Nebraska Law Review

Volume 96 | Issue 2 Article 10

2017

Networking Emergency Response: Empowering FEMA in the Age of Convergence and Cyber Critical Infrastructure

Christopher M. Bailey
United States Air Force

Comment*

Networking Emergency Response: Empowering FEMA in the Age of Convergence and Cyber Critical Infrastructure

TABLE OF CONTENTS

* Major Christopher M. Bailey is a Judge Advocate for the United States Air Force. He earned his Juris Doctor Degree from Chicago-Kent College of Law in May 2010 and his Masters of Law in Space, Cyber, and Telecommunications Law from the University of Nebraska College of Law in May 2017. The views expressed in this Comment are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

I. INTRODUCTION

There were no signs anything was wrong. Workers and staff at the Baku–Tbilisi–Ceyhan (BTC) oil pipeline in eastern Turkey regularly reviewed the computer network's readouts on pipeline pressure, and there were no warning or distress signals.[1] The BTC pipeline, majority owned by British Petroleum (BP), was designed to be one of the most secure pipeline systems in the world.[2] The pipeline consisted of a total of 1099 miles and ran from the Caspian Sea to the Mediterranean Sea.[3] To maintain security, the pipeline was outfitted with dozens of sensors and cameras to monitor each section of the pipeline, including a sophisticated backup satellite system to send alerts back to the main control center if the nodes along the pipeline failed.[4] These protocols and safety measures, however, would prove useless in the face of a determined adversary.

On August 8, 2008, unidentified hackers launched a cyber attack by infiltrating the surveillance cameras through the cameras' wireless-connection feature and then using this access to connect to the pipeline's operating systems.[5] Once inside, the hackers manipulated the pressure along the pipeline by breaking into computer controls at several different valve stations along the line.[6] The hackers then tampered with the alarm systems to stop any alerts or warnings, including blocking the redundant satellite-warning-systems signals, so the

1. Jordan Robertson & Michael Riley, *The Map that Shows Why a Pipeline Explosion in Turkey Matters to the U.S.*, BLOOMBERG (Dec. 10, 2014), https://www.bloomberg.com/news/2014-12-10/the-map-that-shows-why-a-pipeline-explosion-in-turkey-matters-to-the-u-s-.html [https://perma.unl.edu/2J67-NSLT].
2. *Id.*
3. Jordan Robertson & Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*, BLOOMBERG TECH. (Dec. 10, 2014), https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.
4. *Id.*
5. *Id.*
6. *Id.*

control center never detected the increase in pressure at any point along the pipeline.[7] The hackers triggered a massive explosion that destroyed significant sections of the pipeline, spilled over thirty thousand barrels of oil into an adjacent aquifer, inflicted five million dollars a day in closure costs on BP, and caused a one-billion-dollar loss for the Republic of Azerbaijan in export revenue.[8] In the aftermath, Turkish authorities claimed a system malfunction caused the blast, and it was not until six years later that it was conclusively proven the incident was a cyber act of terrorism.[9] While much of the coverage of the BTC pipeline event rightfully focused on whether the event was a new cyber war or new front in international terrorism,[10] the less obvious, but just as important, issue is: How should critical infrastructure be designed in order to be protected in an interconnected and wireless world?

The BTC pipeline incident is a clear example of the challenges posed in a cyber-enabled world. This pipeline incident created significant public health risks in the immediate explosion, accompanying oil spill, contamination of an entire aquifer, substantial financial loss for a private company, and potentially disastrous foreign policy implications for Turkey and Azerbaijan.[11] The narrative of dark, shadowy hackers just a click away from Armageddon, while sensational and thrilling, makes it too easy for lawmakers and policy advocates to ignore the most important message that should be gleaned from this example and those like it: modern infrastructure is almost completely reliant on computer systems and networks, fundamentally changing how to prepare for and respond to catastrophes whether precipitated by a terrorist event or a natural disaster.

Cybersecurity is not a topic that should be addressed in a vacuum. Cyber is everything and everywhere in the modern world, but most individuals still think about infrastructure in a pre-computer-networked way.[12] Take for example a large power outage that could be caused by high temperatures, over use of electricity, or a squirrel chewing through transmission lines.[13] Prior to the advent of widespread computer networks and Internet-enabled communications, most businesses would have some sort of limited function without power and could wait until power was restored, but not in today's

7. *Id.*
8. *Id.*
9. *Id.*
10. *Id.*
11. *Id.*
12. *Foreign Policy's The Editor's Roundtable: Behind the Latest WikiLeaks Dump: New News?*, FOREIGN POL'Y MAG. (Mar. 9, 2017) [hereinafter *The Editor's Roundtable Podcast*] (downloaded using iTunes).
13. *See* GRETCHEN BAKKE, THE GRID: THE FRAYING WIRES BETWEEN AMERICANS AND OUR ENERGY FUTURE 190 (2016).

world.[14] The cyber-enabled economy is powered by companies like Google, Apple, and Cisco that are entirely reliant on regular and consistent provision of electricity for powering servers and computer networks for customers.[15] A devastating real-world example was the immediate aftermath of Hurricane Katrina where overreliance on modern communications infrastructure proved disastrous. The near total collapse of landline, satellite, and cell-phone communications made it practically impossible for local law enforcement and the Louisiana National Guard to coordinate response efforts.[16] Cyber policy, regulation, and infrastructure affect private companies; private individuals; and local, state, and federal governments, both individually and collectively.[17] The true question posed by events like the BTC attack and the communication-infrastructure collapse during Hurricane Katrina is how policymakers encourage resiliency and security in cyber critical infrastructure and enable first responders to react timely when that infrastructure is under threat.

The United States has wrestled with how to promote both the development of cyberspace and maintain its security and redundancy for nearly two decades.[18] That tension, however, has largely missed the forest for the trees. By defining cybersecurity as something reserved to the national-security apparatus, key players in emergency management and response have largely seen cyber as outside of their expertise until the past several years.[19] Despite this reliance, the policy and legislative spheres suffer from tunnel vision and therefore largely only focus on terrorism or bad-actor threats to network-enabled infrastructure.[20] What is missed is the additional threat posed by simple human error, natural disaster, and ad hoc integration of these systems.

In order to address the current gaps in cybersecurity legislation, it is important to place the gaps and threats in context. Part II will address the vulnerabilities of our cyber-physical systems and the threats natural disasters and even simple human error pose to these systems. These vulnerabilities are uniquely highlighted in two recent events:

14. *Id.*
15. *Id.*
16. Erin Ryan, *Federalism and the Tug of War Within: Seeking Checks and Balance in the Interjurisdictional Gray Area*, *in* DISASTER LAW AND POLICY 101, 103 (3d ed. 2015).
17. *Id.*
18. *See* Peter Burnett, *The Vital Role of Critical Information Infrastructure Protection (CIIP) in Cybersecurity*, *in* REPORT ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE IN THE AMERICAS 13, 14 (2015), https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf [https://perma.unl.edu/L9VK-45FP].
19. PAUL STOCKTON, JOHNS HOPKINS APPLIED PHYSICS LAB., SUPERSTORM SANDY: IMPLICATIONS FOR DESIGNING A POST-CYBER ATTACK POWER RESTORATION SYSTEM 13 (2016).
20. *The Editor's Roundtable Podcast*, *supra* note 12.

(1) the wide-scale power outage and degraded communications during Superstorm Sandy in 2012[21] and (2) the 2005 Taum Sauk Water Storage Dam failure in eastern Missouri triggered by the transmission of incorrect readings to an off-site monitoring-and-management facility in the Lake of the Ozarks, Missouri.[22] Each of these cases is symptomatic of three different types of cyber incidents that planners and emergency-response professionals must prepare for: (1) degradation of cyber infrastructure due to natural disaster, (2) human error in installation of infrastructure hardware, and (3) poor software design that was not discovered until after the system failure. Part II argues President Obama's Presidential Policy Directives (PPDs) 21 and 41 on United States Cyber Incident Coordination were good first steps toward creating an emergency-response framework but insufficient to push both states and private entities to develop truly resilient, redundant, integrated cyber infrastructure.

Part III addresses these cyber-related challenges by redesigning how the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) operates in an event involving cyber systems.[23] The Stafford Act should be amended to explicitly address the unique nature of cyber-enabled critical infrastructure and give the Federal Emergency Management Agency (FEMA) authority to develop interstate emergency-response agreements explicitly identifying key cyber critical infrastructure.[24] Next, the FEMA Administrator, through her review authority under 42 U.S.C. §§ 5196–96f, should promote the creation of a three-tier incident-classification system for interstate compacts: (1) localized harm or destruction to physical computer hardware, (2) infected or destroyed network nodes that hinder or degrade independent systems from communicating, and (3) software or computer-logic degradation that effectively renders computer systems useless.[25] Finally, to ensure the widest compliance possible, the Administrator should condition provision of any financial contributions to the states on the acceptance of the three-tier system and the adoption of the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. This

21. David Talbot, *As Sandy Bashes the Northeast, Emergency Communications Remain Flawed*, MIT TECH. REV. (Oct. 29, 2012), https://www.technologyreview.com/s/506596/as-sandy-bashes-the-northeast-emergency-communications-remain-flawed [https://perma.unl.edu/APB2-XM48].

22. KEITH STOUFFER, JOE FALCO & KAREN SCAREONE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBL'N NO. 800-82, GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) 3–21 (2011).

23. Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. §§ 5121–5207 (2012).

24. *Id.*

25. *See* 42 U.S.C. § 5196(h)(1) (2012) (charging the FEMA Administrator with creating a "program supporting the development of emergency preparedness compacts for acts of terrorism, disasters, and emergencies").

requirement will incentivize states and private parties to better develop resilient and redundant computer infrastructures within their state as well as promote overall security through the interstate compacts. Further, these interstate compacts can serve as effective ways to assess state-level emergency response during an event and serve as a component of the governor's state-of-emergency declaration as proscribed under the Stafford Act.[26] This amendment should authorize federal financial aid, in line with current cost-sharing arrangements for states and private parties for emergency response, when state governors and the President declare a disaster or emergency.[27] This combination of mandating a common vocabulary in classifying cyber vulnerabilities within and across states in addition to financial incentives for taking common-sense approaches to classifying the threat environment is a simple and effective way to better protect U.S. critical infrastructure from accidents, terrorist threats, and natural disasters. Part IV applies this revamped Stafford Act to a hypothetical hurricane hitting Houston, Texas, to test the effectiveness of expanding FEMA's authority and responsibility for promoting cybersecurity in the face of a natural disaster.

II. PLACING CYBERSECURITY IN THE CRITICAL-INFRASTRUCTURE CONVERSATION

A. What Makes Cybersecurity Critical to Critical Infrastructure?

Societies increasingly rely on computer technology and on network-connected or Internet-based services and products. This is the case for individuals, corporations, and the governmental entities that provide critical infrastructure. Critical infrastructure is defined as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[28] President Barack Obama issued PPD 21 in 2013, which identified sixteen key sectors he determined fell under the definition of critical infrastructure.[29] These sixteen sectors included communications, chemical, wastewater and treatment, energy, dams, emergency

26. 42 U.S.C. § 5191(a) (2012).

27. *See id.*

28. Critical Infrastructure Act of 2001, 42 U.S.C. § 5195c(e) (2012).

29. *Presidential Policy Directive—Critical Infrastructure Security and Resilience*, WHITE HOUSE (Feb. 12, 2013) [hereinafter PPD-21], https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [https://perma.unl.edu/JQ94-8379].

services, information technology, transportation, and nuclear energy.[30]

These sectors and industries have two distinct qualities they do not share with other similarly sized industries: (1) widespread use and reliance on industrial control systems (ICS) or supervisory-control-and-data-acquisition (SCADA) systems and (2) the increasing use of remote sensor management and control of these complex industrial systems.[31] Before the advent of networked computer systems, these ICSs were manually operated and often worked using proprietary computer software unique to that industry or to the particular company operating it.[32] This practice meant relatively few engineers and computer technicians would be familiar with the operating systems, and there was no connection between one ICS and another.[33] Today, however, these systems are becoming more reliant on remote access, which allows a small number of technicians to access off-site systems and sensors spread out across a wide geographic area.[34] To accomplish this, these systems are now being connected to the same Internet communications software and systems that all other public, private, and personal users operate.[35]

This means these once secure systems are now vulnerable to the same malware, viruses, glitches, and poor programming the rest of the Internet is vulnerable to.[36] Further, all entities, including individuals, corporations, and critical infrastructure, are becoming increasingly detached from the systems and data on which they rely.[37] Cybersecurity technologist Bruce Schneier argued this detachment is primarily the result of the rise of cloud computing and that organizations of all sizes are "progressively outsourcing much or even most of their [information technology] infrastructure."[38] This means degradation in one critical-infrastructure sector, communications or information

30. The full list of sectors is: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear facilities and waste, transportation systems, and water and wastewater treatment. *Id.*

31. Burnett, *supra* note 18, at 14.

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341, 348–49 (quoting Bruce Schneier, InfoQ, Keynote Address at QCon (Dec. 12, 2014), http://www.infoq.com/presentations/Schneier-security-keynote-qcon [https://perma.unl.edu/7BWA-GLSP] (describing role of cloud computing)).

38. *Id.*

technology for example, can create a cascading failure across other sectors like energy and wastewater treatment.

This interdependence between systems and industries is a hallmark of the contemporary just-in-time economy.[39] The goal of the just-in-time economy is for companies to reduce inventory and produce goods and services as close to the time of demand as possible.[40] This formula, while efficient, is completely dependent on rapid and reliable communications provided by the Internet and networked systems.[41] Further, this drastic reduction in inventory and reliance on interconnected critical infrastructure eliminated the buffers that would minimize the effects of disaster-related supply-chain disruptions.[42] The interdependence seen today, where physical infrastructure is becoming more reliant on cyber capabilities, is just the tip of the iceberg for next-generation technologies in logistics, city planning, and infrastructure build-outs. Municipalities around the globe are starting to experiment with cyber-physical systems where autonomous machines are communicating with each other and humans are less and less involved.

> One example [of a cyber-physical system] is "smart grid" technology, where networked computers and communications technology would be used to work autonomously to resolve problems in the electric grid, manage consumer electronic usage during peak and off-peak times, and administer energy production. Cyber-physical systems may be incorporated into transportation infrastructure (e.g. automated traffic control), water infrastructure (e.g. "smart" water meters), and to monitor the structural health of all physical infrastructure.[43]

The concept of cyber-physical systems may seem far-fetched, but take a moment to think about next-generation technologies that fill today's news. A smart city would include a range of autonomous vehicles (including passenger cars, semitrucks, trains, ships, and aircraft), microenergy grids utilizing solar and wind power through networked battery storage to power homes and businesses, advanced water and wastewater systems reliant on automated systems to manage use and distribution to reduce waste, and smart homes designed to automate mundane tasks like grocery shopping, laundry, and other domestic work.[44]

---

39. Ryan, *supra* note 16, at 11.
40. *Id.*
41. Nicholas S. Kelley & Michael T. Osterholm, *Pandemic Influenza, Electricity, and the Coal Supply Chain: Addressing Crucial Preparedness Gaps in the United States*, *in* DISASTER LAW & POLICY 11, 11 (3d ed. 2015).
42. *See id.* at 11–12.
43. STRATEGIC FORESIGHT INITIATIVE, CRITICAL INFRASTRUCTURE: LONG-TERM TRENDS AND DRIVERS AND THEIR IMPLICATIONS FOR EMERGENCY MANAGEMENT 3 (2011), https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf [https://perma.unl.edu/FML3-PBYU].
44. *See* OFFICE OF CYBER & INFRASTRUCTURE ANALYSIS, U.S. DEP'T OF HOMELAND SEC., THE FUTURE OF SMART CITIES: CYBER-PHYSICAL INFRASTRUCTURE RISK 3

This shift to automation pervades discussions of our cities and our livelihoods. Although coverage of the 2016 U.S. presidential election centered on the demise of manufacturing employment in the United States and blamed it on free-trade agreements, most experts agree the real culprit is automation.[45] Most think automation only applies to low-skill, manual-labor positions, but the real target of automation is increasingly middle-class jobs. It is the "[r]outine jobs on the factory floor or in payroll or accounting departments [that] tend to fall in between. And it's these middle-class jobs that robots have the easiest time [replacing]."[46] Similarly, when someone thinks of emergency services, they tend to think of 9-1-1, police officers, firefighters, or rescue canines. In the next decade, a person is just as likely to reach an automated 9-1-1 service, be spotted by an autonomous search-and-rescue drone, and be picked up by an autonomous ground-rescue vehicle during an emergency.[47] Thus, the ability of governments at the federal, state, and local levels to respond to issues from the day-to-day workings of their communities to wide-scale natural disasters is becoming increasingly reliant on computer systems and autonomous processes and devices. These systems provide significant benefits to society, but it is important that elected officials and first responders—at all levels—understand the risks associated with these systems.

The intent of this initial discussion is not to further cyber doomsday scenarios. Fear of cyber doomsday is often over exaggerated because writers tend focus on worst-case scenarios.[48] Instead, the goal is

---

(2015), https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf [https://perma.unl.edu/59DV-W7VP]; *see also* Kashmir Hill, *When "Smart Homes" Get Hacked: I Haunted A Complete Stranger's House Via the Internet*, FORBES (July 26, 2013), https://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/#363cbf06e426 [https://perma.unl.edu/9U78-KPL3] (explaining the ability to control other people's devices from afar without their permission).

45. Elizabeth Kolbert, *Our Automated Future: How Long Will It Be Before You Lose Your Job to a Robot?*, NEW YORKER (Dec. 2016), http://www.newyorker.com/magazine/2016/12/19/our-automated-future [https://perma.unl.edu/DZF9-FLEU].

46. *Id.*

47. Alex Brokaw, *Autonomous Search-and-Rescue Drones Outperform Humans at Navigating Forest Trails*, VERGE (Feb. 11, 2016), http://www.theverge.com/2016/2/11/10965414/autonomous-drones-deep-learning-navigation-mapping [https://perma.unl.edu/5NMS-EBDL].

48. For example, see Sean Lawson, *Does 2016 Mark the End of Cyber Pearl Harbor Hysteria?*, FORBES (Dec. 7, 2016), https://www.forbes.com/sites/seanlawson/2016/12/07/does-2016-mark-the-end-of-cyber-pearl-harbor-hysteria/#5736bcaf22c2 [https://perma.unl.edu/B236-UWQE]; Robert McMillan & Jennifer Valentino-Devries, *Russian Hacks Show Cybersecurity Limits*, WALL ST. J. (Nov. 1, 2016), https://www.wsj.com/articles/russian-hacks-show-cybersecurity-limits-1478031535. Both discuss how cybersecurity discussions are consumed by warnings that states like Russia or China are on the verge of launching a complex cyber attack on dams or the power grid, killing thousands. These warnings have not borne out

to highlight how cyber technology has become woven into practically every aspect of critical infrastructure and disaster response in order to bring attention to the lack of any thoughtful incorporation of cybersecurity into disaster-response legislation. Before assessing the limited effectiveness of PPD-21, PPD-41, and the Stafford Act to manage cyber emergency response, it is worth looking at two recent cases highlighting why cybersecurity should be incorporated into federal- and state-level emergency response. The cases include telecommunications-network degradation and destruction in contrast to the relatively quick return of electricity and power in the wake of Hurricane Sandy in 2012, and the Taum Sauk Water Storage Dam failure near Lesterville, Missouri, in 2005.

1. Superstorm Sandy

Superstorm Sandy was a late-season hurricane that began in the southwest Caribbean on October 20, 2012, and proceeded to move north across the Atlantic and batter the U.S. eastern seaboard.[49] It struck the New Jersey and New York coastlines with a catastrophic storm surge causing 147 deaths and approximately fifty-two billion dollars in damage.[50] One of the immediate victims was the power grid across both New York and New Jersey, leading to blackouts and reduced power output in several areas flooded due to the storm surge.[51] These blackouts caused significant Internet and wireless-phone outages due to the lack of backup generators for power distribution to cable-television operators, wireless-phone operators, or even customers' handheld devices.[52]

While the blackouts caused major disruption, the energy grid was brought back online relatively quickly because responders were prepared and energy blackouts were anticipated.[53] Unlike the lack of redundancy and planning by Internet providers in both cable and telephone industries, the energy sector previously negotiated a number of mutual-assistance agreements that brought tens of thousands of technicians and support personnel into the affected area to return

in reality and instead ignore more mundane cybersecurity issues like poor programming, incompatibility of systems, and more general influence operations.

49. ERIC S. BLAKE ET AL., NAT'L HURRICANE CTR., TROPICAL CYCLONE REPORT: HURRICANE SANDY 1–3 (2013), http://www.nhc.noaa.gov/data/tcr/AL182012_Sandy.pdf [https://perma.unl.edu/T6R7-DWQC].

50. *Id.*

51. ALEXIS KWASINSKI, UNIV. OF TEX. AT AUSTIN, HURRICANE SANDY EFFECTS ON COMMUNICATION SYSTEMS PRELIMINARY REPORT 2–4 (2012), http://users.ece.utexas.edu/~kwasinski/preliminary%20telecom%20report%20v3%20comp.pdf [https://perma.unl.edu/GK93-8DS3].

52. *Id.* at 4.

53. STOCKTON, *supra* note 19, at 2–3.

energy service.[54] In response to the growing number of natural disasters, energy utilities proactively developed robust decision-making frameworks and aid agreements for allocating and distributing personnel and capabilities to support utilities harmed by disaster.[55] Prior to Superstorm Sandy, energy utilities prepared for power loss due to downed lines or inclement weather and developed clear plans and protocols to respond to those disasters, but there was no prepared response for cyber degradation or significant loss of communication networks.[56]

Further, energy production is a good example of a critical infrastructure that is fundamentally changing with the adoption of cyber-controlled and -enabled systems. This risk can best be categorized as a hybrid risk where an attack or loss from a cyber event can cross over into the physical realm.[57] In 2016, over eighty percent of oil-and-gas-industry companies experienced an increase in cyber attacks in addition to degraded performance from computer malfunctions or poor system interoperability.[58]

The threats posed to these systems are rapidly increasing, and by 2018, "the oil and gas industry is expected to face up to $1.87 billion in cybersecurity spending in an effort to protect against cyber risks."[59] As highlighted by Superstorm Sandy and its response, energy companies are prepared for natural disasters, but the mindset surrounding cyber threats has been wrongfully narrowed to focus only on cyber-criminal threats. Cyberspace must be seen as a new domain to prepare for wherever the threat comes from. The World Energy Council's annual report emphasized the increased importance of cybersecurity. It noted, "energy companies must get used to the fact that cyber is now [the] same kind of risk to large infrastructure as a flood or fire."[60] Put another way, critical infrastructure, especially the energy sector, should not get caught up on whether to classify a cyber event as arson or wildfire but plan and exercise how to put out the fire.

2. Failure of the Taum Sauk Water Storage Dam

The energy sector is uniquely interconnected with Internet and computer systems due to computer infrastructures' total reliance on regular and steady electricity.[61] The problem of inadequate focus on

54. *Id.* at 2.
55. *Id.*
56. *Id.* at 3.
57. World Energy Council, The Road to Resilience: Managing Cyber Risks 4 (2016).
58. *Id.* at 10.
59. *Id*. at 11.
60. *Id.* at 10.
61. Bakke, *supra* note 13, at 190.

cybersecurity and overreliance on networking systems in emergency response is just as relevant for other critical areas of infrastructure. This point is clear when looking at the Taum Sauk Water Storage Dam failure in central Missouri in 2005.

The Taum Sauk Reservoir Dam, from its inception in the 1950s, was designed to be a completely autonomous dam that would be managed and operated remotely from Bagnell Dam, located approximately 120 miles away.[62] The Dam provided energy production for AmerenUE, a utility company, and was hailed as an engineering feat for dam design and efficiency.[63] In fact, AmerenUE employees were on site at the Dam on September 26, 2005, for a ceremony with the Institute of Electrical and Electronics Engineers (IEEE), who declared the facility an engineering milestone.[64] It was at this ceremony employees first noticed something was wrong.[65] Company engineers noticed significant amounts of water overtopping the reservoir, and after an initial inspection, realized the "fail-safe" water-level sensors in the reservoir had come unattached.[66] Company personnel reattached the sensors inside the reservoir, and personnel at the site supposedly reprogrammed the sensors to reduce the operating level to provide a wider margin of safety.[67] At this point, the company thought the issue was fixed but never verified the entire sensor network in the reservoir was synced to the same water level.[68] On December 14, 2005, less than three months after the repairs, a different set of reservoir sensors failed to shut down the pumps feeding water into the reservoir, and the "fail-safe" probes failed to activate because the water level elevations were mischaracterized in the programming.[69] The failure of both sets of probes was not detected at the off-site operations center because the computer software displaying the gauges to operators was programmed with a different water cutoff level than the sensors, so no alarms were raised for operators.[70] In addition, the auto-safe backup system failed to activate in time because the repairs done in September were only completed on one set of probes and not the other.[71]

62. J. David Rogers, Conor M. Watkins & Jae-Won Chung, *The 2005 Upper Taum Sauk Dam Failure: A Case History*, XVI ENVTL. & ENGINEERING GEOSCIENCE 257, 262 (Aug. 2010).
63. *Id.* at 268.
64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. *Id.* at 269.
70. *Id.* at 285.
71. *Id.*

The overflow became catastrophic for dam structural integrity as the overflowing water landed into a rock-and-dirt berm immediately below the reservoir and eroded it to the point of total collapse.[72] The collapse led to over one billion gallons of water being released in Proffitt Mountain, destroying a state park superintendent's home and seriously injuring the family.[73] Multiple investigations ensued, including one by the Federal Energy Regulatory Commission (FERC), and each investigation determined a number of factors contributed to the failure.[74] During the investigations, it became clear a number of failures led to the dam overflow, but the worst was that AmerenUE had "no formalized oversight to oversee modifications to the reservoir's instrumentation."[75] Further, the company became too reliant on the networked systems, and a lack of visual oversight on the water levels meant that no human operator actually verified water levels, even after the initial overflow in September 2005.[76] Finally, investigators found the software system itself was never programmed to report or flag abnormal water-flow rates to plant operators, but the operators assumed the computer readings incorporated an adequate margin of error to trigger the auto "fail-safe" system.[77]

The Taum Sauk Dam failure highlights two central points key to this discussion. First, modern-day computer systems are evolutionary and are never in a complete state. Every computer or smartphone user is faced with the constant need to update apps and software to have the latest version that incorporates bug fixes or security patches. The same is true for the ICS and SCADA systems, which are used in critical infrastructure.[78] Many operators and users of these systems are not well versed on the network capabilities of these devices, how they interact with other SCADA or ICS systems, or the simple fact that these systems are oftentimes connected to the worldwide Internet.[79] This lack of understanding may not expose itself during regular operations but rather prove catastrophic when these networked elements fail during an event like the one at Taum Sauk. There was no process for ensuring that different network components and sensors operated

72. Rudi Keller, *Taum Sauk Levee Breaks*, SE. MISSOURIAN (Dec. 15, 2005), http://www.semissourian.com/story/1131499.html [https://perma.unl.edu/RMG7-5JXY].
73. *Id.*; *see also* STOUFFER ET AL., *supra* note 22, at C-13 (summarizing the Taum Sauk Water Storage Dam failure).
74. FED. ENERGY REGULATION COMM'N, FERC NO. 2277, REPORT OF FINDINGS ON THE OVERTOPPING AND EMBANKMENT BREACH OF THE UPPER DAM—TAUM SAUK PUMPED STORAGE PROJECT 7–8 (2006).
75. Rogers et al., *supra* note 62, at 285.
76. *Id.* at 286.
77. *Id.*
78. Kim Zetter, *10K Reasons to Worry About Critical Infrastructure*, WIRED (Jan. 24, 2012), https://www.wired.com/2012/01/10000-control-systems-online [https://perma.unl.edu/73ZL-D4KU].
79. *Id.*

in concert with the plant control systems at Taum Sauk.[80] The "fail-safe" mechanisms were subject to the same automation failures and risks as the primary sensors; thus, the staff did not fully appreciate the risk posed by the limitations of the technology.

The second lesson from the Taum Sauk failure is the dichotomy between natural disasters and man-made disasters is becoming less relevant in today's technologically driven world. Taum Sauk served as a technological marvel in engineering and was designed to be a nearly autonomous system.[81] The ensuing flood and destruction, while a natural occurrence, was precipitated by human error. Thus, attempts to separate natural disasters from man-made disasters, like under the Stafford Act,[82] are inherently lacking in today's interconnected world because "no disaster is completely 'natural;' human exposure and vulnerability to risk is a product of cultural patterns influenced heavily by law."[83]

B. PPD-21 and Recognition of Cyber in Critical Infrastructure

In order to understand why FEMA, the key federal organization responsible for emergency response, has not taken a more proactive role in cybersecurity for critical infrastructure, it is important to understand the cybersecurity landscape from 2013 to present day. In 2013, President Obama issued PPD-21.[84] PPD-21's stated goal was to create a national unity of effort "to strengthen and maintain secure, functioning, and resilient critical infrastructure."[85] PPD-21 was not the Federal Government's first attempt to get a handle on critical infrastructure and the need for cybersecurity to be incorporated into the broader discussion.[86] Over a two-year period, Congress attempted and failed to pass the Cybersecurity Act of 2012, an Act designed to set cybersecurity baselines in response to an uptick in reported cyber attacks on oil-and-gas-pipeline infrastructure.[87] This proposed Act, although passing the House of Representatives, floundered in the Senate because of too many competing interests and more headline-grabbing topics at the time including national debt, sequestration, and

80. Rogers et al., *supra* note 62, at 285.
81. *Id.* at 262.
82. *See* 42 U.S.C. § 5122 (2012).
83. Ryan, *supra* note 16, at 9.
84. PPD-21, *supra* note 29.
85. *Id.*; *see also* Deborah Norris Rodin, Note, *The Cybersecurity Partnership: A Proposal for Cyberthreat Information Sharing Between Contractors and the Federal Government*, 44 PUB. CONT. L.J. 505, 516–17 (2015) (explaining the purpose of PPD-21).
86. Hillary Hellmann, *Acknowledging the Threat: Securing United States Pipeline SCADA Systems*, 36 ENERGY L.J. 157, 167 (2015).
87. *Id.*

tax-cut extensions.[88] The competing interests included discussions of whether the Act should cover "information sharing, critical infrastructure regulatory structures, [and] workforce challenges" in cybersecurity.[89] With the failure of the Cybersecurity Act, the Executive Branch was left with few options to expand cybersecurity.[90] In order to provide some guidance in the ensuing loss of the Cybersecurity Act, PPD-21, in combination with Executive Order 13,636, took the discussion of cybersecurity out of an attack framework and instead argued the Federal Government must take steps to address cyber threats.[91] Although subtle, PPD-21 went further than the defunct Cybersecurity Act by taking cybersecurity out of the national-security box and tying the resiliency of physical infrastructure to the resiliency of the cyber infrastructure.[92] Because "[j]ust as the physical and cyber elements of critical infrastructure are inextricably linked, so are the vulnerabilities."[93]

The connection between the two was reflected in PPD-21 through President Obama's order directing all federal departments and agencies to create a number of joint operational centers, reporting mechanisms, and information-sharing protocols to ensure unity of effort to maintain a robust and functioning critical infrastructure in the face of a disaster or emergency.[94] The central purpose of PPD-21 was to provide federal support and attention to key critical-infrastructure components but not management or oversight.[95] This attention was also highlighted in Executive Order 13,636 because it called for the Secretary of the Department of Commerce to order NIST to develop a voluntary information-sharing program to promote coordination but not require adoption of any security mechanisms.[96] Further, PPD-21 attempted to connect critical infrastructure regulated by sector-specific agencies (SSAs) and provide a forum for expanded public–private

88. Jessica Herrera-Flanigan, *July Fireworks: Senate May Take Up Cybersecurity, But Then What?*, NEXTGOV (June 25, 2012), http://www.nextgov.com/cybersecurity/cybersecurity-report/2012/06/july-fireworks-senate-may-take-cybersecurity-then-what/56448/?oref=NG-channelriver [https://perma.unl.edu/ZKT7-VZZW].

89. *Id.*

90. Hellmann, *supra* note 86, at 167.

91. PPD-21, *supra* note 29; *see also* Exec. Order No. 13,636, 3 C.F.R. § 101 (2014) ("The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we confront.").

92. PPD-21, *supra* note 29.

93. *Id.*

94. *Id.*

95. Paul Rosenzweig, *No, DHS Is Not Going to "Take Over" the Electoral System*, LAWFARE BLOG (Sept. 6, 2016), https://www.lawfareblog.com/no-dhs-not-going-take-over-electoral-system [https://perma.unl.edu/72GZ-TFTG].

96. Hellmann, *supra* note 86, at 167.

partnerships with other sectors and their regulators.[97] This last component is key because, as seen in the response to Superstorm Sandy and the Taum Sauk Dam failure, critical infrastructure is networked and interdependent in ways not seen before.[98] Thus, a common vernacular and approach to protecting critical infrastructure is crucial. There are two key issues, however, with PPD-21 that required the issuance of PPD-41. First, PPD-21 attempted to address cybersecurity through its employment in critical infrastructure but failed to address the unique qualities of cybersecurity within critical infrastructure. Second, PPD-21 placed the impetus on federal agencies but largely missed the role that local and state governments and private parties play in the protection of critical infrastructure. It was these gaps, and the broader lack of cybersecurity oversight, that led to the issuance of PPD-41 in mid-2016.

C. PPD-41: Cybersecurity Has Its Day

PPD-41—United States Cyber Incident Coordination—is the most comprehensive "whole of government" approach to cybersecurity to date and was designed to provide a framework for federal-government responses to cyber incidents by clearly delineating the role of federal, state, and local governments.[99] Building off PPD-21, PPD-41 places the responsibility of cybersecurity on all parties, both public and private.

> The nature of cyberspace requires individuals, organizations, and the government to all play roles in incident response. . . . [E]ffective incident response efforts will help support an open, interoperable, secure, and reliable information and communications infrastructure that promotes trade and commerce, strengthens international security, fosters free expression, and reinforces the privacy and security of our citizens.[100]

This collaborative approach is vital because, as demonstrated in Superstorm Sandy, critical industries are often completely reliant on the ability of state and local governments to quickly respond, while government at all levels is equally reliant on private-sector infrastructure.[101] The most important role of PPD-41 is that it clearly articulates cybersecurity is about much more than deterring bad actors and explains cyber infrastructure is "vulnerable to malicious activity, mal-

97. *Id.* at 166–67. A common example of an SSA is the Department of Energy's oversight authority over public utilities.
98. Trautman, *supra* note 37, at 368.
99. Sean D. Carberry, *Why PPD-41 Is Evolutionary, Not Revolutionary*, FCW (Oct. 24, 2016), https://fcw.com/articles/2016/10/24/ppd41-cyber-carberry.aspx [https://perma.unl.edu/CB23-SFD9].
100. *Presidential Policy Directive—United States Cyber Incident Coordination*, WHITE HOUSE (July 26, 2016) [hereinafter PPD-41], https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident [https://perma.unl.edu/28QK-NJDZ].
101. WORLD ENERGY COUNCIL, *supra* note 57, at 10.

function, human error, and acts of nature, placing the Nation and its people at risk."[102] This articulation of the vulnerability in cyber is key because it highlights the multifaceted approach necessary in order to respond to a cyber incident. Unlike PPD-21, PPD-41 directly addresses the fundamental challenges posed by cybersecurity and expands the ecosystem from just critical infrastructure to the role cyber increasingly plays in modern democracy.[103]

Under PPD-41, the expanded view of the cyber ecosystem is guided by five principles for incident response: (1) shared responsibility, (2) risk-based response, (3) respect for affected entities, (4) unity of governmental effort, and (5) enablement of restoration and recovery.[104] At the core, these principles attempt to streamline a response to a cyber incident and communicate to state and local authorities, as well as private-sector parties, that the federal government will provide support in response to a cyber incident. PPD-41 defines a cyber incident as "an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon."[105] The event does not need to be perpetrated by a malicious actor and includes not only the event that occurs but also includes any vulnerabilities in those systems that "could be exploited by a threat source."[106] Further, PPD-41 distinguishes between a standard cyber incident and a significant cyber incident. A significant cyber incident is an incident that is "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the . . . public health and safety of the American people."[107] For the purpose of this discussion, the focus is centered on the more egregious significant cyber incident. The shutdown of critical-infrastructure components or systems is much more likely to rise to the level of a significant cyber incident than theft of company or client data or software glitches in non-critical-infrastructure industries.

In order to respond to a significant cyber incident, PPD-41 directs three concurrent lines of effort: (1) threat response, (2) asset response, and (3) intelligence support.[108] Threat response includes activities related to criminal or forensic investigation aimed at identifying the threat and the attacker, if there is an attacker; potentially linking re-

102. PPD-41, *supra* note 100.
103. *Id.*
104. *Id.*
105. *Id.*
106. *Id.*
107. *Id.*
108. *Id.*

lated threats; and mitigating the immediate threat to any network or system.[109] Through asset response, federal agencies can provide technical assistance to victims of a cyber incident to "stop the bleeding," mitigate vulnerabilities, protect victims' network assets, and pass this information on to other potential victims in hopes of stopping wider damage or preventing a cascading effect from the threat.[110] Finally, intelligence support is a synchronization between federal agencies, local authorities, and private parties to look at threat trends and promote sharing of intelligence to identify knowledge gaps in industries in order to degrade or limit future threats.[111]

After defining the principles and threats for federal agencies, PPD-41 explains how the Federal Government will conduct its three lines of effort. PPD-41 creates a cyber unified coordination group (UCG) that serves as the focal point for coordinating federal agencies. The UCG would be activated at the request of the National Security Council (NSC) or at the request of two or more federal agencies including SSAs.[112] Further, the Department of Homeland Security (DHS) could call for the UCG when a significant cyber incident affects critical infrastructure "for which a cyber incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[113] It is the UCG that would serve as the primary federal-response entity in the event of an incident and is designed to promote unity of effort in the federal response. However, the UCG would not be the lead entity;[114] each line of effort has a different lead agency. The Department of Justice (DoJ) would lead the threat-response effort, DHS would lead the asset-response effort, and the Office of the Director of National Intelligence (ODNI) would lead the intelligence support.[115]

PPD-41, at its core, attempts to wrestle cybersecurity into some sort of workable framework for coordination and oversight, and seat it in the traditional national-preparedness framework.[116] It is useful because it defines the problem and provides a context and structure to harness federal support.[117] PPD-41, like many PPDs, is only of lim-

109. *Id.*
110. *Id.*
111. *Id.*
112. *Id.* (discussing SSA list pulled directly from the critical-infrastructure designation under PPD-21).
113. *Id.*
114. *Id.*
115. *Id.*
116. *Id.*
117. Frank J. Cilluffo & Sharon L. Cardash, *Overview and Analysis of PPD-41: US Cyber Incident Coordination*, LAWFARE BLOG (July 27, 2016), https://www.lawfareblog.com/overview-and-analysis-ppd-41-us-cyber-incident-coordination [https://perma.unl.edu/HFA4-PQWV].

ited use because it lacks any legal authority or financial support to turn the theoretical frameworks into practical responses.[118]

There are four key gaps in PPD-41 that necessitate an expanded role for FEMA in cybersecurity response. First, PPD-41's definition of a "significant cyber incident" is inadequate to reasonably be able to categorize the harms caused by a particular cyber incident.[119] In the world of cyber intrusions and malware, something as minor as hacking a single Gmail account has huge repercussions because of the account owner's identity,[120] while a software glitch that temporarily took Amazon Cloud servers offline along the entire East Coast for several hours was largely fixed and forgotten the next day.[121]

Second, PPD-41 directs a federal structural response but does not provide state or local governments any direction or advice on how to utilize that system. PPD-41 attempts to place the UCG within the National Incident Management System that relies on state-level agencies to coordinate with federal authorities to monitor events to determine the right level of response.[122] However, these coordination centers or fusion cells are not predictable and suffer from competing interests and manpower issues, and therefore are not reliable in every emergency.[123] Further, state agencies are often ill-equipped to correctly classify a cyber incident and suffer from a lack of cyber expertise to quickly and efficiently report incidents to federal authorities.[124] Further, with the limited guidance on categorizing the severity of a cyber incident, local and state authorities are prone to confusion on what incidents will warrant federal assistance.[125] In addition, FEMA's inclusion in PPD-41 is limited to incorporating the PPD-41 policy into

118. HAROLD C. RELYEA, CONG. RESEARCH SERV., ORDER CODE 98-611, PRESIDENTIAL DIRECTIVES: BACKGROUND AND OVERVIEW CRS-2 (2008) (providing review of different presidential directives, orders, and statements, and laying out the legal authority of each).

119. *See* PPD-41, *supra* note 100.

120. Gregory Krieg & Tal Kopan, *Is This the Email that Hacked John Podesta's Account?,* CNN (Oct. 30, 2017), http://www.cnn.com/2016/10/28/politics/phishing-email-hack-john-podesta-hillary-clinton-wikileaks [https://perma.unl.edu/ZGH5-H23W].

121. Alex Hern, *How Did an Amazon Glitch Leave People Literally in the Dark?*, GUARDIAN (Mar. 1, 2017), https://www.theguardian.com/technology/2017/mar/01/amazon-web-services-outage-smart-homes [https://perma.unl.edu/UA5A-WWNR].

122. PPD-41, *supra* note 100.

123. Brian Nussbaum, Assistant Professor, State Univ. of N.Y. at Albany, Address at University of Nebraska College of Law State, Local and Regional Issues in Cybersecurity Conference (Mar. 17, 2017).

124. *Id.*

125. *Id.*

its Unified Coordination training but makes no mention of assisting in state- or local-level plan development.[126]

Third, PPD-41 makes no mention of developing a framework for public–private partnerships in order to conduct cyber-incident exercises or security frameworks.[127] This is especially important in the critical-infrastructure context because upwards of eighty-five percent of critical infrastructure is owned by private entities.[128] While it is vital the federal government be involved with cybersecurity, it is important private entities are just as capable and nimble in this realm.[129]

Finally, PPDs are not federal regulations or statutory law and carry no binding authority for successive administrations, so any gains created in PPD-41 can be easily lost or rewritten under successive administrations.[130] This is the most poignant point regarding PPD-41's future and its usefulness in responding to a cyber incident. President Obama issued PPD-41 approximately six months prior to leaving office, and ironically, issued the directive four days after the first WikiLeaks publication of sensitive Democratic National Committee emails, arguably as part of a Russian intelligence campaign to influence the 2016 U.S. Presidential election.[131] The investigation into the alleged Russian hacking campaign continues as of this writing, but it highlights a significant cyber incident need not destroy dams or cause blackouts to threaten national security or public confidence in the U.S. government. As Cilluffo and Cardash highlight, the true test of PPD-41 is "the manner and nature of its implementation. Were the United States to experience a cyber-attack on its grid . . . the Directive would surely be triggered and tested. Whether and how the country will respond to the DNC hack, however, remains an open question."[132] As of this writing, PPD-41 has not been triggered or utilized to respond to the DNC hack or any cyber event. PPD-41 is not a binding legal authority,[133] and it is unclear so early in the Trump Administra-

126. *Annex to Presidential Policy Directive—United States Cyber Incident Coordination*, WHITE HOUSE (July 26, 2016) [hereinafter PPD-41 Annex], https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident [https://perma.unl.edu/A8KR-D5G7].

127. Carberry, *supra* note 99.

128. STRATEGIC FORESIGHT INITIATIVE, *supra* note 43, at 2.

129. Cilluffo & Cardash, *supra* note 117.

130. RELYEA, *supra* note 118.

131. Justin Fishel & Veronica Stracqualursi, *A Timeline of Russia's Hacking into US Political Organizations Before the Election*, ABC NEWS (Dec. 15, 2016), http://abcnews.go.com/Politics/timeline-russias-hacking-us-political-organizations-ahead-election/story?id=44140526 [https://perma.unl.edu/Z5XC-YH74].

132. Cilluffo & Cardash, *supra* note 117.

133. RELYEA, *supra* note 118.

tion as to whether President Trump will maintain the two PPDs or look to change the structure during his tenure.

After reviewing PPD-21 and PPD-41, it is clear the federal government has made significant strides in promoting cybersecurity in emergency response. However, what is also clear is that it has not done enough to empower state and local authorities or private entities to take a more proactive role in cybersecurity. The best option to fill this gap is to utilize the United States' primary emergency-response statute, the Stafford Act, to empower FEMA to be more involved in coordination for emergency response during a cyber incident. Further, FEMA, partnered with any relevant SSA, should be given expanded authority to provide tools and potential funding to the parties to incorporate preemptive cybersecurity in their emergency-response preparedness.

III. EMPOWERING FEMA IN THE AGE OF CYBERSECURITY

A. The Stafford Act in Practice

The Stafford Act is the principle federal emergency-response statute in the United States.[134] The Act, administered by FEMA, has a number of specific purposes, including the creation of a disaster- or emergency-declaration process, oversight mechanisms during an emergency response, and a system to distribute aid during such disaster or emergency.[135] While a powerful tool for the Executive Branch, the scope of the Stafford Act is narrow, and the key "provisions are triggered only by severe, natural, or manmade disasters that exhaust local and state resources."[136] The Stafford Act attempts to strike a balance between honoring states' prerogatives in addressing local and state events, and providing a federal coordination scheme when emergency events are too severe for local or state authorities to handle.[137]

The Stafford Act creates two categories of events where a President can provide federal support during an event: a major disaster or an emergency. A "major disaster" is defined as:

> any natural catastrophe . . . or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under [the Stafford Act] to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.[138]

134. Gregory J. Lake, *Federal & State Disaster Response: An Introduction*, 41 COLO. LAW. 95 (2012).
135. *Id.*
136. *Id.*
137. *Id.*
138. 42 U.S.C. § 5122(2) (2012).

An "emergency" is defined as:

> any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.[139]

The importance of these definitions is the President is not authorized to provide federal support without a declaration that either a major disaster or emergency occurred.[140] The process for both declarations is the governor of the affected state must submit a request for federal support by declaring either a natural disaster or emergency exists and the event is "of such severity and magnitude that an effective response is beyond the capabilities of the state and the affected local governments."[141] The President does have the authority under § 5191(b) to unilaterally declare a state of emergency.[142] However, for the purposes of this discussion the focus is on when the requests come from the state level. An additional prerequisite of this requirement is the governor must have directed and taken any necessary steps to execute the state's emergency plan.[143] Each state must have an emergency plan, and under § 201(a)–(d), the President must provide state agencies technical assistance in "developing comprehensive plans and practicable programs for preparation against disasters, including hazard reduction, avoidance, and mitigation."[144] In addition, the President shall also provide similar assistance to individuals, private businesses, and local governments following a disaster and in recovery efforts.[145]

Once this process is complete, the President, through any applicable federal agency, is then authorized to provide disaster relief.[146] An important caveat is that even if a Presidential declaration is issued, federal agencies are not required to provide aid. Thus, there is no process for funds or support to be automatically disbursed to any state agency or other party eligible for relief.[147] Further, private businesses or other for-profit organizations are generally considered ineligible for any type of assistance under the Stafford Act.[148] This prevents private businesses that provide resources, equipment, and personnel in re-

139. § 5122(1).
140. 42 U.S.C. §§ 5170(a), 5191(a) (2012).
141. §§ 5170(a), 5191(a).
142. § 5191(b).
143. §§ 5170(a), 5191(a).
144. 42 U.S.C. § 5131(a)–(d) (2012).
145. *Id.*
146. Lake, *supra* note 134, at 95.
147. *Id.*
148. Ernest B. Abbott, *Recent Developments in Homeland Security and Emergency Management: Representing Local Governments in Catastrophic Events: DHS/FEMA Response and Recovery Issues*, 37 URB. LAW. 467, 475 (2005).

sponse to a federal disaster from being reimbursed under the Stafford Act public-assistance program.[149]

B. The Stafford Act's Current Approach to Cybersecurity

With a broad understanding of the Stafford Act and its coordinating role for declared natural disasters or emergencies, How does the Stafford Act approach cybersecurity in emergency management and preparedness? Like PPD-21, which fails to address the unique qualities of cybersecurity that converge multiple infrastructures and networks, the Stafford Act misses the opportunity to push for cyber resiliency in emergency planning. The Stafford Act only mentions cybersecurity or cyber infrastructure twice in the entire Act, and both references recognize that critical infrastructure includes both the physical components of infrastructure as well as the cyber components.[150] No explicit tasks are assigned to FEMA other than assisting in "[m]odeling, simulation, and analysis of the systems comprising critical infrastructures, including cyber infrastructure . . . in order to enhance understanding of the large-scale complexity of such systems."[151] This general inclusion of cyber infrastructure in the broader context of critical-infrastructure protection is similar to the model used in PPD-21.[152] Any further guidance, however, is missing under 44 C.F.R. § 1, "Emergency Management and Assistance," which does not provide any significant mention of cybersecurity or FEMA-promulgated regulations regarding cybersecurity preparation or planning.[153] Without any specific mention of cybersecurity under the Stafford Act or implementing regulations, the question is whether a cyber event would meet the definition of either a major disaster or emergency under the Stafford Act. Under the current Stafford Act definition of major disaster, a cyber incident would likely not meet the criteria because a cyber incident would not meet the examples of a natural catastrophe and not all cyber incidents would necessarily cause fire, flood, or explosion.[154] It is true, some cyber threats are explicitly intended to cause a hazard leading to a fire, flood, or explosion and may fit under this definition; however, cyber threats resulting in loss of communication networks or power generation would not meet this standard.

149. *Id.*

150. 42 U.S.C. § 5195(c)–(d) (2012).

151. § 5195(d).

152. PPD-21, *supra* note 29.

153. Emergency Management and Assistance, 44 C.F.R. § 1 (2016).

154. 42 U.S.C. § 5122(2) (2012) (enumerating several examples of "natural catastrophes," including: hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought).

In drafting both the current Stafford Act and Critical Infrastructures Protection Act of 2001, Congress directed FEMA to take an all-hazards approach to preparedness and emergency response but never explicitly identified cybersecurity as a focus.[155] Under the current phrasing of the Stafford Act and the uncertain future of PPD-41, it is unclear whether FEMA "should develop cyber capabilities to actively mitigate cyber threats . . . so public-private risk-management programs are conducted fluidly by a single government entity" or whether FEMA should defer all cybersecurity planning to its parent agency, DHS.[156]

C. Modernizing FEMA and the Stafford Act for a Networked World

After reviewing both the Stafford Act and the Code of Federal Regulations for "Emergency Management and Assistance,"[157] it is clear FEMA is not equipped with the tools necessary to fulfill its statutory obligations to lead and support the United States in a "comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation."[158] There are three key tools that if adopted would empower FEMA to take a proactive and unifying role in cybersecurity for critical infrastructure. First, the FEMA Administrator under its rulemaking authority under 42 U.S.C. § 5197(g) should create a classification of three types of cyber events under the broad definition of cyber incident provided under PPD-41, including: (1) physical-system hardware destruction or loss, (2) network degradation or destruction, and (3) software malfunction or exploitation incident.[159] Second, the FEMA Administrator should provide financial aid through the form of grants under FEMA's emergency-preparedness-compact authority[160] to promote and streamline the adoption of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*[161] in each state's emergency-preparedness compact established by the National Emergency Management Association (NEMA) through the Emergency Management Assistance Compact (EMAC).[162]

155. David G. Delaney, *Cybersecurity and the Administrative National Security State: Framing the Issues for Federal Legislation*, 40 J. LEGIS. 251, 273–74 (2014).
156. *Id.* at 275.
157. 44 C.F.R. § 302 (2016).
158. Delaney, *supra* note 155, at 274–75.
159. 42 U.S.C. § 5197(g) (2012).
160. 42 U.S.C. § 5196(h) (2012).
161. NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Jan. 10, 2017) [hereinafter NIST FRAMEWORK], https://www.nist.gov/document/draft-cybersecurity-framework-v11pdf [https://perma.unl.edu/7EJX-HJUV].
162. NAT'L EMERGENCY MGMT. ASS'N, THE EMERGENCY MANAGEMENT ASSISTANCE COMPACT: A HISTORY AND ANALYSIS OF THE EVOLUTION OF NATIONAL MUTUAL AID POL-

Third, the President, through FEMA, should condition any post-cyber-incident disaster-relief aid on a showing by the governor that all state agencies and private partners adopted and implemented the NIST Framework prior to the event.

1. Putting Cyber Incidents in Context by Defining the Incident

As discussed earlier, one of the shortcomings of PPD-41 is its failure to define types of cyber incidents.[163] A working vernacular that is incorporated at both the federal and state emergency-response levels is vital to ensuring a timely response to events but is something that is still lacking in cybersecurity. According to the Government Accountability Office's (GAO) *Critical Infrastructure Protection* report, "There are too many government agencies with different cyber-missions working independently, with project duplication to the point that it is not uncommon for several different groups to be working on the same thing."[164] FEMA's primary role is coordinating and synchronizing emergency response; thus, FEMA should issue an incident-classification guide enabling first responders to better understand the problem.

Three types of incident classification would help to place a cyber incident in context: (1) physical-system hardware destruction or loss, (2) network degradation or destruction, and (3) software malfunction or exploitation incident. The first classification would cover physical-system hardware destruction or loss. This can be caused by noncyber means like flooding and fire or by cyber intrusion or accident.[165] In these types of incidents, emergency responders can prioritize sourcing-replacement systems for distribution and utilize the state emergency compacts to procure temporary or replacement hardware or assistance for critical infrastructure.[166]

---

icy and Operations 1 (2014) [hereinafter EMAC], https://www.desmogblog.com/sites/beta.desmogblog.com/files/EMAC%20History.pdf [https://perma.unl.edu/Z6TD-BFLB] (explaining Congress created the EMAC structure in 1996 as a national, interstate mutual-aid agreement that empowered FEMA to assist states through the NEMA nonprofit organization in developing emergency-response capabilities by encouraging states to adopt common vernacular, emergency-management structures, and emergency frameworks).

163. PPD-41, *supra* note 100.

164. Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor"*, 18 Va. J.L. & Tech. 289, 329 (2014) (citing U.S. Gov't Accountability Office, GAO-10-628, Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed 14 (2010)).

165. Talbot, *supra* note 21. Mr. Talbot finds that the physical location of network infrastructure can often determine its survivability during a crisis: "[D]uring [Hurricane] Katrina . . . although one carrier had built a very robust cellular tower above the water line, the cable connecting that tower to the central office was underwater and out of service." *Id.*

166. EMAC, *supra* note 162, at 45.

Second, network-degradation incidents are those where the individual systems used by critical sectors are not damaged or otherwise inoperable but instead the communications infrastructure is offline or experiencing intermittent connectivity. As highlighted earlier, the hallmark of modern technology is the expansion of interdependent systems that communicate and operate together autonomously and across a wide geographic area.[167] These incidents are prone to interstate coordination because network towers or transmission points may be across county or state lines, thus necessitating rapid communications between multiple parties to avoid cascading failures.[168]

Third, software malfunction or exploitation is the most common classification seen today.[169] This is a malfunction that degrades or compromises a single computer system or network without any physical damage or loss.[170] This is the typical software glitch that affects one system and requires patching or other minor steps to correct.[171] Despite being typical, these incidents can have a dramatic effect on critical infrastructure, as demonstrated in the Amazon glitch that severely limited access across the East Coast of the United States for several hours.[172] The third category also includes malicious malware or hacking that targets systems for exploitation or espionage. While not typically thought of as an emergency-management concern, this category can be used to quickly classify a cyber incident for notification to local, state, and federal law enforcement.

2. Developing Cyber-Emergency-Preparedness Pacts Through FEMA Grant Funding

Including FEMA in cybersecurity and critical-infrastructure development is important because FEMA's central role is to be the coordination agency for the whole government.[173] Unlike the Department of

167. James E. Scheuermann, *Cyber-Physical Attacks on Critical Infrastructure: What's Keeping Your Insurer Awake at Night?*, K&L GATES (Jan. 24, 2017) (citing LLOYD'S, BUSINESS BLACKOUT: THE INSURANCE IMPLICATIONS OF A CYBER ATTACK ON THE US POWER GRID (2015)), http://www.klgates.com/cyber-physical-attacks-on-critical-infrastructure—whats-keeping-your-insurer-awake-at-night-01-24-2017/#_ftn12 [https://perma.unl.edu/X2GP-KZ7U].

168. STOCKTON, *supra* note 19, at 13.

169. Sabine Vollmer, *How to Protect Against the 9 Most Common Cyber-Attacks*, CGMA MAG. (Jan. 13, 2015), http://www.cgma.org/magazine/2015/jan/20151162 4.html [https://perma.unl.edu/7N2A-FD7C]. Ms. Vollmer identifies the nine "most common cyber-attacks," and seven of the nine are related to software malfunctions or deliberate hacks targeting software vulnerabilities. *Id.*

170. *See id.*

171. Hern, *supra* note 121.

172. *Id.*

173. David M. Crane, *A National Imperative Americans Want to Serve: The Public Assistance Service Responding to America's Man-Made or Natural Disasters*, 65 SYRACUSE L. REV. 247, 260 (2015).

Energy (DoE), the Department of Treasury, or the Department of Agriculture, FEMA is not identified as the designated sector-specific agency for any of the critical-infrastructure sectors.[174] Instead, FEMA's primary function is "to direct assistance from Federal Government agencies that facilitate preparation, prevention, response and recovery."[175] Under 42 U.S.C. § 5131, the President "shall provide technical assistance to the States in developing comprehensive plans and practicable programs for preparation against disasters, including hazard reduction, avoidance, and mitigation."[176] In the cybersecurity context, FEMA can utilize its statutory authority to drive expertise and coordination to the state and local level through the EMAC.[177] It is important to note that when these events occur, it is the local first responders who are often faced with the most challenging aspects of response.[178] State agencies in particular play a vital role in coordinating efforts between federal and local authorities because it is state agencies that "formulate policy, coordinate the delivery of federal assistance, and engage in . . . pre- and post-disaster capacity-building initiatives that target local governments."[179] Thus, the key is providing FEMA a cyber coordination role to empower state agencies to cooperate and develop plans to implement at the local level.

To truly be effective, FEMA cannot only provide coordination but must also provide certain levels of funding to drive the parties to prioritize cybersecurity. Under 42 U.S.C. § 5131(d), FEMA is authorized to create grants for no more than fifty percent of the cost of "improving, maintaining, and updating State disaster assistance plans."[180] Further, § 5131(d) grants FEMA the authority to recommend and push standardization protocols in addition to funding authority to persuade states to adopt those protocols.[181] Simply working with state and local agencies, however, does not fully address the need to engage with private businesses and organizations. As discussed in section II.C., any cybersecurity planning must include private businesses, if for no other reason than the fact private ownership makes up approximately eighty-five percent of critical infrastructure.[182] FEMA can utilize its coordination authority with other federal agencies to empower SSAs and give teeth to SSA recommendations in the private

174. PPD-21, *supra* note 29.
175. *Id.*
176. 42 U.S.C. § 5131(b) (2012).
177. EMAC, *supra* note 162, at 31, 54.
178. Crane, *supra* note 173, at 248.
179. Gavin Smith, Dylan Sandler & Mikey Goralnik, *Assessing State Policy Linking Disaster Recovery, Smart Growth, and Resilience in Vermont Following Tropical Storm Irene*, 15 VT. J. ENVTL. L. 66, 81 (2013).
180. § 5131(d).
181. *Id.*
182. STRATEGIC FORESIGHT INITIATIVE, *supra* note 43, at 3.

sector. For example, in the aftermath of an event, FEMA often partners with SSAs to provide disaster aid and relief to private parties despite FEMA not being authorized to directly provide aid to private business.[183] For cybersecurity purposes, FEMA can utilize the expertise of the SSAs on cybersecurity issues in a particular industry, then push incorporation of plans and programs through the state agencies to reach private parties through state regulation. Finally, FEMA can connect state agencies with SSA-sponsored industry consortiums in each infrastructure sector or cybersecurity-focused consortiums. These industry consortiums improve safety and planning by drawing on resources and knowledge of multiple companies and lower technical-planning requirements for public institutions.[184]

3. Hazard Declarations Must Include Verification of NIST Framework Adoption

The final and arguably most necessary component is the adoption of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, a vetted cybersecurity framework that can actually reduce cyber threats and vulnerabilities through effective risk management.[185] The NIST Framework principles are a clear example of the effectiveness of coordination for companies wrestling with cybersecurity.[186] The NIST Framework outlines five high-level functions that should be incorporated in any cybersecurity plan: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover. The Framework is not a checklist an organization runs for compliance but is a strategy document designed to encourage a security mindset.[187] The Framework provides implementation tiers and security profiles designed to help organizations identify weaknesses in their own planning and system.[188] At its core, the Framework is a strategy document that different sizes and types of organizations can adopt and incorporate into their own planning. Further, this proactive approach to cybersecurity, which identifies the underlying vulnerabilities of systems instead of responding after a singular attack, is an approach that is currently

183. Joseph E. Aldy, *Real-Time Economic Analysis and Policy Development During the BP* Deepwater Horizon *Oil Spill*, 64 VAND. L. REV. 1795, 1803 (2011) (explaining FEMA coordinated with the Small Business Administration to provide economic-injury disaster loans to small businesses operating in Louisiana in response to the BP oil spill).

184. *Id.* at 1810.

185. PRICEWATERHOUSECOOPER, WHY YOU SHOULD ADOPT THE NIST CYBERSECURITY FRAMEWORK 3 (2014), www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf [https://perma.unl.edu/ZV8R-3CQU]; *see also* Hellmann, *supra* note 86, at 170 (explaining the Framework and analyzing criticisms of its current lack of implementation).

186. PRICEWATERHOUSECOOPER, *supra* note 185, at 4.

187. NIST FRAMEWORK, *supra* note 161, at 14.

188. Hellmann, *supra* note 86, at 170.

being adopted in disaster response.[189] The idea is these broad frameworks are better able to address interconnected physical, social, economic, and environmental systems.[190] Thus, the goal of the NIST Framework is adding the virtual and cyber ecosystem to the list.[191]

Although highly regarded, the NIST Framework does have its critics.[192] The focus of most criticism is private companies and local and state organizations are not required to adopt the NIST Framework.[193] At the time President Obama issued Executive Order 13,636 and PPD-21, DHS argued grants were the most effective way to incentivize private companies to adopt the NIST Framework, but a grant incentive program would require new statutory authority.[194] This assessment, however, was prior to PPD-41 and the explicit inclusion of FEMA in the broader cybersecurity context.[195]

The major drawback of the NIST Framework is it is largely voluntary, and there is no enforcement mechanism to push states to better prepare and adopt cybersecurity protocols for disaster response.[196] The key to success would be to include the NIST Framework in the state-level emergency plans so governors would be required to verify the NIST Framework was incorporated and executed at the state level during any request for disaster or emergency relief.[197] As specified earlier, the governor's request for aid must articulate the state's resources cannot handle the incident and the state executed its state emergency plans.[198] It is in those emergency plans that FEMA can mandate adoption of the NIST Framework.[199] This enforcement mechanism would be narrowly applied to cyber incidents during an emergency response. States would continue to receive federal aid to mitigate and stop the physical flooding or fire, but any financial relief requested for cyber infrastructure systems would require a showing the NIST Framework was adopted and utilized prior to the event in question pursuant to FEMA authorities.[200]

189. Smith et al., *supra* note 179, at 72–73.
190. *Id.* at 74.
191. Hellmann, *supra* note 86, at 170.
192. *Id.* at 170–71.
193. *Id.*
194. *Id.*
195. PPD-41 Annex, *supra* note 126.
196. Hellmann, *supra* note 86, at 170–71.
197. 42 U.S.C. § 5170(a) (2012).
198. *Id.*
199. 42 U.S.C. §§ 5170(a), 5191(a) (2012).
200. Lake, *supra* note 134, at 95.

IV. TEST CASE: HURRICANE ZOE STRIKES GULF OF MEXICO

The intent behind the proposed modification to the Stafford Act and rulemaking by FEMA is not to add another federal agency to the cybersecurity ecosystem but instead to modernize FEMA and its authorities to coordinate and respond to disasters or emergencies that are either caused by a cyber event or worsened due to a cyber event. The hypothetical test case is a Category 3 Hurricane, Hurricane Zoe, that starts in the Gulf of Mexico, makes landfall on the southeast coast of Texas, and ultimately strikes the Houston metropolitan area. Houston serves as the location for the hypothetical hurricane due to its significant role in the U.S. economy.[201] The Port of Houston and its supporting infrastructure are uniquely vital to the U.S. economy.[202]

> Approximately 17 million people live within 300 miles of Houston, 50% of the Unites States gasoline is refined in the port, it is the second largest petrochemical facility in the world and the second largest port in the United States in tonnage processed. [In addition, Houston is home to] Exxon-Mobil's largest refinery in the world and Dow's largest petrochemical plant in the western hemisphere.[203]

After Hurricane Zoe makes landfall in Galveston, Texas, the hurricane moves northwest into Houston Bay and significantly damages the Exxon Mobil Baytown Refinery before moving along the Houston Ship Channel destroying other oil refineries, chemical storage facilities, and power production plants and severing several natural-gas pipelines.[204] These facilities, each representing different key infrastructure components, are modern facilities that are almost completely reliant on modern computer and networking systems.[205] Similar to the circumstances at the Taum Sauk Dam, in subsection II.A.2., a single pipeline facility has thousands of sensors, valves, pumps, and controllers that are operated autonomously through the facility's SCADA system.[206] It is likely the hurricane would trigger a cascading failure where widespread power outages coupled with flood

---

201. *See* JOSEPH KRAMEK, THE CRITICAL INFRASTRUCTURE GAP: U.S. PORT FACILITIES AND CYBER VULNERABILITIES 13–16 (2013), https://www.brookings.edu/wp-content/uploads/2016/06/03-cyber-port-security-kramek.pdf [https://perma.unl.edu/E4F8-NR8F].

202. *Id.*

203. SUSAN VANDIVER ET AL., S. METHODIST UNIV., SYSTEMS ENGINEERING APPROACH TO THE ANALYSIS OF THE CRITICAL INFRASTRUCTURE OF THE UNITED STATES 5 (2004).

204. Roy Scranton, *When the Next Hurricane Hits Texas*, N.Y. TIMES, Oct. 7, 2016, at SR1, https://www.nytimes.com/2016/10/09/opinion/sunday/when-the-hurricane-hits-texas.html.

205. JOSEPH A. WALSH II, CYBER THREATS TO PIPELINE SAFETY: VULNERABILITIES AND EVOLVING STANDARDS OF CARE—WHAT THE C-SUITE AND PRACTITIONER NEEDS TO KNOW (2017).

206. *Id.*

waters would cause extensive damage and destruction to these facilities and sever the distribution networks for the products of these facilities to the broader United States.

A. Applying the Modified Stafford Act to the Hypothetical Hurricane Zoe

Assume Houston's emergency-response managers incorporated the NIST Framework prior to the hurricane. The Governor of Texas determines the destruction is too severe for a state-level response, declares a state of emergency, and requests assistance from the federal government with certification of adoption of the NIST Framework. First, this event would meet the broad definition of an incident causing physical destruction or loss of cyber infrastructure. The definition is not concerned with whether the event was initiated by a cyber system; instead, it is focused on which components are destroyed. In the case of Hurricane Zoe, the storm surge and high winds damaged and destroyed facilities including the SCADA-system hardware on which the facilities rely. Second, the Houston Port Authority, along with state emergency-response authorities, would have been provided grants through FEMA prior to the hurricane to incorporate the NIST Framework in their emergency planning. Utilizing the NIST Framework, the refineries and pipeline operators would have previously identified vulnerabilities within their systems to see what infrastructure components their facility relies on (e.g., electric utilities) and what infrastructure is relied on by other facilities (e.g., transportation and fuel distribution).[207] The key here is these entities would have identified the reliance prior to the hurricane and been able to build redundancy by having backup systems further north, outside likely hurricane zones. Under FEMA's authority and oversight for state preparedness compacts, neighboring states like Oklahoma, Arkansas, and Louisiana would likely be aware of the same linkages and identified backup suppliers or alternate distribution networks for key infrastructure. Finally, FEMA can then provide disaster aid for replacing state-owned cyber infrastructure and coordinating with the SSAs and Small Business Association (SBA) for interest-free loans and other similar forms of relief for the private corporations involved.[208]

207. *Id.*

208. Smith et al., *supra* note 179, at 81 (noting that FEMA empowers state agencies to distribute federal assistance at state level); *see also* Aldy, *supra* note 183, at 1803 (noting that FEMA can utilize SSAs to distribute aid to private parties despite general ban on aid relief to private entities).

B. Loss of Network Communications Between Southeast Texas Refineries, West Texas, and Electric Utilities

The bulk of any destruction related to a natural disaster is typically localized to the area where the event occurred; however, the increasing interconnectivity of autonomous systems allows the reach of an incident to expand.[209] This would be the case if a significant hurricane struck Houston because of the substantial amount of regional infrastructure that relies on Houston's energy sector.[210] This is especially true when it comes to the increasing use of networked and smart electric utilities across all of Texas powered by wind energy.[211] In the case of Hurricane Zoe, the concern is that a widespread destruction of natural gas refining and distribution, a key component to the energy sector, could trigger ripple effects across Texas and neighboring states that would not typically be thought of as at risk from effects of a hurricane in the Gulf of Mexico.[212] Specifically, there is no guarantee the thousands of network nodes and sensors are designed for such catastrophic failure of key pieces of the infrastructure.[213] The risk is that misread or miscommunicated signals can instead overwhelm distant SCADA systems and trigger large-scale power failures.[214]

Applying the new FEMA procedures will garner a similar response to the actual physical destruction of the refineries in Houston. While not directly affected by the hurricane itself, the West Texas windfarms are a part of a complex chain of renewable-power generation that relies on just-in-time supply of natural-gas energy from around the state of Texas.[215] Under the three types of cyber incidents, this would fit squarely in the network-degradation-or-destruction category. The communication infrastructure that empowers these networks, al-

209. Scheuermann, *supra* note 167.
210. Scranton, *supra* note 204.
211. Daniel Gross, *The Night They Drove the Price of Electricity Down*, SLATE (Sept. 18, 2015), http://www.slate.com/articles/business/the_juice/2015/09/texas_electricity_goes_negative_wind_power_was_so_plentiful_one_night_that.html [https://perma.unl.edu/2TCQ-3ERA]. The hallmark of smart grids is "nodes in the electricity network can communicate in real time with one another and respond to new circumstances or needs. If a tornado knocks out the transformer at a gas plant, a smarter grid could quickly pull more power from a wind farm." Rob Verchick, *Our Energy Grid Is Incredibly Vulnerable*, SLATE (Aug. 26, 2016), http://www.slate.com/articles/technology/future_tense/2016/08/our_energy_grid_is_incredibly_vulnerable_to_climate_change.html [https://perma.unl.edu/C2P9-9U9M]. These smart grids can revolutionize how the United States distributes energy by increasing both resiliency and efficiency but are almost totally reliant on robust cyber networking. *Id.*
212. Verchick, *supra* note 211.
213. *Id.*
214. *Id.*
215. Gross, *supra* note 211.

though not physically harmed or destroyed, may nonetheless be offline or require rapid response to avoid broader cascading power failures. The second component, building the NIST Framework into state compacts, is geared toward forcing state utility regulators and private organizations both within and between states to better understand the interdependencies inherent in their critical infrastructure.[216] Here, FEMA's funding authority would enable Texas regulators and state emergency personnel to receive funds to incorporate the NIST Framework into emergency preparation. This preparation would likely have highlighted the interdependency of these systems through application of the NIST Framework to public utilities, specifically addressing contingencies to power generation across the state with the loss of networks and nodes based in the Houston area. Finally, like the physical destruction, the governor's declaration of a natural disaster and certification the NIST Framework was incorporated would authorize FEMA to provide direct assistance to state authorities and coordinate funding and loan relief with the DoE and SBA.[217]

C. Cyber Attacks During Ensuing Hurricane Zoe Emergency Response

The focus of this Comment is to highlight not all cyber incidents or breakdowns are caused by malignant actors. Instead, cybersecurity should be viewed more holistically as a means to maintain the integrity, confidentiality, and availability of computers and computer networks.[218] That said, critical-infrastructure entities and governments at all levels are the victims of regular and expansive cyber attacks, and this will likely increase during some sort of natural disaster or emergency.[219] The Hurricane Zoe hypothetical focuses on how the modifications to the Stafford Act and FEMA's coordination responsibility affect infrastructure at the corporate or government level but have not addressed individual victims of a cyber incident. Often in the aftermath of major natural disasters, opportunistic thieves and criminal groups prey on individuals and companies as they attempt to rebuild.[220] Assume that during Hurricane Zoe, a nonstate criminal group utilizes the disarray after the storm to launch a sophisticated spear-phishing attack on Exxon Mobil.[221] The spear-phishing is

216. Hellmann, *supra* note 86, at 170.
217. Aldy, *supra* note 183, at 1803.
218. PPD-41, *supra* note 100.
219. WALSH, *supra* note 205.
220. Sue Marquette Poremba, *How to Protect Your Identity During a Natural Disaster*, NBC NEWS (May 23, 2011), http://www.nbcnews.com/id/43134564/ns/technology_and_science-security/t/how-protect-your-identity-during-natural-disaster/#.WPDc9VAzqL8 [https://perma.unl.edu/WZB7-BW55].
221. *See* Kim Zetter, *Hacker Lexicon: What is Phishing?*, WIRED (Apr. 7, 2015), https://www.wired.com/2015/04/hacker-lexicon-spear-phishing [https://perma.unl.edu/

targeted at Exxon Mobil's Nigerian headquarters where the thieves pose as staff from the Houston office needing help accessing Exxon Mobil's network for recovery. Posing as Houston engineers, the email states they need help to backup several important files and requests the Nigerian office download the file and upload it to the company server. In reality, the file is a program that installs malware onto the Nigerian system to gain access to Exxon Mobil servers. In the process, the criminal group steals large amounts of sensitive logistical and proprietary data on energy distribution across the United States.

Take a less sinister example where instead of targeting sensitive data that could harm U.S. national security, the criminal group instead launches a spear-phishing attack on Baker Botts LLP, a prestigious Houston law firm with several offices around the world that specializes in energy and natural-resource law. In this attack, the criminal group targets several of the attorneys in the Houston office, hoping to gain access to the firm's London-based office to steal draft agreements for a pending corporate merger. The phishing email poses as the Texas Bar Association and contains a message that the Texas Bar is trying to contact attorneys located in Houston to provide counseling and assistance services. It provides a link to a website to register that secretly contains malware that once uploaded onto the victim's computer is used to gain access to the Baker Botts network.[222]

Both attacks, while targeting two very different types of organizations and two different types of data, would both clearly fall into the criminal realm and outside the scope of FEMA's expanded role of cybersecurity. The central purpose of PPD-41 was to create a clear cybersecurity framework at the federal level, and both of these incidents are classic examples of incidents that should be investigated and addressed through organizations like the Federal Bureau of Investigation (FBI) and potentially DHS's United States Computer Emergency Readiness Team (US-CERT).[223] The goal of incorporating FEMA's coordination authority is primarily to encourage and incentivize, through grants and potentially post-disaster aid, the state and

6F44-CAYQ] (explaining spear-phishing emails are "designed to appear to come from someone the recipient knows and trusts—such as a colleague, business manager, or human resources department" and are "designed to trick [the recipient] into clicking on a malicious attachment or weblink").

222. *See id.*

223. PPD-41, *supra* note 100; *see also* Kim Zetter, *DHS Fears a Modified Stuxnet Could Attack U.S. Infrastructure*, WIRED (July 26, 2011), https://www.wired.com/2011/07/dhs-fears-stuxnet-attacks [https://perma.unl.edu/JWT8-LSVZ] (explaining Stuxnet could be modified to threaten other systems and describing US-CERT as "a division of DHS that is responsible, in part, for coordinating the defense of federal networks and working with the private sector to mitigate cyberattacks against the nation's critical infrastructure").

local levels to proactively address cybersecurity through adoption of the NIST Framework and build better networked ecosystems that take into account both the benefits and risks associated with cyber-enabled systems. In this hypothetical, the goal would be for organizations like Exxon Mobil and Baker Botts to apply the NIST Framework in order to anticipate an increased risk of spear-phishing and to have exercised scenarios detecting and responding to such incidents. Thus, FEMA's central role is to promote coordination on minimizing the harms suffered during a disaster or emergency, or in the words of Ben Franklin, "an ounce of prevention is worth a pound of cure."

V. CONCLUSION

In today's constant news cycle, it is easy to be bombarded by an overly optimistic or pessimistic view of technology. The fact of the matter, however, is technology is neither inherently good nor bad. Instead, society's focus should be on a thoughtful analysis of how to utilize technology and incorporate it into the community. Societies have undoubtedly benefited from the rise of personal computing and the Internet, but with those benefits come associated risks and responsibilities. It is these risks and responsibilities that require a new way of thinking about cybersecurity, especially in critical infrastructure and disaster response. Cyber technology has become interwoven through the rise of smart cities, autonomous systems, and the entire emergency-management apparatus. It is time FEMA and its authorities under the Stafford Act reflect this shift and empower FEMA to serve its coordination role to enable state and local authorities, in partnership with private interests, to build resilient cities and communities for the modern age.