LSU Journal of Energy Law and Resources

Volume 6
Issue 2 *Spring 2018*

6-6-2018

Naked and Afraid? Vulnerabilities in the ElectricityInfrastructure and Criminal Law

Melissa Wheeler

Naked and Afraid? Vulnerabilities in the Electricity Infrastructure and Criminal Law

INTRODUCTION

It is April 12, 2018. Dozens of terrorists just attacked the United States in a conspiracy to launch a cyberattack on the power grid. Cities around the country lose electricity immediately. Utility providers and the Federal Emergency Management Agency (FEMA) respond quickly, but the terrorists have also physically attacked the backup transformers and cut off power lines essential for restoring electricity. A third of the United States is without power and will be for weeks, causing great inconvenience, billions of dollars in damage, and—in some cases—serious bodily injury or death.

Americans depend on electricity culturally, economically, and politically. Without electricity, it would be impossible to charge cell phones and computers; receive news or get on the Internet; pump gas, preserve food, access clean water, heat homes; or retrieve money. Doctors would be powerless to keep many of their hospital patients alive, and the military would be unable to coordinate strategy or communicate. The effects of electricity loss would be apocalyptic.

This scenario is not farfetched; an attack on the United States' electricity infrastructure could really happen. If it did happen, the federal government is ill-equipped, both to restore the grid and to prosecute the terrorists.

Unfortunately, Americans have had enough experience with terrorism to have learned how not to address the issue. The first step to addressing a national security risk must be to debate the character of the problem.[1] The problem is that the United States' electricity grid is old and haphazardly patched together; as a result, it is extremely vulnerable to attack.[2]

The U.S. electricity grid is in the initial stages of transformation to a Smart Grid, which will take twenty-five to thirty years.[3] One purpose of this transformation is to improve security.[4] More specifically, the government's goal is to make the electrical system resistant to natural disasters and various forms of attack.

---

1. Richard Danzig, *Foreword to* ANDREAS WEGNER & RETO WOLLENMANN, BIOTERRORISM: CONFRONTING A COMPLEX THREAT, at vii (2008).

2. GRETCHEN BAKKE, GRID: THE FRAYING WIRES BETWEEN AMERICANS AND OUR ENERGY FUTURE, at xiv (2016).

3. *The Future of the Grid*, SMARTGRID, https://perma.cc/AN23-RMB9 (last visited Jan. 21, 2017).

4. *See What is the Smart Grid?*, SMARTGRID, https://perma.cc/J3GP-NPNA (last visited Jan. 21, 2017).

While energy sector actors are trying to identify vulnerabilities in the current grid, the legal system has yet to respond to the evolution or the risks of the infrastructure.

The legal regime criminalizing terrorism must evolve with the electricity infrastructure to anticipate sophisticated terrorist threats. Preparation is essential to national security; according to the U.S. Department of Justice, prevention of terrorism and promotion of the nation's security consistent with the rule of law is an essential strategic goal.[5] This goal will be impossible to accomplish until there are sufficient laws on the subject.[6]

There are no federal criminal laws that condemn cyberattacks against electricity-utilities' computer systems or the physical attacks a terrorist might perpetrate. Even on an international scale, the failure of nation-states to create a single definition of terrorism leaves electric grids and millions of people unprotected. There must be a comprehensive legal framework to simplify the prosecution of terrorists and protect citizens from long-term blackouts.

This article will emphasize the importance of preparedness as a means to enhancing national security and promoting peace of mind. Part I will explain how the electricity infrastructure works and further, will describe the proposed Smart Grid. Part II will explain how the grid is vulnerable to both physical and cyber terrorist attacks. Part III will explain shortcomings in both international and domestic anti-terrorist law. Part IV will propose solutions for how the criminal justice system can adequately address an attack.

I. THE ELECTRIC GRID

A. History of the Grid

Electricity is a fundamental part of American life and therefore essential to national security. Knowing the history of the grid is crucial to understanding its current design, vulnerabilities, and the industry's need to upgrade to the Smart Grid. The grid exists in its current form for two

5. OFF. OF THE ATT'Y GEN., DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE 2014-2018 STRATEGIC PLAN 13 (2012) [hereinafter STRATEGIC PLAN].

6. An attack on electricity infrastructure may not seem as dramatic as an attack on nuclear structure or bioterrorism. While romanticizing the tragic end of our democracy is a fascinating pastime, risks of both nuclear and biological attacks are explored extensively in scholarly literature and are specifically addressed in our laws. Attacks on electricity infrastructure are not specifically addressed. *See generally* CHARLES FERGUSON ET AL., THE FOUR FACES OF NUCLEAR TERRORISM (2005); WEGNER & WOLLENMANN, *supra* note 1.

reasons: (1) the nature of electricity and (2) the methods that its discoverers used to make electricity accessibility cheaper for the general public.

The electric grid is a power delivery system.[7] Researchers first explored the nature of electricity in the eighteenth and nineteenth centuries.[8] Because magnetic movement of electrons—electricity—is instantaneous, electricity must be consumed the moment it is produced and before it converts to heat energy.[9] Researchers found that an efficient electric system requires a connected grid of wires to carry electricity straight from its generation to its use.[10]

After thinking about how to make electricity accessible and affordable, scientists concluded that generators would need to be connected to many users at once.[11] Therefore, they built grids to maximize the scale of the operation at a minimal cost.[12]

The resulting technological advances in generation and transmission quickly led to the aggregation of small companies into larger monopolies over U.S. regions.[13] The first electricity supply systems were private and unregulated.[14] Utility companies made bilateral and multilateral agreements to pool power; over decades, economies of scale[15] and technological advancement led to very large power markets and huge interconnected regions sharing electricity.[16]

Today, these power markets are so large that the United States has a total of only three of them.[17] One grid provides electricity for the West, a bit of Mexico, and much of western Canada; the second for all of the East; and the third for Texas exclusively.[18] Through these grids, energy is generated from many power sources, sent through power lines to substations and

---

7. NAT'L RES. COUNCIL, THE NAT'L ACADEMIES, TERRORISM & THE ELECTRIC POWER DELIVERY SYSTEM 21 (2012).

8. *History of Electricity*, INST. FOR ENERGY RES., https://perma.cc/9YQ7-5M9Z (last visited Oct. 20, 2017).

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.*

13. TERRORISM & THE ELECTRIC POWER DELIVERY SYSTEM, *supra* note 7.

14. *Id.* at 20.

15. Economies of scale arise when average costs decline with the increasing size of a unit. *See generally* Raymond Hartman, *The Efficiency Effects of Electric Utility Mergers: Lessons from Statistical Cost Analysis*, 17 ENERGY L.J. 425 (1996).

16. *Id.*

17. BAKKE, *supra* note 2.

18. *Id.* Texas chooses to manage its entire electricity infrastructure independently.

transformers, distributed by utility companies, and finally consumed by the public.[19]

The private sector owns more than eighty percent of the electricity infrastructure system;[20] this system contains approximately 6,413 power plants.[21] From those power plants, more than 200,000 miles of power lines transfer electricity to almost all of the 318 million people in the United States.[22] As a whole, the United States' electric power industry includes over 3,000 businesses, institutions, and regulatory bodies.[23] All of these actors must cooperate for the system to function. An attack on this infrastructure has the potential to affect every single actor, from plants to individuals.

B. The Innovations of the Smart Grid

Currently, electricity infrastructure is going through extensive changes to become a "Smart Grid." The Smart Grid is: "[t]he integration and application of real-time monitoring, advanced sensing, communications, analytics, and control, enabling the dynamic flow of both energy and information to accommodate existing and new forms of supply, delivery, and use in a secure, reliable, and efficient electric power system, from generation source to end-user."[24]

The principal purpose of the Smart Grid is to update the electricity infrastructure because the grid has aged quickly and has not been significantly redesigned since it was originally implemented.[25] Over seventy percent of transformers and transmission lines are twenty-five years old; power plants, on average, are thirty-four years old.[26] The age of the infrastructure has personal and economic costs because as the grid ages, it is more likely to break down, which causes intermittent power outages. Every year, both the number of power outages and the length of time power outages last continue to increase in direct correlation to the age of the infrastructure.[27] In most industrialized countries, blackouts last less

---

19. Sarah Gerrity & Allison Lantero, *Infographic: Understanding the Grid*, U.S. DEP'T OF ENERGY (Nov. 17, 2014, 2:05 PM), https://perma.cc/6FJE-DF4C.

20. *Energy Sector*, DEP'T OF HOMELAND SEC., https://perma.cc/APN5-L6NE (last updated July 11, 2017).

21. *Id.*

22. TERRORISM & THE ELECTRIC POWER DELIVERY SYSTEM, *supra* note 7.

23. *Id.* at 23.

24. N. AM. ELEC. RELIABILITY CORP., RELIABILITY CONSIDERATIONS FROM THE INTEGRATION OF THE SMART GRID 96 (2010), https://perma.cc/VRF6-2DLH.

25. Mark Chediack et al., *Crumbling U.S. Grid Gets Jolt Driving Smart Houston Power*, BLOOMBERG (June 25, 2014), https://perma.cc/R3AP-PLJ7.

26. BAKKE, *supra* note 2.

27. *Id.*

than ten minutes, but in the United States the average outage is 120 minutes.[28] Outages cost the country over $188 billion annually.[29] Ideally, once upgraded, the Smart Grid will facilitate more efficient transmission of electricity, quicker restoration of electricity after disturbances, reduced peak demand, reduced operations and management costs for utilities, increased integration of renewable energy systems, increased integration of customer-owner power generation, and improved security.[30] The four main updates intended to make the grid "smarter" are: (1) Distribution Intelligence, (2) batteries, (3) microgrids, and (4) smart meters.

First, Distribution Intelligence is a "self-healing" system designed to detect power outages and immediately respond to reroute energy around the outage.[31] Distribution Intelligence is meant to pinpoint the source of the problem in transmission lines on its own.[32] This system will incorporate fully automated rerouting of electricity when an outage occurs.

Second, the electricity industry has also been working on developing new and stronger batteries. New energy storage technology helps to integrate renewable energy into the power grid by managing the supply of energy.[33] Scientists built the power grid to transmit a consistent flow of energy from generation to consumption.[34] Yet, renewable energy, such as solar and wind power, is not generated in consistent amounts. Batteries alleviate this problem because they can collect and store energy until it is needed, allowing electricity to flow through the grid consistently.

Third, microgrids are designed to protect the electric grid. If a disruption or outage on the grid occurs, microgrids can disconnect from the larger grid and function as an electrical island.[35] Isolation of critical systems is essential to increasing the security of the grid because interconnection puts the entire system, rather than just individual parts, at risk.[36]

Lastly, smart meters are the parts of the grid that most directly impact the consumer. They facilitate communication between consumers and utility companies regarding energy use and notify utility companies immediately

---

28. *Id.*
29. *Improving Grid Reliability*, TOLLGRADE, https://perma.cc/QX6X-ULP2 (last visited Nov. 6, 2017).
30. *What is the Smart Grid?*, *supra* note 4.
31. *Id.*
32. *Id.*
33. Gerrity & Lantero, *supra* note 19.
34. BAKKE, *supra* note 2, at xvi.
35. Gerrity & Lantero, *supra* note 19.
36. TERRORISM & THE ELECTRIC POWER DELIVERY SYSTEM, *supra* note 7, at 44.

when the power goes out.[37] In 2014, 58.5 million smart meters were installed; about eighty-eight percent of them were residential.[38] Even though smart meters are currently being implemented, their benefits will not be realized anytime soon.

The industry has commenced implementation of the Smart Grid, but the upgrades will not be complete for decades.[39] Until then, America's system will be vulnerable to traditional forms of attack. Although transformation will take time and investment, having a "strong," or resilient, grid is just as important as having a "smart" grid.[40] The industry should move forward with changes that will truly improve security as citizens await the long-term improvements in design.

II. THE VULNERABILITIES OF THE GRID TO A TERRORIST ATTACK

There is no evidence that the government is considering any new legal approaches to terrorism in the realm of energy infrastructure.[41] The threat is not hypothetical. In 2013, the energy sector was the most targeted sector for hackers in the United States, accounting for fifty-six percent of the 257 attacks reported to the U.S. Department of Homeland Security.[42] In 2015, according to the U.S. State Department, there were 255 terrorist attacks targeting utility companies worldwide, out of 12,204 terrorist attacks total.[43] This section considers the vulnerabilities of the electricity infrastructure and risk of a terrorist attack in three parts: types of potential terrorist attacks; the likelihood that the Smart Grid will improve security; and the actual risk of an attack. Governments must consider all three issues as they develop and refine anti-terrorism laws.

---

37. Gerrity & Lantero, *supra* note 19.

38. *How Many Smart Meters are Installed in the United States and Who Has Them?*, U.S. ENERGY INFO. ADMIN., https://perma.cc/T6UJ-YEM5 (last visited Jan. 21, 2017).

39. *The Future of the Grid*, *supra* note 3.

40. Kennedy Maize, *The Electric Grid: Civilization's Achilles Heel?*, POWER MAGAZINE (Jan. 1, 2013), https://perma.cc/YPL7-G2DB.

41. Matthew L. Wald, *Terrorist Attack on Power Grid Could Cause Broad Hardship, Report Says*, N.Y. TIMES, Nov. 14, 2012, http://www.nytimes.com/2012/11/15/science/earth/electric-industry-is-urged-to-gird-against-terrorist-attacks.html?_r=0.

42. Nicole Perlroth, *Smart City Technology May Be Vulnerable to Hackers*, N.Y. TIMES, Apr. 21, 2015, https://perma.cc/6K8N-2JK2.

43. NAT'L CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM, ANNEX OF STATISTICAL INFORMATION: COUNTRY REPORTS ON TERRORISM 2015, 15 (2016).

A. Types of Attacks on Electricity Infrastructure

The current electricity infrastructure was not designed to withstand well-organized acts of terrorism aimed at key elements of the system.[44] The grid is susceptible to two general types of attack: physical attack and cyberattack.

Targets for physical attacks might include any equipment used in the production or transmission of electricity.[45] Much of the equipment is so large that it must be located outdoors, where it is vulnerable to weapons ranging from rifles to laser-guided missiles.[46] Because electric energy converts to heat, electricity equipment often operates at elevated temperatures. The high temperatures make the equipment even more susceptible to heat-seeking missiles or homemade bombs.[47] Even a drone strike could harm much of the outside equipment.[48] Consider transmission towers that span thousands of miles. An attack on transmission towers could happen without observation in more remote parts of the nation.[49] Transformers are other potential targets; if lost, they would require replacing, which creates considerable revenue loss. Large power transformers are challenging to replace because they are usually custom-made and can cost between three and ten million dollars each.[50] Notably, the power industry has not publicly disclosed the number of these transformers; officials of the Department of Energy have stated that the agency is not even aware of the official number.[51] Finally, other physical targets include the electric utility companies' office buildings and warehouses. The loss of computers controlling parts of the grid could be devastating for many companies. Replacement of physical embodiments of the electricity infrastructure after an attack would be costly for the utility companies affected, the government, and the consumer.

A cyberattack target might include any components used to monitor and control the production, transmission, and flow of electricity.[52] An actor would have to intrude into the control systems through the Internet or the utility's private networks. The interconnectedness of a benign social

44. NAT'L RES. COUNCIL, THE NAT'L ACADEMIES, MAKING THE NATION SAFER: THE ROLE OF SCIENCE AND TECHNOLOGY IN COUNTERING TERRORISM 177 (2002).

45. *Id.* at 181.

46. *Id.*

47. *Id.*

48. *Drones: What Are They and How Do They Work?*, BRITISH BROADCASTING CHANNEL (Jan. 31, 2012).

49. MAKING THE NATION SAFER, *supra* note 44, at 181.

50. TED KOPPEL, LIGHTS OUT: A CYBERATTACK, A NATION UNPREPARED, SURVIVING THE AFTERMATH 95 (2015).

51. *Id.*

52. MAKING THE NATION SAFER, *supra* note 44, at 181.

network, like the Internet, can also provide countless paths of access for an attacker.[53] Cyberattacks are already common in the United States, but one unique challenge to addressing them is that both the target of a cyberattack and the attacker are disinclined to make the attack known for privacy or public relations reasons.[54]

Computerization of the electric industry makes it more vulnerable to cyberattack because companies rely on information management and computer systems. Computerization has reduced the need for personnel at key facilities such as electric substations and congested transmission corridors and has increased reliance on unsecured telecommunications or Supervisory Control and Data Acquisition (SCADA) systems.[55] SCADA systems allow automatic remote access to utilities and are designed to increase functionality rather than security.[56] Because of their connection to the Internet, SCADA systems are extremely susceptible to cyber-intrusion.[57] The use of simple technologies such as firewalls, encryption techniques, and surveillance technologies can help protect these systems. The issue with these technologies is that they are not designed to block and identify breaches as quickly as the rest of the SCADA systems operate.[58]

Another threat to the electric grid is an electromagnetic pulse attack (EMP). Similar to a cyberattack, an EMP would involve the introduction of radio or micro frequency waves into the circuits of the control systems, upsetting the electronics and leading to network destabilization and outages.[59] This type of attack might not lead to a need to replace equipment, but an attack of this sort could affect enormous portions of the grid.[60] Cyber and electromagnetic attacks are possible due to the multiple points of entry into systems and the number of Internet experts with the ability to perpetrate an attack.

Since both physical and cyberattacks, on their own, could cause extensive damage, a terrorist attack combining them would certainly ensure a blackout. Measuring the cost of large-scale or long-duration blackouts is not easy. After the August 2003 blackout that struck the Midwest, the Northeast, and parts of Canada, the estimated final cost was six billion

---

53. KOPPEL, *supra* note 50, at 63.
54. *Id.* at 9.
55. MAKING THE NATION SAFER, *supra* note 44, at 178.
56. Jennifer Alvey*, Digital Terrorism: Holes in the Firewall?,* PUB. UTIL. FORT., March 2002, at 12, 14.
57. *Id.* at 13.
58. *Id.* at 17.
59. MAKING THE NATION SAFER, *supra* note 44, at 182.
60. *Id.*

dollars.[61] That blackout was not intentional—the combination of a computer bug and an overgrown tree caused fifty million people to lose power for two days.[62] One projection from the National Research Council, based on a theoretical 2005 blackout of New Jersey Utility Public Service Electric & Gas found that a ninety-five percent loss of power in one day, and restoration of ten percent power after two months, would result in a loss of $389 billion for that state.[63] Disruption from an intentional attack could cost the country billions of dollars. If large and extended outages occurred during severe weather, hundreds of people could die from exposure to extreme heat or cold.[64] An isolated assault on an individual station, substation, or control center could cause a local disruption. A coordinated attack on multiple points in the system could potentially lead to a multistate blackout. Power would be restored in days or weeks at best, but acute shortages could result in rolling blackouts for years.[65] Cascading failure is when the collapse of a system in one spot sets off a chain of failures. This occurred in the August 2003 blackout; the power failure spread from Detroit to New York in just a few moments.[66] The enormity of target possibilities that could cause such a widespread blackout necessitates legal protection.

B. The Smart Grid and Resiliency in Case of Attack

Ideally, the implementation of the Smart Grid will decrease the vulnerability of the infrastructure to terrorist attacks. There are five main challenges to security that should be addressed as the industry updates the grid: (1) the large amount of consumer information the grid will transmit, (2) the greater number of control devices in the Smart Grid, (3) the poor physical security of a great portion of these devices, (4) the use of Internet Protocol as a communication standard, and (5) the greater number of stakeholders the grid will rely on for its smooth operation.[67] According to a European study of the first steps of implementation of a Smart Grid, the

61. TERRORISM & THE ELECTRIC POWER DELIVERY SYSTEM, *supra* note 7, at 16.
62. BAKKE, *supra* note 2, at xv.
63. TERRORISM & THE ELECTRIC POWER DELIVERY SYSTEM, *supra* note 7, at 16.
64. *Id.*
65. *Id.* at 180-81.
66. Matthew L. Wald*, As Worries Over the Power Grid Rise, a Drill Will Simulate a Knockout Blow*, N.Y. TIMES, Aug. 16, 2013, http://www.nytimes.com/2013/08/17/us/as-worries-over-the-power-grid-rise-a-drill-will-simulate-a-knockout-blow.html?_r=0.
67. VINCENZO GIORDANO ET AL., EUR. COMM'N, SMART GRID PROJECTS IN EUROPE: LESSONS LEARNED & CURRENT DEVELOPMENTS 56 (2013).

information technology concept of "defense in depth"[68] must be applied to a Smart Grid system to keep it secure—especially for SCADA systems—even if protections become redundant.[69]

A loss of control over utilities' control system communications would be disastrous. An inability to open and close circuit breakers, load signals to generators, or communicate with adjacent organizations would reduce the utility of the Smart Grid. The result would be a large-scale power outage and likely a slow recovery.[70] Losing telemetry to individual devices or losing the ability to communicate with individual devices is fairly frequent and inconsequential; introduction of smart meters would mitigate this issue.[71] An inability to communicate between SCADA and regional systems would be detrimental to real-time data exchange. Communication within the Smart Grid is essential to prevent cascading failure;[72] loss of control of the grid would lead to unreliable operation and possibly a blackout.[73]

Although the Smart Grid has many benefits, the more electronic, sophisticated, and "smart"—or computer assisted—the system becomes, the more vulnerable it is to code hacking.[74] Three of the main vulnerabilities are: inadequately secured wireless communication, use of a non-dedicated communications channel for command and control, and unauthenticated command and control data.[75] One of the safest ways to protect the grid is to split it into "islands;" the less interconnected the grid is, the fewer the number of people that will be affected by an attack.[76] Once implemented, the microgrid innovation would address and solve this issue.

In its final state, a Smart Grid might prevent cascading blackouts with quick identification of failures in the grid and isolation of the issue, but the transition will take time. Smart meters enable utility companies to immediately recognize when the power goes off. Most disturbances happen

---

68. "Defense in depth" is a strategy for mitigating cybersecurity threats. "Defense in depth" works by creating layers of protection to catch attacks. *See generally* Trevor Ford*, Cybersecurity Legislation for an Evolving World*, 50 U.S.F. L. REV. 119 (2016).

69. GIORDANO ET AL., *supra* note 67 at 57.

70. N. AM. ELEC. RELIABILITY CORP., *supra* note 24, at 78.

71. *Id.*

72. *Id.*

73. *Id.*

74. Maize, *supra* note 40.

75. TERRORISM & THE ELECTRIC POWER DELIVERY SYSTEM, *supra* note 7, at 45.

76. Maize, *supra* note 40.

earlier in the electricity distribution system, however, rather than at a consuming building.[77]

The grid is similarly vulnerable to an inside attack. Insiders have the knowledge and access to damage physical aspects such as transformers and switchgear. Employees with access to the utility company's software could insert viruses or change programs to wreak havoc on control systems.[78] Background checks are essential and may be one of the few ways to prevent an attack. The system is hard to regulate because so many actors oversee its maintenance and protection, and each is becoming more dependent on computers.[79] Many companies are pouring money into updating their infrastructure, but the ones who do not update will be the weakest links.[80]

Other actors in the electricity and energy sectors are putting effort into improving security. Batteries are still an important innovation; as companies design and develop new energy storage mechanisms, they will also need to be protected from attack. Some companies are working on bulletproof transformers.[81] Transformers are an essential part of all power transmission networks and must be protected from external damage, including from firearms, the ownership of which is permitted in many jurisdictions in the United States.

For example, an attack on transformers occurred on April 16, 2013, in San José, California, where snipers knocked out seventeen transformers in twenty minutes.[82] Restoration cost about $15.4 million.[83] Such events underscore the necessity of developing bulletproof transformers.

The issue with both batteries and transformers is that they are physical embodiments of the grid and are therefore subject to physical attack. For cyberattack protection, one company, the Edison Electric Institute, has been working on a program called the Cyber Risk Information Sharing Program (CRISP).[84] CRISP's purpose is to help share real-time data, but

77. Diane Cardwell, *Grid Sensors Could Ease Disruptions of Power*, N.Y. TIMES, Feb. 3, 2015, http://www.nytimes.com/2015/02/04/business/energy-environment/smart-sensors-for-power-grid-could-ease-disruptions.html.

78. TERRORISM & THE ELECTRIC POWER DELIVERY SYSTEM, *supra* note 7, at 48.

79. KOPPEL, *supra* note 50, at 28.

80. *Id.*

81. SIEMENS, TRANSFORMING FUTURE TRENDS INTO INNOVATIONS: SIEMENS BULLETPROOF TRANSFORMERS & REACTORS (2014), https://perma.cc/2N9P-HU8J.

82. *Id.*

83. Petter Fiskerud, *Grid Resilience: Come Hell or High Water*, ELECTROINDUSTRY, Sept. 2016, at 11, https://perma.cc/6MM9-67TE.

84. KOPPEL, *supra* note 50, at 48.

the data focuses on amounts of traffic and identifying IP addresses or malware.[85] The project is still in its infancy.[86]

Some actors in the electricity industry have been participating in drills to prepare for security breaches and test grid security. GridEx, or Grid Exercises, are emergency drills organized by utilities and government agencies in Canada, the U.S., and Mexico to simulate physical attacks and cyberattacks that could take down large sections of the grid.[87] Of course, as detrimental to the civilian population as an attack might be, the electric power industry has a greater interest in protecting itself; security efforts are complicated by the necessity of profiting and staying in business.[88] While some government actors say the industry has a conflict of interest, some actors in the energy and electricity industry say that the government does not know enough about the science behind the grid.[89] Either way, GridEx is a commendable team effort that should be continued.

The biggest issue with the current infrastructure is that there are a limited number of alternative paths that an electric current can take. Destruction of one cable could knock out power to a remote town. It would be simple for terrorists to short circuit cables, forcing a shutdown of supply to a main or local substation. Even if electricity was quickly rerouted, any immediate attacks on transformers further down the lines could cause new failures even when power is returned.[90] Very little risk exists for the attacker of electric power transmission and distribution systems, especially if there is only a cyberattack.[91]

The updates the Smart Grid is intended to provide are necessary because of the increased age of the infrastructure, which creates safety risks and economic inefficiencies. Although computerization will always leave every computer and program at risk, instant identification of issues through Distribution Intelligence and smart meters as well as instant restriction of a blackout from spreading through microgrids are the best ways a cascading blackout can be prevented. Insofar as the Smart Grid blocks alternative paths for a blackout to spread and creates alternative paths for electric current, it can increase grid security. As the National Research Council suggests in a 2012 report:

> Even if all reasonable steps are taken to ensure the reliability of the electric power transmission and distribution system, and to speed its rapid restoration after outages, there is no way that it can be made

85. *Id.*
86. *Id.*
87. Wald*, supra* note 66.
88. KOPPEL, *supra* note 50, at 45.
89. *Id.*
90. MICHAEL O'CONNOR, TERRORISM … THE SOLUTIONS 62 (1987).
91. TERRORISM & THE ELECTRIC POWER DELIVERY SYSTEM, *supra* note 7, at 32.

> completely reliable in the face of major disruption by natural causes or large, well-planned terrorist attacks. For this reason, and because modern society is increasingly dependent on electric power for the provision of critical social services, steps should be taken to ensure that the most important of these services can continue to be sustained if power from the grid is not available.[92]

Preparation is an imperative response to the risk of an attack perceived by the industry.

III. TERRORISM IN NATIONAL AND INTERNATIONAL LAW

A survey of both international and national law reveals that legal systems are unprepared to handle many types of terrorist threats, especially those on electricity infrastructure. Although discussion of terrorism permeates the news and the American psyche, laws on terrorism do not seem to be promulgated until after something goes wrong. If an attack took place and there were no legal remedy for victims, terrorists would accomplish all of their goals: spreading fear and provoking reactive policies through psychological warfare.[93] The international community must continue to consider and discuss different legal approaches to the threat of terrorism and the best methods by which to prevent and punish it. This consideration and discussion should focus on three issues: (1) the nature of terrorism, (2) typical terrorist tactics, and (3) the reasons why people engage in terrorism to accomplish their goals.

Terrorism is the systematic application of terror.[94] More specifically, it is the "use or repeated threat of violence, in support of or in opposition to some authority, where violence is employed to induce fear or similar attack in as many non-immediate victims as possible so that those so threatened will accept and comply with the demands of terrorists."[95] Attacks usually provoke increased security measures, which lead to a reduction in civil liberties, and "thus the people will be turned against their leaders."[96] Reactionary decision-making limiting citizens' rights, especially in the form of law, is evidence of terrorists justifying their resort to the use of fear-inducing tactics.

Although methods may vary, typical terrorist tactics have several common features, including: (1) the use of violence to persuade; (2)

---

92. *Id.* at 89-90.
93. JESSICA STERN & J.M. BERGER, ISIS: THE STATE OF TERROR 199 (2015).
94. O'CONNOR, *supra* note 90, at 1.
95. *Id.* at 2.
96. *Id.* at 10-11.

selection of targets and victims for maximum propaganda value; (3) the use of unprovoked attacks; (4) maximum publicity at minimum risk; (5) use of surprise to circumvent countermeasures; (6) threats, harassment, and violence; (7) disregarding women and children as victims; (8) propaganda to maximize the effect; or (9) loyalty only to themselves and kindred groups.[97] Most terrorists aim for publicity over sympathy; an act as simple as kidnapping and issuing a statement can bring worldwide attention to a cause.[98] Indiscriminate, or preferably—for the terrorists—unpredictable, attacks will ensure a worldwide reaction.

People engage in terrorism for many reasons, for terrorism is a product of individual convictions as well as culture. Defining terrorism and providing legal consequences for it is important, but what some call terrorism could also be the product of another's singular and exclusive understanding of the world.[99] The most important lesson from recognizing the individualism of terrorism is that no single discipline or approach will ever eliminate violence.[100] Recognizing how someone chooses to embrace terrorist tendencies is as important to crime prevention as building infrastructure.

Electricity infrastructure is an advantageous target for terrorists because of the violent effects (some people may die immediately, others may die in the following weeks or months due to weather or starvation), the propaganda value, and the lack of risk to perpetrators in physical attacks and especially cyberattacks.[101] There should be laws criminalizing these types of terrorist attacks, but none exist.

A. Indecisiveness in International Law

One reason for the absence of laws criminalizing these attacks is that international legal scholars and bodies have been unable to agree on a general legal definition for terrorism. In 1937, the League of Nations adopted a treaty requiring nation-states to criminalize acts of terrorism under their own laws, which was the first modern attempt to codify the crime of terrorism in international law.[102]

---

97. FRANK BOLZ JR. ET AL., THE COUNTER-TERRORISM HANDBOOK: TACTICS, PROCEDURES, AND TECHNIQUES 4-6 (2011).

98. *Id.* at 8.

99. MICHAEL P. ARENA & BRUCE A. ARRIGO, THE TERRORIST IDENTITY: EXPLAINING THE TERRORIST THREAT 20-21 (2006).

100. *Id.*

101. TERRORISM & THE ELECTRIC POWER DELIVERY SYSTEM, *supra* note 7, at 15.

102. BETH VAN SCHAACK & RONALD C. SLYE, INTERNATIONAL CRIMINAL LAW & ITS ENFORCEMENT 662 (Robert C. Clark et al. eds., 2015).

International Conventions for the Suppression of Financing of Terrorism were held in 1998 and 1999. They did not define terrorism explicitly, but they asked states to criminalize any activity that violated certain treaties, caused death or serious bodily injury, or attempted or conspired to commit an act of terrorism.[103]

The United Nations General Assembly, in Resolution 51–201 of 1999, said, "Criminal Acts intended or calculated to provoke a state of terror . . . are in any circumstance unjustifiable," which is a very broad condemnation.[104] States struggle to agree on a definition for several reasons: (1) they reject definitions that are redundant—that is, overlap with war crimes or crimes against humanity; (2) some of them reject definitions that arguably include their own particular behavior; and (3) some reject definitions that do not include what they consider to be terrorist acts by their enemies.

The International Convention for Suppression of Terrorist Bombings of 1998 provides an actual definition of terrorism:

> Any person commits an offence within the meaning of this convention if that person unlawfully and intentionally delivers, places, discharges, or detonates an explosive or other lethal device in, into or against a place of public use, a state or government facility, a public transportation system or *an infrastructure facility: (I) with the intent to cause death or serious bodily injury, (II) with the intent to cause extensive destruction of such a place, facility or system, where such destruction results in or is likely to result in major economic loss.*[105]

A definition that mentions infrastructure, such as this one, directly protects part of the electricity infrastructure as well as other types of energy. This definition, however, exclusively focuses on bombing for the method of attack. A terrorist might attack electrical infrastructure in other ways. One can also find definitions for terrorism in the Convention of the Islamic Conference on Combating International Terrorism (1999), which does not mention infrastructure, and the Organization of African Unity Convention on the Prevention and Combating of Terrorism, which mentions only disrupting public services.[106]

The closest the international community has come to a consensus was in the United Nations' Draft Comprehensive Convention Against

---

103. International Convention for the Suppression of the Financing of Terrorism art. II, Dec. 9, 1999, 2178 U.N.T.S. 197.

104. SCHAACK & SLYE, *supra* note 102, at 664.

105. *Id.* (emphasis added).

106. *Id.* at 665.

International Terrorism. This convention includes infrastructure in its definition of terrorism, last updated in 2002:

> Any person commits an offense within the meaning of the present Convention if that person, by any means, unlawfully and intentionally, causes: (a) Death or serious bodily injury, (b) Serious damage to public or private property, including a place of public use, a state or government facility, a public transportation system, *an infrastructure facility* or to the environment; or (c) damage to such property, places, facilities or systems resulting in or likely to result in major economic loss; When the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.[107]

States have heavily debated this definition without ever coming to a solution. The main issue is to whom this definition would apply and when it would apply, especially in cases of armed conflict. To this day, no international consensus exists about what constitutes the optimal legal definition of terrorism.

Other components of the international system that could provide protection for attacks on electricity infrastructure without a consensus on the definition of terrorism include international organizations, international humanitarian law, and international criminal law.

One international organization with this power is the United Nations. The United Nations Security Council has proposed several resolutions on terrorism, but they are extremely limited in scope—for example, one is limited to plane hijackings. The first to address terrorism in general was Resolution 1269 (1999);[108] Resolution 1269 also urged states to implement the terrorism conventions.[109] Second, Resolution 1373, which was adopted in September 2001,[110] required states to enact criminal laws prohibiting terrorism, especially the financing of terrorism.[111] Third, Resolution 2178 (2014), which links violent extremism and terrorism, required member states collectively to prevent radicalization and honor their agreements

---

107. *Id.* at 666.

108. *Security Council 'Unequivocally' Condemns ISIL Terrorist Attacks, Unanimously Adopting Text that Determines Extremist Group Poses 'Unprecedented' Threat*, U.N. (Oct. 19, 1999), https://perma.cc/CX2U-HEK4.

109. *Id.*

110. *Security Council Unanimously Adopts Wide-Ranging Anti-Terrorism Resolution; Calls for Suppressing Financing, Improving International Cooperation*, U.N. (Sept. 28, 2001), https://perma.cc/9SE7-PQQC.

111. *Id.*

under international human rights law.[112] Fourth, Resolution 2199 obligated states to block the flow of profits from trade in oil, antiquities, and hostages to Iraq and Syria.[113] Lastly, Resolution 2253 (2015) reaffirms the powers of the Security Council Committee Pursuant to [Resolutions] Concerning ISIL (Da'esh), Al-Qaida, and Associated Individuals, Groups, Undertakings, and Entities and reestablishes a freeze on assets, an arms embargo, and a travel ban.[114] None of these resolutions directly mentions electricity infrastructure. Trade of oil and assets is a higher priority, possibly because electricity infrastructure is seen as an internal consideration for states. Even the Secretary General's Plan of Action Preventing Violent Extremism fails to mention infrastructure. The Plan lists the possible reasons for extremist activities on state and individual levels and establishes expectations for nations.[115] Its only energy concern, however, is oil trade among terrorist groups.[116]

Second, international humanitarian law can and should condemn terrorist attacks on electricity infrastructure. The Geneva Conventions and the Additional Protocols are codifications of international humanitarian law, or the law of armed conflict; the four separate Geneva Conventions were adopted in August 1949, Protocol I and II in 1977, and the third Protocol in 2005.[117] Whether the conventions apply to a given attack depends on several factors: whether the terrorist is a state or non-state actor, the extent of damage to property, and the effect on citizens. The Geneva Conventions make several references to infrastructure, but none clearly provide for a terrorist attack on it.

Each of the conventions has two important shared elements. First, common to the four Geneva Conventions, is Article III, which provides minimum standards of conduct for states in situations of non-international armed conflicts.[118] This article requires humane treatment of people taking no active part in hostilities and prohibits murder, cruel treatment, taking

112. U.N. Secretary General, *Plan of Action to Prevent Violent Extremism*, ¶ 5, U.N. Doc. A/70/674 (Dec. 24, 2015).

113. *Unanimously Adopting Resolution 2199 (2015), Security Council Condemns Trade with Al-Qaida Associated Groups, Threatens Further Targeted Sanctions*, U.N. (Feb. 12, 2015), https://perma.cc/QA5N-FXKW.

114. *United Nations Security Council Subsidiary Organs*, U.N., https://perma.cc/AQ67-NF2X (last visited Nov. 6, 2017).

115. *Plan of Action to Prevent Violent Extremism*, *supra* note 112, at ¶ 8.

116. *Id.* ¶¶ 14, 44.

117. *The Geneva Conventions of 1949 and Their Additional Protocols*, INT'L COMM. OF THE RED CROSS (Jan. 1, 2014), https://perma.cc/W4D9-2AQD.

118. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 3, Aug. 12, 1949, 6 U.S.C. 3224, 75 U.N.T.S. 31.

hostages, and more.[119] These requirements and prohibitions are important because many armed conflicts today are not international. Non-international armed conflict is a conflict not between two or more high contracting parties to the convention, including conflicts internal to states.[120] Usually, terrorists are not state actors, so Article III could apply. Second, these four Geneva Conventions also define "grave breaches" of humanitarian law, which are the most egregious violations.[121] The Fourth Geneva Convention—which is most relevant to the discussion of infrastructure because it focuses on civilians—lists "taking of hostages and extensive destruction or appropriation of property" as a grave breach.[122] A terrorist attack that destroyed electricity infrastructure could possibly qualify as a grave breach. This provision is the only one of the four conventions that could possibly apply.

Protocol I expands the list of grave breaches. The most relevant addition for the purposes of electricity security is Article 85(3)(c): "launching an attack against works or installations containing dangerous forces in the knowledge that such attack will cause excessive loss of life, injury to civilians or damage to civilian objects."[123] This definition seems to include many types of infrastructure. Depending on the circumstances, a physical attack on some power plants might very well qualify. Similarly, Article 56 prohibits attacks on "[w]orks or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations . . . if such an attack may cause the release of dangerous forces and consequent severe losses among the civilian population," with an exception for nuclear electricity generation stations that provide significant support for military operations.[124] This provision would protect the generation components of the electric grid, but because it requires the works or installations to contain dangerous forces and for the attack to have the potential to release dangerous forces, the provision is very limited in scope.

---

119. *Id.*

120. *See* David Weissbrodt & Amy Bergquist, *Extraordinary Rendition and the Humanitarian Law of War and Occupation*, 47 VA. J. INT'L L. 295, 303 (2007).

121. Geneva Convention Relative to the Protection of Civilian Persons in Time of War art. 147, Aug, 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

122. *Id.*

123. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 85, June 8, 1977, 1125 U.N.T.S. 3.

124. *Id.* art. 56.

Protocol II expands on Common Article III by adding to the list of prohibited acts in non-international conflicts.[125] For the purposes of electricity infrastructure, there are three important additions. First, Article 13(2) provides that "the civilian population as such, as well as individual civilians, shall not be the object of attack. *Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited*."[126] This is a direct prohibition of terrorism. Second, Article 14 prohibits "starvation of citizens as a method of combat" which is a possible outcome of an attack on electricity infrastructure depending on the areas affected and the amount of time a blackout lasts.[127] Too many factors influence the application of that provision. Third, Article 14 prohibits destruction of "objects indispensable to the survival of the civilian population."[128] The provision lists "foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works" as examples of objects indispensable to survival.[129] Electricity is not listed. The necessity of water infrastructure is comparable to the necessity of electricity infrastructure, suggesting that an analogy should be made to extend the protection.

Given these provisions, the Geneva Conventions and Additional Protocols can be interpreted to include a terrorist attack on energy infrastructure. Still, this interpretation requires some skillful argumentation.

Third, international criminal law could provide protection for attacks on electricity infrastructure without a consensus on the definition of terrorism. The Rome Statute of the International Criminal Court creates individual criminal liability rather than state liability.[130] It came into effect in 2002 and has jurisdiction over the crime of genocide, crimes against humanity, war crimes, and the crime of aggression.[131] Under the Rome Statute, a terrorist attack on electricity infrastructure would be most likely to qualify as either a crime against humanity or a war crime. A crime against humanity is an act "committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack" that falls within the provided list or is similarly inhumane, causing great suffering, or serious injury to body or to mental or physical

125. *Id.* art. 1.
126. *Id.* art. 13 (emphasis added).
127. *Id.* art. 1.
128. *Id.* art. 14.
129. *Id.*
130. Rome Statute of the International Criminal Court art. 1, July 17, 1998, 2187 U.N.T.S. 90.
131. *Id.* art. 5.

health.[132] An attack on electricity infrastructure would probably not fall into the enumerated list of crimes against humanity in the Rome Statute but possibly could fall into the "other inhumane acts" category. Such an attack, if carefully planned, could cause great suffering, but it must rise to the standard of attacking human dignity with great humiliation or degradation to fall into this category.

An attack might qualify as a war crime under Article 8 of the Rome Statute. All grave breaches under the 1949 Geneva Conventions qualify as war crimes, namely, "extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly."[133] Infrastructure that qualifies as private property—which is the majority of electricity infrastructure in the United States—should fall under this definition. Other war crime provisions that might include attacks on infrastructure include: "intentionally directing attacks against civilian objects," "destroying or seizing the enemy's property," and "intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects."[134] These enumerations seem to address the terrorist attack method in question.[135] There is no precedent to say a cyberattack on infrastructure would qualify as an attack on a civilian object, but the provisions might cover some physical attacks.

Finally, "intentionally using starvation of civilians as a method of warfare by depriving them of objects indispensable [sic] to survival" is a war crime, as previously discussed regarding Protocol II.[136] For many Americans, deprivation of electricity could certainly lead to starvation—but this argument is weak.

The first issue with using war crimes to charge alleged terrorists under international law is that they are not state actors, and technically could not declare war. Article 8(e), however, extends many of these provisions to armed conflicts not of an international character, similar to Common Article 3 of the Geneva Conventions.[137]

---

132. *Id.* art. 7.
133. *Id.* art. 8.
134. *Id.*
135. *Id.*
136. *Id.*
137. As an example: The international community does not recognize ISIL (Da'esh) as a state. If any members were charged in the ICC for their actions, they might argue that they did not commit war crimes because they were refused statehood status. However, if an actor is operating as if it is a state, maybe the ICC should hold it accountable as states would be. Hopefully, Protocol II and Art. 8(e) of the Rome Statute can be construed to hold these people accountable for their actions.

The second issue is that the Rome Statute does not directly address terrorism; terrorism is not its own offense. While acts of terrorism might occur during a war, not all of them do.[138] In cases where classifying terrorism as a crime against humanity rather than a war crime would be preferable, the "other" category does not satisfy the need to address the condemnable acts. International criminal law would ideally be a remedy for prosecution of terrorists, but International Criminal Court (ICC) prosecutors might struggle to squeeze an attack on electricity infrastructure into the ICC's narrow definitions of crimes.

Terrorists, as non-state actors, may not hold themselves to the standards or principles of international organizations, international humanitarian law, or international criminal law, so no limit exists to the atrocities they could commit against citizens. International politics in the post-Cold War period are characterized by an unprecedented fluidity, where it's unclear who can do what to whom and with what means they can do it.[139] The Westphalian system—a political scheme that recognized the nation-state as the exclusive sovereign actor—has transformed, so that it is almost impossible not to recognize the plurality of actors.[140] Unrestrained by borders in the way that states are, terrorist actors can recruit and perpetrate crimes around the world. The concept of conventional warfare is not as relevant in the twenty-first century due to the diffusion of modern technology.[141] Terrorists have influence in international politics because they use violence to create, rather than express, identity.[142] The law must explicitly condemn those possible atrocities.

B. Failures in Federal Criminal Law and Energy Policy

If either a physical or cyberattack on electricity infrastructure occurred, federal criminal law would not provide an explicit remedy in

138. Aviv Cohen, *Prosecuting Terrorists at the International Criminal Court: Reevaluating an Unused Legal Tool to Combat Terrorism,* 20 MICH. ST. INT'L L. REV. 219, 249 (2012).

139. PETER CHALK, NON-MILITARY SECURITY & GLOBAL ORDER: THE IMPACT OF EXTREMISM, VIOLENCE,& CHAOS ON NATIONAL AND INTERNATIONAL SECURITY 1 (2000).

140. The Westphalian theory of international relations suggests that since the Peace of Westphalia in 1648, a Eurocentric bias has dominated politics and the formation of states. *See generally* Turan Kayaglu, *Westphalian Eurocentrism in International Relations Theory*, 12 INT'L STUDIES REV. 193 (2010).

141. This is even true for the United States: Congress has not officially declared war since World War II. *Official Declarations of War by Congress*, U.S. SENATE, https://perma.cc/ZZ5Y-A2QS (last visited Jan. 21, 2017).

142. ARENA & ARRIGO, *supra* note 99.

most situations. Four statutes in the section on terrorism might implicate an attack on infrastructure. First, 18 U.S.C. § 2332b criminalizes terrorist attacks from foreign sources.[143] This statute never directly references electricity infrastructure, but it does criminalize the destruction of property. Any terrorist attack on infrastructure from a domestic source could not be prosecuted under this statute.

Second, 18 U.S.C. § 2332f criminalizes bombings of infrastructure facilities if the actor intends to cause death or serious bodily injury or "inten[ds] to cause extensive destruction of such a place, facility, or system, where such destruction results in or is likely to result in major economic loss."[144] This statute only applies to bombings, however, and does not extend to any other kind of physical attack, including cyberattacks.

Third, 18 U.S.C. § 2339B establishes the crime of providing material support or resources to a designated foreign terrorist organization.[145] "Material support or resources" means providing to a terrorist "any property . . . financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel . . . and transportation."[146] Material support prosecutions do not require an act of terrorism, as the statute criminalizes both attempt and conspiracy, so they have been essential to post-9/11 strategies of preventive prosecutions.[147] If a terrorist is not working with a designated foreign terrorist organization, the provisions will not apply.

Fourth, alternatively or in conjunction with criminal liability, 18 U.S.C. § 2333(a) creates a civil action for persons, property, and businesses subject to an act of international terrorism.[148] Whether "international terrorism" in this statute would include a situation where an American citizen plans an attack in the United States for a foreign terrorist organization is unclear, although that situation would qualify as material support. It would not apply to an American national without ties to foreign terrorist groups.

The problem with these four statutes is that they are under-inclusive. They exclude terrorists from the United States or terrorists that do not support a specific organization. None of them contemplate a terrorist attack that does not cause physical damage. A terrorist attack that causes physical damage without a bomb would not fall under these statutes. Even worse, none of them consider a cyberattack. Congress fails to acknowledge a basic concept of

143. 18 U.S.C. § 2332b (2015).
144. 18 U.S.C. § 2332f(a)(1)(B) (2002).
145. 18 U.S.C. § 2339B (2015).
146. 18 U.S.C. § 2339A(b)(1) (2009).
147. RICHARD B. ZABEL & JAMES J. BENJAMIN, JR., IN PURSUIT OF JUSTICE: PROSECUTING TERRORISM CASES IN THE FEDERAL COURTS 6 (2008).
148. 18 U.S.C. § 2333(a) (2016).

terrorism: anyone might desire to cause fear and influence the government. With an infrastructure so widespread, intricate, and integral as the electric grid, anyone with the right skills and intent to cause fear can succeed in an attack. Terrorism is not limited to the organizations that the United States has chosen to label. Clearly, American policy is to condemn terrorism, but no statute is written in a way that provides sufficient actus reus for attacking electricity infrastructure in the likely ways that a terrorist might.

It would be Congress's responsibility to pass a statute regarding attacks; Congress also plays an essential role in the recognition of issues with the grid—whether efficiency or safety—and providing funding. In 2008, a congressional commission first investigated the likelihood of an EMP attack.[149] The commission found that several states, including Russia, North Korea, China, and Iran, were capable of perpetrating such an attack; some terrorist organizations also had this ability.[150] More recently, the Senate committee of Homeland Security and Governmental Affairs considered CIPA, or the Critical Infrastructure Protection Act of 2015.[151] Its purpose is to amend the Homeland Security Act of 2002 to require the Department of Homeland Security to assess the threat posed by EMPs and geomagnetic disturbances (GMD) to infrastructure.[152] Geomagnetic disturbances, like EMPs, which occur naturally or with nuclear devices, could cause immediate damage to the grid—at a minimum, some experts predict, twenty to forty million people could lose power for two years.[153] The Electromagnetic Pulse Commission stated that the Department of Homeland Security has addressed threats to the electric grid at large, but it is problematic that it has no statutory obligation to address the commission's recommendations.[154] CIPA would require the Department of Homeland Security to prepare a strategy to protect infrastructure against EMP and GMD specifically. CIPA was introduced in 2013 and has not moved out of committee.[155] A second piece of legislation, the Secure High-Voltage Infrastructure for Electricity from Lethal Damage Act, or SHIELD, was introduced the same year.[156] Neither piece of legislation has moved past their committees. It is doubtful that members of Congress have suddenly found that an EMP attack is unlikely. Addressing the concerns could cost a couple billion dollars, so the failure to pass legislation is most

149. ZABEL & BENJAMIN, JR., *supra* note 147.
150. *Id.* at 22.
151. S. REP. NO. 114-250 (2015).
152. *Id.*
153. *Id.*
154. *Id.*
155. *Id.*
156. KOPPEL, *supra* note 50, at 24.

likely related to funding or political gridlock.[157] If Congress is genuinely concerned about terrorism, it should consider a response to terrorism post-attack as well, which includes funding a preventive increase in the resiliency of the grid.

As representatives of the American population, Congressmen fall into the hysteria-induced trap of terrorism's systematic application of panic by focusing on the most dramatic types of attacks rather than the ones that are likely to happen and failing to address simpler vulnerabilities.

It would be detrimental to everyone if a terrorist used nuclear, biological, or chemical weapons to harm Americans. Nuclear terrorism, bioterrorism, and chemical warfare, however, all have their own criminal provisions while the vulnerable electric grid is unprotected.[158] Congress's concern over an EMP attack is good news, but it overlooks the more simple ways a terrorist attack could work.

Congress's usual reaction to a terrorist attack is to fund the rebuilding of stronger, more solid systems that could withstand the stressor that failed the previous one, but resiliency is about more than taking preventive action. Resiliency is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions."[159] Developing the ability to recover rapidly is as important as having strong preventive protections. Our electricity infrastructure will improve with Smart Grid updates, but it will still be vulnerable to attack. Criminal statutes are an essential part of a response plan to a terrorist attack. Grid resiliency is an unattainable goal as long as there is no punishment for attacking it.

IV. A COMPREHENSIVE LEGAL FRAMEWORK TO SIMPLIFY PROSECUTION AND PROTECT CITIZENS

The severity of a potential terrorist attack on the currently vulnerable electric grid justifies revamping the electric grid. As helpful as the Smart Grid sounds, it will be years before it is completely implemented throughout the country. Legal systems should be prepared for an attack in the meantime. The unsatisfactory legal framework to address criminal activity leaves victims naked and afraid—allowing terrorists to be successful in their goals of inflicting violence and fear.

---

157. *Id.*

158. 18 U.S.C. § 175 (2002); 18 U.S.C. § 229 (1998); 18 U.S.C. § 2332a(c)(2) (2004); 18 U.S.C. § 2332i (2015).

159. *What is Security and Resilience?,* U.S. DEP'T OF HOMELAND SEC., https://perma.cc/99BE-HKLZ (last updated Dec. 8, 2017).

A. Options for a Unified International Approach

There are two solutions to the issue of impunity for alleged terrorists under international law. First, the international legal regime has thus far failed to create a comprehensive legal framework regarding terrorism. Revisiting the Draft Comprehensive Convention Against International Terrorism would be beneficial for any state hoping to establish legal justifications for potential terrorist attacks against it. This convention should grant criminal jurisdiction to the ICC, and—in case a state conducts a cyberattack—jurisdiction to the International Court of Justice. While many acts of terrorism rise to the level of crime against humanity under the Rome Statute, the physical, cyber, and electromagnetic methods of attack on electricity infrastructure do not fall directly under the language. Considering that the purpose of establishing crimes against humanity is to capture the most egregious of offenses against human beings, it is inappropriate to include these attacks unless a long-term blackout does occur. Relief should be created elsewhere in the law.

Second, a provision extending the Rome Statute to acts of terror with a new clause adding a *mens rea* to incite terror would clarify the applicability of those provisions. Article 8 of the Rome Statute, regarding war crimes, does not provide consolation either; whether people can be punished for acts of terrorism should not depend on statehood status. War crimes are either grave breaches of the Geneva Conventions or violations of other laws applicable in international armed conflict.[160] If a terrorist is not a member of a government or commits an act that does not fall into the Conventions' common Article III non-international conflicts extension, then he cannot be prosecuted in the ICC.

Leaders of terrorist organizations should be liable for their organized acts of violence and lone wolf terrorists should still be culpable for their unilateral acts. Currently under the Rome Statute, the ICC does not have jurisdiction over terrorism as its own offense, and it is unlikely member states would approve of the change.[161] Terrorist attacks can be severe enough to match or include some of the other crimes the court has jurisdiction over.

Adding a section to the crimes against humanity or war crimes sections providing that any of the listed actions with the "intent to incite fear or terror" is under the ICC's jurisdiction would be the smallest extension of authority possible to include terrorism in the Rome Statute. Terrorism, by definition, is using violence to incite fear, and the acts of violence are already listed. Adding this requisite intent specifically implicates terrorism and clarifies the

160. Rome Statute of the International Criminal Court, *supra* note 130, art. 8.

161. Beth van Schaack, *Finding the Tort of Terrorism in International Law*, 28 REV. LITIG. 381, 422-23 (2008).

jurisdiction of prosecutors. This is a narrow extension of jurisdiction compared to adding an entire category of crimes to the Rome Statute.

Out of the two solutions, ratification of the Draft Convention on Terrorism or a similar instrument would be the preferable solution because of the unified approach, but criminal liability under the Rome Statute would also solve the issue of the absence of specific laws to address a terrorist attack on electricity infrastructure. Either way, international law on the issue of terrorism is essential because it provides a safety net for nations without terrorism laws, jurisdiction restraints, or other reasons for inability to individually prosecute. Impunity is unacceptable. The pooled power of nation-states in condemnation of terrorism would have more influence in ending the phenomenon than the classic and problematic West-East dichotomy.[162]

B. Proposal for a Specific and Targeted Domestic Statute

The United States justice system is vast, but it may need the international law safety net because the criminal laws are insufficient to prosecute terrorists to the extent that its policy condemns them. Prosecution of terrorists is essential to incapacitate them, gather intelligence, and deter future acts of terrorism.[163]

A recent study[164] on prosecuting terrorism cases in federal courts came to several conclusions. First, the criminal justice system is insufficient to address international terrorism alone, and the government must draw on its military, intelligence, diplomacy, economic, and law enforcement systems as well.[165] Second, terrorism cases are extremely complex and produce strain on the criminal justice system.[166] Third, the criminal justice system is prone to many types of errors but is workable and credible in general.[167] A statute covering an attack on electricity infrastructure must simplify the complexities and challenges for the criminal justice system.

There are three main reasons passing a specific federal statute is the best solution for protecting the electricity infrastructure. First, as of today, if a physical or cyberattack were to take place, a prosecutor would most likely pick the most relevant statutes on terrorism and the individual acts of harming private property and list them all in a complaint to get the terrorist into court. The statutes might not all be optimally targeted to address particular acts. Procedurally, this does not hurt the prosecutor because a more accurate

---

162. *See* EDWARD W. SAID, ORIENTALISM (1979).
163. STRATEGIC PLAN, *supra* note 5, at 16.
164. SCHAACK & SLYE, *supra* note 102, at 669.
165. *Id.*
166. *Id.*
167. *Id.*

superseding indictment can always be filed later. This approach, however, is an inefficient waste of government time and money.

Second, a specific statute would streamline prosecutions. Nuclear terrorism, bioterrorism, and chemical warfare all have their own criminal provisions;[168] therefore, a separate statute criminalizing an attack on an enumerated list of Smart Grid components would have precedent. An attack on electricity infrastructure could be as damaging to businesses and lives as any other type of terrorism. A more specific provision would make prosecution simpler and clarify the actions that would violate the law.

Third, a specifically tailored statute is necessary to avoid excessive rights infringements. Legislators should keep in mind that terrorists intend, through their attacks, to motivate increased security measures, which restricts freedom at home. The vicious cycle of violence followed by increased security measures limits U.S. citizens without preventing terrorism. A statute punishing a specific type of crime, rather than sweeping restrictions or regulations, is narrow and will not negatively affect citizens that choose not to engage in terrorist attacks.

An ideal statute criminalizing a terrorist attack on electricity infrastructure would include several elements. First, it must be aimed at several types of terrorists, whether lone actors or groups.

Second, it would also criminalize attempt and conspiracy. Inchoate liability could deter many attacks.

Third, it would have separate and detailed sections on physical attacks and cyberattacks. The physical attacks section would criminalize property damage as other statutes do, but broaden the methods by which it is possible. For example, shooting a transformer with guns, bombing a power plant, or dropping weapons on a power station via drone should all fall under the language of the statute. The cyberattacks section would contemplate an attack from someone inside a utility company and from a basement on the other side of the world. It would protect the SCADA systems and each component of the new Smart Grid system so that the statute does not become outdated as the grid updates. In both the physical and cyberattacks sections, each component of the grid should be covered. The statute should be written to protect both the current electrical grid and the anticipated technologies of the Smart Grid.

Fourth, the statute would include a *mens rea* element of purpose or knowledge. The language should include the intent to incite fear or perpetrate violence on the grid, the industry supporting it, and the citizens using it.

Fifth, the statute would have a section on jurisdiction similar to 18 U.S.C. § 2339B(d), the material support statute, which establishes that the United States has jurisdiction whether the offender is a U.S. national or not.

---

168. 18 U.S.C. § 175 (2002); 18 U.S.C. § 229 (1998); 18 U.S.C. § 2332a(c)(2) (2004); 18 U.S.C. § 2332i (2015).

A statute satisfying these five conditions would sufficiently protect the electricity grid. The danger of enumerated lists of any crimes or types of crimes is that it could be under-inclusive. To address adequately the risk of a terrorist attack of any type, however, a framework should be laid out ahead of time. If deterrence is truly a value of the criminal justice system, potential defendants deserve knowledge that an act is criminalized before they commit it. Providing a specific legal framework for terrorism improves protection of due process rights. Terrorism is common enough in the twenty-first century to justify a specific and targeted legal response.

With respect to criminal liability, federal government regulations will continue to address the risk of an attack on energy infrastructure inadequately because of the transnational quality of terrorism. Industry and the government must work together to an extent to decide on an optimal level of information sharing for terrorism prevention. It is good business for the electric industry to protect itself.[169] The energy sector may be more successful operating on its own rather than working to meet federal regulations, which is why the government should reciprocate those efforts through laws that directly punish threats to the industry.

CONCLUSION

International and national laws should more expressly address threats to the electricity infrastructure. Experts agree that the severity of a possible attack is a sufficient reason to focus on improving the electricity infrastructure. The Smart Grid is a crucial step towards improving security and a necessary twenty-first century update to infrastructure, but care should be taken in increased interconnectivity between grids. In the immediate future, before the Smart Grid is completed, legal steps are necessary to deter and protect the industry from attack. The electric industry must take steps towards updating the Smart Grid as quickly as economically feasible, and the government must quickly create a response plan that includes criminal liability for alleged terrorists. Preparation for such an attack should build confidence that if anything happens, the United States will be ready.

Melissa R. Wheeler

---

169. Alvey*, supra* note 56, at 23.

J.D./D.C.L., 2018, Paul M. Hebert Law Center, Louisiana State University. The author extends her gratitude to Professor Ken Levy for his encouragement and assistance during the writing process. Additionally, she thanks her parents for two decades of supporting her aspiration to be a published author.