Title

Protecting the Texas Electric Grid: A Cybersecurity Strategy for ERCOT and the PUCT

ISBN

9781728121352

Authors

Stanaland, Les
Baldick, Ross
Cardenas, Alvaro A
et al.

Publication Date

2019-11-04

DOI

10.1109/rws47064.2019.8972002

Peer reviewed

Protecting the Texas Electric Grid: A Cybersecurity Strategy for ERCOT and the PUCT

***Abstract*—The electrical system serves as the fundamental base of a country's economic activity, and it is therefore, a likely target for cyberattacks. As the modern economy continues its evolution towards greater digitization and interconnectedness, policymakers must outline and enforce regulations protecting those critical assets, without which the economy would suffer.**

The Texas Interconnection, due to being independently operated and to a large-extent legislated by the state of Texas, enjoys a simpler regulatory environment than its national counterparts. We exploit this relative independence to offer policy solutions to better protect Texas against a cyberattack on its electric grid. Specifically, ERCOT and the PUCT have the authority and ability to streamline and simplify the potentially confusing protocols enforced by NERC to make adoption more likely. We also discuss grant programs for smaller utilities and the role of cyber-insurance in helping utilities navigate the difficulties in understanding the protocols so that compliance can occur.

I. Introduction and Research Motivation

Two recent events have alerted American policymakers at all levels of government to refocus their efforts on grid security. First, the December 2015 and 2016 successful cyberattacks on the Ukraine's electric infrastructure represented a "wake-up-call" for policymakers, industry insiders, and the population at large. Another warning came in the summer 2017 during an attempted cyberattack on a petrochemical plant in Saudi Arabia. This attack, although foiled due to an error in the code, could have led to a complete takeover of the plant by the attackers, including the possibility of the release of toxic gases (Giles, 2019).

These attacks are not performed by antisocial individuals wishing mayhem. Rather, these attacks are committed by state-sponsored teams working in collaboration with their clients to engage in geopolitical cyberwarfare, representing a new twist in what it means for a country to defend itself against its enemies. The United States is an especially valued target. It is no surprise then that at the legislative and executive levels of government, the US is seeking to harden its grid against such attacks.

However, preventing cyberattacks is expensive, while the events themselves are rare, but extremely disruptive to the economy. Therefore policymakers need to be acutely aware of the risks a successful cyberattack would cause. The Ukraine event makes such a case for preparation and prevention, but only if the various governmental agencies can work together on a specific course of action.

Since cyberattacks have not only private but also social costs, negative externalities arise, leading to underinvestment by the private sector in mitigating the costs. In turn, this proclivity to underinvestment leads to underinsurement: a 2015 Lloyd's white paper (Lloyd's, 2015) suggests that an 'Erebos' malware attack on the eastern US grid could have a $243 billion impact; even if power were restored within 24 hours, many places would be without power for several weeks.

Given the negative externalities of cyberattacks, and their concomitant underinvestment, the proper role of the government should be to invest in such protections at a socially optimal level so that attacks can be prevented. State governments can experiment within an existing framework of cybersecurity standards to find a solution that meets the needs of all stakeholders: governments, utilities, their customers, and regulatory agencies.

II. Goal of this Study

The goal of this white paper is to discuss different policy options that might be applicable to the State of Texas, specifically the Texas Public Utility Commission (PUCT) and the Electrical Reliability Council of Texas (ERCOT). Given its relative energy independence compared to the other states in the US, Texas has a simpler jurisdictional path, granting it more space to experiment with different cybersecurity policy options. NERC CIP standards, which ERCOT must abide by, are a good starting point for such experimentation. The main difficulty will be in compliance of these standards, not in their adoption or implementation; therefore, if solutions for noncompliance can be overcome, the result would be a safer, more secure electric grid for all Texans.

This paper is organized as follows: The overall physical and regulatory environments are described, with a special emphasis on the relative independence of the Texas grid. Next, different state-based approaches to cybersecurity are discussed to give Texas policymakers an idea of what types of solutions are being used throughout the country; 2019 Texas legislation is described to underscore the salience of the issue and how it may impact ERCOT and the PUCT.

The central crux of the paper follows, which is the importance of NERC CIP standards to the cybersecurity of the electric grid. Likelihood of compliance is discussed at a utility level, namely investor-owned utilities, municipalities, and cooperatives. Lastly, reasons for non-compliance are analyzed from a theoretical perspective, and three potential solutions are outlined: a grant program, a streamlined auditing process, and insurance reform.

III. Regulatory Environment

Electricity generation, transmission, distribution, and delivery in the United States is regulated at federal, state, and local levels of government. Three key organizations at the federal level are responsible for ensuring reliable power flow throughout the US - the North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC), and the Department of Energy (DOE). These organizations have statutory authority to ensure that the nation's power grid can effectively and safely handle the nation's increasing electricity demand.

Created in 1968 by the electric industry as a way to coordinate planning and reliability efforts across the US and Canada, NERC now serves as a nationwide Electric Reliability Organization (ERO). Electrical power across Canada and the US is divided into 4 grids, the Quebec, Eastern, Western, and Texas Interconnections. The Texas Interconnection is the only one wholly contained in one geographic state. NERC works with FERC in establishing the necessary guidelines to ensure reliability by subdividing the 4 Interconnections into 7 different reliability entities; this paper will focus on the Electric Reliability Council of Texas (ERCOT) and the Texas Reliability Entity (TRE).

Beginning in 2000, NERC established an analysis center devoted to the protection of the physical and software components and furthered their oversight of the member organizations. After the 2003 blackout, federal legislation was passed granting NERC with its current status as a nationwide reliability organization with legal authority to enforce its rules. In the United States, NERC sets up security protocols through its Critical Infrastructure Plan (CIP) which was created in 2006. While the protocols are created by NERC, they must be approved by FERC to go into effect.

Set up as an independent regulatory agency in the 1930s as electrical systems proliferated throughout the country, FERC is responsible for licensing projects, regulating sales and transmission of natural gas and oil, and ensuring reliability of the transmission systems. Since the Energy Policy Act of 2005, the role of cybersecurity has become an increasingly important regulatory area of concern.

FERC oversees 10 different regional transmission organizations (RTO) which coordinate multi-state (except for Texas) grids in areas of power generation, transmission, and sale. Independent System Operators (ISO) have similar functions; sometimes they operate only in one state, other times in multiple states. RTOs have an added responsibility of transmission planning (FERC Order 2000). The key to the oversight function of FERC resides in US Const, Art 1, Sec. 8 which grants to the federal Congress the authority to "To regulate Commerce with foreign Nations, and among the several States,". Since electric power transmission and sales frequently cross state lines, the federal government has the authority to regulate such actions. However, in the case of Texas, power is generated and sold only within the state; therefore, FERC has no direct authority over ERCOT, except for sales between ERCOT and other regions.

Both FERC, as the government "side", and NERC, as the industry "side", work to oversee the RTOs as they work to ensure reliability on the issue of cybersecurity. Therefore, while there may be investment differences between the RTOs, they all are supposed to abide by the same standards, known as Critical Infrastructure Protection (CIP) standards, which are NERC's protocols for cybersecurity. We focus on these because ERCOT is only held to the NERC standards, and not the FERC. They are however, for all intents and purposes, the same as FERC's protocols.

The CIP standards revolve mainly around traditional expectations of physical security such as controlled access into the facilities, as well as digital-based security for computer network segmentation, access controls, and detection of an attack. Punishments are meted out in case of non-compliance; the same IT survey that demonstrated an overall unreadiness of the grid operators also mentioned a potential weakness is that many operating systems use legacy computer software like Microsoft XP 2014, which due to its common use, is a popular target for hackers who code especially to exploit the weaknesses in that operating system.

IV. Problem of NERC CIP Compliance

A. The industry perspective

Jason Miller, managing partner of the Archer Security Group, a NERC compliance consulting firm, states that overall, CIP standards force compliance, but not necessarily enhanced security or reliability. He further suggests a disconnect between the goal of energy policies and regulations, and how they are being implemented by the industry. The goal is to strengthen the nation's electric grid, but in practice this may merely mean that a company can point to a locked security fence and argue

their facility is secure, in his view. Furthermore, the level of detail found in the CIP standards is meant to allow freedom for different utilities, but instead only adds to the confusion and frustration of working with them. For this reason, Miller states, companies are willing to forgo the standards and take the risk of non-compliance on themselves instead of attempt to reform their facilities to be in compliance.

Secondly, not all utilities are subject to CIP standards. Any utility that either generates or transmits less than 300 MW of electricity is exempt from the requirements. This is approximately 84% of all utilities in Texas. Clearly a problem arises; these utilities, small though they may be, are more susceptible to attack. For example, the Ukraine attack was on three of the dozens of distribution companies in that country. Hackers, be they government-sponsored or not, can study the US' decentralized electrical grid enough to expose weak spots such as these. Electric grid breakdowns are also an area where a panic may set in; previous blackouts in the United States led to a temporary fear about the reliability and security of the system. By starting small, hackers may use these smaller utilities as a "test run." In any case, allowing smaller utilities to continue to be out of compliance with cybersecurity standards needs to be addressed.

In 2009, a self-certification survey perform by NERC found that less than one-third of generation owners believed they had a critical asset which required following CIP standards (Hegrat and Case, 2010). The question then arises—-if this is the case, then why have the standards at all? Miller suggests that the standards do set a "high minimum bar" in best practices. The process works at the individual facility level—utilities are frustrated with the detailed standards and are unsure how to implement them, so they choose a standard that incorporates all equipment (the "high bar") and then uses that standard for all equipment. This process helps utilities streamline their processes while maintaining compliance. The CIP standards take a very decentralized system and attempt to create one set of rules. The problems of CIP compliance are a manifestation of that central issue; some utilities are better equipped to handle the additional requirements while others are not.

Trey Fitzgerald, representing another compliance consulting firm, ABZ, Inc., said on 16 May in a Husch Blackwell webinar that designing programs for CIP compliance is challenging and that CIP 003-7, becoming in force on 1 January 2020 will be even stricter in terms of physical and cyber security. This regulatory update brings to "low" assets what is currently in force for "medium" and "high" impact assets. He implied this may be difficult for low assets to do; this is an area perhaps our policy proposals can aid these utilities currently ranked as "low" impact to meet the upcoming 2020 implementation. Following Miller's argument regarding self-regulation, Fitzgerald mentions that currently the Texas Reliability Entity allows exactly that; the Initial Risk Assessment (IRA) is done at each individual utility level; they document their own internal control effectiveness, with audits and random spot checks being used as the central mechanism by which the regulator ensures compliance.

B. The policy perspective

Both Miller and Fitzgerald, representing the viewpoint of the industry, seeks to minimize costs while also ensuring a well-defended system that complies with all applicable laws. A Brookings Institute white paper by Langham and Pederson (2013) suggests that the entire risk-based approach taken in the US will not result in a safer, more reliable grid, but rather the opposite. Instead, Langham and Pederson argue that the policy effort to shift the burden of cybersecurity onto the private sector will always result in inefficiencies. Instead, they see they problem as inherently political, offering the examples of the air traffic security and pollution, two common public goods, as evidence more federal authority is needed. Their policy solution is to remove the profit motive of the companies by offering tax incentives and subsidies, a solution we also offer.

Also, Langner and Pederson argue for a pragmatic, gradual approach by only incorporating new standards into newly built equipment; retrofitting is cumbersome and expensive, leading to companies balking at its cost. If that private sector critique of increased standards is also removed, the authors suppose the overall grid will become more secure. Lastly, they argue that utility companies ought not see only critical systems as worthy of protection, but rather all of the systems, implying a more holistic approach that what is currently done.

Our policy prescriptions take from both perspectives; it would be imprudent to only look at one side of this complicated issue since it is clear that both governments and the private sector have a role and a stake in the cybersecurity of the electric grid. Both of their respective interests must be taken into account in any solution.

V. State Approaches to Cybersecurity in the Power Grid

Since cyberattacks are such high impact, low probability events, the federal and state governments have a difficult time in knowing the best methods to detect and defeat them. Cohen and Nussbaum (2018) studied three different approaches to cybersecurity in Arizona, New Jersey, and Washington and compared them to gather insights into best practices. Arizona's "community

approach" leverages relevant public-private partnerships to keep each other abreast of any cybersecurity issues or development opportunities. New Jersey's "bureaucratic superstructure" used the public sector as a centralized organizer from which decisions are handed down to utility companies. Lastly, the Washington "multidisciplinary" approach melds the public sector organizational structure of the New Jersey model with the private-public trust model of Arizona to create, in their view, a mature model of how cybersecurity issues ought to be handled. Here, the state government has in essence an IT department for the state. Utility companies then have individual IT departments which must coordinate with the state office on cyber issues and compliance.

The Texas approach is more akin to the Arizona model than the other two, but it is possible that given ERCOT's independence, the centralizing aspect of cyber coordination as found in the Washington model is still possible; however those functions would be carried out by ERCOT and not the state of Texas. The Cybersecurity Act of 2017 (HB 8) in Texas, signed in June of 2017 by Governor Abbott, strengthened the requirements for state agencies in how they handle data; this could be the beginning of a move towards the Washington model if they so choose because it allows for information-sharing programs to be used for all "state agencies and political subdivisions."

This move towards greater public and private cooperation could also ensure communication between all parties can lead to more rapid reactions.

A clear dividing line in the regulatory environment is between the bulk transmission of electricity and its distribution. NERC and FERC have regulatory authority over the transmission, but not the distribution. Here is where state legislatures, along with their respective utility commissions, can enhance the strength of the entire electric grid. Caution is warranted here, however, as most state laws around cybersecurity deal with state records and best practices such as training for employees to detect a phishing email. These cybersecurity laws do not speak to strengthening their electric grids.

Michigan, Pennsylvania, California, and Texas have created regulations that enforce mandatory reporting requirements on investor-owned utilities and electric coops. The Michigan Public Service Commission (MPSC) uses the NIST protocol for cybersecurity, but has made no further additions (California PUC report). The Pennsylvania PUC has a review process in which audits are done for all investor-owned utilities every five years, while California has incorporated cybersecurity protections into its laws on data privacy.

VI. How Texas can lead the way

A. ERCOT

Given the fact that Texas' electric grid was kept independent, ERCOT is the only RTO that is not directly regulated by the federal government. So for the 75% of Texans who get their electricity from ERCOT, most of them have a deregulated electricity market in which they can compare rates and buy from several different retailers. Under the 2002 law, unless electricity is provided by a cooperative or municipality, consumers are given choice. It also sets ERCOT as the primary transmission and distribution authority, and grants to the Texas Reliability Entity the job of ensuring that ERCOT is meeting all applicable federal reliability standards. As the sole RTO for the Texas Interconnection, it is independent of all the other grids and interconnections, with only two ties to the Eastern Interconnection and one to the Western Interconnection.

While states have authority to regulate the distribution and sale of power within their borders, the independence of the ERCOT connection means that the Texas legislature has more power than other states in regulating the generation and transmission of power. This is done through the Public Utility Commission; they are responsible for both the generation/transmission and the consumption side for the entire state, not just ERCOT.

B. PUCT

The PUCT can use its relative independence from FERC as well as its role as chief regulator for both the generation and transmission sides of the industry to better effect change in how utilities in Texas apply the CIP standards. In the ERCOT region of Texas, the regulatory structure is easier to navigate than its national counterparts, the Eastern and Western Interconnections. For this reason, they can more efficiently implement policies meant to incorporate the CIP standards by listening to utility company concerns, working with ERCOT (at least in the beginning, future work could branch out to the remaining parts of Texas not under ERCOT authority), and can work with the legislature on any potential reforms. In short, Texas can take advantage of its independence in such a way that allows centralized solutions to be tested and improved upon.

Since only one state government and regulatory authority are the key decision makers, no other state or electricity interconnection can experiment with regulations like Texas can. The main issue, which we would expect would be similar in other areas, is that different utilities have different acceptance preferences of new or increased regulation.

In summation, the overall problem of CIP standards from the utilities' point of view is that they are too

difficult to understand and implement, leading them to avoidance when possible. Secondly, if procurement companies and other vendors don't wish to incorporate CIP into their products, they will "no bid" jobs and force the utility to either abandon the standards to pay a premium for the work. On the supply side, they enforce compliance without adequately providing an increase in security or reliability. Texas is uniquely placed among the states as a laboratory to experiment and improve the standards at the supply and demand levels.

C. Current legislation

To that end, the Texas legislature, realizing the importance of the issue, in the 2019 session has introduced two more bills aimed at strengthening cybersecurity readiness. Senate Bills 936 and 475 take complementing approaches; 936 allows the PUCT to assign a cybersecurity monitor to electric utilities that are not exempt. Utilities not in the ERCOT region would have the ability to refuse participation; municipalities and coops would also be exempt. The bill was passed unanimously. Likewise, Senate Bill 475 sets up an electric grid security council with the goal of serving as a body that can recommend best security practices and preparation against attacks. Together, these two bills give ERCOT and the PUCT the authority they need to begin grid strengthening; however, SB 936 exempts many utilities and SB 475 only allows for the security council to amend that state's emergency plan *after* an attack. These bills are evidence though that policymakers are taking the issue seriously; ERCOT and the PUCT can use this opportunity to create wise regulations to better protect the grid.

In the next section, we look at the different characteristics of the three types of utility companies to find if potential solutions can be tailored to the industry at a granular level. A solution to CIP standards implementation may be found in the fact that electric utilities can be one of three types: Investor-owned, municipal, or cooperative. The differences of each utility type may allow for exogenous experimentation based on their individual preferences.

VII. Potential solutions

The 300 MW requirement allows most municipalities[1] and cooperatives in Texas to avoid CIP standards; however better protection of the grid is still needed. A key insight into the fundamental weakness of the current approach is that the successful attacks witnessed to date have been on the *distribution* systems, and not the generation systems. CIP standards focus on protecting generation assets. However, a cyberattacker may still cause significant damages by targeting distribution utilities.

Potential solutions coming from the state regulatory agencies must then take these realities into account. By doing so, we will advocate for two seemingly divergent tactics: a centralization of communication at the state regulatory level, but increased flexibility to effectively deal with problems at the individual utility level. First, we advise that Texas adopts the Washington model as described by Cohen and Nussbaum (2018) to create both a bureaucratic hierarchy within the regulatory agencies to centralize command and communication operations. This way, the state agency can be quickly notified of any problems at the individual level; solutions can be crafted by utilizing power from other plants. In this model, the existing "public-private" partnerships that exist in Texas can be augmented with ERCOT and the PUCT providing best practices and a clearinghouse for communications.

From a technical standpoint, this strengthening of partnerships would take place through the enhancement of existing Information and Communications technologies (ICT) approaches. Called the "E + I" paradigm, Masera (2010) suggests that a complete integration of the electricity (E) components merge with the information (I) components to create a more robust technological apparatus than currently exists. This robustness would lead to real-time cooperation and coordination (Bialek, 2010). Through this process, cyber attacks or load imbalances could more quickly be remedied.

With this new approach to regulation, communication, and organization in place, we then suggest the following three options that the PUCT and/or ERCOT can implement to harden the electricity infrastructure in the state of Texas: 1) Establish a grant program for CIP compliance specifically aimed at municipalities and cooperatives, 2) Streamline the auditing process to set one "high water mark" for meeting standards, and 3) promote the role of grid insurance companies.

The first two options are preventative in nature; if implemented, they should make it less likely that a successful attack will occur. The third revolves around a market-based solution to the negative externality aspect of cyberattacks. If insurance companies began to demand CIP compliance as a precondition for coverage, utilities may respond favorably.

A. Grant program

A common criticism of regulation is its cost to the agency responsible for its implementation. CIP standards increase the cost to an organization; it is more expensive to harden infrastructure than leaving it in a less protected state. Therefore, it could be the case that utilities want to adopt the standards or are at best ambivalent towards

[1] Clearly the largest exceptions would the Austin and San Antonio areas, which easily have more than 300 MW in output

them; they simply blanch at their costs. Here a grant program designed either by the state or within ERCOT's or the PUCT's existing budgets could be used to ameliorate this concern. It could also be used to strictly enforce the standards; continued funding could be conditional upon meeting the guidelines ERCOT sets.

This funding mechanism could give utilities the "nudge" they need to incorporate CIP standards over their objections. This program should be geared towards municipalities and cooperatives, as IOUs are already implementing these standards largely as a result of regulatory fiat. As previously mentioned, since municipalities and cooperatives don't face the same regulations, reform may be more difficult.

B. Streamline the auditing process

A major area of confusion regarding CIP compliance revolves around the different standards assigned to different pieces of equipment. If each different piece of equipment in a grid has a separate standard, then we would expect workers to eventually find themselves exasperated at the idea of compliance. Miller found their way "around" the standards was to analyze the most stringent standard, and then adopt it as a "high-water" mark for *all* equipment, while Fitzgerald argued that internal compliance programs were difficult policy instruments to create, especially for "low" impact utilities.

If the process is made simpler through a streamlined process in which most, if not all, equipment is held to the same CIP standard, then utilities would be able to easier handle compliance, and, perhaps more importantly, regulators could become more efficient at performing audits and spot checks. If the audits are too infrequent, then utilities may get lax in their internal processes; if spot checks aren't robust enough, the same result may occur.

ERCOT and the PUCT could alter their regulations to allow this streamlining. This solution would remove another key objection to the standards; if they are easier to understand and implement, they are more likely to be incorporated. Likewise, if utilities better understood what constituted a violation versus what was acceptable, then adoption could be more robust across all utility types.

C. Insurance Reform

The last mechanism to enhance Texas utilities' cybersecurity protection is found in the insurance industry. A burgeoning industry for the last 10 years, cyber insurance has attempted to solve three problems: one, pooling and transferring risk, two, protection and prevention of data breaches, and three, compliance aid (Talesh, 2018). This third area of focus is a possible solution for recalcitrant utilities. If they are refusing to abide by CIP standards because they are too burdensome (Miller interview), then their insurance company could offer to fill in that gap and offer services to better aid in their compliance.

If utilities aren't adopting CIP standards because they fall under the 300 MW output standard, then insurance companies could still discuss the utility's exposure in a worst-case scenario. It could be that utilities think it is worth the risk to not be in compliance, but that may not be the case. Likewise, nothing is preventing insurance companies from going beyond the existing CIP standards and selling policies dependent upon adoption of such standards. Insua and Musaraj (2018) find in their risk analysis that segmentation of the cyber insurance market can force reinsurers to demand stronger policies; the risk of a cascade failure for them would be potentially ruinous.

Disaster insurance is a common approach for businesses to mitigate risks of events they cannot control; usually these types of policies refer to "Acts of God" or *force majeure* to denote protection for things completely outside the control of the insured. One historical example would be the 1906 San Francisco earthquake and subsequent fires. Damage to the city's gas mains lead to the fires, which ended up causing more damage to the city than the earthquake. Subsequent analysis found that the fire damage was greater because of the risk exposure: fire damage was covered, while earthquake damage was not. Telegraph evidence of the time found that people were committing arson on their own property so that they could recoup their losses.[2] The reason for this lack of coverage was that at the time, earthquakes were considered "uninsurable"; this event led directly to insurers beginning to model natural disasters (Brady, 2006).

Another historical example of a low probability, high impact event that went from uninsurable to insurable was 9/11. The idea of terrorism insurance was quite rare at the time; however, in the aftermath of the attacks, the US federal government passed the Terrorism Risk Insurance Act of 2002 so that the government could serve as a "backstop" for any claimed losses as a result of the attack. This government action took place because of the market failure; both insurers and reinsurers didn't appropriately price terrorism likelihood and immediately left the market due to overexposure.

These two historical examples give us the outline of an approach that ERCOT can use in the area of cybersecurity. First, it should be mentioned that progress in the industry didn't occur until *after* an attack had occurred - earthquakes in one, terrorism in the other. Texas should want to avoid the possibility of insurance market reform only after an attack; a more proactive response is preferable to waiting for a cyberattack to

[2] http://www.sfmuseum.org/1906.2/arson.html

happen. Second, insurers will not enter a market unless they can appropriately price the risk; they have a self-interest to make sure they don't unwittingly bankrupt themselves. If we surmise that cybersecurity insurance doesn't exist because it cannot be modeled, we propose a public-private partnership of sorts whereby ERCOT and/or the PUCT "game" the possibilities of what different types of cyberattacks on various utility generation and transmission companies would do to the companies' infrastructure. This data could in turn be shared with insurance and reinsurance companies so they could model and therefore price the risk.

Under this approach, the state of Texas would not have to backstop utilities in the aftermath of an attack like the US did after 9/11; this would be prohibitively expensive for the state. On the other hand, the state government, as well as ERCOT, has an interest preventing cyberattacks. Insurance companies have no issues with insuring against low probability, high impact events, but they must be able to model the risk. This policy solution answers both concerns.

A current area where this type of collaborative approach is working is in the pricing of climate change insurance. The state of Washington is working with insurance companies to model and price the expected effects of natural disasters strengthened by climate change (Washington Office of the Insurance Commissioner). The key difference between pricing climate change and cyberattacks, however, is that a cyberattack cannot be forecast like the effects of climate change. This is where ERCOT can use its expertise of the industry to forecast where an attack is likely to be.

VIII. Conclusion

As global technological interconnectedness proliferates, policymakers face increasing cyber threats against their critical infrastructure systems. The decentralized nature of the US grid makes coordinated responses to such an attack more difficult; however, it also reduces the likelihood of a catastrophic event. The state of Texas, along with the Public Utility Commission and ERCOT, has an opportunity to lead the way forward of grid preparedness due to its relative independence from federal regulations.

Through leveraging its regulatory independence, Texas can experiment with stronger security protocols as well as policy reforms to make cybersecurity adoption more robust across the electric grid. Specifically, the Texas legislature can create a grant fund, to be assigned through ERCOT and/or the PUCT, for municipalities and cooperatives who may be more hesitant to adopt the reforms. Also, ERCOT and the PUCT can take the existing NERC CIP standards and remove their more confusing aspects, thereby streamlining the compliance aspect. Finally, they can ensure that utilities still unwilling to adopt standards can implement more robust procedures for a quick transition away from a digital operating process to a manual one in the case of an attack, thereby removing the affected utility from the remainder of the grid.

Acknowledgments

This work was supported in part by NSF CRISP awards CMMI-1925524 and CMMI-1541159, and by the Texas National Security Network.

References

Bialek, J. W. (2010). Critical interrelations between ict and and electricity systems. In Z. Lukszo, G. Deconinck, and M. P. C. Weijnen (Eds.), *Securing electricity supply in the cyber age: Exploring the risks of information and communications technology in tomorrow's electricity infrastructure*, Chapter 4, pp. 53–70. London: Springer.

Brady, M. (2006). 1906 san francisco earthquake shook up the insurance industry worldwide. *National Underwriter Property & Casualty*.

Cohen, N. and B. Nussbaum (2018). Cybersecurity for the states: lessons from across america. *New America Working Paper*.

Giles, M. (2019). Triton is the world's most murderous malware, and it's spreading. *MIT Technology Review*.

Hegrat, B. and C. Case (2010). Protecting critical infrastructure and cyber assets in power generation and distribution. *Rockwell Automation*.

Insua, David Rios, A. C.-V. and K. Musaraj (2018). Some risk analysis problems in cyber insurance economics. *Estudios de Economia Aplicada 36*(1), 181–194.

Langham, R. and P. Pederson (2013). Bound to fail; why cyber security risk cannot simply be 'managed' away. *Brookings Institution*.

Lloyd's (2015). Business blackout: The insurance implications of a cyber attack on the us power grid. *Emerging Risk Report, Innovation Series*.

Masera, M. (2010). Governance: How to deal with ict security in the power infrastructure? In Z. Lukszo, G. Deconinck, and M. P. C. Weijnen (Eds.), *Securing electricity supply in the cyber age: Exploring the risks of information and communications technology in tomorrow's electricity infrastructure*, Chapter 6, pp. 111–128. London: Springer.

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: how insurance companies act as 'compliance managers' for businesses. *Law & Social Inquiry 43*(2), 417–440.