Enhancing cybersecurity in the energy sector: a critical priority

Don C Smith

To cite this article: Don C Smith (2018) Enhancing cybersecurity in the energy sector: a critical priority, Journal of Energy & Natural Resources Law, 36:4, 373-380, DOI: 10.1080/02646811.2018.1516362

To link to this article: https://doi.org/10.1080/02646811.2018.1516362

Published online: 24 Sep 2018.
EDITORIAL

Enhancing cybersecurity in the energy sector: a critical priority

The growing anxiety among United States policy-makers, and the American energy sector in particular, about cyberattacks on the nation’s energy infrastructure was vividly underscored recently in a front page article in The Wall Street Journal headlined, ‘U.S. Officials Push New Penalties for Hackers of Electrical Grid’1. As the story reported, ‘The push for explicit action is coming from top federal agencies to fight worsening threats to the country’s electricity system and other critical industries, particularly menacing actions from Russia, China, Iran and North Korea.’2 Despite the assertion by federal authorities, Russia, in particular, has denied ‘targeting critical infrastructure’3.

The Wall Street Journal front page story followed just days after an announcement by the US Department of Homeland Security (DHS) that a new office, the National Risk Management Center (NRMC), was being established to focus on defending the nation’s critical infrastructure.4 In making the announcement at the National Cybersecurity Summit, DHS Secretary Kirstjen M Nielsen said, ‘I believe that cyber threats collectively now exceed the danger of physical attacks against us. This is a major sea change for my Department and for our country’s security,’ adding, ‘An attack on a single tech company, for instance, can rapidly spiral into a crisis affecting the … energy grid [and] water systems.’5 Speaking at the same conference, US Department of Energy (DOE) Secretary Rick Perry noted, ‘The economy of the world is driven so much by energy. It’s our national security interest to continue to protect these sources of energy.’6

The ‘largest interconnected machine’ in the world

To put the American threat into larger context, the US electricity grid, which has been referred to as the ‘largest interconnected machine’ in the world, consists of ‘more than

---

2 Ibid.
5 Ibid.
7,000 power plants, 55,000 substations, 160,000 miles of high-voltage transmission lines and millions of miles of low-voltage distribution lines.

The threat of cyberattacks on United Kingdom electricity systems has also provoked significant concern. The former Chair of the House of Commons Defence Committee, Lord Arbuthnot of Edrom, has warned that ‘protecting the electricity network must be a priority since many services, including sewage and water, depend on electricity,’ adding, ‘If you take down the electricity network you very quickly take down everything else as well. The vulnerability is real.’

While only several years ago the thought that a cyberattack could disable an electricity system ‘was the stuff of science fiction,’ today in a rather startling, if not disconcerting, admission, US-based utility companies owned by private investors have said ‘they don’t have the resources on their own to protect the country’s three big electric grids – one in the east, one in the west and one in Texas – against foreign governments.’ Moreover, Marina Krotofil, an expert on systems that control utilities, has said, ‘The frequency of the attacks and potential attack scenarios are becoming so dangerous that we can’t wrap our brains around it,’ adding that rather than a few Russian hackers, ‘It’s a cyber army.’

In March, the DHS released a report titled ‘Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.’ Among other things, the report said that, since March 2016, and perhaps before, ‘Russian government cyber actors … targeted government entities and multiple U.S. critical infrastructure sectors including the energy, nuclear … [and] water’ sectors.

In June, the President’s National Infrastructure Advisory Council, which includes many energy sector leaders, said, ‘The [US] needs to prepare for a “catastrophic power outage” possibly caused by a cyberattack.’ The Council reviewed a presentation that included this cautionary tale: ‘Given the interconnected nature of critical systems and networks, new broad-scale approaches are needed to adequately prepare for, and respond to, and recover from catastrophic disasters that can create significant power outages with severe cascading impacts to multiple critical sectors.

An increase in cyber threats from ‘sophisticated actors’

To provide further context, early this year, Symantec Corporation, which specialises in cybersecurity services, said its tracking indicated an increase in energy sector

---

9 See Smith, ‘U.S. Officials Push New Penalties’ (n 1).
10 Ibid.
11 Ibid.
13 Ibid.
cyberattacker groups, from 87 in 2015 to 140 in early 2018. Moreover, Duke Energy, which serves nearly eight million customers, ‘reported more than 650 million attempted cyberattacks in 2017 alone’. Scott Aaronson, Edison Electric Institute Vice President of Preparedness and Security, has observed, ‘Are we seeing an increase in threats from sophisticated actors? Yes I think we are.’

In response to the cyberattack risks, the NRMC has been described by Secretary Nielsen as ‘an initiative driven by industry needs and focused on fostering a cross-cutting approach’ to defend critical US infrastructure. The NRMC, which will be a part of the DHS, will emphasise information sharing involving cybersecurity in several business sectors, including energy. In particular, the Center will draw together industry representatives and experts from government to discuss all government initiatives to defend against cyberattacks. It will employ a more strategic approach to risk management borne out of the re-emergence of nation-state threats, our hyperconnected environment, and our survival and its need to effectively and continually collaborate with the private sector,’ Nielsen said.

The National Security Summit, which took place in late July, brought together government and private sector leaders to consider cybersecurity threats. ‘The summit was an attempt by the Trump administration to project a united front on prioritizing cybersecurity as a top national security concern, amid criticism from lawmakers in both [US political] parties that it hasn’t developed a coherent cybersecurity strategy,’ The Wall Street Journal reported. The announcement of the NRMC followed ‘some skepticism over the White House’s level of concern over election security,’ which involves another type of cybersecurity threat.

‘Planning to unplug American power systems in a time of conflict’

Meanwhile, David Sanger, a journalist for the New York Times who has significant expertise in cybersecurity, has reported, ‘State-sponsored Russian hackers appear far more interested this year in demonstrating that they can disrupt the American

---

16 See Malik and Nussbaum (n 6).
21 See US DHS (n 4).
22 Ibid.
electric utility grid than the [November 2018] elections, according to United States intelligence officials and technology company executives.\textsuperscript{26} In the same article, Singer reported, ‘[T]he Department of Homeland Security reported [in late July] that over the last year, Russia’s military intelligence agency had infiltrated the control rooms of power plants across the United States. In theory, that could enable it to take control of parts of the grid by remote control.’\textsuperscript{27} Thus far, the DHS has ‘understated the scope of the threat’ he stated.\textsuperscript{28} The ultimate fear, Sanger reported ‘is that Russia may be planning to unplug American power systems in a time of conflict. But such an attack would almost certainly result in a military response, as General [Paul M] Nakasone obliquely suggested’ at a recent public policy forum.\textsuperscript{29}

In 2017, Russian hackers, according to US federal officials, “claimed hundreds of victims”… in a giant and long-running campaign that put them inside the control rooms of U.S. electric utilities where they could have caused blackouts\textsuperscript{30}. Jonathan Homer, DHS Chief of Industrial Control System Analysis, said the cyberattacks occurred in the spring of 2016 through 2017. The attacks ‘exploited relationships that utilities have with vendors who have special access to update software, run diagnostics on equipment and perform other services that are needed to keep millions of pieces of gear in working order\textsuperscript{31}.

Interestingly enough, the attacks aimed at the US electrical grid have been linked by some security experts to the same group of Russian intelligence figures accused of meddling in the 2016 US presidential election.\textsuperscript{32} Attacks typically begin when intruders hack into energy sector software suppliers’ networks, from where the intruders pivot ‘to their real focus: the utilities. It was a relatively easy process, in many cases, for them to steal credentials from vendors and gain direct access to utility networks,’ according to The Wall Street Journal.\textsuperscript{33}

In addition to electricity utilities, pipelines have also been targeted by hackers. In early 2018, the communications systems of five US pipeline firms were attacked according to the firms.\textsuperscript{34} Moreover, Anthony Pugliese, a high-ranking official at the US Federal Energy Regulatory Commission (FERC), said in August that ‘more and more, you have adversarial countries … who see pipelines, for example, as an area of great opportunity’\textsuperscript{35}. And the matter of whether oil and gas companies are prepared to withstand a cyberattack remains uncertain. A firm that researches information security issued a 2017 report saying that more than 60 per cent of individuals surveyed

\textsuperscript{27} Ibid.
\textsuperscript{28} Ibid.
\textsuperscript{29} Ibid.
\textsuperscript{30} See Smith, ‘Russian Hackers Reach U.S. Utility Control Rooms’ (n 3).
\textsuperscript{31} Ibid.
\textsuperscript{33} See Smith, ‘Russian Hackers Reach U.S. Utility Control Rooms’ (n 3).
\textsuperscript{34} See Malik and Nussbaum (n 6).
believe their organizations have difficulty mitigating cyber risks across the oil and gas value chain.\(^{36}\)

**The crippling of Ukrainian utilities**

US electric utilities are not the only ones to have been targeted by cyberattackers. According to reporting in *The Wall Street Journal*, ‘Cyberhackers working for Russia crippled three Ukrainian utilities on Dec. 23, 2015, plunging hundreds of thousands of civilians into the darkness on a chilly winter’s eve.’\(^{37}\) And, despite the fact that no successful cyberattack has been launched against UK-based electric utilities, British utility firms were warned in March to ‘tighten their scrutiny of blackouts across the country … because frequent or long periods of disruption could be the sign of a cyber attack.’\(^{38}\)

FERC, the independent regulator that supervises the North American Electric Reliability Corporation (NERC), has also become increasingly concerned about cyber threats. FERC has ordered NERC to expand cyber threat incident reporting by transmission operators and owners of power plants.\(^{39}\) ‘Cyber threats to the bulk power system are ever-changing, and they are a matter that commands constant vigilance,’ Kevin McIntyre, FERC Chair, has said.\(^{40}\) In this regard, former FERC Commissioner Suedeen Kelly has said the mandatory reporting of cyber incidents ‘is an important step forward.’\(^{41}\) However, NERC and FERC rules apply only to large companies, not small ones that have also been of interest to hackers.\(^{42}\)

Another enormous risk that has yet to generate much attention is the lack of insurance by electricity companies to cover major catastrophic power outage-related losses. One firm, Brit Insurance, caps cybersecurity policies at about $300m.\(^{43}\) Such caps force companies to ‘piece together policies from different insurers to boost that limit,’ an effort that can be cost prohibitive.\(^{44}\) Energy firms often have a ‘superman fallacy,’ Dante Disparte, head of Washington, DC-based firm Risk Cooperative has said, noting, ‘They don’t believe bad things will happen to them, or they believe the government will help them get back on the field.’\(^{45}\)

---


37 See Smith, ‘U.S. Officials Push New Penalties’ (n 1).


40 *Ibid*.


42 See Sobczak and Behr (n 32).


44 *Ibid*.

45 *Ibid*. 

---
Meanwhile, energy sector firms have been criticised for a lack of spending on cybersecurity in the wake of growing risks, leading one industry observer to say that, while ‘US utilities have been slow to awaken to this danger … now they must direct significant resources to enhancing cybersecurity’. Estimates in April from two major security companies, the CAP Group and Precision Analytics LLC, indicated that energy firms spend only about 0.2 per cent of total revenue on cybersecurity-related measures. And some observers have criticised the Trump White House for scrapping the National Security Council coordinator position for cybersecurity earlier this year.

Looking ahead, the DOE is preparing for an ‘unprecedented’ test in November to assess the ability of the grid to recover from a hacker-caused blackout. The DOE aims to ‘gain insights into how industry, with DOE support, would execute response to a significant cyber incident,’ documents seen by E&E News indicate. The test, named Liberty Eclipse, will combine the challenges of fending off a cyberattack on natural gas, oil and electric infrastructure while re-energising the power grid.

Necessary immediate steps to address the cyber risk
Bearing in mind the risks to governments and societies, there are some steps that should receive immediate consideration. First, the lack of insurance coverage for catastrophic events must be remedied. In the US, for example, the federal government, trade associations and energy companies are beginning to discuss a ‘cyber version’ of the Federal Deposit Insurance Corporation, an independent agency created by the US Congress that insures customer deposits with financial institutions in return for fees paid by the institution.

Second, while large electricity generators and grid operators must abide by strong federal rules to protect infrastructure, smaller companies that are also part of the entire electricity system often ‘have inadequate resources to invest in full cybersecurity protections’. This vulnerability needs to be carefully analysed and measures taken to address shortcomings if need be. At a minimum, state utility commissions should require these smaller firms to implement security protections similar to those required of large companies.

Third, public resources should be invested in programmes to train cybersecurity professionals. It is particularly worrying that not enough of these professionals are

---

46 See Malik and Nussbaum (n 6).
48 See Malik and Nussbaum (n 6).
51 Ibid.
52 Ibid.
53 See Malik (n 43).
being trained: globally there may be a ‘cybersecurity workforce gap’ of nearly two million workers by 2022 unless action is taken now.56

Fourth, operators of gas pipelines should be required to ‘share operating information about potential vulnerabilities’ rather than today’s totally inadequate ‘voluntary’ sharing practice.57

Fifth, adequate public funding must be provided for cybersecurity research. Among other things, research related to grid security as well as how to reduce the complexity of the grid must be a priority.58

Finally, and perhaps most importantly, overall governmental efforts, particularly in the US and the European Union, have not been up to the task. According to one strategic research consultancy, ABI Research:

Public sector efforts have petered out since 2012-2013, when both the United States and European Union were actively driving national cybersecurity strategies. The current U.S. administration seems to have dropped cybersecurity from its list of priorities, and the European Commission is struggling to get its [directive on security of network and information systems] off the ground and obtain adequate funding for [the EU Agency for Network and Information Security] to fulfill its mandate.59

This observation was underscored by Michela Menting, ABI Research Digital Security Research Director, who warned, ‘It seems that the United States and the European Union have forgotten that cybersecurity needs to be a continuous effort, not a one-time announcement to tick all the boxes.’60

Thus far, the US has not suffered a catastrophic cyberattack. But that provides little solace for cybersecurity experts. ‘We have been incredibly lucky that there hasn’t been a catastrophic cyberattack against national critical infrastructure,’ Vice President for computer forensics firm Mandiant Charles Carmakal has said.61

The Willoughby Prize for 2017

Each year the Willoughby Prize is awarded to the author or authors of a Journal of Energy & Natural Resources Law article of outstanding merit. The winners of the 2017 Willoughby Prize are Fenner L Stewart and Allan Ingelson, authors of ‘Regulating energy innovation: US responses to hydraulic fracturing, wastewater injection and induced seismicity,’ which was published in the May 2017 issue. Messrs Stewart and Ingelson are both professors at the University of Calgary Faculty of Law. The Prize is awarded in memory of Geoffrey Willoughby (1936–1989), a leader in the development

58 See Govindarasu and Hahn, ‘As Russians Hack the US Grid’ (n 54).
60 Ibid.
of UK energy law. To win this prestigious prize is no small achievement. All of us associated with the *Journal* send our warm congratulations to Professors Stewart and Ingelson and our thanks to the Willoughby Prize Committee.

Don C Smith

*Editor, Journal of Energy & Natural Resources Law,*

*University of Denver, US*

Email: dcsmith@law.du.edu