinated and systematic physical and cyber attacks on the bulk power grid occur and cause substantial long-term damage.

We are mindful of the work of the ABA Task Force on Cybersecurity and of its current plans to produce at least two written products by late spring 2013: (i) a guide for enterprises on how to respond to a cyberattack, and (ii) a cyber and data security guidebook for lawyers and law firms. The guide contemplated by this essay, and towards which it makes a provisional step, is intended to supplement without duplicating the work products currently in progress by the ABA Task Force. Moreover, the guide is intended to be of assistance not only to electricity industry

---

[2] Roland L. Trope is a partner at Trope and Schramm LLP in its New York City office, an Adjunct Professor in the Department of Law, U.S. Military Academy at West Point, and a member of the ABA Task Force on Cybersecurity. His bio can be accessed at http://www.linkedin.com/in/tropelaw. He can be contacted at rltrope@tropelaw.com.

[3] Stephen J. Humes is a partner at Holland & Knight in its New York City office and a member of the ABA Section of Environment, Energy & Resources. His bio can be accessed at http://www.hklaw.com/Stephen-Humes/. He can be contacted at Steve.Humes@hklaw.com. Mr. Humes acknowledges with appreciation the research assistance of Nicole Kipnis, associate at Holland & Knight.

company counsel, but to counsel for any enterprise whose operations depend on the reliable supply of electricity and whose current contingency and disaster recovery plans may not adequately address the probable consequences of a slow and incomplete recovery from a combined physical and cyber attack on the North American bulk power grid.[4]

In pursuit of the aforementioned objectives, this essay will address five topics in quick succession:

(1) Recent reports of cyber threats and/or cyberattack incidents and their significance for corporate Boards of Directors, and particularly those of electric utility enterprises and independent power producers;

(2) The rigorous balancing required to ensure reliability of the North American Grid and its growing vulnerability to cyberattacks;

(3) Regulatory efforts to improve cybersecurity of the North American Grid and the ability of electric power generation and delivery enterprises to recover from damaging attacks; and

(4) Why cybersecurity threats to the Grid and their potential consequences have become issues for electric industry Boards of Directors.

* * * * * *

1. *Recent reports of cyber threats and/or cyberattack incidents and their significance for corporate Boards of Directors.*

The U.S. corporate experience with cyber attacks recently has been real, tangible, and severely damaging (many such attacks arguably state-sponsored, state command-and-controlled, and carried out for the benefit of state(s) that denied responsibility). Companies successfully attacked in the last three years included Google, Intel, Morgan Stanley, and several dozen other firms (dubbed "Operation Aurora"). Targets struck also included RSA – and with data stolen from it – Lockheed Martin (dubbed "Operational Shady RAT"). In 2011, McAfee's vice president observed,

> "There are only two types of companies – those that know they've been compromised, and those that don't know. If you have anything that may be valuable to a competitor, you will be targeted, and almost certainly compromised."[5]

In April 2012, in an article entitled, "Security tops boardroom agendas," the Financial Times reported that company IT chiefs are most concerned about security and that the issue is now a top priority for board agendas:

---

[4] For the purposes of this discussion, many threshold issues (*e.g.*, concerning ambiguities and differences among definitions, legal standards, and threat assessments) must be deferred to another writing (or to the deliberations and written product of the proposed project for the Cybersecurity Subcommittee of the ABA's Cyberspace Law Committee).

[5] Michael Joseph Gross, *Enter the Cyber-dragon*, Vanity Fair, September 2011, accessed at http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109.print.

> "Securing corporate intellectual property assets, customer data and other information in the face of an onslaught of attacks from cyber thieves, spies and 'hactivists' is now a top priority for most chief information officers and – increasingly – for the corporate boardroom.
>
> …
>
> While some of these attacks, like the attack on Lockheed Martin…become public, security experts say many more are never disclosed and some, typically carried out by three teams of hackers each responsible for a different phase of the attack, may last for years. 'The average 'nation state' espionage attack that we see has been going on for 12 to 24 months or longer, says Mr Lobel [of PwC].
>
> It is these attacks – and the potential for nation states to use hacking as a cyber warfare or cyber terrorism tool – that has intelligence agencies, the military and politicians most exercised, and has led to proposed legislation in the US and elsewhere designed to buttress the defence of vital infrastructure such as power grids and transportation systems."[6]

Subsequently, however, Congress did not act on the proposed legislation. Instead, three developments of significance occurred. First, there were reports beginning in September and October 2012 of cross-border cyberattacks against U.S. banks:

> " Cyber attacks on the biggest U.S. banks, including JPMorgan Chase & Co. (JPM) and Wells Fargo (WFC) & Co., have breached some of the nation's most advanced computer defenses and exposed the vulnerability of its infrastructure, said cybersecurity specialists tracking the assaults.
>
> The attack, which a U.S. official yesterday said was waged by a still-unidentified group outside the country, flooded bank websites with traffic, rendering them unavailable to consumers and disrupting transactions for hours at a time.
>
> Such a sustained network attack ranks among the worst-case scenarios envisioned by the National Security Agency, according to the U.S. official, who asked not to be identified because he isn't authorized to speak publicly. The extent of the damage may not be known for weeks or months, said the official, who has access to classified information."[7]

(A further wave of cross-border cyberattacks against U.S. banking websites occurred three months later, in December 2012.[8])

Second, in October 2012, President Obama signed Presidential Policy Directive 20, which was classified TOP SECRET,[9] but that, according to a Washington Post report,

---

[6] Paul Taylor, "Security tops boardroom agendas," FINANCIAL TIMES, April 24, 2012, accessed at http://www.ft.com/intl/cms/s/0/47b3bfec-8978-11e1-85b6-00144feab49a.html#axzz1t4lvlUlt.

[7] Chris Strohm and Eric Engleman, "Cyber Attacks on U.S. Banks Expose Computer Vulnerability," BLOOMBERG, September 28, 2012, accessed at http://www.bloomberg.com/news/print/2012-09-28/cyber-attacks-on-u-s-banks-expose-computer-vulnerability.html.

[8] Mark Clayton, "Cyberattacks on US banks resume, aiming to block their websites," THE CHRISTIAN SCIENCE MONITOR, accessed at http://www.csmonitor.com/USA/2012/1214/Cyberattacks-on-US-banks-resume-aiming-to-block-their-websites.

> "effectively enables the military to act more aggressively to thwart cyberattacks on the nation's web of government and private computer networks … [by addressing] what constitutes an 'offensive' and a 'defensive' action in the rapidly evolving world of cyberwar and cyberterrorism. … For the first time, the directive explicitly makes a distinction between network defense and cyber-operations to guide officials charged with making often-rapid decisions when confronted with threats. The policy also lays out a process to vet any operations outside government and defense networks …"[10]

Third, a "Pre-Decisional/ Deliberative" draft White House Executive Order on "Improving Critical Infrastructure Cybersecurity" (the "Draft Cybersecurity EO") began to circulate. The Draft Cybersecurity EO opens with what amounts to a current cyber threat assessment and declaration of a rather abstract strategy to thwart such threat:

> "Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nationa's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the protection and resilience of the Nation's critical infrastructure …We will achieve these goals through a partnership with the owners and operators of critical infrastructure that includes cybersecurity information sharing and collaborative development and the adoption of risk-based standards."[11]

Some details of the strategy partially emerge in later sections, and include the following:

- "The Secretary of Homeland Security (the Secretary) shall produce timely unclassified versions of all Department of Homeland Security reports of cyber threats to the U.S. homeland that identify a specific targeted entity … and shall establish a coordinated process that rapidly disseminates all [such] reports … to the U.S. targeted entity."[12]
- "[T]he Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security[13] … and shall confidentially notify [their] owners and operators …"[14]

---

[9] See Pamela N. Phillips, Chief, FOIA/PA Office, National Security Agency Central Security Service, LETTER TO ELECTRONIC PRIVACY INFORMATION CENTER, dated November 20, 2012, regarding FOIA Case #69164, accessed at http://epic.org/foia/nsa/EPIC-PPD-20-FOIA-NSA-Reply.pdf.

[10] Ellen Nakashima, "Obama signs secret directive to help thwart cyberattacks," WASHINGTON POST, November 14, 2012, accessed at http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_print.html.

[11] Executive Order, "Improving Critical Infrastructure Cybersecurity," Pre-Decisional / Deliberative Unclassified Draft of November 21, 2012, Section 1, copy available from this essay's authors.

[12] Ibid, Section 4(a) and (b).

[13] Ibid, Section 9(a).

[14] Ibid, Section 9(c).

- "The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the Director) to coordinate the development of a framework to reduce cyber risks to critical infrastructure (the Cybersecurity Framework) … [which] shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks … [and] shall incorporate existing consensus-based standards and industry best practices to the fullest extent possible."[15]
- "The [Cybersecurity] Framework shall … [use an approach] to help owners and operators of critical infrastructure identify, assess, and manage cyber risk … [and] shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure … [and] will also identify potential gaps that should be addressed through collaboration with particular sectors and industry-led standards organizations."[16]

In short, the draft Cybersecurity EO appears to attempt a two-pronged strategy. One prong focuses on the broad category of any commercial enterprise and one prong on a narrower category of a certain apparently high-value target, critical infrastructure enterprises.

For the first category, the Cybersecurity EO would authorize giving unclassified notice to the owners and operators of an enterprise if a known "cyber threat to the U.S. homeland" had targeted their company (we will refer to it as an "Imminent Target Notice"). There is no mention or suggestion that the US Government would provide the recipient of a Target Notice any guidance on the precise nature or source of the threat (particularly since the Imminent Target Notice must contain only unclassified information), its timing, ways to avert or defend against it, nor is there any requirement that the notified enterprise make timely use of the information or report back if the threat materialized, in what form the attack came, from where, or the extent of damage. Furthermore, there appears to be no express consideration in the draft Cybersecurity EO of the particular legal challenges that receipt of an Imminent Target Notice would pose to a publicly traded company (*i.e.*, a registrant) in light of the October 13, 2011 SEC Staff CF Disclosure Guidance on Cyberscurity; for example, would such a registrant be obligated to disclose, or excused from disclosing, receipt of such notice? Would it be required to include it when it evaluates whether and what to disclose to investors regarding its risk of a cyber incident occurring?[17] These are only a few of the serious issues that could well become immediate priorities for a Board of Directors and its legal counsel. But addressing these issues will be made far more complex and difficult if the recipient of an "Imminent Target Notice" receives little or no information that its directors, officers, and legal counsel will need in order to make prompt, prudent, and practical decisions to "harden the target," protect personnel and assets (tangible and intangible), and to adjust disaster response and recovery plans to be ready for what could prove to

[15] Ibid, Section 7(a).

[16] Ibid, Section 7(b).

[17] The SEC Staff Guidance informs registrants that they are expcted "to evaluate their cybersecurity risks and take into account all available relevant information" and should "consider the probability of cyber incidents occurring" when deciding whether and what to disclose as the registrant's "risk of cyber incidents." See Division of Corporation Finance, Securities and Exchange Commission, "CF Disclosure Guidance: Topic No. 2 Cybersecurity," accessed at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm and discussion of that Guidance in Roland L. Trope and Sarah Jane Hughes, "The SEC Staff's 'Cybersecurity Disclosure' Guidance: Will It Help Investors or Cyberthieves More?, BUSINESS LAW TODAY, December 19, 2011, accessed at http://apps.americanbar.org/buslaw/blt/content/2011/12/article-3-trope-hughes.shtml.

be a prolonged period of degraded operations – and which may need to be "gracefully degraded operations" if the enterprise is to continue to compete successfully in its markets.[18]

For the second category, not all critical infrastructure enterprises would appear to be the focus – only those that, if damaged by a cyberattack the consequences could "reasonably result in catastrophic regional or national effects." The owners and operators of these select critical infrastructure enterprises would be "notified confidentially" that they are in that category ("Catastrophic Target Notice"). It is unclear whether the Cybersecurity EO would require a Catastrophic Target Notice to do more than warn the recipient that if struck by a damaging cyberattack there could be "catastrophic regional or national effects on public health or safety, economic security, or national security." It is unclear whether such notice would include a caution or guidance on what the recipient might do to reduce the probability of such "catastrophic …effects." There appears, however, to be no express recognition of the legal challenges that receipt of such a notice would create for the enterprise, and particularly for its Board of Directors and legal counsel. Corporate counsel may wonder how such a silo-narrow perspective could dominate an Executive Order with such a broad and far-reaching impact for Boards of Directors.

There is, of course, a third (implicit) prong to the strategy: an enterprise that finds itself a recipient of both kinds of notice: that if struck and damaged by a cyberattack the consequences regionally or nationally could be "catastrophic" and that a known cyber threat to the U.S. homeland has targeted the enterprise. For these select few critical infrastructure enterprises, the legal challenges faced by a Board of Directors to fulfill its duties and obligations and the need for legal counsel are immediate and serious, and since the risks are potentially "catastrophic," it may be reasonably inferred that so might be the exposure of the company and its Board to legal liability resulting from the decisions taken in response to receipt of such notices.[19]

Moreover, it is unclear whether the Cybersecurity EO contemplates allowing a limited set of personnel, with a sufficiently high security clearance, at such an enterprise to receive any of the classified information on which the Imminent Target Notice was based. The fact that the Cybersecurity EO authorizes the Secretary to "expedite the provision of security clearances to appropriate personnel employed by" recipients of a Catastrophic Target Notice seems to suggest either a missed opportunity or an instance in which the drafter's hand was quicker than the reviewer's eye: if any enterprise's Board needs to be assured that some of its company personnel will receive expedited processing of security clearances it should be the recipients of the non-confidential, unclassified Imminent Target Notice; but instead, the Cybersecurity EO contemplates providing that expedited benefit solely to enterprises that receive Catastrophic Target Notice that may not even be based on any classified information. Perhaps the intent is to focus the benefit on recipients of both kinds of notices, but then it should say so and provide a policy to justify the decision, because the probable result will be to give a substantial protective advantage to such companies over recipients of solely an Imminent Target Notice or of solely a Catastrophic Target Notice (and thus giving such recipients of single notices far less data with

[18] For discussion of the legal challenges for a Board when faced with knowledge that their company is at an elevated risk of being a target of a terrorist attack (as, for example, an iconic landmark or other iconic enterprise), see Roland L. Trope, Monique Witt, and William J. Adams, "Hardening the Target," IEEE SECURITY & PRIVACY, September/October 2008, accessed at http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4639031&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F8013%2F4639007%2F04639031.pdf%3Farnumber%3D4639031.

[19] We note, however, that the draft Cybersecurity EO creates some unnecessary ambiguity by referring initially to cyber "threats" to the U.S. homeland, but thereafter discussing only cyber "risks."

which to comprehend the threat profile, the necessary preparations, and the risks to their response and recovery plans).

A Board would need to take great care in responding to the receipt of such notices, but mindful that such risks may well be overseen by a Board using its customary procedures for evaluating and managing risks. As observed in a November 2012 New York Law Journal article (written without reference to the draft Cybersecurity EO):

> "Cybersecurity risk is a difficult and intimidating topic for corporate boards to consider. However, it is important to keep in mind that cybersecurity risk is only one of many areas of risk that are overseen by boards of directors and that, in most cases, the usual strategies and procedures for evaluating and managing risk can apply. … The business judgment rule remains the standard for evaluating decisions taken by a board in this area."[20]

However, the article's authors note that cybersecurity crises may differ from other crises faced by Boards and may need to be addressed accordingly:

> "One potential difference between cybersecurity crises and other corporate crises is that both internal and external aspects of crisis management with respect to a cyber incident must begin within hours rather than days, in order to be as effective as possible. Directors should expect management to be prepared to respond very quickly to any cyber attack. … Unless the full board perform both [audit and risk committee] functions, it would be advisable to separate the task of developing cybersecurity management programs from that of reviewing the controls and effectiveness of these programs. Depending on the needs of the company, it may be worthwhile for the nominating committee to consider seeking one or more director candidates with some expertise in the area of cybersecurity and information technology."[21]

Even such sound guidance would probably need recalibration if the Cybersecurity EO is issued in substantially its draft form.

Moreover, if any critical infrastructure enterprise is at greatest probability of finding itself a recipient of both kinds of notice contemplated by the Cybersecurity EO, it would appear to be one of the nation's major electric power utility companies or independent power producers.[22] Put differently, if the Cybersecurity EO had been issued and fully implemented by now, electric power transmission and delivery companies and independent power producers would probably be among the earliest recipients of both of kinds of notices. The operators of the bulk power system

---

[20] David A. Katz and Laura A. McIntosh, "Corporate Governance Update: Cybersecurity Risks and the Board of Directors," New York Law Journal, November 29, 2012, accessed at http://www.newyorklawjournal.com/PubArticleNY.jsp?id=1202579604862&Cybersecurity_Risks_and_the_Board_of_Directors&slreturn=20130022234600.

[21] Ibid.

[22] Depending on the region, some electric utilities are vertically integrated operators of nuclear and fossil generation facilities and interstate transmission lines and local or regional distribution systems (such as parts of the southeast and west) whereas in the northeast, midwest and Texas, for example, regulated "electric utilities" continue to operate transmission lines and local/regional distribution systems while independent power producers operate power plants connected to the grid. Collectively, these parties and the independent system operators or regional transmission operators are contributing to the operation of the North American bulk power system.

clearly come within the critical infrastructure category.[23] And, the possibility that if seriously damaged, the regional or national consequences could be "catastrophic" has recently been analyzed and found to be highly probable if a major operator of facilities in the bulk power system was the target of a coordinated and systematic physical and cyber attack. The analysis, reportedly the "most authoritative yet on the grid's vulnerability,"[24] was conducted by the National Academy of Sciences, which released its report in November 2012, entitled *Terrorism and the Electric Power Delivery System*. The report's conclusions included the following:

> "The electric power delivery system that carries electricity from large central generators to customers could be severely damaged by a small number of well-informed attackers. … A terrorist attack on the power system … could deny large regions of the country access to bulk system power for weeks or even months. An event of this magnitude and duration could lead to turmoil, widespread public fear, and an image of helplessness that would play directly into the hands of terrorists. If such large extended outages were to occur during times of extreme weather, *they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold*.
>
> The largest power system disruptions experienced to date in the United States have caused high economic impacts. Considering that a systematically designed and executed terrorist attack could cause disruptions that were even more widespread and of longer duration, it is no stretch of the imagination to think that such attacks could entail costs of hundreds of billions of dollars – that is, perhaps as much as a few percent of the U.S. gross domestic product (GDP), which is currently about $12.5 trillion.
>
> Electric systems are not designed to withstand or quickly recover from damage inflicted simultaneously on multiple components. …
>
> Cyber attacks are unlikely to cause extended outages, but if well coordinated they could magnify the damage of a physical attack. For example, a cascading outage would be aggravated if operators did not get the information to learn that it had started or if protective devices were [cyber] disabled."[25]

If a company's U.S. Board of Directors views such an assessment as premature, it might take it more seriously if its counsel brought to its attention the occurrence in late November 2012 of a German power utility that experienced a cyber-attack that lasted five days, knocked its internet

---

[23] Pursuant to Section 215 of the Federal Power Act, 16 USC § 824o(e), the Federal Energy Regulatory Commission ("FERC") has jurisdiction to mandate that the operators of FERC-jurisdictional assets, including electric utilities and independent power producers, comply with the Critical Infrastructure Protection ("CIP") Reliability Standards developed and submitted to FERC for approval by the North American Electric Reliability Corporation ("NERC"), an Electric Reliability Organization. Among other details, the CIP Reliability Standards provide a cybersecurity framework for the identification and protection of "Critical Cyber Assets" to support the reliable operation of the bulk power system and establish "bright line" criteria for the identification of Critical Assets. See 139 FERC ¶ 61058 (Issued April 19, 2012).

[24] Matthew L. Wald, "Terrorist Attack on Power Grid Could Cause Broad Hardship, Report Says," The New York Times, November 14, 2012, accessed at http://www.nytimes.com/2012/11/15/science/earth/electric-industry-is-urged-to-gird-against-terrorist-attacks.html?hp&_r=0.

[25] Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack, Board of Energy and Environmental Systems, Division on Engineering and Physical Sciences, National Research Council of the National Academies, TERRORISM AND THE ELECTRIC POWER DELIVERY SYSTEM, 2012, pp. 1 and 2, accessed at http://www.nap.edu/catalog.php?record_id=12050#toc. [Emphasis in original.]

communications systems offline, and constituted the "first confirmed digital assault against a European grid operator." [26] However, the kind of attack considered by the National Academy of Sciences would aim at much more important systems of an electrical power utility – its supervisory control and data acquisition ("SCADA") systems. SCADA System security has been a serious concern to the U.S. Government at least since November 2008 when the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability issued a SCADA risk assessment report entitled "Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program" (the "2008 Report"). The 2008 Report derived from a program whose key part is the "assessment of control systems to identify and provide mitigation approaches for vulnerabilities that could put the systems at risk to a cyber attack."[27] The assessment, performed by the Idaho National Laboratory, covered 16 control systems from 2003 through 2007, found vulnerabilities that included: firewall filtering deficiencies, remote access deficiencies, buffer overflow in control system service, Structured Query Language (SQL) injection vulnerabilities, unpatched systems – and

> "There was a general lack of adequate control system indicators of abnormal conditions. Onsite assessments also found intrusion detection systems to be lacking in their installation, monitoring, and/or updating."[28]

If cyber threats and an enterprise's ability to respond to them have not already become a Board priority at most companies, it would now appear likely to do so – particularly at electric power transmission and distribution delivery system enterprises and independent power producers – if President Obama soon issues the contemplated Cybersecurity EO. Among the concerns, bulk power system operators will need then to address is the possibility that their enterprise's vulnerability to cyberattacks, particularly through attacks on its SCADA systems, could destabilize the critical balance required to ensure reliability of their portion of the North American grid, or could prevent a wholesale generator or power delivery company from detecting and responding correctly to an imbalance caused by a physical attack. The public and Boardroom perception of the Cybersecurity EO will be influenced by widely reported recent outages – one in India in July 2012 after three grids collapsed and left hundreds of millions of people without electricity for days (halting trains, forcing hospitals to run on backup generators)[29] and, of course, the tri-state weeks-long blackout experienced in the aftermath of superstorm Sandy and its accompanying tidal surge.[30] Easily overlooked, however, is that the far greater costs of such outages rests in the resulting economic disruption rather than in the price of electricity lost:

> "[T]here is growing recognition that the true cost of disruptions, in terms of gasoline lines, lost workdays and business sales, and shivering homeowners, is far higher than the

---

[26] "European renewable power grid rocked by cyber-attack,"

[27] U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability, COMMON CYBER SECURITY VULNERABILITIES OBSERVED IN CONTROL SYSTEM ASSESSMENTS BY THE INL NSTB PROGRAM, INL/EXT-08-13979, November 17, 2008, p. 1, accessed at

[28] Ibid, p. 29.

[29] "Hundreds of millions without power in India," BBC News, July 31, 2012, accessed at http://www.bbc.co.uk/news/world-asia-india-19060279.

[30] Michael Wilson, "Cold, Dark and Damp, Pockets of Misery Persist 2 Weeks Later," The New York Times, November 12, 2012, accessed at http://www.nytimes.com/2012/11/13/nyregion/pockets-of-misery-persist-2-weeks-after-hurricane-sandy.html.

> simple dollars and cents spent to protect the power system. A recent report from the National Academy of Sciences about the vast 2003 blackout in the Eastern United States determined that the economic cost of that disruption was about 50 times higher than the price of the actual electricity lost, and that didn't take into account deaths or other human consequences."[31]

Thus, public perception of the possibility of prolonged electrical outages over widespread areas and the public understanding of the severe burdens placed on individuals and businesses because of their high dependence on reliable supply of electricity has transformed such issues from science fiction into personal experience and probably will result in enhanced scrutiny of companies responsible for recovery from outages. In the next section of this essay, we review the kind of balancing required (by the laws of physics and certain applicable regulations) for reliability of the grid and why that balance is increasingly vulnerable to (and thus a soft target for) coordinated physical and cyber attacks.

2. *The rigorous balancing required to ensure reliability of the North American Grid and its growing vulnerability to cyberattacks*.

Early in the 20th Century, power systems in the United States involved small generating stations located in proximity to local distribution systems to supply low voltage power to the then new electric-driven devices – incandescent lights replacing oil lamps in homes and streetlights replacing gas lights in neighborhoods. The growth and dispersal of the capability to supply electricity led to larger systems, but these had to deal with the laws of physics. As power moves through a power line, it dissipates heat, and diminishes the quantity of power being transmitted. The farther that electrical power has to travel through a power line, the greater the loss of power that occurs – and the loss is so considerable that increased voltage is needed to overcome such line losses. As explained by the National Academy of Sciences November 2012 report,

> "High voltage is used to move power long distances in order to minimizer losses that result from the current heating the line. The power carried by a line is the product of the current and the voltage. However, for a given line, losses from heating go up as the square of the current. In moving a given amount of power, using a higher voltage reduces the current, and thus reduces the loss due to heating."[32]

As high-voltage transmission lines became more efficient, it became possible to replace small local power generators in cities with much larger generators built in remote rural locations. Starting in the mid-20th century, "system operators began to connect individual high-voltage systems together so that power could be moved from region to region, both to promote economic efficiency and to increase reliability by making it possible to move power into regions suffering from temporary shortages."[33]

---

[31] Diane Cardwell, Matthew L. Wald, and Christopher Drew, "Hurricane Sandy Alters Utilities' Calculus on Upgrades," The New York Times, December 28, 2012, accessed at http://www.nytimes.com/2012/12/29/business/hurricane-sandy-alters-utilities-calculus-on-upgrades.html?pagewanted=all.

[32] Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack, Board of Energy and Environmental Systems, Division on Engineering and Physical Sciences, National Research Council of the National Academies, TERRORISM AND THE ELECTRIC POWER DELIVERY SYSTEM, 2012, p. 7, footnote 1, accessed at http://www.nap.edu/catalog.php?record_id=12050#toc.

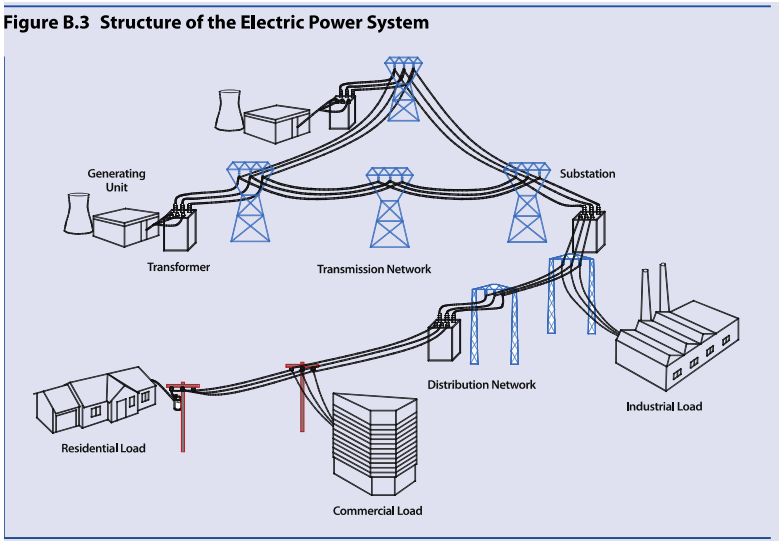
[33] Ibid, p. 7.

With the development of regional transmission systems and very large generating stations, including nuclear power plants with installed capacities in excess of 2,000 megawatts, electric utilities expanded systems throughout states and often across state lines.

The resulting system consists of generators that produce power (at 10,000 to 25,000 volts) in remote locations where the transmission system is energized at very high voltages (*i.e.*, 230,000 to 765,000 volts) and transmitted over long distance, high-voltage lines (visible in the tall towers from which they are suspended). At specific points, substations are located, each containing transformers to lower the voltage from transmission to distribution voltages, as well as SCADA controlled "switching gear that connects the system in desired configurations, and circuit breakers that open and close connections while also acting as giant fuses to protect expensive equipment from damage."[34] When the power lines (and the power they carry) reaches the vicinity of enterprise and individual customers, the voltage is reduced or "stepped down" further to service lines so that it can be distributed (for large industrial customers at intermediate voltage levels of 12,000 to 115,000 volts and for residential customers at 120 and 240 volts) over lower-voltage distribution and service lines. To summarize,

> "the electric power system is composed of four interacting physical elements: energy generation, high-voltage transmission, lower-voltage distribution, and energy consumption or load. Two less tangible elements are also important: the operational systems that protect and control the physical elements, and the regulatory and governance structures that shape the system's evolution."[35]

The figure below[36] depicts the structure of the electric power system:



[34] Ibid, pp. 7 – 8.

[35] MIT, THE FUTURE OF THE ELECTRIC GRID, 2011, p. 1, accessed at http://web.mit.edu/mitei/research/studies/the-electric-grid-2011.shtml.

[36] Ibid, p. 248.

In this essay, the term "grid" will refer to the wholesale power generation and physical transmission and distribution systems (from power generators to customer loads) and to the operational systems (especially the SCADA systems) on which the balancing of power and system reliability ultimately depend. In addition to these systems, modern electric utility industry "deregulation" in approximately half of the United States has created fragmented systems owned by multiple market participants with generating resources dispatched regionally by independent system operators ("ISOs") or regional transmission operators ("RTOs"). In these deregulated systems, the transmission and distribution utility's wire systems are monitored by the ISOs and wholesale power plants are dispatched based on economic principles (ideally, least cost dispatch first) and locational demand or system constraints (some plants are dispatched for reliability reasons even when not offered into the system at the lowest cost).

The technology does not yet exist to permit the economic storage of electricity in bulk and may not exist earlier than 2030.[37] Customers accustomed to flipping a switch in a room and seeing the lights immediately illuminate are seldom, if ever, aware of the complex system of systems (consisting, in part of computerized sensors and controls) that need to be monitored, responded to swiftly, and adjusted continuously in order to ensure the regional and local reliable provision of electricity that makes these quotidian activities seem normal (when they work) and so shockingly miraculous (when they don't and then finally are restored so that they do again work). As explained in major studies respectively of the grid and of the August 14, 2003 blackout in Canada and the United States:

> "[E]lectric power systems must vary the supply of electricity to meet minute-to-minute changes in demand and in the output of variable energy sources such as wind and solar generators. Power systems must be built with enough capacity to meet expected peak demand with some excess capacity for safety."[38]

> "Providing reliable electricity is an enormously complex technical challenge, even on the most routine of days. It involves real-time assessment, control and coordination of electricity production at thousands of generators, moving electricity across an interconnected network of transmission lines, and ultimately delivery the electricity to millions of customers by means of a distribution network."[39]

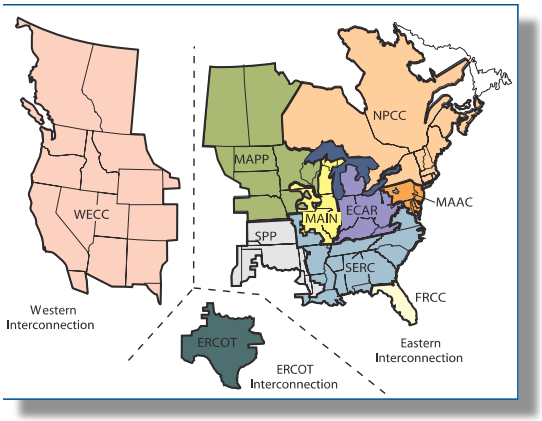
The North American Grid consists of three interconnected grids: Western Interconnection, Eastern Interconnection, and ERCOT Interconnection, shown in the figure below:

---

[37] Ibid, p. 2.

[38] Ibid.

[39] U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004, p. 5, accessed at https://reports.energy.gov/BlackoutFinal-Web.pdf.



It is important to note, however, the following:

> "The three interconnections are electrically independent from each other except for a few small direct current (DC) ties that link them. Within each interconnection, electricity is produced the instant it is used, and flows over virtually all transmission lines from generators to loads."

Regulation of electricity supply companies, however, evolved in part because for the North American Grid (hereafter the "Grid") reliable and safe operation are paramount priorities, and reliable operation is both complex and demanding for two reasons:

> "First, electricity flows at close to the speed of light (186,000 miles per second …) and is not economically storable in large quantities. Therefore electricity must be produced the instant it is used.
>
> Second, without the use of control devices too expensive for general use, the flow of alternating current (AC) electricity cannot be controlled like a liquid or gas by opening or closing a valve in a pipe, or switched like calls over a long-distance telephone network. Electricity flows freely along all available paths from the generators to the loads in accordance with the laws of physics – dividing among all connected flow paths in the network, in inverse proportion to the impedance (resistance plus reactance) on each path."[40]

Reliability of the Grid depends on the ISOs/RTOs (and the wholesale market participants under their control) in competitive markets and electricity utility companies in vertically integrated regions performing seven key tasks, some of which are briefly described below and which are the concepts developed by the NERC and its ten Regional Reliability Councils for ensuring the reliability of a transmission grid. In reading the description, however, consider how a cyber adversary would view the delicate balancing required and the serious consequences that can result if that balance is destabilized briefly or disrupted for a sustained period:

> "**1. Balance power generation and demand continuously.** To enable customers to use as much electricity as they wish at any moment, production by the generators must be scheduled or 'dispatched' to meet constantly changing demands, typically on an hourly basis, and then fine-tuned throughout the hour … Failure to match generation to demand

[40] Ibid, p. 6.

> causes the frequency of an AC power system (nominally 60 cycles per second or 60 Hertz) to increase (when generation exceeds demand) or decrease (when generation is less than demand). … Random, small variations in frequency are normal … However, large deviations in frequency can cause the rotational speed of generators to fluctuate, leading to vibrations that can damage generator turbine blades and other equipment. Extreme low frequencies can trigger automatic under-frequency 'load shedding' which takes blocks of customers off-line in order to prevent a total collapse of the electric system. …
>
> **4. Keep the system in a stable condition.** Because the electric system is inconnected and dynamic, electrical stability limits must be observed. Stability problems can develop very quickly – in just a few cycles (a cycle is $1/60^{th}$ of a second) – or more slowly, over seconds or minutes. The main concern is to ensure that generation dispatch and the resulting power flows and voltages are such that the system is stable at all times. … There are two types of stability limits: (1) Voltage stability limits are set to ensure that the unplanned loss of a line or generator … will not cause voltages to fall to dangerously low levels. If voltage falls too low, it begins to collapse uncontrollably, at which point automatic relays either shed load or trip generators to avoid damage. (2) Poer (angle) stability limits are set to ensure that a short circuit or an unplanned loss of a line, transformer, or generator will not cause the remaining generators and lods being served to lose synchronism with one another. … Loss of synchronism with the common frequency means generators [or transmission assets] are operating out-of-step [i.e., phases] with one another. Even modest losses of synchronism can result in damage to generation equipment. Under extreme losses of synchronism, the grid may break apart into separate electrical islands …
>
> **5. Operate the system so that it remains in a reliable condition even if a contingency occurs…** The central organizing principle of electricity reliability management is to plan for the unexpected. The unique characteristics of electricity mean that problems, when they arise, can spread and escalate very quickly if proper safeguards are not in place. … This principle is expressed by the requirement that the system must be operated at all times to ensure that it will remain in a secure condition … following the loss of the most important generator or transmission facility (a 'worst single contingency'). This is called the 'N-1 criterion.' … Further, when a contingency does occur, the operators are required to identify and assess immediately the new worst contingencies, given the changed conditions, and promptly make any adjustments needed to ensure that if one of them were to occur, the system would still remain operational and safe. …"[41]

However, in order for electric power utilities, wholesale power generators and power grid operators to fulfill these NERC standards – of continuously balancing power generation and demand, keeping the system in a stable condition, and operating the system to remain in a reliable condition despite occurrence of a contingency – such companies have had to rely increasingly and heavily on "automation, centralized control of equipment, and high-speed communications." In short, they have increasingly deployed and relied upon computerized systems, the most critical of which are the supervisory control and data acquisition ("SCADA") systems and the new "Smart Grid" devices.

[41] Ibid, pp. 7 – 9.

Deployments of SCADA and "smart grid" systems have increased the Grid's vulnerabilities to cyberattacks for three reasons: first, they tended to replace earlier communication and control systems that had been isolated from the outside and had been kept separate from a company's business information systems; second, each addition of computerized devices has usually brought with it a significant number of unknown vulnerabilities that can be exploited through Internet or wireless connections or through direct insertion into devices located on a plant's premises; and third, there was an incautious replacement of systems whose design did not anticipate or reflect the need for security, let alone the high degree of security to minimize the risks of sustained and successful cyberattacks. Several reports have highlighted the growing vulnerability, including:

- The Final Report on the August 14, 2003 Blackout in the U.S. and Canada, noted that "a failure in a software program not linked to malicious activity may have significantly contributed to the power outage,"[42] and cautioned that –

  > "Current assessments suggest that there are terrorists and other malicious actors who have the capability to conduct a malicious cyber attack with potential to disrupt the energy infrastructure."[43]
  >
  > "The generation and delivery of electricity has been and continues to be, a target of malicious groups and individuals intent on disrupting this system. Even attacks that do not directly target the electricity sector can have disruptive effects on electricity system operations. Many malicious code attacks, by their very nature, are unbiased and tend to interfere with operations supported by vulnerable applications."[44]

- A report in 2009, based on the Idaho National Laboratory's 58 assessments over several years of SCADA systems, including those used to control and monitor electric power grid facilities. It observed these assessments of the legacy power grid: "Many vulnerabilities were found … All these results are applicable to products and installations that are part of the current power grid." In addition, the report "identified many vulnerabilities associated with substation automation devices … Potential consequences of successful substation cyber attacks include the destruction of generators, power outages, and grid instability."[45]

- A NERC sponsored study, released in June 2010, that focused on "rare risks with the potential to cause long-term, catastrophic damage to the bulk power system" – what are referred to as "High-Impact, Low-Frequency" or "HILF" events. The study observed that a principle type of HILF event that puts the bulk power system at risk is a "concerted, well-planned cyber, physical or blended attack conducted by an active adversary against multiple points on the system."[46] And it highlighted the tradeoff between the gains in

---

[42] U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004, p. 131, accessed at https://reports.energy.gov/BlackoutFinal-Web.pdf

[43] Ibid, p. 135.

[44] Ibid, pp. 132 – 133.

[45] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, STUDY OF SECURITY ATTRIBUTES OF SMART GRID SYSTEMS – CURRENT CYBER SECURITY ISSUES, April 2009, p. 2.

[46] North American Electric Reliability Corporation, High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, June 2010, p. 26, accessed at http://www.nerc.com/files/HILF.pdf.

control and responses achieved through deployment of smarter devices and the losses in cyber security incurred through the import of unknown vulnerabilities in such devices. For example, the use of SCADA systems offered improved controls, but created potential vulnerabilities. However, what makes that tradeoff much more disadvantageous than may have been appreciated is the fact that these systems were being connected to the Internet without addressing such vulnerabilities.[47] Most importantly, the NERC sponsored study concluded:

> "The consequences associated with a coordinated cyber and/or physical attack[48] could result in the physical damage or destruction of critical assets, such as generators, substation components, and large transformers. If conducted on a large enough scale, it is possible that the bulk power system *could not recover in its present form, but would need to be restored in islands or using rotating outages* where enough equipment was still available to operate the system."

- The earlier mentioned National Academy of Science's November 2012 report. This report also viewed the most serious risk to the Grid as that of a coordinated physical and cyber attack. It noted that the vulnerabilities to such cyber attack resulted from the "lack of attention to connections from system control centers to the outside world," because such connections, if not safeguarded and handled carefully, "can in principle become a route for attackers from the outside world to create disruption, take control, and cause damage." The study cautioned about three other vulnerabilities: disgruntled insiders, the adding of insecure code to programs in a center computer, and linkages to other system control centers that whose lack of care can expose a well-managed control center to severe cyber attacks. And it warned of the growing risk from advanced persistent threats that could cause a "common modal failure of assets, meaning that a single exploitation of a vulnerability can be propagated across a cyber or power system network and potentially affect an entire class of assets at once."[49]

The identification of such vulnerabilities in a system would not be of such great concern were it not for the fact that the high reliability of the Grid depends on such a delicate and dynamic balancing throughout the electric power transmission system among multiple private enterprises, some of which are not regulated as utilities. Because that system is interconnected and dynamic, stability limits are critical and must be maintained through continuous monitoring (though computer-based and linked sensors) in order to remain stable at all time. Stability problems can

---

[47] Ibid, p. 31. The last sentence of the quoted text ends with a footnote citation to *In the Crossfire: Critical Infrastructure in the Age of Cyber War*. Stewart Baker, Shaun Waterman, George Ivanov, McAfee, 2009.

[48] The study noted that "coordinated attacks" have a profile that is quite different from "higher frequency (better understood) and probabilistic outages," namely, (i) they can "potentially affect specific key assets over a broad geographic area," (ii) they may be planned to take advantage of severe weather, (iii) they can "recur or be launched in a sequential fashion" and thereby reintroduce instability, (iv) they may result in the "loss of visibility and control of the system, severely complicating restoration efforts" thereby causing "severe restrictions on market operations and reliability measures," and (iv) they are "adaptive in nature, meaning the adversary can anticipate and respond to efforts by grid operators to restore the system" – a feature that raises particular concern with respect to a cyber attack, because "operators could be given spurious information from a typically trusted source, causing them to make decisions that may worsen the situation." North American Electric Reliability Corporation, High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, June 2010, pp. 31 - 32, accessed at http://www.nerc.com/files/HILF.pdf.

[49] Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack, Board of Energy and Environmental Systems, Division on Engineering and Physical Sciences, National Research Council of the National Academies, TERRORISM AND THE ELECTRIC POWER DELIVERY SYSTEM, 2012, pp. 40 - 41, accessed at http://www.nap.edu/catalog.php?record_id=12050#toc.

develop within a few cycles (less than a second) and can cause swiftly cascading outages over a wide area.

In response to the growing recognition of cyber vulnerabilities, the multiple regulatory agencies for electric power utilities, wholesale power generators, power grid operators launched several initiatives to improve cyber security and the ability of the bulk power grid to recover from a severe and prolonged degraded level of operations. We discuss some of the most important regulatory initiatives in the next section of this essay.

3. *Regulatory efforts to improve cybersecurity of the North American Grid and the ability of electric power generation and delivery enterprises to recover from damaging attacks*.

When the electricity industry started, vertically integrated utilities met their customer loads from their own generation of electricity. During World War I, U.S. electricity utilities were compelled to interconnect and eventually began to form regional interconnections that were self-regulated until the advent of deregulation beginning in the 1990s. Nonetheless, since different utilities often had established their own standards for transmission voltages, when they merged, transformers, interties and substations had to be installed to link the different utilities' power lines whose voltages differed. In 1965, a major power blackout in the northeast – and the demonstrable breakdown in reliability – caused concerns for reliability of "interconnected power networks" and prompted the electric utility industry to form the self-regulating committee they called the North American Electric Reliability Council. Following deregulation and the federal government's response to the 2003 blackout in the Northeast and Midwest, this Council was spun off into an independent regulatory organization, a non-profit subsequently renamed the North American Electric Reliability Corporation ("NERC").[50] NERC and its regional reliability councils undertook to address issues of the bulk power supply's reliability and adequacy through issuance of standards and procedures, but compliance with them, though firmly encouraged, remained voluntary.

In 2005, in part as an effort to provide for development of a stronger energy infrastructure and in part to respond to significant reliability concerns arising out of the 2003 blackout, Congress passed the Energy Policy Act of 2005 ("EPAct"). The EPAct enhanced the electricity authorities of the Federal Energy Regulatory Commission ("FERC")[51], with the most important being the grant of authority to FERC to "oversee mandatory reliability standards governing the nation's electricity grid."[52] After EPAct and subsequently-issued decisions of FERC implementing EPAct's various mandates, both FERC and NERC have authority to enforce reliability standards and impose significant penalties for non-compliance.

Thereafter, FERC issued final rules on the certification of an Electric Reliability Organization ("ERO") and on "procedures for the establishment, approval and enforcement of mandatory electric reliability standards."[53] In July 2006, FERC certified NERC as the ERO, *i.e.,* as an

---

[50] MIT, THE FUTURE OF THE ELECTRIC GRID, 2011, p. 238, accessed at http://web.mit.edu/mitei/research/studies/the-electric-grid-2011.shtml.

[51] FERC regulates the interstate transmission of electricity, natural gas, and oil. See FERC website, "What FERC Does," accessed at http://www.ferc.gov/about/ferc-does.asp.

[52] Federal Energy Regulatory Commission, Energy Policy Act of 2005 Fact Sheet, August 8, 2006, p. 2, accessed at http://www.ferc.gov/legal/fed-sta/epact-fact-sheet.pdf.

[53] Ibid, pp. 2 – 3.

independent, self-regulating, non-profit corporation "established to carry out and execute the regulatory obligations of FERC."[54] As explained by FERC, "Once approved, the Reliability Standards may be enforced by the ERO [now NERC], subject to Commission [FERC] oversight, or the Commission can independently enforce Reliability Standards."[55] However, in April 2007, FERC approved agreements between NERC and each of the eight Regional Entities, under which NERC, as the ERO, delegated responsibility to the Regional Entities for compliance monitoring and enforcement of the mandatory Reliability Standards.[56]

In its role as the ERO, NERC reviews and approves Reliability Standards that have been developed by the electric industry. The Reliability Standards are the planning and operating rules that electric utilities must follow to ensure maximum system reliability. To become enforceable, each Reliability Standard must first be reviewed and approved by NERC, then submitted to FERC for review and approval. NERC filed its first set of 107 reliability standards with FERC for review and approval on April 4, 2006, and eleven months later, on March 16, 2007, FERC issued a final rule approving 83 of the proposed 107 Reliability Standards (FERC also directed NERC to develop modifications to 56 of the 83 approved Reliability Standards).[57] NERC has legal authority to enforce compliance with the NERC Reliability Standards.[58] However, it should be noted that prior to FERC's certification of NERC as the ERO, "NERC had developed a cyber security standard for the electric industry on a voluntary basis."[59] NERC's voluntary cyber security standard, known as Urgent Action 1200 standard, remained in effect until June 1, 2006, when it was replaced by the eight CIP Reliability Standards.[60]

Under this scheme, cyber security is treated by NERC as a reliability issue and certain Reliability Standards address it. Before reviewing the cyber security Reliability Standards, we should clarify the computer security industry's use of the term "cyber security" to distinguish it from the meaning it is given in the applicable NERC Reliability Standards. As explained by Shari and Charles Pfleeger, since any computer-related system has “both theoretical and real weaknesses.” the purpose of computer security is “to devise ways to prevent the weaknesses from being exploited.”[61] Cyber security must prevent exploits that could compromise three critical features of a computer-related system:

---

[54] Gilbert N. Sorebo and Michael C. Echols, Smart Grid Security, CRC Press, 2012, p. 20.

[55] FERC, Final Rule Order No. 706, "Mandatory Reliability Standards for Critical Infrastructure Protection," 18 CFR Part 40, January 18, 2008, pp. 1 - 2, accessed at http://www.ferc.gov/whats-new/comm-meet/2008/011708/e-2.pdf.

[56] Ibid.

[57] FERC, Final Rule Order No. 706, "Mandatory Reliability Standards for Critical Infrastructure Protection," 18 CFR Part 40, January 18, 2008, p. 2, accessed at http://www.ferc.gov/whats-new/comm-meet/2008/011708/e-2.pdf.

[58] NERC website, "About NERC: *Company Overview*," accessed at http://www.nerc.com/page.php?cid=1|7.

[59] FERC, Final Rule Order No. 706, "Mandatory Reliability Standards for Critical Infrastructure Protection," 18 CFR Part 40, January 18, 2008, p.3, accessed at http://www.ferc.gov/whats-new/comm-meet/2008/011708/e-2.pdf.

[60] Ibid.

[61] Shari and Charles Pfleeger, *Security in Computing*, Third Edition, p. 9.

(i) its confidentiality (ensuring that "computer-related assets are accessed only by authorized parties"[62]);

(ii) its integrity (ensuring that "assets can be modified only by authorized parties or only in authorized ways"[63]); and

(iii) its availability (ensuring that "assets are accessible to authorized parties at appropriate times"[64]).

To those three, a fourth should be added when the computer-related asset is a SCADA system: its adherence to operational constraints (ensuring that assets operate as designed and within specified constraints as required for the safe and proper operation of plant machinery). "The protective measures or "controls" that safeguard a cyber system's confidentiality, integrity, availability, and adherence to operational constraints should reduce to as low as reasonably possible the system's vulnerability to existing threats and threats that may be created."[65] Note that, "for a control systems operator to take appropriate actions based on the readings or status of the system, the integrity of the information is important,"[66] a fact that is crucial to SCADA systems in nuclear power plants and one that Stuxnet targeted and successfully attacked in the Iranian facilities. It is important to note that integrity and adherence to operational constraints are arguably the most important cyber security factors for SCADA systems, particularly in facilities involved in nuclear or electric power generation.

Each NERC Reliability Standard explains its purpose, applicability, the requirements to be met, the measures to be used to fulfill the requirements, the means of verifying compliance, and the levels on non-compliance. There are sometimes also additional sections that provide for regional variance granted to a particular interconnection (such as the ERCOT Interconnection that covers Texas).

On January 17, 2008, FERC issued a 217 page, Final Rule No. 706 ("Order No. 706") approving an initial eight critical infrastructure protection ("CIP") standards that NERC had proposed and that "require certain users, owners, and operators of the Bulk-Power system to comply with specific requirements to safeguard critical cyber assets."[67] The CIP Reliability Standards are intended to "provide a framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System."[68] The initial eight CIP Reliability Standards addressed the following matters:

---

[62] Ibid at p. 10.

[63] Ibid.

[64] Ibid.

[65] Roland L. Trope and Geoffrey Schwartz, "Cyber Security for SCADA Systems," unpublished essay for the Cyberspace Winter Working Meeting Continuing Legal Education Program, January 2011, p. 7. Copy available from the authoris.

[66] Department of Homeland Security, National Cyber Security Division, CYBER SECURITY PROCUREMENT LANGUAGE FOR CONTROL SYSTEMS, VERSION 1.8, February 2008, p. ix, accessed at http://www.msisac.org/scada/documents/4march08scadaprocure.pdf.

[67] FERC, Final Rule Order No. 706, "Mandatory Reliability Standards for Critical Infrastructure Protection," 18 CFR Part 40, January 18, 2008, p. 1, accessed at http://www.ferc.gov/whats-new/comm-meet/2008/011708/e-2.pdf.

[68] FERC, "Version 4 Critical Infrastructure Protection Reliability Standards," 18 CFR Part 40, April 19, 2012, accessed at http://www.nerc.com/files/OrderApprovingV4CIPStds-Order761_20120419.pdf.

- CIP-002-1 – **Critical Cyber Asset Identification**: Requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology;
- CIP-003-1 – **Security Management Controls**: Requires a responsible entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP-002-1;
- CIP-004-1 – **Personnel and Training**: Requires personnel with access to critical cyber assets to have identity verification and a criminal check. It also requires employee training.
- CIP-005-1 – **Electronic Security Perimeters**: Requires the identification and protection of an electronic security perimeter and access points. The electronic secvurity perimeter is to encompass the critical cyber assets identified pursuant to the methodology required by CIP-002-1.
- CIP-006-1 – **Physical Security of Critical Cyber Assets**: Requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter;
- CIP-007-1 – **Systems Security Management**: Requires a responsible entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.
- CIP-008-1 – **Incident Reporting and Response Planning**: Requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets; and
- CIP-009-1 – **Recovery Plans for Critical Cyber Assets**: Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.[69]

However, FERC did not give blanket to approval to these CIP Reliability Standards, but instead qualified its approval with a number of expressed concerns that it directed NERC to address and, in some instances, FERC refused to approve. For example, when NERC submitted the proposed eight CIP Reliability Standards, NERC's proposal included an interpretation that was clearly of considerable importance to the Boards of Directors of the corporations subject to the CIP Reliability Standards, namely that each such Standard "incorporates the concept of 'reasonable business judgment' as a guide for determining what constitutes appropriate compliance with those Reliability Standards," and to make that clear the Purpose statement of Reliability Standard CIP-002-1 provided that: "Responsible entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment."[70] NERC apparently wanted to ensure that corporations subject to the Standards and their Boards of Directors that they would have the

[69] FERC, Final Rule Order No. 706, "Mandatory Reliability Standards for Critical Infrastructure Protection," 18 CFR Part 40, January 18, 2008, pp. 3 - 4, accessed at http://www.ferc.gov/whats-new/comm-meet/2008/011708/e-2.pdf.

[70] FERC, Final Rule Order No. 706, "Mandatory Reliability Standards for Critical Infrastructure Protection," 18 CFR Part 40, January 18, 2008, p. 33, accessed at http://www.ferc.gov/whats-new/comm-meet/2008/011708/e-2.pdf.

protection of the "business judgment rule" to avoid having their decisions, in the area of compliance with the Standards, second-guessed by a court. However, FERC disagreed. FERC set forth the basis for its disagreement in the same Order No. 706 in which it approved the CIP Reliability Standards. Although FERC acknowledged that "Cyber security problems do not lend themselves to one-size-fits-all solutions," and that "cost can be a valid consideration in implementing the CIP Reliability Standards," FERC nonetheless concluded that the business judgment rule "is ill suited to the task of implementing an appropriate program of cyber security pursuant to section 215 of the FPA," and, in a passage that may cause concern among many corporate counsel, justified its view as follows:

> "[T]he concept of reasonable business judgment takes on a very different meaning when removed from its original context and applied to a different factual situation where very different assumptions apply.
>
> …[C]yber security standards are essential to protecting the Bulk-Power System against attacks by terrorists and others seeking to damage the grid. Because of the interconnected nature of the grid, an attack on one system can affect the entire grid. It is therefore unreasonable to allow each user, owner or operator to determine compliance with the CIP Reliability Standards based on its own 'business interests.' Business convenience cannot excuse compliance with mandatory Reliability Standards.
>
> … [T]he issue under section 215 of the FPA is not whether the management of a business is acting in the interest of its own shareholders, but rather whether an entity is taking appropriate action to avert risks that could threaten the entire grid. Finally, the Commission [FERC] noted that in the corporate governance context, the business judgment rule is invoked only in extreme circumstances, generally when an officer or director is found to have acted fraudulently, in bad faith, or with gross or culpable negligence."[71]

For all of those reasons, FERC determined that the concept of "reasonable business judgment" was "inappropriate in the context of mandatory CIP Reliability Standards," and directed the ERO (NERC) to "develop modifications to the CIP Reliability Standards that do not include this term."[72]

Another important kind of qualification that accompanied FERC's approval of the 8 CIP Reliability Standards concerned provisions that appeared in some of the Standards that appeared to give a responsible entity authorization to opt out of compliance at its discretion, either by finding a justification to do so for an entire Standard or by taking advantage of ambiguity in the phrasing of a Standard so that while appearing to comply with it, the responsible entity would have escaped all the potentially burdensome actions that it should have taken. We will discuss an example of each.

First, concerning language in a Standard that could give a responsible entity an apparent opt-out of compliance with the Standard, FERC noted that some Requirements in the CIP Reliability Standards (and "Requirements" refers to a specific section in each Standard bearing that title) –

---

[71] FERC, Final Rule Order No. 706, "Mandatory Reliability Standards for Critical Infrastructure Protection," 18 CFR Part 40, January 18, 2008, pp. 34 - 35, accessed at http://www.ferc.gov/whats-new/comm-meet/2008/011708/e-2.pdf.

[72] Ibid, p. 38.

> "permit an entity not to take the actions specified in the Requirement if they 'document compensating measures applied to mitigate risk exposure or an acceptance of risk.' … [T]he phrase 'acceptance of risk' essentially allows a Responsible Entity to opt out of certain provisions of a mandatory Reliability Standard at its discretion."[73]

For those reasons, FERC directed the ERO (NERC) to remove the acceptance of risk language from the CIP Reliability Standards, and to substitute for it the concept of exceptions based on technical feasibility.[74]

Second, concerning ambiguities in the phrasing of a Standard that would permit a responsible entity to narrow or possibly circumvent the obligation to fulfill a Standard's Requirements, FERC expressed concern with the term "risk-based" as used in Reliability Standard CIP-002-1 – Critical Cyber Asset Identification, which states "Requires a responsible entity to identify its critical assets and critical cyber assets using a *risk-based* assessment methodology." It is important to be aware that FERC provided a definition of "cyber assets" in Order No. 706 (footnote 2) where it states:

> "In the context of the CIP Reliability Standards, cyber assets are programmable electronic devices and communication networks including hardware, software, and data."[75]

In FERC's view, the term "risk-based" would benefit from further clarification, because certain assets would not clearly qualify or be disqualified as a "cyber asset" under such a standard. An example that FERC gave was "marketing data:"

> "The Commission remains concerned that, while not all marketing data or other data may be considered a critical cyber asset essential to the proper operation of a critical asset, there may be times where it is properly classified as such. For example, if a critical asset is configured such that it cannot operate and support the reliability and operability of the Bulk-Power System without a real-time stream of data, that data fits the definition of a critical cyber asset, and should be protected. Once a particular piece of data is no longer needed by the critical asset, it is no longer a critical cyber asset. On this point, we agree with commenters that there is a temporal characteristic to data as a critical asset."[76]

FERC concluded that CIP-002-1 would benefit from greater clarity and guidance, and therefore directed the ERO (NERC), to develop guidance regarding the identification of critical assets, and to consider the designation of various types of data as a critical asset or critical cyber asset, and "to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."[77] That direction, in Order No. 706, was issued in 2008.

However, as of January 2013, the CIP Reliability Standards as a whole remain incomplete,

---

[73] FERC, Final Rule Order No. 706, "Mandatory Reliability Standards for Critical Infrastructure Protection," 18 CFR Part 40, January 18, 2008, pp. 41 – 42, accessed at http://www.ferc.gov/whats-new/comm-meet/2008/011708/e-2.pdf.

[74] Ibid, pp. 44 – 45.

[75] Ibid, p. 1, footnote 2.

[76] Ibid, p. 75.

[77] Ibid, pp. 75 – 76.

because NERC is still making efforts to complete the actions required by the directions it received from FERC in Order No. 706. NERC had submitted, and FERC had approved, Versions 2 and 3 of the CIP Reliability Standards, but these still did not achieve full compliance with Order No. 706 issued years earlier.

One of the areas of continuing discussion (and some disagreement) between FERC and NERC on that effort concerned Reliability Standard CIP-002-1, Critical Cyber Asset Identification as expressed in Version 3. FERC had determined that Version 3 of that Standard, as currently applied, generally did not adequately identify Critical Assets (and thus left too many of them outside the scope of the other Standards).[78] That Standard is, of course, of particular importance to each of the responsible entities because each tangible and intangible asset that is so identified then becomes subject to several of the other Reliability Standards, and increases the costs and burdens for the responsible entity to come into compliance with those Standards.

Further progress, however, was reached, on April 19, 2012, when FERC issued Order No. 761 approving "Version 4 Critical Infrastructure Protection Reliability Standards." One of the key items of Order No. 761 was FERC's approval of NERC's proposed Version 4 of the Reliability Standards, including in particular Reliability Standard CIP-002-4 in which the use of the existing "entity-defined risk-based assessment methodologies" was replaced by certain "bright line criteria to identify Critical Assets" and that would, as a result, identify certain types of Critical Assets that might not be identified under Version 3 of the Standard.[79]

It should be noted, however, that even this recent approval leaves work to be done by NERC. NERC described Version 4 as an "interim step," and FERC expressed the concern in Order No. 761 (approving it) that "Version 4 does not provide enough protection [of Critical Assets and of the Grid] to satisfy Order No. 706."[80] Therefore, in Order No. 761 FERC determined that it was appropriate to "impose a deadline for the ERO [NERC] to achieve full compliance with Order No. 706" and set a deadline of March 31, 2013 for submittal by NERC of what will be Version 5 of the Reliability Standards.

In the next section, we discuss why, in light of the Reliability Standards and the SEC Staff's Guidance on Cybersecurity, it would be prudent for the Boards of responsible entities subject to FERC's jurisdiction to include on their agendas a review of management's understanding of cybersecurity threats to the Grid and of management's plans to have their enterprise address such threats, including what preparations the enterprise may need to make in anticipation of the possible receipt of an Imminent Threat Notice and/or of a Catastrophic Target Notice as contemplated by the draft Cybersecurity EO.

4. *Why cybersecurity threats to the Grid and their potential consequences have become issues for electric industry Boards of Directors.*

---

[78] FERC, Final Rule Order No. 761, "Version 4 Critical Infrastructure Protection Reliability Standards," 18 CFR Part 40, 139 FERC ¶61,058, p. 9, April 19, 2012, accessed at http://www.nerc.com/files/OrderApprovingV4CIPStds-Order761_20120419.pdf.

[79] Ibid.

[80] Ibid, p. 11.

In 2007, federal researchers discovered that a hacker, outside the premises of an electricity generator plant, could gain control of the generators, and cause them to self-destruct. The feat or exploit prompted analysts to warn that a co-ordinated attack on the Grid could cause outages throughout a region, not unlike those that a hurricane often causes. Despite efforts to shore up the Grid's resilience and defenses against cyberattacks, and particularly against combined physical and cyber attacks, it appears that the Grid is even more vulnerable to such threats.[81] In comments made to the CIO Network Conference, excerpts of which were published on January 22, 2013, former Secretary of the Department of Homeland Security ("DoHS"), Michael Chertoff, noted that there is at present heightened concern for the cybersecurity of physical systems – such as power, water, and other utilities – that are controlled by SCADA systems. He also referred to a report issued a few days earlier, by the DoHS,

> "that estimated last year there were almost 200 serious attacks on SCADA and control systems in the U.S Most of them involved energy, and then second came water and utilities."[82]

He emphasized, however, that a study of certain firms had revealed that many attacks and adversary intrusions into a corporate enterprise's networks entered not via the Internet and through the company's firewalls, but through the incautious conduct of company personnel. Reflecting on that, Secretary Chertoff observed –

> "I always throw thumb drives in the garbage because to take one that you've been given [say, at a conference] or to pick one up that you find and put it in your computer is a little like eating food that you found on the floor. They actually did a study where they scattered thumb drives in a parking lot and found that 50% were picked up and put into computers. That's cyberhygiene. It's education."[83]

If personnel of a "responsible entity" might be so incautious with storage media they bring into an electric utility company's premises and might thoughtlessly insert into a USB port that could allow the injection of malicious code into the company's networks and possibly thereby into its SCADA systems, then it would appear that the company might be far from coming into real compliance with the Reliablity Standards, particularly CIP-004-1 – Personnel and Training and CIP-007-1 – Systems Security Management.

However, reports of such incidents are unlikely to make their way to the company's Boardroom. Far more likely, the company Board will have on its agenda events or occurrences that will appear not only on their agenda, but on the agendas of other Boards within their industry-sector (such as the forthcoming Version 5 of the Reliabilty Standards), or within their region of the country (in response to the regional experience of a low-frequency, high-impact event like Hurricane Sandy), or that have in common that their enterprises are subject to the same multiple regulatory concerns.

For Boards of Directors of electric power utilities, wholesale power generators, and power grid operators the issues related to cyber threats will almost certainly become increasingly higher priorities for their agendas, their Risk and/or Audit Committees, and their companies' executive

---

[81] Joseph Menn, "Power grid looks exposed to assault," Financial Times, October 12, 2011, p. 6.

[82] Michael Chertoff, "How Safe Is Your Data?," The Wall Street Journal, p. B16.

[83] Ibid.

officers as the result of the following developments:

- *The pending issuance of the Cybersecurity EO* – And, as that EO is implemented, many "responsible entities" should anticipate that it is highly probable that their owners and operators will receive Catastrophic Target Notices within the next two years; and some may anticipate receiving Imminent Target Notices, or both;
- *The forthcoming submittal by NERC to FERC of Version 5 of the Reliability Standards* – Boards will certainly need to be apprised of the changes that Version 5 brings, if approved by FERC, and what adjustments their responsible entity will need to make in order to achieve (and ensuring continuing) compliance with the completed Reliability Standards;
- *The reported lessons being drawn from the experiences of Hurricane Sandy* – Each major prolonged and widespread electrical outage makes an impression on the public that experiences it and on the electric utility companies that endeavor to restore full service to their customers and who are keenly aware that they and their reputations will be strongly affected – for better or worse – by their performance, and that issues of potential liability will often turn such perceptions as juries and judges interpret regulations in light of their own understanding of such experiences.
- *The SEC Staff Guidance on Cybersecurity Disclosures* – For "responsible entities" (subject to the CIP Reliability Standards) that are also "registrants" (subject to the SEC's Guidance) and that are therefore also likely to be recipients of Catastrophic Target Notices (issued pursuant to the Cybersecurity EO) the need to arrive at a clear understanding and reasonable response to these multiple regulatory issues will clearly make it prudent for a Board of Directors to treat them as priorites on their agenda. And clearly, some have observed, as can be seen from the fact that one of the few "registrants" to make a filing with the SEC that reflected the influence of the SEC's Guidance on Cybersecurity disclosures, was ConEdison. In November, Consolidated Edison of New York, whose customers are in New York City and Westchester County, included cyber-attacks as a "risk factor" for the first time in the 10Q it filed in November 2012, where it stated:

> "A Cyber Attack Could Adversely Affect the Companies. The Utilities and other operators of critical energy infrastructure may face a heightened risk of cyber attack. In the event of such an attack, the Utilities and the competitive energy businesses could have their operations disrupted, property damaged and customer information stolen; experience substantial loss of revenues, response costs and other financial loss; and be subject to increased regulation, litigation and damage to their reputation."[84]

For all of these reasons, it is reasonable to infer that most, if not all, "responsible entities" are, or soon will, have the issue of cyberattacks on their Board's agenda and particularly in the context of the need to oversee management's addressing of the issues raised by the increasing regulation in this field.

[84] Willian Pentland, Forbes, "Cyber Threat to Power Grid Puts Utility Investors at Risk," December 27, 2012, accessed at http://www.forbes.com/sites/williampentland/2011/12/27/cyber-threat-to-power-grid-puts-utility-investors-at-risk/.

Conclusion. In closing, it seems appropriate to ask: would it be prudent also for Boards of companies that are not involved in the generation, transmission, or distribution of electricity to treat such issues as priorities and ensure that they are on their agendas? We believe that whether a company is a small, privately owned firm or a large, publicly owned multi-national corporation, the answer in most cases should be "yes." Boards of such companies need only reflect upon the widespread disruption of business operations in the wake of Superstorm Sandy, the tidal surge, and the weeks of blackout in order to see that if a widespread electrical outage occurred in their region, and was discovered (during or after the outage) to have been caused by coordinated physical and cyber attacks, that they would have wanted to address certain issues in the calm and quiet of an illuminated Boardroom with operative telecommunications and at tolerable room temperatures (with HVACs operating) than in the conditions that many businesses found themselves during the period after "Sandy" when lower Manhattan, Staten Island, and large parts of New Jersey, Long Island, Westchester and Connecticut were without power for days and weeks.

The issues that such Boards may want to address will vary, but will likely include: insurance coverage, "force majeure" provisions in commercial and corporate transaction agreements, supply-chain integrity and reliability, and a careful reconsideration of disaster response and recovery plans to see if they are based on possibly errant, possibly unreliable assumptions, such as those faced by hospitals that believed they could continue operations in the event of a prolonged outage, but whose on-site backup generators proved unreliable or exposed to other effects of Sandy, such as the salt-water tidal surge. Each of the businesses that experienced those effects has drawn lessons from them, but it will remain to be seen if they implement them. A Board will want to ensure that management is aware that when such widespread problems are reported on the front page or appear continuously in the media (TV, radio, and online) that there will be little excuse for ignoring the need to address such issues. And, of course, for "responsible entities" involved in the generation, transmission, or distribution of electricity, these issues should be viewed as necessitating immediate attention. Whether they need to consider resuming operations with a "blackstart" or mitigating damages, we believe that ultimately they will find that their highest priority will be to ensure that they are in the best position to handle the difficult tasks of response and recovery. Avoiding or defending against cyber attacks and physical attacks may become an issue, but far more attention is likely to be focused by the public, by counter-parties, by customers, potential plaintiffs, and by courts and juries on how well the enterprise handled the challenges of response and recovery from a serious degrade or collapse of a region of the Grid. These are challenges best addressed when there is power to do so.

R.L.T. S.J.H.