LIGHTS OUT

By Ted Koppel

*Reviewed by Jonathan D. Schneider**

Ted Koppel has had a storied career. Beginning with his years as a Vietnam War correspondent, later as ABC News' bureau chief, and finally the anchor of ABC's Nightline between 1980 and 2005. Koppel was the face of TV news for over forty years, winning nearly every news award in broadcasting. He is a member of the Broadcasting Hall of Fame, won forty Emmy Awards, and received more than twenty honorary degrees from universities in the United States.[1]

Koppel's run as Nightline's anchor during the Iranian Hostage Crisis may be his defining moment. For 444 evenings, under the banner "America Held Hostage," Koppel honed his craft selling sensational news to a riveted nation. Each night for well over a year, Koppel followed events in the streets of Tehran and the halls of power in Washington, fueling a sense of national outrage and powerlessness that helped lead to Jimmy Carter's loss of the White House and Ronald Reagan's Presidency.

Lights Out is a return to form for Koppel.[2] Subtitled "A Cyberattack; A Nation Unprepared; Surviving the Aftermath," the book is focused on our vulnerability in the face of international threats, and on the perceived fecklessness of institutions designed to protect us. Opening with a fictionalized account of the nightmare that would follow a power outage of some weeks or months in a major population center, Koppel aims to awaken us from our stupor and rally the nation's defenses. He deserves credit for raising a serious subject, in greater depth than generally covered in the media, and for touching many of the right bases in getting his arms around the subject.

There are good reasons to be concerned, and Koppel highlights some of the most prominent. But Koppel has little in-depth expertise to bring to the subject, he gets certain fundamental things wrong, and his "gotcha" style journalism elicits ostensible concessions from serious people who are unwilling to extend a security guarantee while grappling with a real challenge.

I. WHAT ARE THE RISKS?

Koppel's catalogue of cyberattacks over the past several years is a useful primer for the uninitiated, highlighting eye-opening incidents that signal genuine vul-

* Jonathan Schneider is a partner with Stinson, Leonard Street, resident in the Washington, D.C. office.

1. *Columnist Biography: Ted Koppel*, N.Y. TIMES, http://www.nytimes.com/ref/opinion/koppel-bio.html?_r=0 (last visited Oct. 18, 2016).

2. TED KOPPEL, LIGHTS OUT (2015).

nerability. The evidence of our exposure includes the attack disabling 30,000 Aramco computers in 2012 through use of the "Shamoon" virus,[3] reports in 2014 by the Mandiant Consulting of widespread hacking linked to the Chinese military of major U.S. institutions,[4] and a denial of service attack on JEA disabling the utility's customer interface. Utilities also routinely report to the Electric Sector Information Analysis Center (ES-ISAC) and the Department of Homeland Security (DHS) a large number of on-going hacking attempts, though most are thwarted.[5] And, while not a cyber incident, the physical attack in April 2013 on Pacific Gas & Electric Corporation's Metcalf electric transformer substation suggests a level of sophistication in targeting critical electric infrastructure that may presage yet more threatening activity.[6] Referencing the event in an interview with *The Wall Street Journal*, former Chairman of the Federal Energy Regulatory Commission (FERC) Jon Wellinghoff commented on a FERC study suggesting that the successful attack on nine of the nation's most critical substations could black out most of the United States.[7]

The cyberattack on the Ukrainian electric grid on December 23, 2015 further underscores concern over the electric grid's vulnerability, though it occurred after the release of Koppel's book. As reported by the DHS on February 25, 2016,[8] and later in additional detail by ES-ISAC and SANS Industrial Control System (ICS),[9] the successful cyberattack on the Ukrainian Kyivoblenergo, a regional electricity distribution company plunged approximately 225,000 customers into darkness, in an attack widely attributed to Russian security services. While service was restored within some hours, the attack underscored the destructive potential of a cyberattack on the electric grid, and highlighted points of vulnerability. As disclosed in the ES-ISAC/SANS ICS report, hackers gained access to the Ukrainian utility's ICS network and its SCADA system, enabling them to shut the system down remotely. Access to the Ukrainian utility's control systems was gained through spear phishing, the use of malware and the manipulation of Microsoft Office documents to harvest credentials enabling remote access to the ICS network.

In other sectors of the economy, reports of major cyber intrusions and data theft have become disquietingly routine, ranging from those like the 2014 hack of

3. Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. TIMES (Oct. 23, 2012), http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

4. David E. Sanger et.al., *Chinese Army Unit is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

5. *See generally* U.S. DEP'T HOMELAND SEC., ICS- CERT MONITOR 4 (Nov./Dec. 2015), https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.

6. PAUL W. PARFOMAK, CONG. RESEARCH SERV., R43604, PHYSICAL SECURITY OF THE U.S. POWER GRID: HIGH-VOLTAGE TRANSFORMER SUBSTATIONS (2014), https://www.fas.org/sgp/crs/homesec/R43604.pdf.

7. KOPPEL, *supra* note 2, at 19 (referencing Rebecca Smith, *U.S. Risks National Blackout From Small-Scale Attack,* WALL STREET JOURNAL (Mar. 12, 2014), http://www.wsj.com/articles/SB10001424052702304020104579433670284061220).

8. *Cyber-Attack Against Ukrainian Critical Infrastructure*, ICS-CERT (Feb. 25, 2016), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 [hereinafter *Cyber-Attack*].

9. SANS INDUS. CONTROL SYS., ANALYSIS OF THE CYBER ATTACK ON THE UKRAINIAN POWER GRID (Mar. 18. 2016), https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Sony Pictures, widely attributed to North Korea and causing major business embarrassment,[10] to those with a more commercial purpose such as the massive hack of J.P. Morgan, now the subject of a criminal indictment in New York alleging a widespread profitable conspiracy involving stock manipulation and credit card fraud.[11] These risks are real, and no serious policy-maker or electric industry executive would say otherwise.

II. HOW EFFECTIVE IS OUR RESPONSE?

Koppel dismisses altogether the efforts of the electric industry, the North American Reliability Council (NERC) and the FERC. According to Koppel:

> Prudence suggest that we at least consider the possibility of a cyberattack against the grid, the consequences of which would be so devastating that no administration could consider it anything less than an act of war . . . It would be reassuring to report that the grid is adequately defended against cyberattack. It is not.[12]

According to Koppel, the electric industry's motivation to protect the grid is undermined by a for-profit business model, while NERC is captive to industry. Koppel says:

> Certainly no one has a greater interest in protecting the security of the electric power industry than the industry itself – if only cost were not a factor and profit were not an essential ingredient of staying in business. It is not altogether reassuring, then, to consider that the only institution with real power to decide how the power industry is protected is the power industry.[13]

Koppel concedes that "[r]egulations that were once optional are now mandatory," but goes on to say that "the industry continues to have the last word on which of the regulations put forward for the governance of its conduct it is prepared to accept."[14] He quotes as a fact the charge of one Congressman that: "Nobody's in charge there . . . nobody has responsibility. One would think that FERC could direct and require more cybersecurity be employed by owners and operators of the electric grid. They do not."[15]

This is incorrect. Under section 215(c)(2)(A) of the Federal Power Act (FPA),[16] the FERC's certification of NERC as the Nation's Electric Reliability Organization (ERO) was contingent on its development of rules assuring its independence from "users and owners and operators of the bulk-power system."[17] The FERC's certification of NERC appropriately found that NERC's then-proposed (and now operative) rules assured NERC's independent governance.[18] Further,

10. *See* Andrea Peterson, *The Sony Pictures Hack, Explained*, WASHINGTON POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

11. *See* Greg Farrell & Patricia Hurttado, *JP Morgan's 2014 Hack Tied to Largest Cyber Breach Ever*, BLOOMBERG (Nov. 10, 2015), http://www.bloomberg.com/news/articles/2015-11-10/hackers-accused-by-u-s-of-targeting-top-banks-mutual-funds.

12. KOPPEL, *supra* note 2, at 10-11.

13. *Id.* at 45.

14. *Id.* at 30.

15. *Id.* at 33 (quoting Rep. James Langevin (D., RI)).

16. 16 U.S.C. § 824o(c)(2)(A) (2005).

17. § 824o(c)(2)(A).

18. *North Am. Elec. Reliability Corp*., 116 F.E.R.C. ¶ 61,062 at PP 6-7, 40, 43-44, 545 (2006); *order on reh'g and compliance* 117 F.E.R.C. ¶ 61,126 (2006); *order on compliance* 118 F.E.R.C. ¶ 61,190 (2007); *order*

NERC itself, not the industry, is charged under FPA section 215(d)(1)[19] with the responsibility of developing reliability standards, including those governing cyber standards. While NERC's rules provide for an industry-engaged stakeholder process in order to assist in the development of standards,[20] the ultimate responsibility for filing and supporting the standards lies with NERC, and the standards are subject to the FERC's approval.[21] Further, and directly contrary to Koppel's contention, FPA section 215(d)(5)[22] authorizes the FERC "[to] order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section."

Under this authority, the FERC has directed the development of additional standards, most notably governing measures that utilities must take to ensure the physical security of critical assets (substations),[23] and those addressed to vulnerability posed by entities in the utility supply chain.[24] Further, at the FERC's direction, NERC's rules of procedure were revised in order to ensure that the industry stakeholder process cannot stand in the way of NERC's development of standards responsive to a FERC directive.[25] NERC's rules now provide that the NERC Board of Trustees is responsible for the development and filing standards responding to FERC directives if the industry stakeholder process is unable to respond.[26] As well, NERC's enforcement regime is completely independent of electric industry stakeholders and subject to FERC oversight under FPA section 215(e)(2).[27] In addition, the FERC has independent prosecutorial authority to enforce NERC standards under FPA section 215(e)(3). These provisions, along with the FERC's and NERC's implementation, thoroughly contradict Koppel's contention that the electric industry is the last word on cybersecurity standards and enforcement.

The list of vulnerabilities to which Koppel says the industry, NERC, and the FERC have failed to respond include the failure to airgap operating systems and

on reh'g, 119 F.E.R.C. ¶ 61,046 (2007); *rev. denied sub nom.*, Alcoa Inc. v. FERC, 564 F.3d 1342 (D.C. Cir. 2009).

19. 16 U.S.C. §§ 824o(d)(1)-(2).

20. *North Am. Elec. Reliability Corp*., 125 F.E.R.C. ¶ 61,056 at P 24 (2008); *North Am. Elec. Reliability Corp*., 116 F.E.R.C. ¶ 61,062 at PP 10-11 (2006).

21. *Rules of Procedure*, NORTH AM. ELEC. RELIABILITY CORP., http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx (last visited Oct. 21, 2016) (§ 300 (Reliability Standards Development) and Appendix 3A (Reliability Standards Development Procedure)).

22. 16 U.S.C. § 824o(d)(5).

23. *See* Order No. 802, *Physical Security Reliability Standard,* 149 F.E.R.C. ¶ 61,140 (2014) (to be codified at 18 C.F.R. pt. 40). The Commission's order directing NERC to submit what eventuated in NERC Standard CIP-014 was in direct response to the Metcalf incident, and requires utilities to develop and implement procedures providing for the physical protection of transmission stations and substations, along with their associated primary control Centers, the loss of which could result in loss of reliability of the Bulk Electric System. *See* NORTH AM. ELEC. RELIABILITY CORP., STANDARDS (Oct. 21, 2016), http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=Physical Security.

24. Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards*, 156 F.E.R.C. ¶ 61,050 (2016) (to be codified at 18 C.F.R. pt. 40).

25. *North Am. Elec. Reliability Corp.*, 134 F.E.R.C. ¶ 61,216 (2011).

26. *Id.* at P 16, 29.

27. 16 U.S.C. § 824o(e).

related reliance on the internet, the risks of decentralized generation ownership, the networked exposure created by large RTOs, the failure to establish an adequate information sharing network, and the failure to apply cyber standards to utility distribution networks. Here, while Koppel is not wrong to highlight these areas of concern, he gives unreasonably short shrift to the efforts undertaken by the electric industry, NERC, and the FERC to grapple with known risks.

As to the use of air gaps, Koppel says that "[i]n theory, the administrative network is 'air-gapped' from the operational side of each power company, meaning that there is no physical connection between the two. Power companies insist that these two networks are absolutely separate and not connected."[28] Koppel then reports that DHS and the FERC have nonetheless found "minute" connections, which Koppel explains this way: "The problem with air-gapping, one academic specialist warmed me, is that it fails to take the human factor into account. 'Every time a worker brings in a thumb drive or laptop from home and hooks it up to an "isolated" site, the mobility of workers bridges the air gap.'"[29]

In fact, control systems such as SCADA are generally isolated from utility business systems. And while Koppel is right in saying that thumb drives and laptops ("transient devices," under the NERC Standards) open additional attack vectors,[30] he does not reveal that in November of 2013, the FERC ordered NERC to develop and implement mandatory security protections for employing transient devices.[31]

Further, the FERC launched in July of this year a Notice of Inquiry (NOI) into the potential for standards that would further isolate electrical control systems,[32] and NERC is studying the issue. But, there are serious operational concerns and reliability implications associated with full operational isolation, including the loss of remote operational capability routinely employed in emergency situations. As NERC put it, in response to the FERC's NOI:

> As the Commission recognizes in the NOI, any added security benefit from Internet isolation must also be weighed against operational impact. Mandating complete Internet isolation for BES Cyber Systems in Control Centers performing transmission operator functions may not be feasible as it could impact, among other things, data exchange, remote access, patch management, and transmission scheduling capabilities. . .[33]

No doubt, this is an area that warrants further study, and perhaps additional protective protocols. FERC's NOI was substantially motivated by a DHS alert

28. *Id.* at P 42.

29. *Id.* at P 43.

30. The Stuxnet virus, initially engineered by the West in order to undermine the Iranian nuclear centrifuge operation and later reengineered and employed in the Aramco Shamoon attack, was introduced into Iran's computer networks by thumb drive. *See* Farhad Manjoo, *Don't Stick It In*, SLATE, (Oct. 5, 2010), http://www.slate.com/articles/technology/technology/2010/10/dont_stick_it_in.html.

31. Order No. 791, *Version 5 Critical Infrastructure Protection Reliability Standards*, 145 F.E.R.C. ¶ 61,160 (2013) (to be codified at 18 C.F.R. pt. 40). The Standard (CIP-010-2, R4) was approved by FERC earlier this year, in an order directing additional protections for devices associated with lower impact BES Systems. *See* Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* 154 F.E.R.C. ¶ 61,037 (2016) (to be codified at 18 C.F.R. pt. 40).

32. Order No. 1000, *Cyber Systems in Control Centers,* 158 F.E.R.C. ¶ 61,051 (2016) (to be codified at 18 C.F.R. pt. 35).

33. Comments of N. Am. Elec. Reliability Corp. in Response to Notice of Inquiry, *Cyber Sys. in Control Centers*, No. RM16-18-000 (Sept. 26, 2016).

following the Ukrainian grid attack recommending the isolation of utility control systems from the internet.[34] It is true, as Koppel observes,[35] that reliance on the internet has created an area of vulnerability with which the electric industry must grapple. Recent reports Internet-based of Denial of Service attacks disabling internet operations through the manipulation of internet-facing appliances are concerning, and highlight this vulnerability.[36] But it is also true that a great deal of efficiency one expects of the electric grid, and certainly the industry's ability to establish the "smart grid" of the future—one in which utilities and related service providers establish a feedback loop enabling customers to adjust demand and supply in a manner that reflects individualized needs, maximizes system efficiency, and helps minimize environmental impact—depends on use of the internet.[37] As the industry, the FERC, policymakers, and stakeholders grapple with this new environment and its security implications, Koppel's un-nuanced, overheated rhetoric does not seem helpful.

Much the same can be said of Koppel's discussion of the implications of the competitive environment for power supply, and the administration of organized markets by Regional Transmission Operators (RTOs). Of the proliferation of independent power production, Koppel says that "[d]eregulation of the power industry has created a system with more vulnerable points of entry than ever existed previously . . . ."[38] He says further that

> [b]ecause the system's maintenance and protection reside in so many different hands . . . and because its complexity has made each player more dependent on computerized control systems, the grid is also more vulnerable than it used to be. New forms of interconnections between and among firms create new pathways through which malicious cyberattacks may travel.[39]

Yet, Koppel fails to acknowledge that those independent power producers which are defined as part of the Bulk Electric System (BES)[40] and control BES Cyber Assets[41] are governed by mandatory NERC Critical Infrastructure Protection (CIP) Standards. While it is true that the proliferation of generation owners diffuses responsibility for cybersecurity management, there is no evidence that

34. *Cyber-Attack*, *supra* note 8.

35. KOPPEL, *supra* note 2, at 10 ("The unintended consequences of Internet dependency are already piling up.").

36. *See* David Sanger and Nicole Perloth, *A New Era of Internet Attacks Powered by Everyday Devices*, N.Y. TIMES (Oct. 22, 2016), http://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=second-column-region&region=top-news&WT.nav=top-news&_r=0.

37. *See Smart Grid Resource Center*, ELECTRIC POWER RES. INST., http://smartgrid.epri.com/ (last visited Oct. 18, 2016).

38. KOPPEL, *supra* note 2, at 38.

39. *Id.* at 28.

40. As it relates to generation, the BES is generally defined to include real and reactive power resources connected at 100 kV and higher. *See* NORTH AM. ELEC. RELIABILITY CORP., GLOSSARY OF TERMS USED IN NERC RELIABILITY STANDARDS (Sept. 29, 2016), http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

41. A BES Cyber Asset is defined as one that, "if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System." *See id.* at 15.

independent power producers take their responsibilities any less seriously than do traditional utilities.[42]

As to RTO networks linking regional power grids, Koppel implies that the structure is more vulnerable than were traditional utilities. He asserts that the regional balancing process "creates a dangerous point of vulnerability," and goes on to say that "[i]f someone were to hack into an RTO or ISO and deliberately overload the lines, the impact would be swift and physical."[43] But here again, Koppel does not mention the applicability of the comprehensive suite of CIP standards for which RTOs, as transmission operators of the grid, are responsible.

Koppel correctly identifies information sharing between industry entities and government agencies as one of the key elements of a strong defense. But he goes on, incorrectly, to minimize the efforts that are being undertaken, even if they can be improved. Commenting on the electric industry's long-standing complaint that government agencies have been less forthcoming than might be helpful in sharing cyber threat information in their possession, Koppel turns the table with this:

> For any sort of cyber defense system to efficiently protect the electric power industry, information sharing has to be a two-way street. Corporations will have to get over their privacy and liability concerns and give government agencies the security data those agencies say they need in order to be effective. The military and intelligence agencies in turn need to make information relating to cyber threats available in real time, setting aside worries about jeopardizing sources and methods.[44]

Yet, Koppel ignores, first, the fact that the electric industry's primary resource for sharing information of cyber threats—with the government's encouragement—is the Electric Sector Information and Analysis Center (E-ISAC). Administered by NERC, and operated in coordination with the Electric Sector Coordinating Council (ESCC)[45] and the Department of Energy, the E-ISAC was chartered to facilitate sharing of information regarding physical and cyber threats, vulnerabilities, incidents and potential protective measures. It "serves as the primary security communications channel for the electricity sector,"[46] coordinating communications by and between members companies, sharing campaign analysis and incident data from private and public entities and it coordinates event and threat analysis with DOE, FERC and DHS.[47] The E-ISAC was launched following the issuance of Presidential Decision Directive 63 (PPD-63), along with nearly a dozen other ISACs operating critical infrastructure in other sectors of the economy. The E-ISAC is among the most robust and effective of these organizations and the electric industry's vehicle of choice for information sharing.

There is no support for Koppel's charge that electric industry concerns over privacy have stood in the way of robust information sharing, certainly with the E-

42. For all entities subject to NERC Standards, violations carry potential penalties of up to $1,000,000 per day/per violation. *See* 16 U.S.C. § 825o-1(b) (2000).

43. KOPPEL, *supra* note 2, at 37.

44. *Id.* at 48.

45. The ESCC serves as the principal link between the Administration and high-level electric industry executives. It is populated by Cabinet-level members from DOE and DHS, senior electric industry executives and trade association leaders. *Overview*, ELECTRIC SUBSECTOR COORDINATING COUNCIL, http://www.electricitysubsector.org/ (last visited Oct. 19. 2016).

46. *Electricity ISAC*, NORTH AM. ELEC. RELIABILITY CORP., http://www.nerc.com/pa/ci/esisac/Pages/default.aspx (last visited Oct. 19, 2016).

47. *Id*.

ISAC. Though privacy concerns permeate the cybersecurity area, the focus of these concerns lies principally with unprotected access to personal data by the government, and data breaches by hackers for commercial or other reasons. Information regarding the vulnerability of electric industry industrial control systems does not involve those sensitivities, and this author is unaware of any privacy-related obstacle to sharing of threat information with the E-ISAC or other government agencies.[48]

Moreover, shortly after publication of Koppel's book, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA).[49] Sections 105 and 106 of the CISA direct the establishment of procedures for sharing cyber threat indicators and defensive measures with DHS, and relieve any entities doing so from any associated liability. Privacy and liability concerns that animated this protection were voiced largely by entities outside the electric sector. Under this new authority, DHS is implementing new protocols for receiving, processing and further sharing this information.[50] Whether CISA and the associated DHS processing center ultimately serve as a useful supplement for the E-ISAC remains to be seen. There is value in information sharing across industrial sectors, and DHS may ultimately play a valuable role in this respect. Regardless, the statute expressly indicates that it does not preempt existing sharing programs, such as the E-ISAC.[51]

III. HOW SECURE ARE WE?

No responsible electric industry executive or government official would say that the electric grid enjoys absolute protection from cyberattack. The threats are too varied and mutable, and the list of potential adversaries too long, for any such assurance to be credible. So, it is unsurprising that Koppel elicits from high-ranking electric industry officials the concession that grid security is not guaranteed. EEI's Scott Aaronson (National Security Director for Edison Electric Institute), is quoted as saying that he has been "conditioned to say that nothing is impossible."[52] From an unnamed senior utility executive who chairs the ESCC, Koppel secures the representation that "I don't mean to convey 100% confidence."[53] When he asked Howard Schmidt, a former cybersecurity advisor to President Obama, whether he would have guaranteed to the President that a "cyberattack won't knock out one of our power grids." Schmidt is quoted as saying "absolutely not."[54] Still, Aaronson says, reflecting the views of many in the electric industry, that

48. There is some sensitivity regarding customer-identifying and usage data. While data systems containing such information should be protected, information sharing regarding threats to control systems is unrelated, and information sharing regarding breaches of customer data can be designed to protect customer information.

49. 6 U.S.C. §§ 1501-1510 (2015). Though Koppel says that the electric industry actively opposed cybersecurity legislation, with the effect that it "languished in the Senate," the industry actively supported passage of CISA. Koppel, *supra* note 2, at 227.

50. *See* U.S. DEP'T HUMAN SERVS., FINAL PROCEDURES RELATED TO THE RECEIPT OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT (June 15, 2016), https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_(105(a)).pdf.

51. 6 U.S.C. § 1507(f) (2015).

52. KOPPEL, *supra* note 2, at 49.

53. *Id.* at 54.

54. *Id.* at 79.

"taking down the grid is not nearly as simple as I think some people, who may have services they'd like to sell, would have people believe."[55]

Koppel elicits yet more alarming statements from a parade of former government officials, many now in the security consulting business. Former Major General Brett Williams, once director of operations for U.S. Cyber Command, is quoted as saying "obviously, we can't defend against everything, but right now we're vulnerable to almost everything."[56] Richard A. Clarke, once National Coordinator for Security Infrastructure Protection and Counterterrorism in the Clinton and second Bush Administrations, and now head of Good Harbor Security Risk Management in Washington, D.C., instructs that the footprint managed by RTOs exposes the grid to extensive new vulnerability.[57] Retired General Keith Alexander, former Director of the National Security Agency (NSA) and now heading up IronNet Cybersecurity, Inc., is quoted at some length on the vulnerability to which smaller, ostensibly less sophisticated utilities, expose the grid if they are "brought down in the right order." And Janet Napolitano, once President Obama's head of the Department of Homeland Security, asked by Koppel what she thinks the chances are that a nation state actor could knock out one of our power grids, replied "very high—80 percent, 90 percent. You know, very, very high."[58]

Koppel adds to the drama by exploring the implications of long-term, widespread, power outages. The picture is not pretty, with Koppel reporting that the amount of planning by civil authorities, most prominently the Federal Energy Management Administration (FEMA), for a contingency of this nature is substantially less extensive than one might think. Koppel further reports on disagreement among senior managers within FEMA on whether plans for evacuation of major population centers in these circumstances are needed,[59] and he says that there are no plans in place for food supplies over an extended period.[60] Koppel summarizes the situation this way:

> There are emergency preparedness plans in place for earthquakes and hurricanes, heat waves and ice storms. There are plans for power outages of a few days, affecting as many as several million people. But if a highly populated area was without electricity for a period of months or even weeks, there is no master plan for the civilian population.[61]

So, how worried should we be? The answer is "reasonably." Speaking for the industry, Aaronson and Koppel's unnamed Chair of the ESCC are right to pull up short of guaranteeing security. But while Koppel takes this as a concession, it instead seems to be a realistic acknowledgment of the rapidly evolving nature of cyber threats and the multiplicity of actors who may wish us harm. To the latter point, Koppel says that "[w]e literally have no count of how many groups or even

55. *Id.* at 47.

56. *Id.* at 47.

57. KOPPEL, *supra* note 2, at 49.

58. *Id.* at 50. Though he uses statements like Napolitano's regarding nation –state actors to support his view that we are unprepared, Koppel himself discounts such threats ("As we've seen nation-states are restrained by an understanding of networked interests and likely consequences."). *Id.* at 81.

59. *Id.* at 11.

60. *Id.* at 121-124.

61. *Id.* at 5. In something of a distraction, Koppel devotes a substantial portion of *Lights Out* (Chapters 13-17) to the activities of survivalists convinced that the end of civilization as we know it is imminent. As these individuals are not offered as experts, the point of the stories is hard to discern, colorful as they are.

individuals are capable of launching truly damaging attacks on our electric power grids—some, perhaps even most of them, uninhibited by the threat of retaliation."[62] This is true, but as with a good deal of Koppel's book, it sounds threatening without being helpful.

IV. SOLUTIONS

Koppel offers a short list of solutions. On a technical level, he touts the work of former General Keith Alexander, whose IronNet Cybersecurity group is promoting a universal monitoring program, which Alexander describes as a sort of ADT security system capable of monitoring utility systems for cyber intrusions and reporting them to enforcement authorities. It is hard to know how effective a program this may be, though it does not appear to be novel, as system monitoring and detection have long been understood to be basic building blocks of a cybersecurity program.[63]

Turning his attention to the governmental institutions involved in cybersecurity protection, Koppel pans DHS's expertise and authority, commenting that it has "neither the capacity to defend our infrastructure nor the wherewithal with which to retaliate."[64] Instead, he recommends that we involve the NSA and the Department of Defense (DOD). Koppel quotes retired General David Petraeus as saying that the NSA is "far and away the most competent, capable, best in world entity in terms of cybersecurity and analysis."[65] The DOD has similar technical capability, along with the wherewithal to launch counterattacks, and only DOD, Koppel notes, currently has the capability of managing the impact of a massive and long-term blackout on major population centers.

Koppel is certainly right that it is a mistake for us not to marshal our best and most effective resources in defense of the electric grid. The electric industry has good reason to resist extending operational authority to national security institutions. Neither the NSA nor DOD have the expertise to manage the grid, while our long-standing reluctance to intermesh civilian and military institutions is an important element of our democratic tradition. However, it is also true that it would be a mistake for us not to capitalize on expertise wherever available, and there is no denying that the security of the grid has national security implications. Koppel's call for more coordination in this respect seems well-put.

62. KOPPEL, *supra* note 2, at 10.

63. NERC Standard CIP-005, R1.5, requires responsible entities to employ "one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications." Automated Detection and Monitoring are also key elements of the Cybersecurity Framework promulgated by the National Institute of Standards and Technology pursuant to Presidential Order 13636 (February 12, 2013). *See* NATIONAL INST. STANDARDS & TECH, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf ("Detect"). The same is true of the Electric Sector Maturity Model, issued by DOE in 2012. *See* U.S. DEP'T ENERGY, ELECTRICITY SUBSECTOR: CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2) § 7.4 (Feb. 2014), http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

64. KOPPEL, *supra* note 2, at 220.

65. *Id.* at 218.

V. VALUE ADDED?

To the extent *Lights Out* contributes to a thoughtful discussion of the electric grid's vulnerability, it will serve a useful function. Knowing that this vulnerability is real—by anyone's account—may trigger a productive discussion regarding national preparedness and the importance of providing a physical safety net for U.S. citizens and residents in the event of a long-term outage. Our physical security is among the government's fundamental responsibilities and if Koppel is correct that preparedness is wanting, that should be corrected. As well, Koppel's pitch for better coordination between those responsible for the electric industry and the security arms of the U.S. government (NSA and DOD) is well-placed.

What is not helpful is Koppel's inaccurate representation of the machinery already in place to address cyber threats. Koppel's notion that the electric industry is beholden to no one in the manner in which the grid is protected is wrong, as is the implication that measures now being taken are grossly out of step with known risks.