2019-09

Analysis of Energy Delivery Sector Malware Attack Response Mechanisms

Sapienza, Michael

Monterey, California. Naval Postgraduate School

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 18-09-2019	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE
Analysis of Energy Delivery Sector Malware Attack Response Mechanisms

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Sapienza, Michael, L, LCDR

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Civilian Institutions Office (Code 522)
Naval Postgraduate School
1 University Circle, Herrmann Hall Rm HE046
Monterey, CA 93943-5033

10. SPONSOR/MONITOR'S ACRONYM(S)
NPS CIVINS

11. SPONSORING/MONITORING AGENCY REPORT NUMBER

12. DISTRIBUTION AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Recent cyberattacks on the electricity grids in the U.S. and Ukraine, the rise of malware tailored to industrial control systems, failure of basic sanitary and life-saving systems after prolonged power outages, economic losses numbering in the billions: these are the consequences of malware attacks on critical infrastructure sectors across the globe. New and continuously evolving cyber threats demand new and better response mechanisms to mitigate their effects. However, critical infrastructure sectors, and the electricity subsector in particular, are faced with the enormous challenge of identifying gaps in their extremely complex cyber incident response mechanisms.
This thesis takes a novel, systems-level approach to pinpoint deficiencies in incident response mechanisms of the U.S. electricity sector. An analysis of current and future external influences on the electricity sector validates that malware threats and vulnerabilities are rapidly evolving and are already outpacing the sector's ability to adapt its cyber incident response mechanisms. Using the Architecting Innovative Enterprise Strategies (ARIES) Framework to explore current incident response mechanisms reveals that the traditional, all-hazards approach to major incident response is insufficient to keep the grid secure. Instead, improvements in cyber incident response strategies, processes, organizations, information flow, products, and services are all necessary to overcome the disparity. Most importantly, the systems-level approach exposes the culture of cybersecurity in the sector is the systemic driver of those shortfalls and must be the primary consideration for improvement to the electricity sector's cyber incident response mechanisms.

15. SUBJECT TERMS

malware attack, cyberattack, cyber response, industrial control systems, operational technology, electricity sector, energy sector

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	180	**19b. TELEPONE NUMBER (*Include area code)***

THIS PAGE INTENTIONALLY LEFT BLANK

Analysis of Energy Delivery Sector Malware Attack Response Mechanisms

by

Michael Louis Sapienza

Master of Science in Applied Physics
Naval Postgraduate School, 2009

Bachelor of Science in Mechanical Engineering
United States Naval Academy, 2008

Submitted to the System Design and Management Program
in partial fulfillment of the requirements for the degree of

Master of Science in Engineering and Management
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2019

Signature of Author...
System Design and Management Program
July 12, 2019

Certified by ....
Stuart Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management &
Professor of Engineering Systems, MIT School of Engineering
Thesis Supervisor

Certified by ....
Keri Pearlson
Executive Director
Cybersecurity at MIT Sloan
Thesis Supervisor

Accepted by ....
Joan S. Rubin
Executive Director, System Design and Management Program

PAGE INTENTIONALLY LEFT BLANK

Analysis of Malware Attack Response Mechanisms in the Energy Delivery Sector

by

Michael Louis Sapienza

Submitted to the System Design and Management Program on July 12, 2019 in partial fulfillment of the requirements for the degree of Master of Science in Engineering and Management

Abstract

Recent cyberattacks on the electricity grids in the U.S. and Ukraine, the rise of malware tailored to industrial control systems, failure of basic sanitary and life-saving systems after prolonged power outages, economic losses numbering in the billions: these are the consequences of malware attacks on critical infrastructure sectors across the globe. New and continuously evolving cyber threats demand new and better response mechanisms to mitigate their effects. However, critical infrastructure sectors, and the electricity subsector in particular, are faced with the enormous challenge of identifying gaps in their extremely complex cyber incident response mechanisms.

This thesis takes a novel, systems-level approach to pinpoint deficiencies in incident response mechanisms of the U.S. electricity sector. An analysis of current and future external influences on the electricity sector validates that malware threats and vulnerabilities are rapidly evolving and are already outpacing the sector's ability to adapt its cyber incident response mechanisms. Using the Architecting Innovative Enterprise Strategies (ARIES) Framework to explore current incident response mechanisms reveals that the traditional, all-hazards approach to major incident response is insufficient to keep the grid secure. Instead, improvements in cyber incident response strategies, processes, organizations, information flow, products, and services are all necessary to overcome the disparity. Most importantly, the systems-level approach exposes the culture of cybersecurity in the sector is the systemic driver of those shortfalls and must be the primary consideration for improvement to the electricity sector's cyber incident response mechanisms.

Thesis Supervisors:

Stuart Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management & Professor of Engineering Systems, MIT School of Engineering

Keri Pearlson
Executive Director, Cybersecurity at MIT Sloan

Acknowledgments

I would first like to thank Dr. Keri Pearlson and Dr. Stuart Madnick for the opportunity to work with Cybersecurity at MIT Sloan on this project. Keri unselfishly dedicated her time to supporting me through not only the research but my time here at MIT. I simply could not have done it without her help. Stu allowed me to become a part of his incredible team who are doing incredible things in the world of cybersecurity. It has been an honor.

To the REMEDYS team, Jim, Marissa, Joe, Jess, and Bary, thank you for laying the foundation of this important work, allowing me to learn and contribute to the team, and enabling me to continue working on the problem. I hope we get to collaborate on this work in the future.

This work would not have been possible without the kind support of the Cyber Resilient Energy Delivery Consortium. CREDC staff and members assisted me with engaging stakeholders, sharing research, and providing direction that was integral to completing my thesis.

I would also like to thank Mike Steinmetz, the Rhode Island State Cybersecurity Officer, for his invaluable insight into the cybersecurity and operations of the electric grid. His perspective set the foundation for the work laid out within this thesis. And, thanks to all of the other members of the electricity sector who contributed to this work and sincerely want to make the world more cybersecure but preferred to remain nameless.

Next, I would like to thank Dr. Donna Rhodes, who introduced me to her Architecting Innovative Enterprise Strategy Framework. Her astute guidance on how to present the problem in this thesis made the process not only easier but much more enlightening. I am continually learning from the wisdom she has imparted on me.

To the countless MIT faculty and staff, especially those in the System Design and Management program – Joan Rubin, Bryan Moser, Bill Foley, whose desire to help not only a student but to eagerly explore the hard problems, thank you. I have yet to be turned away from anyone whose door I knocked on seeking advice, and to a person, they have all embraced my questions and spent valuable time to assist me on my educational journey. It has been an incredible experience to be part of the MIT community, where everyone genuinely wants to help.

Finally, I would like to thank my family for your love, support, and patience at yet another challenging tour. To Elaine, I truly humbled that you continue to choose me and grateful beyond measure to journey through this world with you. To Allie, I learned more from watching you grow this year than in any of my classes and am so proud to be your Dada. To baby #2, who won’t be here in time for submission of this thesis, I can’t wait to meet you and welcome you into this world – it’s such a fascinating place.

Funding:

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780.

Disclaimer:

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of the author expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Table of Contents

List of Figures

List of Tables

1 Introduction

> *The uncomforting reality is that the majority of asset owners in critical infrastructure, and maybe even those within the U.S. Department of Homeland Security who are responsible for assisting them, would have no idea what to do when learning that a significant cyber attack was imminent. Until this changes, the authors suggest to put less emphasis on information sharing. Where warning time will predictably always be far short of adequate, preparedness must become a strategic priority.*
>
> *– Ralph Langner and Perry Pederson,*
> Bound to Fail: Why Cyber Security Risk
> Cannot Be "Managed" Away [1]

Numerous public and private organizations, as well as many public-private partnerships (PPP), provide valuable cyber resilience services, such as information sharing and malware analysis, to the energy delivery sector (EDS) [2]. Yet there are strong indications, from Federal authorities and private utility companies alike, that dedicated mechanisms capable of coordinating EDS stakeholders to pre-empt, intercept, and otherwise respond to a widespread cyber event is necessary to avoid catastrophic failure of critical infrastructure, loss of life, and adverse economic impact [3], [4].

This thesis supports the Cybersecurity at MIT Sloan (CAMS) project Response Examination of Malware Attacks on the Energy Delivery sector (REMAED) sponsored by the Cyber Resilient Energy Delivery Consortium (CREDC). CREDC is funded by the Department of Energy's Office of Electricity and the Department of Homeland Security Science and Technology Directorate. REMAED is part of an overarching effort to initiate the transformation of the energy delivery sector's approach to responding to cyberattacks. Its objective is to provide a tool to identify deficiencies of cyberattack response on a sector-wide scale and educate EDS stakeholders on unknown complexities of the sector. REMAED examines the EDS, specifically the electricity subsector, to identify requirements of mechanisms capable of coordinating preemptive and reactive response efforts within the electricity subsector.

1.1 Motivation

REMAED builds upon the foundational research performed in the Department of Energy-sponsor project, Research Exploring Malware in the Energy DeliverY Sector (REMEDYS) conducted from 2017 to 2018. REMEDYS discovered that there was no single entity responsible for coordinating a response to a cyber-attack on the electricity sector. Instead, there are multiple agencies and organizations responsible for many, but not all, of the actions necessary to respond to a cyber event. Similarly, REMAED uncovered that the fragmented nature of cyber response in the EDS contributes to significant misunderstanding over the required actions, sector capabilities, roles, responsibilities, and prioritization of resources for cyber event response. Preliminary analysis suggests that this misunderstanding could result in a slower cyber response, particularly for a more significant attack, than if more robust mechanisms were in place.

Moreover, Madnick (2017) highlights examples of the U.S.'s lack of preparedness and its potential consequences on the grid [5]. He, too, concludes that a systems-level approach to cyber preparedness is necessary to mitigate the impact of a major cyberattack. Other studies show that the economic impact for a large scale cyberattack, though not easy to perpetrate, could result in losses between $243B to $1T [6].

Further, cyber resilience approaches for all sectors tend to be reactive and backward-looking as a function of the economic and political factors that influence critical infrastructure sectors. Four primary drivers motivate research into the area of electricity sector cyber response to support a more proactive stance, and each is explored in greater detail in Chapter 2:

1. Recent high profile cyber events affecting the electrical grid in Ukraine and the U.S. that demonstrate the feasibility of widespread cyberattacks and a sharp rise in cyberattacks on critical infrastructure throughout the world [7], [8], [9]
2. Increasingly capable and sophisticated cyber actors and malware [10]
3. The evolution of the energy industry towards the Internet of Things (IoT), smart technologies, distributed energy resources (DERs), and other significant changes in grid architecture that increases the threat surface of the grid [11], [12], [13], [14]
4. Lack of consensus about standards of cyber resilience, roles and responsibilities for a response to a cyberattack, and the nature of cyber threats to the electricity sector stakeholders

Finally, in the Department of Energy's "Assessment of Electricity Disruption Incident Response Capabilities" (2017), the Department rightfully noted that existing response mechanisms focus on severe weather, and while a cyber incident might have many similarities, there are significant differences which must be addressed, including:

(1) no-notice events that prevent the electricity subsector from taking preemptive measures to protect the electricity system, develop restoration plans, or activate key personnel;
(2) unpredictable system responses due to the potentially disparate nature of the impacts and/or the simultaneous failure of targeted critical components;
(3) the additional time required to perform system diagnostics following an incident;
(4) available expertise in cybersecurity, ICS, and other potentially impacted segments of grid operations; and
(5) the ability of existing response mechanisms to fully support restoration due to many complicating factors [3, p. vi]

Additionally, the report notes gaps in the electricity sector's cyber response mechanisms but takes a Federal Government-centric view of the problem and its solution. To accurately assess the electricity sector's ability to respond, an analysis must impartially view the sector through a lens that is independent of influences of existing mechanisms, technologies, political, threats, regulatory, and market factors.

1.2 Objective

The objective of this thesis is to support REMAED by identifying possible improvements in existing cyberattack response mechanisms and current gaps that require new mechanisms to accelerate the U.S. electricity sector's response and better inform risk management decisions.

1.3 Key Terminology

1.3.1 Definition of the Electricity Subsector

Throughout this thesis, the term electricity sector, electricity subsector, and electricity industry are synonymous and include entities that:

- Produce electricity (e.g., private utility companies, municipal electricity utilities, etc.),
- Support electricity production by providing ancillary products and services (e.g., electrical hardware manufacturers, cybersecurity professionals, etc.), and
- Publicly govern it (e.g., Department of Energy, state utility commissions, etc.).

This thesis establishes the terminology as a boundary around those entities specifically because they include all the required elements for the transformation of cyber response mechanisms in the electricity sector. The World Economic Forum captures all of these entities in Figure 1.1 [15, p. 6].

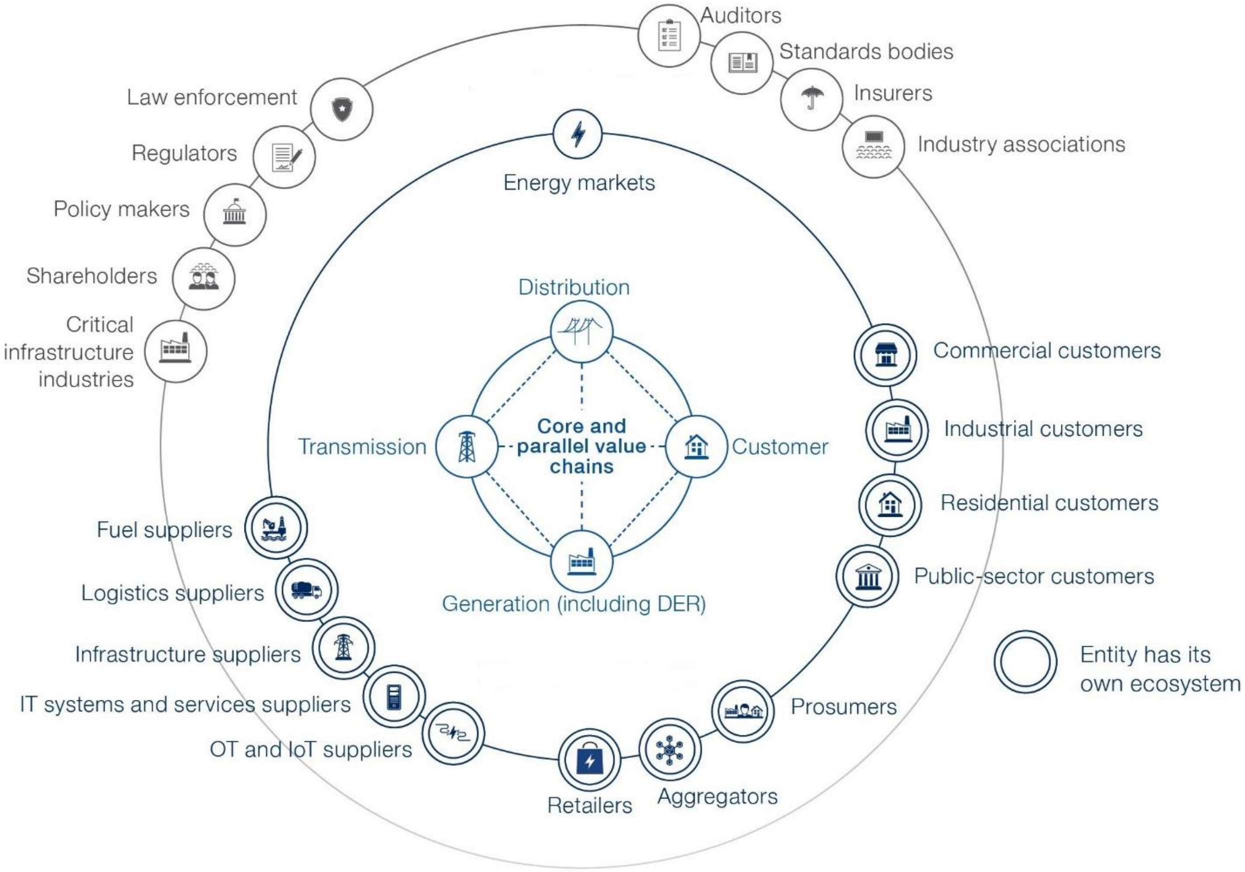


Figure 1.1: Entities in the Electricity Subsector

Though also tempting to use the term ecosystem to describe such an expansive view of a sector, the methodology used in this thesis considers the word ecosystem as a term that distinguishes external stakeholders and factors from internal ones. Since nearly all of the stakeholders in, what would otherwise be termed the electricity ecosystem, are included in the analysis, it does not meet this definition.

1.3.2 Definitions of Electricity Reliability and Resilience

The reliability of electricity can be thought of as the ability of the electricity subsector "to deliver electricity in the quantity and quality demanded by users" [16, p. 1]. More specifically, it involves the planning and operations of the power system and includes "ancillary services" to balance between the supply and demand of electricity in real time. Actions such as frequency support, ramping and balancing of generation, and voltage support that keep electricity consistently accessible to consumers fall into this category [17], [18]. The North American Electricity Reliability Corporation (NERC), the primary entity responsible for enforcing electricity reliability for nationally regulated components of the electrical system, uses two terms to describe reliability:

> ***Adequacy****. The ability of the electricity system to supply the aggregate electrical demand and energy requirements of the end-use customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.*
>
> ***Operating Reliability****. The ability of the bulk power system [BPS] to withstand sudden disturbances, such as electricity short circuits or unanticipated loss of system elements from credible contingencies, while avoiding uncontrolled cascading blackouts or damage to equipment [19, p. 2].*

By some measures, reliability is considered distinct from, but inherently intertwined with, electricity resilience [16]. NERC, however, considers grid resilience as a component of operational reliability and has adopted the National Infrastructure Advisory Council (NIAC) definition of infrastructure resilience. NIAC's defines resilience as the ability to reduce the magnitude and duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its "ability to anticipate, absorb, adapt to, and rapidly recover from a potentially disruptive event," and is the accepted standard for critical infrastructure sectors [20, p. 8], [21]. NIAC also developed a four-feature resilience construct, as shown in Figure 1.2, which further clarifies the components of resilience [21, p. 17].

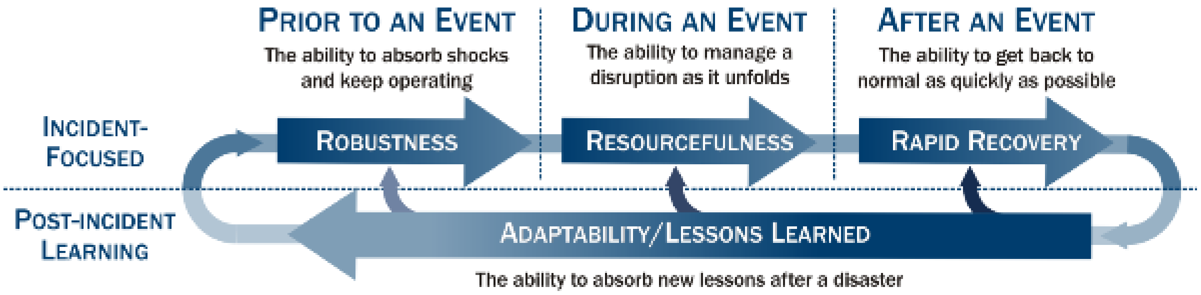

PRIOR TO AN EVENT
The ability to absorb shocks and keep operating
DURING AN EVENT
The ability to manage a disruption as it unfolds
AFTER AN EVENT
The ability to get back to normal as quickly as possible
INCIDENT-FOCUSED
ROBUSTNESS
RESOURCEFULNESS
RAPID RECOVERY
POST-INCIDENT LEARNING
ADAPTABILITY/LESSONS LEARNED
The ability to absorb new lessons after a disaster

Figure 1.2: NIAC Resilience Construct

Thus, in this thesis, cyber resilience in the electricity sector is the ability to reduce the magnitude and duration of cyber incidents on the electricity system by increasing its ability to anticipate, absorb, adapt to, and rapidly recover from them.

1.3.3 Definition of Cyberattack

REMAED focuses on the specific requirements for the electricity subsector to respond to a malware attack as differentiated from other categories of cyberattacks, collectively referred to as cyber incidents or cyber events. Within this thesis, however, the term cyberattack refers to malware attacks and other enabling or packaged cyber threat vectors for the following reasons. First, the nature of actual cyber incidents reveals a trend to use multiple attack vectors, such as a combination of phishing and malware to gain access to a utility's control system environment. Second, as is shown in subsequent chapters, it is often difficult to diagnose the cause of an electrical system malfunction and distinguish between system failure and malicious acts. Likewise, it is difficult to quickly identify and distinguish between the type of attack vector since the immediate effects are similar if not identical. Thus, most cyber response actions, which are primarily concerned with prompt restoration power and recovery of operating systems, are uniform, regardless of threat vector, similar to the Federal Emergency Management Agency's all-hazards model [22]. The need for specific malware response mechanisms separate from other attack vectors still exists. Where those mechanisms appear within this thesis, they are so designated.

1.3.4 Definition of Widespread

REMAED focuses on cyberattacks that are widespread. In this thesis, the term widespread, large-scale, and at scale are used synonymously to represent a cyberattack that affects or has the potential to affect multiple utility systems. In particular, the definition used herein refers to the point at which internal or individual cyber response mechanisms of an electric utility, or multiple utilities, are no longer adequate to operate the utility system reliably. In this case, consequences could result in power outages, brownouts, physical infrastructure damage, loss of control by system operators, or some combination of the above.

Such a cyberattack may affect entire regions or, conversely, noncontiguous geographical areas with similar utility systems. Similarly, the number of utility companies affected does not indicate the scale of the attack. For instance, if a single, large utility that provides electricity across multiple states is infected with malware, loses the ability to provide power to portions of its consumers, and cannot respond with its internal processes and resources, it would be considered a widespread cyberattack.

Additionally, the use of widespread is also assumed to have a temporal element, namely that because the requirement to coordinate and obtain external resources, the response would likely take longer and the consequences would have a longer duration. Specifically, this paper adopts the Department of Homeland Security's definition of long-term interruption of reliable electricity provision, which is an interruption lasting 72 hours or longer [23].

1.3.5 Definition of Cyber Response

Additionally, this paper focuses solely on cyber incident response, or synonymously, cyber response. The spectrum of cybersecurity functions runs from identifying risks to recovery from an incident. Where cyber response begins and ends on the spectrum is difficult to ascertain as the functions are generally considered to be concurrent and continuous. Still, there are aspects of effective cyber response mechanisms which necessitate that measures be put in place before an attack to enable response and, likewise, to facilitate a transition to the recovery phase.

Nearly all sectors recognize the National Institute of Standards and Technology's (NIST) Cybersecurity Framework as the standard for cybersecurity, which offers a useful tool for understanding the scope of the effort [24]. REMAED follows the NIST Cybersecurity Framework's five Framework Core Functions definition of response: to "develop and implement the appropriate activities to take action regarding a detected cybersecurity event" [25, p. 46]. Specifically, cyber response includes cyber-related mechanisms that are needed to restore power as a result of a cyberattack. Figure 1.3 summarizes the activities within each of the five NIST Core Functions [26].

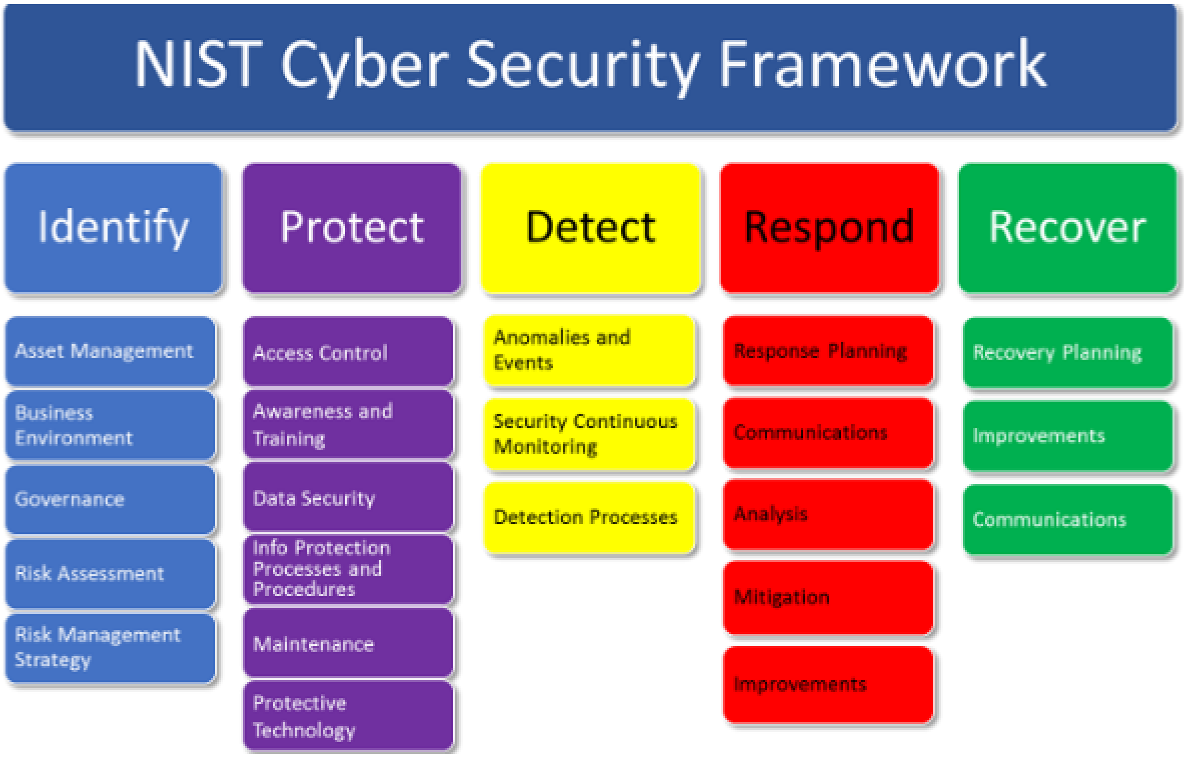


Figure 1.3: NIST Cybersecurity Framework's five Framework Core Functions

1.3.6 Definition of Cyber Response Mechanism

The term mechanism is used to capture a wide array of possible actions that the electricity sector takes or could take to respond to a cyberattack. The NIST Cybersecurity Framework again offers useful cyber response mechanisms that include:

- Response planning
- Communication of response roles and responsibilities, incident reporting to internal and external stakeholders, and information sharing to the broader sector
- Investigation of detected incidents, understanding of impacts from cyber incidents, and forensic analysis of malware
- Containment of cyber incidents to prevent its spread and mitigation of the malware
- Incorporation of lessons learned into response plans and updating response plans and strategies [24]

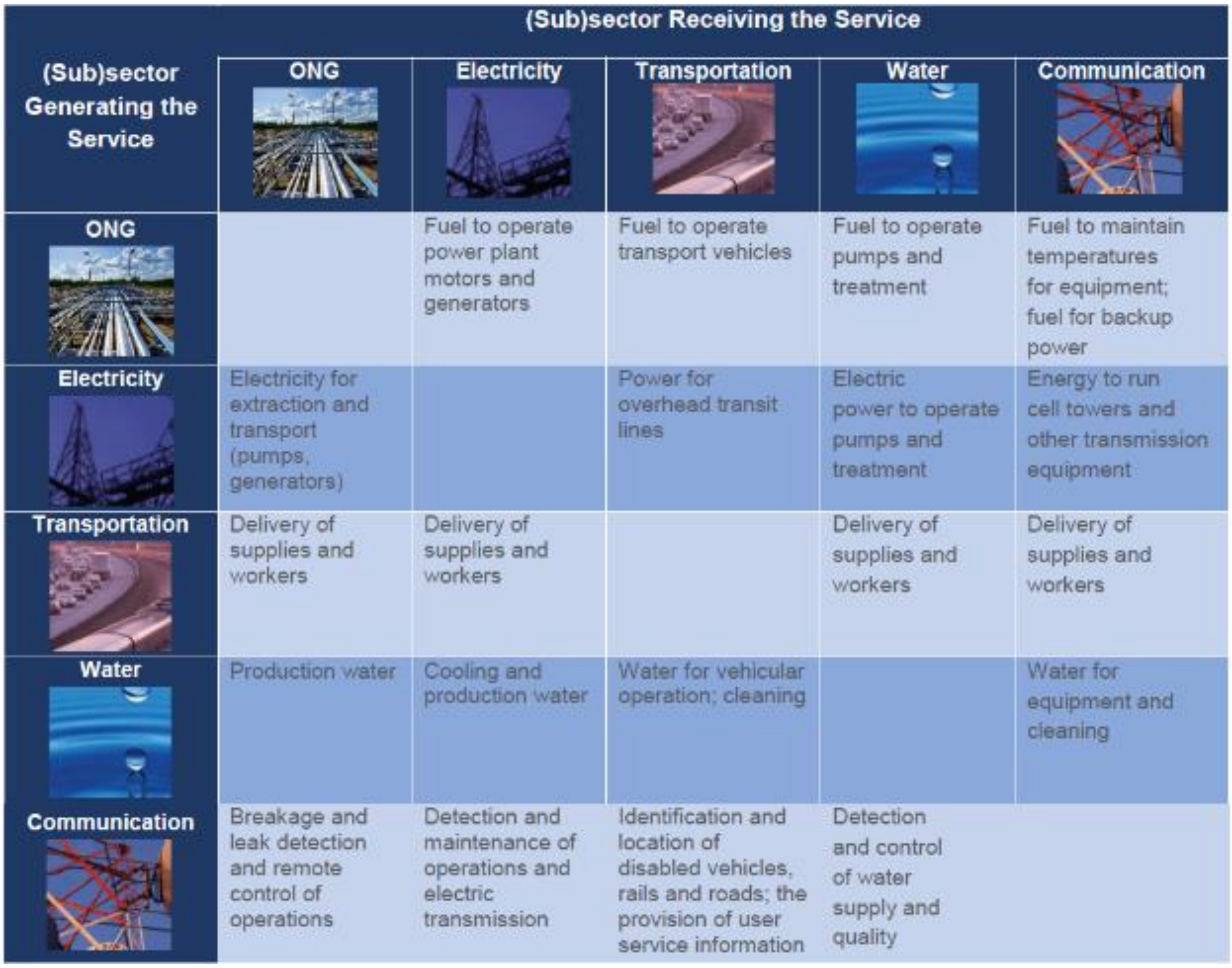
While NIST Framework clearly articulates response mechanisms at the organizational level, it does not include the actions and support structures that enable effective response at a sector-wide level. These include policy and legislation, sector-wide testing, and investment in technology, products, and services.

Additionally, incident response and recovery mechanisms are strongly intertwined at every level of the public and private sector, and often, actions in both categories run concurrently and are difficult to distinguish. The ambiguity between response and recovery is especially true for the electricity sector, in which widespread power outages response and recovery action include rapid power restoration. For this thesis, actions that involve power restoration following a cyberattack, such as black start generator capabilities or substation transformer replacement, are considered critical to sector-wide cyber resilience but classified as recovery mechanisms.

1.4 Scope

1.4.1 Energy Sector and Other Critical Infrastructure Sectors

The energy sector is considered "uniquely critical due to the enabling functions they provide across all critical infrastructure sectors" [27, p. 21]. Previous research has demonstrated that all other critical infrastructure sectors are highly dependent on the energy and information communications and technology sectors as backbones for their operation, and research into the cross-sector interdependencies and needs for comprehensive risk assessments [28], exist and will not be articulated here [4], [23]. [29], [30], [31]. Likewise, the electricity sector has similar dependencies on many other "lifeline" sectors, notably natural gas, telecommunications, transportation, and water, as shown in Figure 1.4 [32, p. 20], [21].



(Sub)sector Generating the Service	(Sub)sector Receiving the Service				
	ONG	Electricity	Transportation	Water	Communication
ONG		Fuel to operate power plant motors and generators	Fuel to operate transport vehicles	Fuel to operate pumps and treatment	Fuel to maintain temperatures for equipment; fuel for backup power
Electricity	Electricity for extraction and transport (pumps, generators)		Power for overhead transit lines	Electric power to operate pumps and treatment	Energy to run cell towers and other transmission equipment
Transportation	Delivery of supplies and workers	Delivery of supplies and workers		Delivery of supplies and workers	Delivery of supplies and workers
Water	Production water	Cooling and production water	Water for vehicular operation; cleaning		Water for equipment and cleaning
Communication	Breakage and leak detection and remote control of operations	Detection and maintenance of operations and electric transmission	Identification and location of disabled vehicles, rails and roads; the provision of user service information	Detection and control of water supply and quality	

Figure 1.4: Interdependencies Between "Lifeline" Critical Infrastructure Sectors

A cyberattack on the energy sector has a potential cascading effect into other critical infrastructure sectors. Coordination of a response to a cyberattack requires a stakeholder to reach across traditional sector boundaries to mitigate the impact, solve common problems, and share resources.

1.4.2 Electricity Subsector and Other Energy Subsectors

This paper recognizes that the electricity sector is a consumer of primary energy, relying on other energy sources to fuel generation, adding to the complexity of formulating effective cyber incident responses. The scope must, however, be reduced to focus foremost on the electricity subsector to identify requirements within the center, which can then translate into requirements for resources, actions, and information external to the subsector. From this foundation, future stakeholder and landscape analysis, inclusive of other sectors and subsectors, will be necessary to identify those gaps and further refine response mechanisms.

1.4.3 Cyberattacks and Large-Scale Electrical Outages

The vulnerability of the entire U.S. electric power system to cyberattacks is a source of much contention. Many hypothetical cyberattack scenarios and real-world events of large-scale outages caused by cyberattacks used to motivate increased attention on cyber resilience fail to acknowledge the current reliability of the U.S. electrical system. In turn, they dilute the probability of such an event occurring in the nation. However, sufficient reports suggest that such an event is not impossible (more in this in Chapter 2). This thesis does not take a position on the probability of a cyberattack successfully causing a widespread outage, only that it is more likely than currently perceived. Neither does the paper articulate a specific threat vector that could be used to cause a widespread outage, only that their constant evolution demands corresponding evolution of cyber response mechanisms. To that end, historical and potential future threats are presented to emphasize the importance of closing gaps in cyber response mechanisms and for better understanding of where those gaps are.

1.4.4 Enterprise Cyber Response Mechanisms vs. Technological

This thesis treats the electricity subsector as an enterprise to apply the Architecting Innovative Enterprise Strategy (ARIES) as discussed in section 1.5. It is essential to distinguish the enterprise elements analyzed herein, from technological ones. This paper asserts that ARIES enterprise elements, such as processes and organizational structures, have been neglected for technology-based solutions. This paper acknowledges the vital role that technology plays in enhancing cyber resilience, and critical technology-related capability gaps are part of this research. However, technology is merely one key component of a comprehensive cyber response mechanism. An appropriate systems approach, including strategy, people, processes, services, information, organizations, and infrastructure, among other elements, must supplement technological solutions to be successful.

1.4.5 Geographic Limits

This thesis analyzes the electricity sector within the U.S. Since the U.S., Canada, and parts of Mexico share the physical electric power system architecture, and supply bulk power across national borders, however, there are international consequences to a cyberattack on the sector. Given the degree of interconnectivity between the electricity sectors and standard North

American regulatory agreements, one may assume any mechanisms proposed as a result of this thesis will also apply to the Canadian and Mexican grids interconnected with those of the U.S. The application of proposed mechanisms, namely amendments to international agreements, may be far more substantial and require significant effort to enact.

1.4.6 Cyberattacks versus Physical Disruption

Recent threat analysis suggests that cyberattacks would likely be perpetrated concurrently with a natural disaster or some other humanmade event that damages the physical infrastructure of the electric power system. However, this thesis assumes that specific mechanisms for responding to cyber-related disruptions in the electricity sector need particular attention separate from physical damage or disruption. Therefore, the scope of this work frames cyber response mechanisms as a complement to responses to physical attacks or for integration into a comprehensive incident response framework.

1.5 Research Questions

This thesis attempts to address three questions to support REMAED's broader goal of transforming the EDS's approach to responding to cyberattacks. The answer to the first question is the primary aim of the thesis, while the answer to the final two support answers to the first:

1. What existing mechanisms can be improved or new ones put in place to accelerate the electricity sector's response to a cyberattack?
2. How can diverse and disparate stakeholder interests be aligned to formulate and implement the mechanisms?
3. What are the correct roles and responsibilities for the public and private sector entities in the energy delivery ecosystem for a cyber response?

1.6 Approach

This thesis studies obstacles to cooperation and collaborative response efforts by examining the historical context, existing conditions, and stakeholder perspectives in the electricity subsector. Primarily, it gathers data through interviews with a representative cross-section of the electricity sector and publicly available information. Admittedly, the study is limited in that it did not gather all perspectives from the thousands of electricity sector stakeholders. While surveying a broader sample size is worth additional effort, the trends that emerge through interviews and publicly available information are sufficient to assert the needs for better cyber response mechanisms.

With that in mind, this thesis utilizes the Architecting Innovative Enterprise Strategy (ARIES) Framework to analyze the electricity subsector in the context of an enterprise. While it is unusual to treat an entire industry as an enterprise, the ARIES Framework provides a robust methodology for analyzing the subsector that is compatible with the aim of this thesis. The following sections describe the ARIES Framework and justification for its use to analyze the electricity subsector.

1.6.1 Electricity Subsector as an Enterprise

The creators of ARIES, Nightingale and Rhodes (2015), do not limit the definition of an enterprise to more traditional constructs which consider an organizations size, e.g., a multinational corporation, or mission, e.g., a business unit within a firm. Instead, they suggest that enterprises need only to have four fundamental characteristics:

> 1. *An enterprise consists of people who generate value for others by producing a product and/or performing a service of some kind*
> 2. *An enterprise is a whole system that has a purpose*
> 3. *An enterprise benefits from being part of its larger ecosystem, the living environment in which it operates*
> 4. *Every enterprise must periodically undergo transformation as it evolves and adapts to an ever-changing world [33, p. 1]*

Given this thesis's definition of the electricity sector in section 1.3.1 and comparing it to Nightingale's and Rhodes's four fundamental characteristics yields the following results:

1. The electricity sector in North America is composed of tens of thousands of people that generate value by providing electricity to U.S. businesses and people.
2. The electricity sector is a system dedicated to the purpose of providing reliable, resilient power to the residential and business customers throughout the U.S. to maintain public welfare and health, enable economic and governmental activities and achieve high standards of quality of life among others.
3. The electricity sector exists within a broader ecosystem comprising other critical infrastructure sectors and energy subsectors, non-critical sectors, public and governmental entities, businesses, residential customers, and a host of other stakeholders who depend on or support its function.
4. The energy delivery sector is undergoing rapid evolution of technology, business models, market structures, and cyber threats, and the sector-wide cyber response mechanisms must undergo transformation to keep pace.

Given these similarities, this thesis treats the electricity sector as an enterprise in order to leverage the methodical, comprehensive approach of the ARIES Framework to identify gaps in its cyber response mechanism.

1.6.2 What is ARIES?

By its creators' definition, ARIES draws from:

> [*T*]*he fundamental theory and practice of multiple fields, including strategic management, stakeholder theory, systems architecting, innovation, scenario analysis, decision science, enterprise theory, and systems science…informed by work with over one hundred different enterprises of various types, sizes, and levels of complexity and maturity, the ARIES framework is designed to guide the exploratory phase of transformation [33, p. 13]*.

Pointedly, the exploratory nature of the ARIES framework is used to focus on finding the right components for an enterprise's architecture, not necessarily designing them in detail. That makes ARIES uniquely suited to identify disparities between current electricity sector cyber response mechanisms and the ideal mechanisms.

The ARIES Framework explores enterprises by applying three main components: the enterprise element model, the architecting process model, and techniques and templates [33]. Given the Framework's unique approach, it is worthwhile to provide a basic understanding of the components as discussed within this thesis.

1.6.3 Enterprise Element Model

The enterprise element model provides ten elements for systematically analyzing all relevant aspects of the electricity sector, as shown in Figure 1.5 [33, p. 14]. These elements originate from assessments and empirical research on over 100 different enterprises conducted by Nightingale and Rhodes. While they acknowledge the existence of other factors and the dynamic nature of an enterprise, their research has revealed that these ten elements are fundamental to all enterprises and are sufficient for gaining insight into the entirety of an enterprise [33].

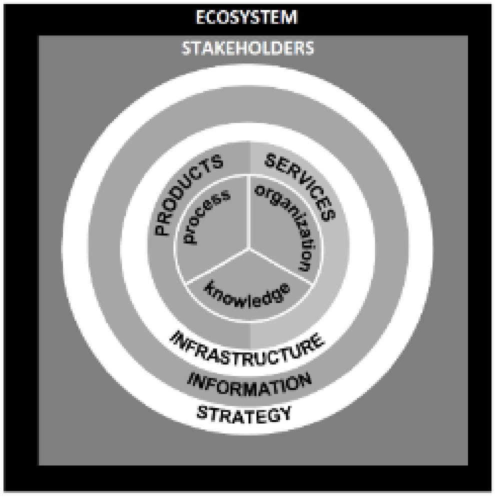


Figure 1.5: The Ten Enterprise Elements of the ARIES Framework

The first element is the ecosystem defined explicitly as the external landscape in which the electricity sector exists. Nightingale and Rhodes use factors such as geopolitics, regulation, economy, competition, market forces, technology, resources, environment to describe the context in which an enterprise exists [33], [34]. The process of analyzing and describing the ecosystem is critical to understanding the external influences that have created the electricity sector's current approach to cyber response.

The second element of the ARIES Framework is stakeholders, including those people and organizations, both internal and external to, the electricity industry. Nightingale and Rhodes contend that enterprises exist to deliver value, defined by the stakeholders' perceptions of it. Further, stakeholders are influenced by their perceived benefit from the enterprise in exchange for their contributions to it [33]. This thesis asserts that the diversity of stakeholders and their respective perceptions of the electricity sector have led to suboptimal response mechanisms, and thorough stakeholder analysis is necessary to understand where to make and sustain changes.

The final eight elements, which the creators collectively refer to as *view elements*, are used to describe the enterprise itself. Nightingale and Rhodes offer the definitions for the view elements, along with their definitions for the first two elements, in Table 1-1 [33, p. 18]:

Table 1-1: Description of the ARIES Framework's Enterprise Elements[33]

Element	Description
Ecosystem	The external regulatory, political, economic, market, and societal environment in which the enterprise operates and competes/cooperates with other enterprises
Stakeholders	Individuals and groups who contribute to, benefit from, and/or are affected by the enterprise
Strategy	The strategic vision along with the associated business model and key strategic thrusts, goals, and performance management system
Information	Information the enterprise requires to perform its mission and operate effectively according to its strategy
Infrastructure	Enterprise enabling systems and information technology, communication technology, and physical facilities that enable enterprise performance
Products	Products the enterprise acquires, markets, develops, manufactures, and/or distributes to stakeholders
Services	Offerings derived from enterprise knowledge, expertise, and competencies that deliver value to stakeholders, including support of products
Process	Key leadership, lifecycle, and enabling processes by which the enterprise carries out its mission and creates value for its stakeholders
Organization	Culture, organizational structure, and underlying social network of the enterprise
Knowledge	Competencies, expertise, explicit and tacit knowledge, and intellectual property resident in and generated by the enterprise

The authors also assert that the view elements cannot be considered separately, but that many of them can influence, drive, or depend upon others. They refer to these relationships as an inherent "entanglement," and the degree to which certain elements are entangled, if at all, varies from enterprise [33, p. 18].

With that in mind, the view elements can be adapted to the electricity sector to demonstrate ARIES suitability for analyzing the entire electricity sector as shown in Table 1-2: ARIES Framework Enterprise Elements Adapted to the Electricity Sector below.

Table 1-2: ARIES Framework Enterprise Elements Adapted to the Electricity Sector

Element	Description
Ecosystem	The external cyber threat, regulatory, political, economic, and market environment in which the electricity sector operates with other subsectors and critical infrastructure sectors
Stakeholders	Organizations who contribute to, benefit from, and/or are affected by the electricity sector's ability to provide reliable, cyber resilient power to the U.S.
Strategy	The strategic vision and key strategic thrusts and goals of electricity market stakeholders and the governments who regulate and provide existing incident response mechanisms
Information	Information that electricity sector needs to measure, prepare for, and respond to widespread malware attacks
Infrastructure	Physical and technological systems that enable cyber response mechanisms to operate efficiently and effectively
Products	Products that the electricity sector develops and uses to enhance cyber resiliency and cyber incident response capabilities

Services	Services that the electricity sector develops and uses to enhance cyber resiliency and cyber incident response capabilities
Process	Processes through which the electricity sector manages cyber risk and communicates, coordinates, mitigates, and evaluates cyber response mechanisms
Organization	Organizational structure, cybersecurity cultural and relational values of the electricity sector that influence its cyber response mechanisms
Knowledge	Competencies, expertise, and explicit and tacit knowledge that the electricity sector stakeholders contribute to or require from the sector in order to enable cyber incident response

The view elements provide a multifaceted approach to examining the electricity sector and its cyber incident response mechanisms. Using the view elements prompts a complete gap analysis of the mechanisms. Further, when proposing changes to, or creation of mechanisms, the view elements allow for a complete design of the mechanism which addresses the requirements for it to be implemented and sustained in the electricity sector. Given the scope of this research and entanglement of the elements, this thesis will focus on the strategy, process, organization, information, products, and services view elements in Chapter 4.

Nightingale and Rhodes also suggest that each of the eight view elements can be better assessed by examining the five parts of its "anatomy," as shown in Table 1-3 [33, p. 24]. By dividing the elements up in this manner, it strengthens understanding of the electricity sector's current mechanisms and helps to develop value propositions for future changes.

Table 1-3: Five Parts of the Element Anatomy

Element Anatomy	Description
Structure	Configuration characteristics
Behavior	Response to certain conditions or triggers
Artifacts	Tangible Evidence
Measures	Quantitative information
Periodicity	Recurring cycles, both with pace and rate

1.6.4 Architecting Process Model

The architecting process model is the second component of the ARIES Framework and defines seven steps to exploring and re-architecting an enterprise, as shown in Figure 1.6 [33, p. 22]. This thesis uses the first four steps of the model to explore the electricity sector's response mechanisms to a cyber event at scale and then create holistic approaches to improving them. This analysis deliberately stops short of detailed mechanism development and implementation plans. Subsequent phases of REMAED solicit feedback from electricity stakeholders to validate the results of presented herein, increase awareness of gaps in sector's ability to respond to a malware attack, craft improved cyber response mechanisms, and build consensus towards potential solutions.

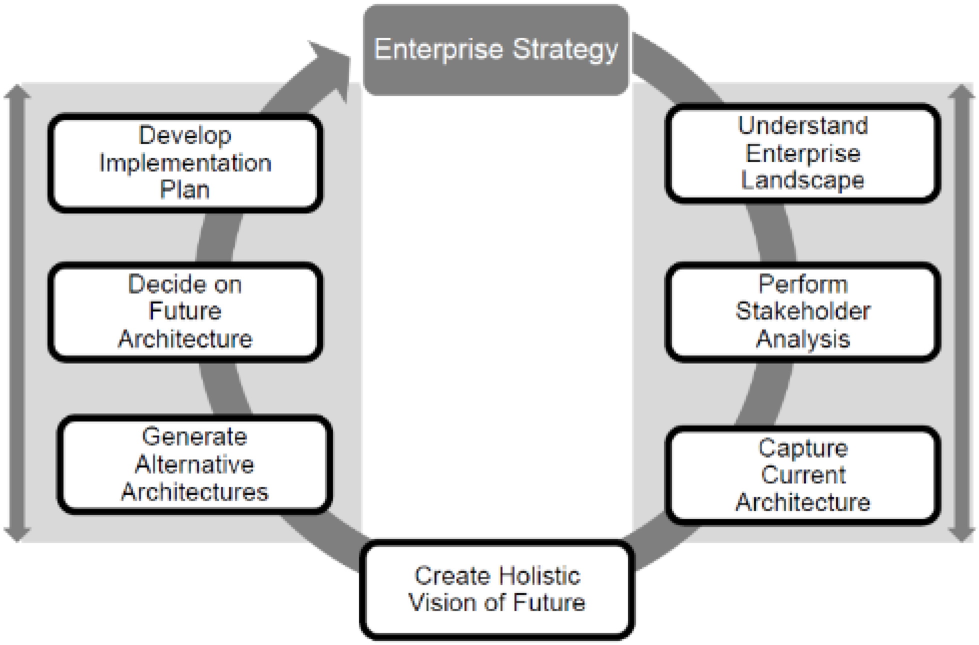

Enterprise Strategy
Understand Enterprise Landscape
Perform Stakeholder Analysis
Capture Current Architecture
Create Holistic Vision of Future
Generate Alternative Architectures
Decide on Future Architecture
Develop Implementation Plan

Figure 1.6: Seven Steps in the ARIES Process Model

1.6.5 Techniques and Templates

The third component of the ARIES Framework is unique to enterprise analysis. Nightingale and Rhodes recommend the use of conventional analysis tools and processes to aid in the exploration and development of enterprise architectures. Examples of recommended tools include the SWOT analysis, Pugh analysis, stakeholder value mapping, and ideation. However, the Framework is sufficiently flexible to incorporate other tools and processes as the user sees fit. In particular, this thesis uses force field analysis, stakeholder saliency analysis, and stakeholder value mapping [35], [36].

1.7 Thesis Structure

The remainder of this thesis follows the first four steps of the ARIES process model. Chapter 2 presents the relevant literature review corresponding to the ecosystem (external) and internal landscape of the electricity sector and analyzes the potential motivations of the sector to change its approach to cyber response. Chapter 3 provides the results of the stakeholder interviews and research as part of a broader stakeholder analysis. Chapter 4 analyzes the current state of the electricity sector's response mechanisms using the eight view elements described in section 1.6.3. Chapter 5 concludes the thesis with next steps in the REMAED project and future research that must be conducted to enhance the development of cyber response mechanisms.

2 Background and Landscape Analysis

This chapter provides context for the remainder of the thesis by presenting a background of the essential electricity supply chain and the importance of electricity and energy security to the U.S. An electricity sector landscape analysis presents a literature review of the factors that shape the sector and its approach to cyber response. An analysis of the electricity sector's cyber response, as the main subject of this research, is presented in detail in Chapter 4, but the effects of the factors to motivate change in the sector's approach to cyber resilience and cyber response is discussed using a force field analysis.

2.1 Background

2.1.1 Electricity Supply Chain

One of the best ways to understand the complexity of the electricity sector's approach to cyber resilience and cyber response is to understand how it delivers electricity. In short, there are four major components in the electricity supply chain, as shown in Figure 2.1 [37, p. 5]. First, electricity generators produce power through multiple methods, including coal, natural gas, nuclear, hydroelectric dams, wind turbines, and solar panels. Second, transmission lines carry wholesale power over inter- and intra-state distances. Taken together, transmission and generation facilities make up the Bulk Power System (BPS). Third, distribution systems form the networks that deliver electricity to customers throughout a defined geographical area. Consumers make up the last of the components, and heavily influence the sector because of the demand they place on the system [38].

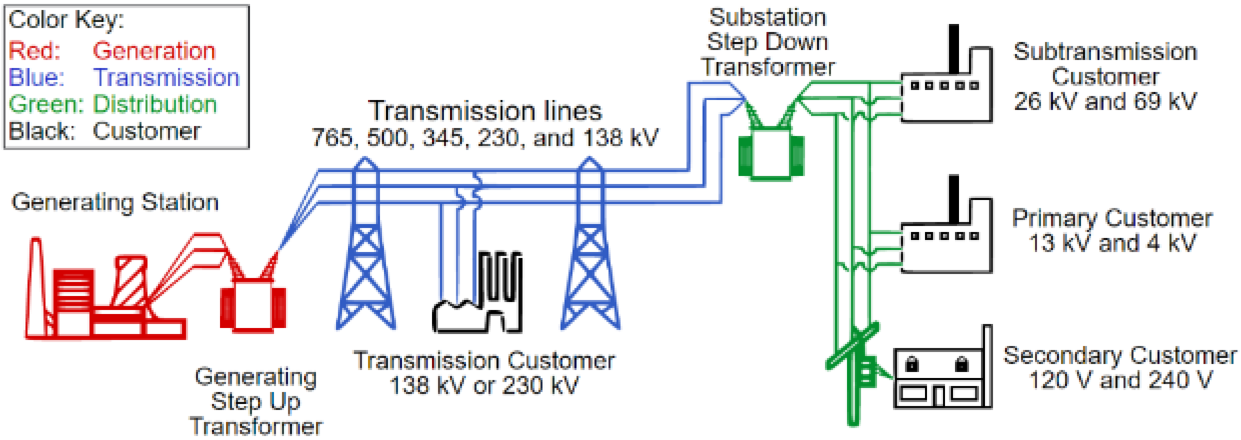


Figure 2.1: Major Components of the Electric System

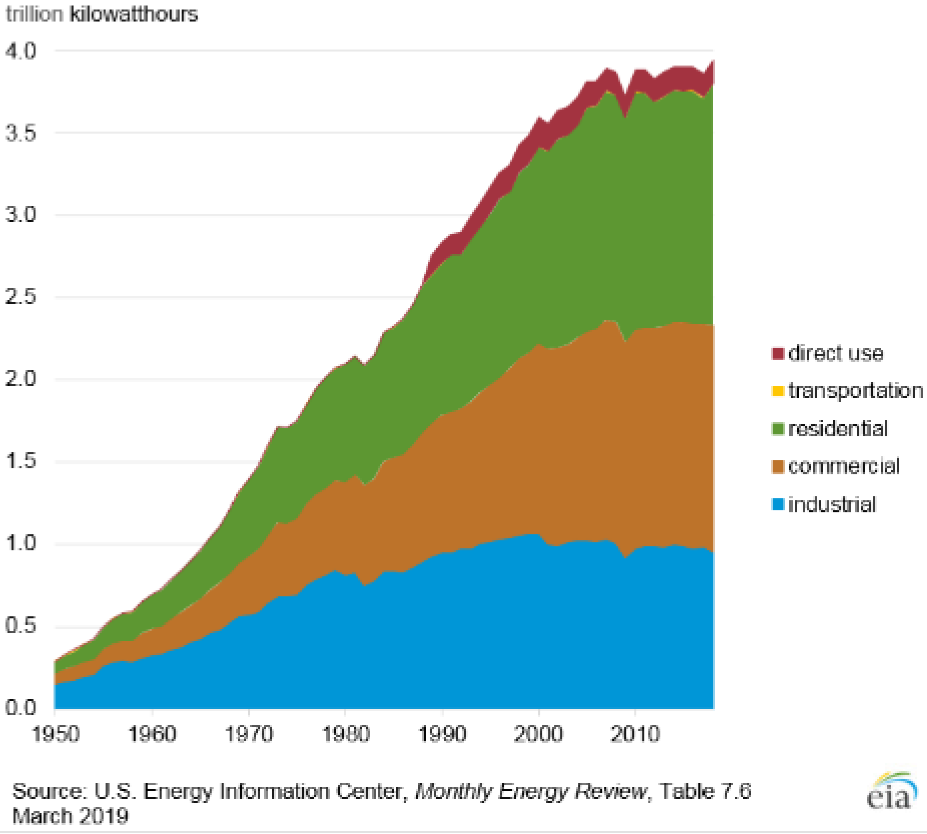
Figure 2.1 provides an accurate but oversimplified view of the electricity industry. It is far more complex and dynamic [37, p. 5]. **Appendix A** more accurately reveals the complex nature through value streams of the four types of markets. While these do not directly correspond to the stakeholder value exchanges related to cyber response, there is significant overlap. In many ways, these value exchanges are complementary to achieving an improved response.

2.1.2 Importance of Electricity Security

The ubiquity and reliability of electricity in much of the Western world might lead consumers to take it for granted. This paper would be remiss if it did not emphasize the significance of electricity on U.S. modern life, particularly the economic, public welfare, and political aspects.

Throughout the world, access to electricity is increasingly viewed as a basic human need, used to cook food, operate healthcare facilities, or enable economic activity, and even directly correlated to national development [39], [40], [41]. For the U.S., energy security, particularly electricity security, is vital to national security, the welfare of its people, and economic prosperity. As such, the U.S. Government labels the electricity sector as one of the 16 critical infrastructure sectors (see more in section 2.2.3.1).

The importance of electricity to daily life in the U.S. is made evident by the nation's consumption patterns. In 2018 alone, the U.S. consumed 3.8 trillion kWh of electricity, and from Figure 2.2, it is easy to observe that electricity continues to grow increasingly significant to all aspects of modern life in the U.S. [42].



Source: U.S. Energy Information Center, *Monthly Energy Review*, Table 7.6
March 2019

Figure 2.2: Electricity Use by Each Consumer Sectors in the U.S., 1950-2018

To accentuate this further, the per capita consumption of electricity depicted in Figure 2.3 highlights electricity's impact on the U.S. relative to other countries [42], [43]. In 2016, the per capita consumption was 12.8 MWh/person. While only 11th in the world by that metric, the U.S. is four times more populous than the top ten countries combined.

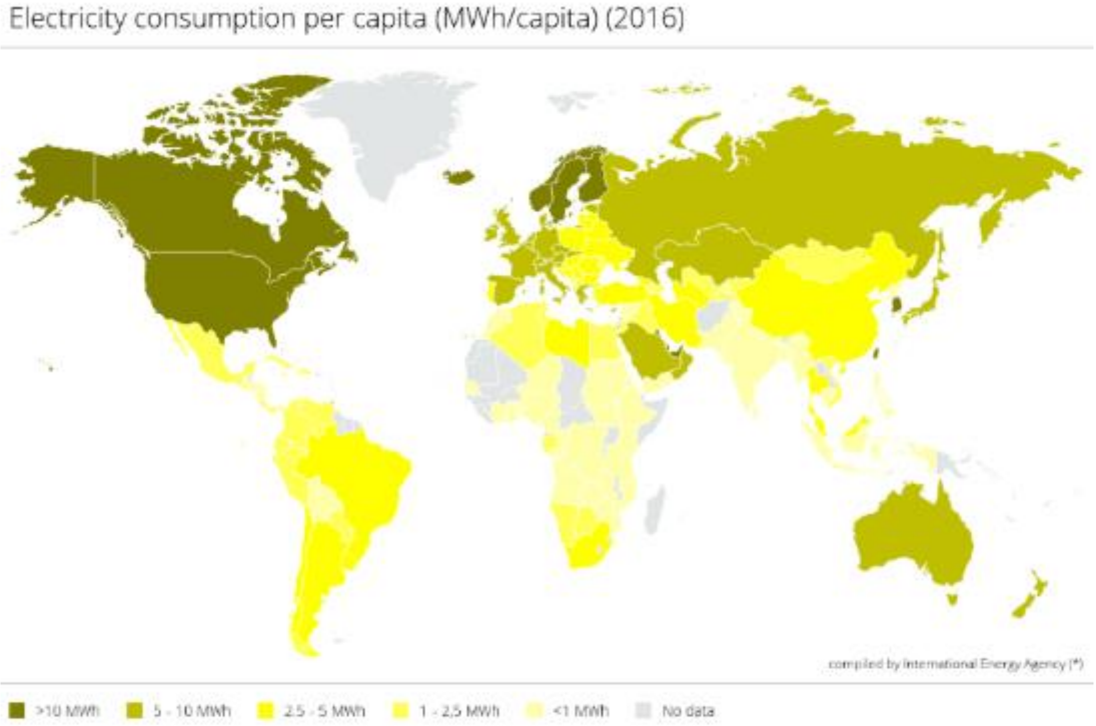

Electricity consumption per capita (MWh/capita) (2016)
compiled by International Energy Agency (*)
>10 MWh
5 - 10 MWh
2.5 - 5 MWh
1 - 2.5 MWh
<1 MWh
No data

Figure 2.3: Electricity Consumption Per Capita (2016)

As many who have experienced a power outage for any length of time can attest, a disruption in electricity, at the very least, presents a nuisance. An outage interferes with the ability to communicate, work on computers, cook, heat and cool an office, and light a residence, for example. By the most recent estimate, sustained power interruptions (greater than five minutes) regardless of cause, cost on average $44B annually (in 2015 $) for all electricity consumers, as shown in Figure 2.4 [44, p. 18]. Other estimates range from $18B to $164B, including costs of spoiled inventory, delayed production, infrastructure damage, lost wages, and unrealized output [45], [46].

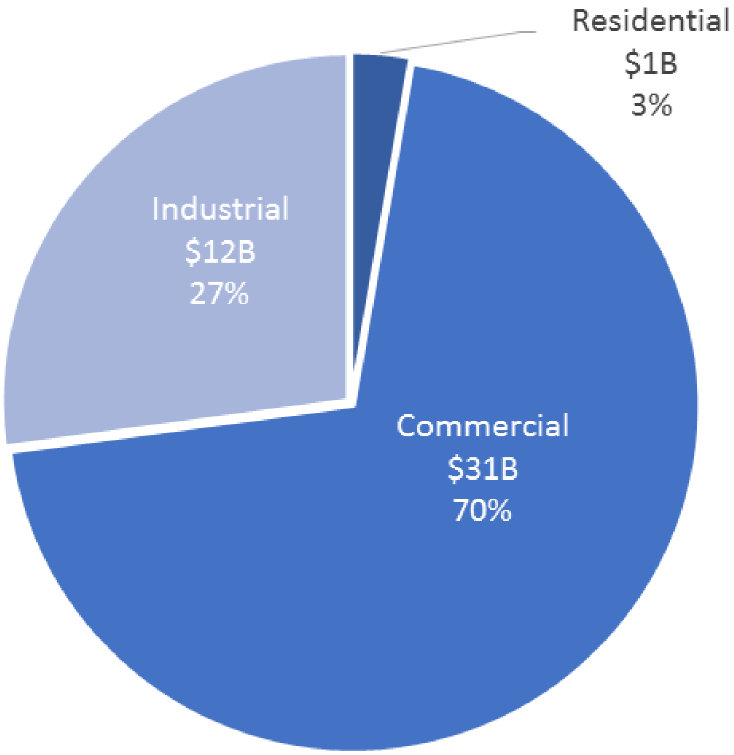


Figure 2.4: Cost of Sustained Power Interruptions for All Customer Types by Sector

While there have been no reported large-scale outages caused by cyberattacks in the U.S., a study performed by Lloyd's of London (2015) calculated the economic toll alone from an extreme cyberattack scenario could range from $243B to $1T [6]. All studies admit to the difficulty in accurately estimating costs of outages, and significantly, they omit injury and loss of life for the same reason, and they all conclude that much can and should be done to improve the resilience of the U.S.'s electric system.

However, increasing resilience requires significant capital investment and endeavoring to eliminate every cyber vulnerability would be cost prohibitive. Instead, risk management strategies provide the basis for tenets of electricity security investments, balancing cost with resiliency [47]. More to the point, there should be continued research and investment in determining acceptable risks, identifying reasonable tradeoffs between cost and resiliency, and finding ways to increase resiliency at decreasing costs.

2.2 Landscape Analysis

The following landscape analysis uses the ARIES Framework's "enterprise ecosystem factors" to explore the external and internal factors that influence the electricity sector and its approach to cyber response [33, p. 30]. Specifically, the importance of cyber threats and political, economic, technological, and market factors are explained to provide context to the sector. Exploration results from a synthesis of publicly available literature and integration of research interview results.

All of the ecosystem factors are deeply entangled, and the categorization of influences on the ecosystem using within a specific factor is debatable. In particular, regulatory factors manifest the entanglement of political, economic, market, and technological factors, so much of the regulatory influence could be captured in any of the other factors. Regardless of the category in which they appear below, the influences remain significant to the understanding of the electricity sector's cyber response mechanisms and identification of the gaps therein. Additionally, the landscape factors that directly influence the electricity sector's current response mechanisms are omitted in here because they require a closer examination and are discussed in Chapter 4.

2.2.1 Cyber Threat Factor

As previously stated in section 1.4.3, this thesis does not discuss the likelihood that a specific threat vector would be utilized to cause a widespread electricity outage, but it is interesting to note that the Director of National Intelligence has gone so far as to say that a cyberattack on U.S. infrastructure is imminent [48]. It is necessary, however, to provide the current perception of cyber-aggressors' motivations and capabilities which drive the investment, actions, and risk management of the electricity sector. As the factor of cyber threats so greatly entwines with all of the other factors, i.e., regulatory, political, economic, technological factors, it is presented separately. Vulnerabilities exploited by cyber-aggressors to execute a cyberattack, conversely, are primarily a function of technology and the architecture and components of the electricity sector's operational and business systems. Section 2.2.4.3 presents further information on these elements.

2.2.1.1 Motivation of Cyber-Aggressors

Any attacker of the electric power system would have to conduct extensive research, possibly navigate interconnected information technology networks to get access to utility ICS, identify the right targets, and then determine how to attack them for the desired result [49]. Consistent with recent threat intelligence and research, the most likely cyber-aggressor to have the necessary resources to do so would be state actors seeking a competitive advantage in case of a conflict. Terrorist groups and cybercriminals may eventually pose a threat as the threat surface increases (see section 2.2.4.3) and as their capabilities increase with time and experience.

However, Knake (2017) states that despite these impending risks, the "likelihood that an attack carried out by a determined and capable adversary would be thwarted by security measures is low" [49, p. 2]. Knake further postulates that it may not take a conflict for state actors to attack. He points to three plausible scenarios:

> 1. *Discrediting Operations. Given the importance of electricity to the daily lives of Americans, an adversary may see advantage in disrupting service to undermine public support for a U.S. administration at a politically sensitive time.*
> 2. *Distracting Operations. A state contemplating a diplomatic or military initiative likely to be opposed by the United States could carry out a cyberattack against the U.S. power grid that would distract the attention of the U.S. government and disrupt or delay its response.*

3. *Retaliatory Operations. In response to U.S. actions considered threatening by another state, such as the imposition of economic sanctions and various forms of political warfare, a cyberattack on the power grid could be carried out to punish the United States or intimidate it from taking further action with the implied threat of further damage [49].*

Of particular note, Knake also elaborates on the potential for miscalculation should state actors cyberattack the electric power system. First, because electricity supports many economic and public welfare institutions, any disruption in service, even if intended to be minor or accidental, might have drastic implications. Second, cyber-aggressors may underestimate the capability of the U.S. to identify the actor responsible and its willingness to retaliate against them. The ambiguity in both instances is significant because many in the industry assume state actors will have correctly estimated both of these factors.

2.2.1.2 ICS Cyber Kill Chain

The ICS Cyber Kill Chain was introduced by Assante and Lee (2015) as an adaption of Lockheed Martin's Cyber Kill Chain to help ICS operators and defenders understand cyber-aggressors' requirements to attack their system [50]. The specific actions and technical requirements of the ICS Cyber Kill Chain are beyond the scope of this thesis. However, the ICS Cyber Kill Chain describes a cyberattack process that has implications on how utilities and Federal, state, local, tribal, and territorial (FSLTT) governments contextualize the threat to critical infrastructure.

Specifically, the current mode of thinking, gathered through interviews, suggests that utilities expect cyberattacks to occur in a single, distinct, and deliberate action to disrupt electricity. In reality, the mode of the ICS attackers is far more gradual, and as Knake has suggested, cyberattacks may be the result of probing efforts or incidental to other actions aggressors take [49]. Therefore, a deliberate cyberattack that causes an outage might be of low likelihood, but prudent cyber risk management strategies must seek to incorporate the increased likelihood of incidental actions.

To provide more insight into this dynamic, Assante and Lee's ICS Cyber Kill Chain (2015) demonstrates the complexity of an ICS cyberattack campaign, the many phases of which do not manifest in an outage but require proportionate levels of response. The first of two stages in an ICS-specific cyberattack is characterized as an "intelligence operation" by the authors. During the first stage, the adversary plans, gathers data on defeating ICS defenses, and gains access to environments to exploit for an attack [50]. Stage 1 has five phases, and its culmination provides the most value in providing consistent access to the ICS for espionage and attack planning. Figure 2.5 [50, p. 2] is taken from the authors' original work and depicts the ICS Cyber Kill Chain. An unintended attack, as described in the previous section, is considered to fall into the "Act" phase of Stage 1.

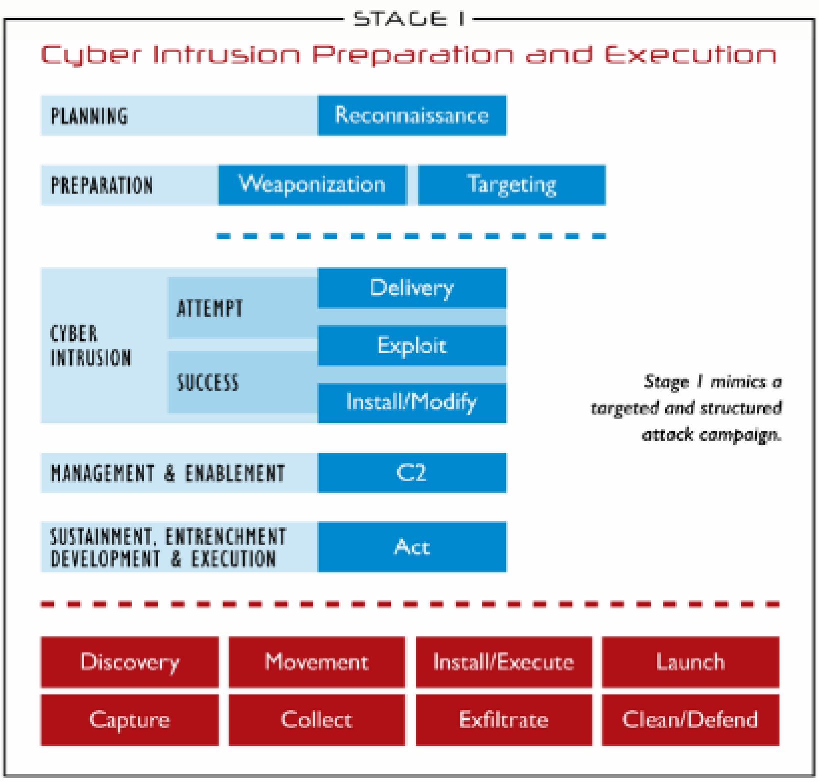


Figure 2.5: Stage 1 of the ICS Cyber Kill Chain

Stage 2 of the Kill Chain continues to demonstrate the measured and deliberate nature of an ICS cyberattack. It contains four phases, the fourth of which requires the aggressor to decide between three generic options of attack, as shown in Figure 2.6 [50, p. 8].

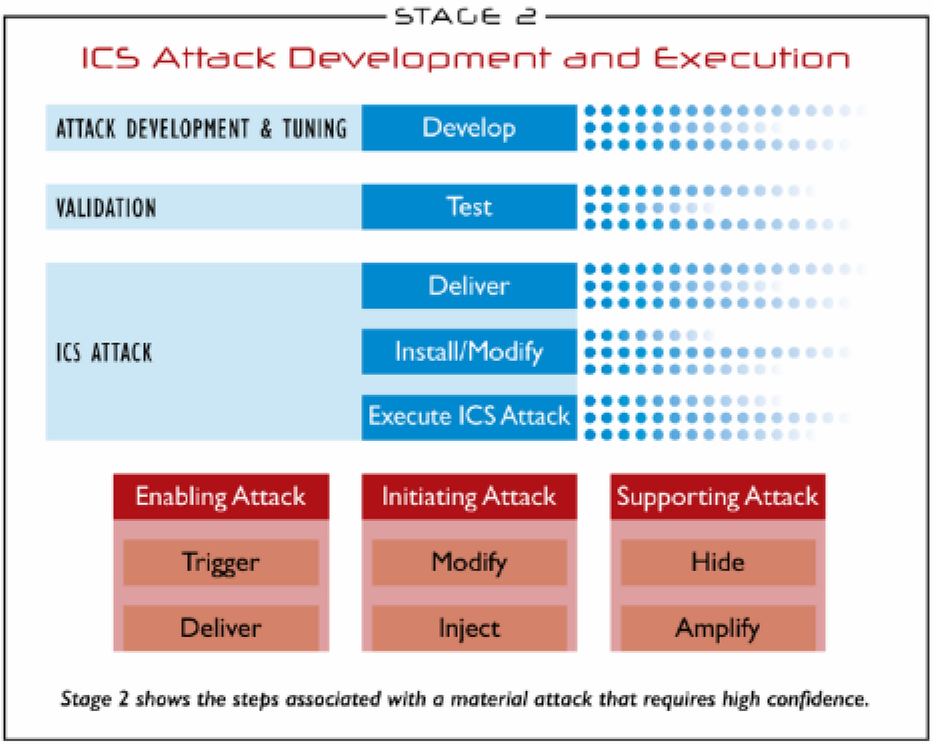


Figure 2.6: Stage 2 of the ICS Cyber Kill Chain

The options of the final phase also indicate that the aggressors may not seek a power outage as the ultimate goal. A successful attack provides them with multiple options to disrupt power, obfuscate their actions, or use the grid to target downstream electricity consumers. Nonetheless, in pursuit of the aggressors' intended effects, such actors encounter a range of challenging obstacles. Assante and Lee again provide insight into relative difficulty, and subsequent likelihood of success, of different attack options in Figure 2.7 [50, p. 10].

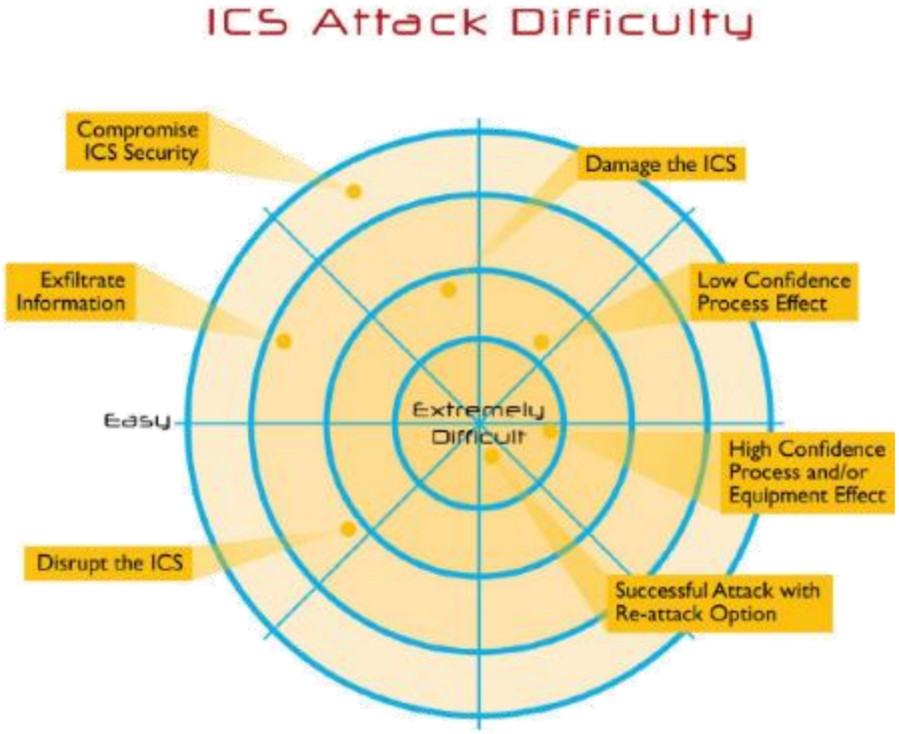


Figure 2.7: Relative Difficulty of ICS Attack Effects

Thus, the electricity sector cannot assume that cyberattacks will always be intentional, occur in some instant loss of operational control or power, or have catastrophic consequences. A high potential for accidental, gradual, and regional cyberattack exists, and cyber response mechanisms need to be equally dynamic and have the flexibility and scalability to be effective in a wide range of scenarios.

2.2.1.3 Overview of Malware Attacks in the Electricity Sector

Malware has been used to disrupt computing functions since the 1980s [51], [52]. However, it has only recently become a significant business risk for its use to steal or ransom financial data and intellectual property. Public recognition of known breaches in many cases have been carefully controlled in order to mitigate damage to a business's reputation, and the economic losses of malware can be calculated in the billions of dollars [53], [11]. Much of this loss is incurred by industries that utilize IT in collecting and storing data, which presents an opportune target for ransom, interference, or destruction. Without the ability to monetize cyberattacks on industrial control systems (ICS) and other operational technology (OT), which focuses on process and control of the system it operates, there has not been a substantial record of attacks on those systems.

Nonetheless, cyber-aggression towards ICS system has become increasingly prevalent. In 2009, STUXNET became the first piece of malware purpose-built for ICS, resulting in physical damage to equipment at an Iranian nuclear enrichment facility [54]. Many in the ICS and cybersecurity industry treated STUXNET as a harbinger of cyberattacks against critical infrastructure that could cause physical damage to electric utility systems and widespread economic and public health issues [54], [55].

More recently, the BlackEnergy 2 and 3 malware attacks against the Ukrainian power grid in 2015 affected approximately 250,000 people. In 2016, the CRASHOVERRIDE malware campaign took down substations, again in Ukraine [9], [56]. Though the latter was less far-reaching in terms of affected customers, it was more advanced and demonstrated the viability of using malware to disrupt service deliberately. More disconcertingly, it revealed the fourth malware tailored specifically for ICS cyberattack. CRASHOVERRIDE, demonstrated that rather than inserting malicious code into the system, attackers gain access through ICT networks, collect information on the network systems and operations, and use automated legitimate ICS commands to disrupt service. Further, CRASHOVERRIDE was designed to be scalable to any size network regardless of its configuration, communications protocol, or location. Its creators modularized the ICS malware explicitly for other attackers to adapt its purpose and deliver yet-to-be-developed payloads [8]. These types of advanced persistent threats have become the main threat to the energy sector. Cybersecurity companies unanimously regard them as indefensible with modern cybersecurity measures [57], [58], [59], [60].

In August 2017, reports emerged of a cyberattack on a Saudi Arabian petrochemical plant. The aggressors targeted the Schneider Electric Triconex safety instrumented system (SIS) and were able to affect the emergency shutdown systems of the plant. The malware, called TRISIS, represented another in a series of ICS-targeting attack tools. Though it reportedly did not result in any adverse effect, TRISIS demonstrated the potential to cause physical equipment damage, injury, and loss of life [61], [62]. Later forensic analysis showed that the attackers had access to the system since at least 2014, had gained intimate knowledge of the plant’s ICS, and took advantage of the end-user to create vulnerabilities. It is also important to note that, by the requirement for a high degree of tailor and integration for an individual SIS, the TRISIS attack was not scalable like CRASHOVERRIDE. Instead, the key takeaways are that aggressors are willing to invest time and resources in malware that can cause physical harm and that the evolution of threats must meet a constant refinement of cyber response measures.

2.2.1.4 Geography of Cyberattacks vs. Other Incidents

Unlike other natural and human-made incidents, cyberattacks can affect a potentially boundless area, and its impacts are not naturally constrained to a single geographical region [63], [64]. In the context of the electricity sector, a cyberattack at scale could affect multiple systems each with distinct, geographically distant impacts. Further, the implications and impact of a cyberattack on the electricity that causes cascading failures is a subject of much research but still not well understood [10], [65].

2.2.1.5 Cyber Threat Factor Analysis

Cyberattacks of all categories have increased rapidly in the energy sector. In 2016, the most current year for which data is available, the sector saw a 77% rise in cyberattacks year over year and similar increases in their success [66]. The data from DHS and DOE in Figure 2.8

show that the energy sector is one of the most heavily targeted of the critical infrastructures, and both agencies admit that the data they collect comes only from reported incidents [3, p. 4]. Unreported incidents or unrealized cyberattacks on the electricity subsector are likely far more numerous.

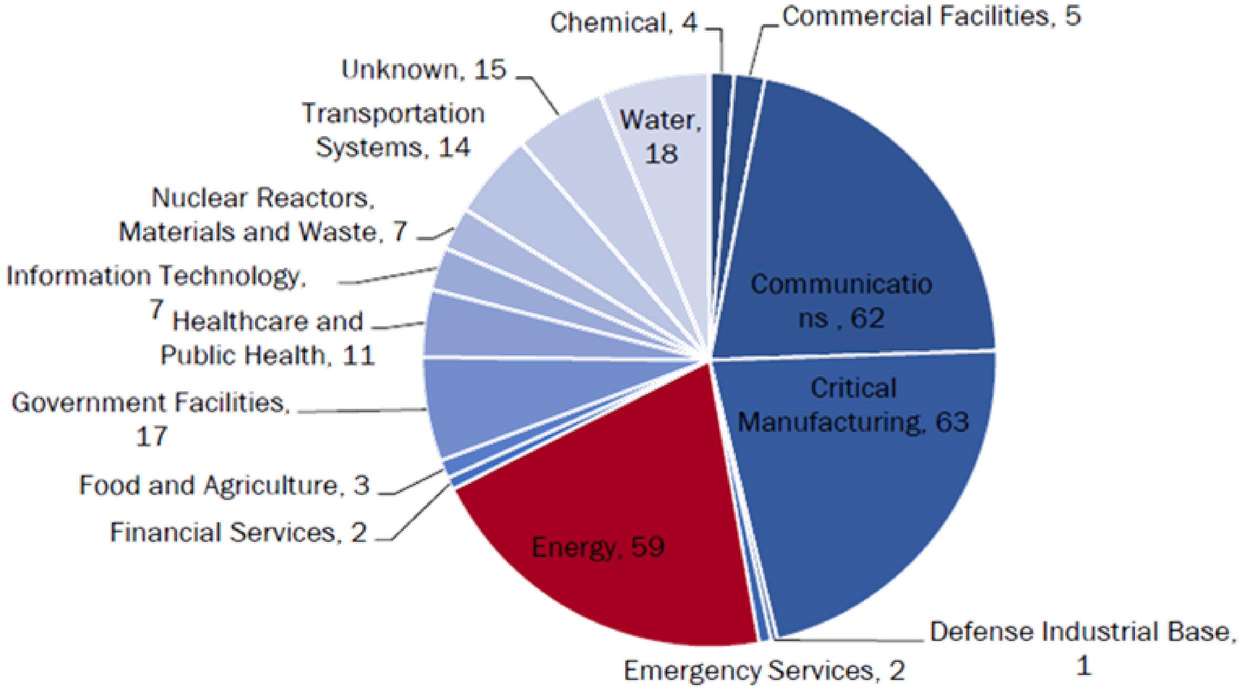


Figure 2.8: Reported Cyber Incidents by Critical Infrastructure Sectors

As malware and other capabilities continue to proliferate and become more accessible to malign actors, the risks to the electricity sector will grow. The DoD and DHS expect that all classes of cyber-aggressors will continue to seek cyberattack capabilities that target critical infrastructure and find novel ways to benefit from those capabilities [67]. Therefore, there is an increased likelihood that an attack affects more than one utility, and the lack of predictable and homogenous geographical boundaries on the attack will make an effective response more complicated. Further, the evolving nature of cyber threats to the energy sector requires that the sector develops the capability to respond to an attack immediately, if not pre-emptively, and in geographically separate areas to appropriately mitigate its effects. Waiting for the sector to be attacked to identify precisely what response mechanisms are needed will waste valuable time, have harsher economic consequences, and may even endanger life.

2.2.2 Regulatory Factor

The regulatory factors that most significantly affect the electricity sector and its cyber response mechanisms fall into two broad categories. The first stems from the regulations that govern commerce and, specifically, the utilities' roles in delivering reliable power. The second, from the regulations that dictate the states have primary responsibility for public health and safety over that of the Federal Government, including emergency management and incident response to cyberattacks on utilities. Arguably, these aspects of government regulation are tightly coupled with political and economic factors. Because of this, the regulation of the electricity market generally remains a contentious issue and must be addressed as a combination of the two. This section does not argue the validity of the U.S.'s approach to regulating the electricity sector but focuses instead on specific effects of regulation on the sector's ability to respond to a cyberattack.

2.2.2.1 Energy Sector Regulations Overview

Between 1935 and the late 1980s, the majority of the energy sector was vertically monopolistic and tightly regulated at the state level by public utility commissions. States closely monitored and permitted utilities to recoup the "cost-of-service" and a return on capital expenditures through rate structures. In the 1990s, the electricity market began the process of deregulation towards a market-based structure driven by the goals of greater economic efficiency and lower electricity rates. Under this proposed model, the distribution and transmission components of the electricity market, natural monopolies, were "unbundled" from the generation and retail components to enable competition in the market.

For the most part, states retained the authority to regulate distribution through public utility commissions given distribution systems' smaller scale and geographic reach. To regulate transmission and the wholesale power market, i.e., generation, the Federal Government exerted its authority to govern interstate wholesale power transactions under the power granted by the Commerce Clause of the U.S. Constitution through the Federal Energy Regulatory Commission (FERC) [68].

However, due to a variety of reasons, including the California Electricity Crisis of 2000, electricity sector deregulation has stalled. Even in deregulated states, electricity is not fully deregulated. Many are waiting until the effects of deregulation can be more fully understood [69]. Figure 2.9 shows the electricity regulation by state as of 2017 [70]. The following sections elaborate on the influences of Federal and state regulations.

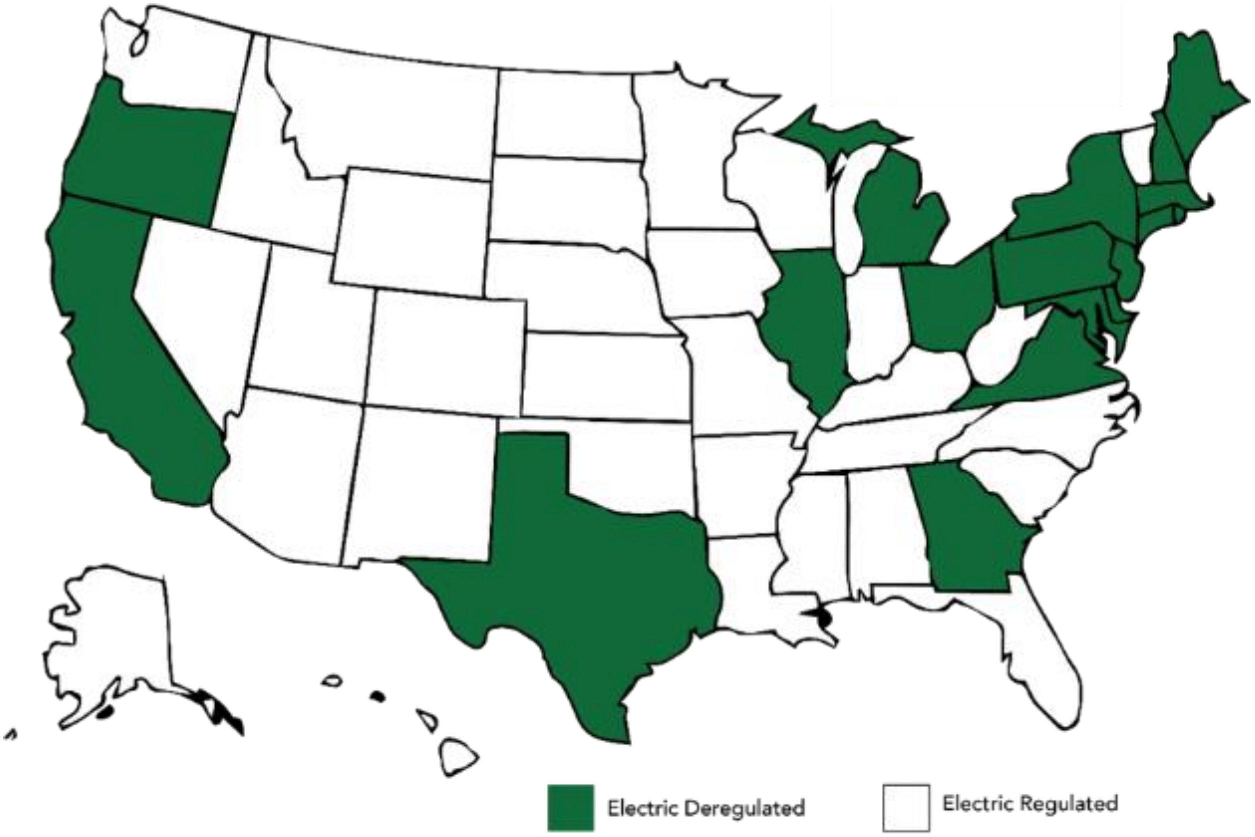


Figure 2.9: Electricity Regulation by State

2.2.2.2 Federal Energy Regulation and Energy Reliability

The Federal Government regulates grid reliability through NERC, which creates and enforces reliability standards for the BPS in the U.S. and Canada. NERC traces its roots back to 1962 when the need to coordinate the BPS between the U.S. and Canada rose from the interconnections of the two countries' grids. Gradually over time, and spurred in response to significant blackouts across the U.S. in the 1960s and 1970s, NERC gained authority through Federal mandates and legislation to enforce reliability standards on the BPS, mainly through fining violators under FERC's regulatory authority [71]. In 2003, NERC was established as the U.S.'s energy reliability organization (ERO).

Born from the 2003 Blackout during which an estimated 55 million people in northeastern and midwestern U.S. and Canada lost power for up to two weeks, the Energy Policy Act of 2005 established the concept of a reliability regulatory body to regulate the BPS [37], [72], [73]. NERC was granted its status as the ERO for both the U.S. and Canada in 2006 and created the first set of mandatory reliability standards. The ERO regulatory model is considered audited self-regulation as defined under U.S. Code of Federal Regulations, Title 1, Chapter III, Part 305.94-1. In this construct, FERC delegated its power to regulate to NERC as a "private self-regulatory organization to implement and enforce laws" on regulated entities [74, p. 2]. While the Code openly admits that audited self-regulation has shortcomings, it recognizes specific instances where such a program is more effective than direct government control. The electricity sector meets these criteria.

Concurrent with NERC's expanding authority and role in the reliability of the BPS, the need for resilience of the power grid arose from increasing attention on the subsector's designation as a critical infrastructure sector and, ultimately, increasing threats from natural disasters and terrorism. As one component of reliability, NERC developed, implemented, and now enforces 11 Critical Infrastructure Protection (CIP) standards composed of 40 rules and nearly 100 sub-requirements related directly to cyber resilience [75], [76]. Relevant to cyber response, CIP-008-6 Cyber Security — Incident Reporting and Response Planning requires regulated entities to report cyber incidents and establish incident response plans for cyberattacks on "critical assets" [76, p. 218].

2.2.2.3 State Regulation and Electricity Reliability

As FERC and NERC have gained authority to regulate the electricity market, the states' Public Utility Commissions (PUC), or their equivalent, have ceded that authority to them. The withdrawal of state regulatory powers and imposition of Federal law onto states has been met with resistance. However, in *FERC v. Mississippi*, the U.S. Supreme Court upheld the power of FERC to regulate many aspects of states' electricity utilities [77].

Of the 18 states that have deregulated electricity markets, PUCs only regulate distribution utilities, which do not fall under interstate commerce regulated by the Federal Government. In the regulated states which have vertically integrated electric utility monopolies (meaning they own generation, transmission, and distribution of electric utilities), the PUCs regulate all three. In all states, FERC regulates the wholesale transactions and transmissions that cross state lines [78].

PUCs are typically accountable for regulating other utilities within their jurisdiction as well, including water, natural gas, and transportation, and engage with different Federal regulatory agency and SSA for each sector. Perhaps their most important, or at least highest visibility responsibility, is a PUC's authority to approve utility rates. Among other costs, most utilities must recoup the cost of cybersecurity within the capital expense of an asset or combine it with the other operating expenses. However, they are often not permitted to recover cybersecurity investments as a direct line item, and because some investments have significant and recurring costs, it deters utilities from making adequate investments.

Further, many PUCs have reportedly lacked the necessary workforce expertise to identify good cybersecurity investments. PUCs must balance affordability for electricity consumers with business risk and profitability considerations for the utility when calculating rates. Often PUCs reject proposed rate increases that utilities require to cover recapitalization costs regardless of their legitimacy, and they apply the same logic to cybersecurity investments. However, PUCs are unable to discern prudent cybersecurity investments or their urgency due to a lack of trained workforce.

State open records statutes often complicate matters further as they often require PUC hearings to be open to the public [79]. Since cybersecurity plans and information tend to be confidential, utilities are often reluctant to provide PUCs with the very information they need to approve rate cases and make more informed cybersecurity policy decisions. Nonetheless, PUCs are often the primary state resource for developing incident response plans for the energy sectors.

2.2.2.4 Cybersecurity and Risk Management in the Electricity Sector

Until very recently, NERC's CIP reliability standards created a relatively "rules-compliance" based system for cybersecurity investments. In Figure 2.10, Massacci et al. [80, p. 7] show the predominance of rules-based compliance in the U.S. electricity subsector relative to those of other countries. The authors expound upon the limitations of purely risk-based and purely rules-based cybersecurity approaches sector and demonstrate that the U.S.'s has led to lower overall investment, resiliency, and preparedness [80].

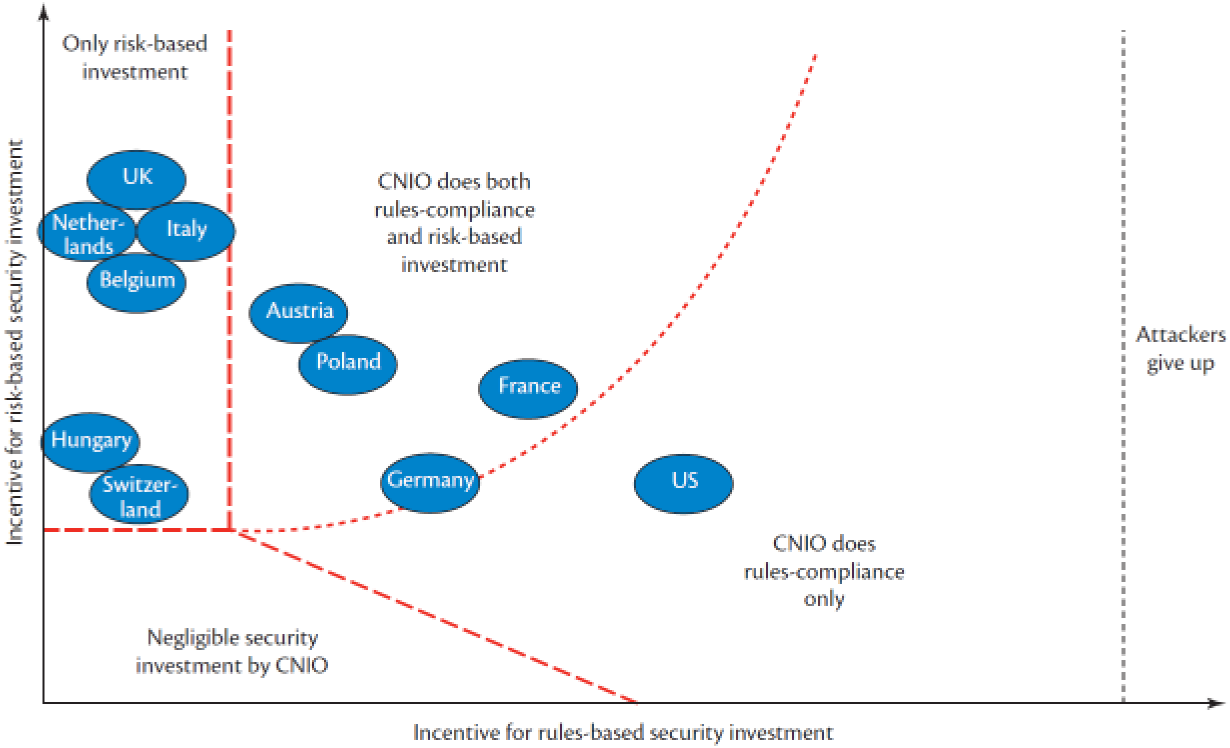


Figure 2.10: Phase Regions of Critical National Infrastructure Operator (CNIO) Behavior Depending on Regulatory Incentives.

Arguably, the culture of compliance in the U.S. electricity sector exists to this day, but in 2013, the Federal Government recognized the benefits of incentivizing risk-based security investments and developed policy to combine it with its traditional approach [81]. The DOE, regulators, such as FERC and NERC, and research institutes, such as NIST, encourage utilities to make risk-based cybersecurity investments [82], [83]. The results have been frameworks and guidelines for risk management of the cybersecurity of electric power systems, such as the DOE's *Electricity Subsector Cybersecurity Risk Management Process*, NIST's *Risk Management Framework for Information Systems and Organizations*, *Framework for Improving Critical Infrastructure Cybersecurity*, and *Framework and Roadmap for Smart Grid Interoperability Standards* [83], [84], [85]. These publications notably do not require strict compliance and are, instead, designed to be “a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks” [86, p. v]. The DOE’s *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2) is another manifestation of the shift in paradigm from rule-based to risk-based management. The ES-C2M2 is a voluntary self-evaluation that “is presented at a high level of abstraction so that it can be interpreted by subsector organizations of various types, structures, and sizes. Widespread use of the model is expected to support benchmarking of the subsector’s cybersecurity capabilities” [87].

The lack of compulsory implementation of strict standards reflects the position that the resources and capabilities between each utility vary greatly, and one-size-fits-all regulations or guidelines will not work. Even NERC CIP standards, specifically CIP-007-6 governing its IT/OT systems, provide wide latitude for individual interpretation [76]. Additionally, the detail of the controls, the sheer volume of them, and the definition of successful implementation as presented in the frameworks, guidelines, and standards are not clear.

As Lipner and Lampson noted, cybersecurity risk management is unlike risk management in other domains [88]. For cyber risks, it is difficult to assess risk as precisely as, say, an insurance actuary can estimate the likelihood and severity of a fire. The authors point to three main reasons that cyber risk determinations are so challenging which echo the information asymmetries interdependent security problems discussed in sections 2.2.4.1 and 2.2.4.2:

1) Uncertainty in cyber-aggressors’ capabilities and resources
2) Uncertainty in cybersecurity technologies
3) Uncertainty in the consequences in the severity of an attack [88]

The Lipner and Lampson and Langner and Pederson (2013) maintain that tradeoffs and risk-based decisions must remain [1], [88]. However, within the context of Federal Government cybersecurity policy for its systems, the authors advocated for mandatory but clear guidelines for critical systems. Enacting baseline requirements to improve cybersecurity, in their mind, would overcome the issues state in sections 2.2.4.2 and 2.2.2.4.

2.2.2.5 Emergency Management, Incident Response, and the Roles of the Federal and State Governments

Under the Tenth Amendment to the U.S. Constitution, the states retain the primary responsibility for public health and safety. The Amendment has been interpreted to mean that states have a mandate to provide for emergency management and incident response. While the Federal Government’s involvement in emergency management has grown over time, it maintains a secondary role. That is, the Federal Government provides resources and assistance to states when they exceed their local capacity to respond. The Federal Government also utilizes Federal funding, and sometimes the threat of withholding it, to establish national programs and standards for emergency management and cybersecurity within the states through the principle of cooperative federalism [89], [22], [90].

For the electricity sector specifically, 16 U.S. Code § 824o-1. *Critical electric infrastructure security* grants the Secretary of Energy authority to “issue such orders for the emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability of critical electric infrastructure” [91]. The statute applies to narrow definitions of emergency, including a cyberattack, and, then, only to the BPS, consistent with its authority under the U.S. Constitution’s Commerce Clause. In 10 CFR Subpart W, the actual procedures for an emergency declaration and issuance of an emergency order are articulated and include significant consultation with private and other public entities [92]. Additionally, 16 U.S. Code § 824a. *Interconnection and coordination of facilities; emergencies; transmission to foreign countries* also grants FERC the authority to establish a temporary connection of transmission lines or operation of generation facilities for specific emergencies. Fortunately, both statutes have yet to be used by the Federal Government, but the substance and timeliness of the orders and their ability to enable the necessary response remain untested.

Chapter 4 further details the coordination between states and the Federal Government, the emergency statutes, and other incident response mechanisms already in place.

2.2.2.6 Regulatory Factor Analysis

In general, the electricity sector, both utilities and government, remains skeptical of the effectiveness of new regulations on improving reliable and resilient energy. Regulations tend to impede the effectiveness of market mechanisms to produce efficient utility rates, deliver affordable electricity, allow for appropriate investments, and achieve a reasonable profit. The sector’s status as a blend of natural monopolies and competitive market structures along with complicated Federal and state jurisdictional structures make it very difficult to regulate the electricity subsector in general, much less its cybersecurity. Regulatory factors in the sector can be distilled down to six main effects on cybersecurity and cyber response:

1. Inconsistent regulations at state and Federal levels
2. Lack of access to cybersecurity knowledge
3. Slow and reactive regulation making
4. Inability to recognize or recoup prudent cybersecurity investments
5. Compliance-driven cybersecurity practices
6. Interference with critical information sharing

Because of the inconsistent utility regulation and authorities across each state, there is no uniform state or Federal scheme for cybersecurity or cyber response requirements for utilities. Where there are competing state and Federal regulatory authorities, utilities must decipher how to comply with both, or if a utility serves multiple states, it may need to have different policies depending on the location of its assets [78]. For states, it is often difficult for them to keep track and harmonize state regulations and cybersecurity policies with Federal policies given the multiple agencies and SSAs. Arguably, the Federal Government is in the best position to identify cyber threats and has the most resources out of any stakeholder to regulate cybersecurity in the sector, but it is disempowered both by statute and traditional approach to partnering with the private sector and state governments.

A state's access to cybersecurity expertise is often limited because of a small pool of qualified personnel, breadth of sector-specific cybersecurity issues, and limited government investment in such a workforce. Thus, their knowledge of cybersecurity may be strained, surpassing their ability to regulate a response within a sector, due to a lack of sufficient technical understanding of cybersecurity.

Also, the creation and revision of regulations tend to be a slow process, sometimes taking years to develop and implement. The emergence of new technologies, new vulnerabilities, and new threats far outpaces the ability for NERC or PUCs to respond equally. The nature of cybersecurity that perpetuates reactive behavior towards current vulnerabilities and threats, rather than taking proactive measures, compounds the delays in rule-making.

Currently, most PUC rate making algorithms do not permit recoupment of direct cybersecurity investments (the establishment of a cybersecurity workforce, for instance), nor do the PUCs typically have the technical knowledge to understand what a reasonable rate would be [78]. In recent years, PUCs have become more actively engaged in encouraging utilities to invest in cybersecurity measures. However, there remains a dearth of expertise and precedence for regulators to evaluate the rate cases for cybersecurity investment [79].

Similarly, the NERC CIP regulations tend to be highly prescriptive, in part due to previous CIP standards allowing utilities to broadly interpret the classification of assets to be included in cybersecurity protocols using a Risk-Based Analysis Methodology. The resultant autonomy led to NERC CIP standards becoming the most frequent violated, as shown in Figure 2.11, before subsequent revisions implemented tighter controls [93, p. 4]. While this has the effect of raising cybersecurity of the electric power system across the board, it disincentivizes, and in some cases even interferes with, increased investment in cybersecurity.

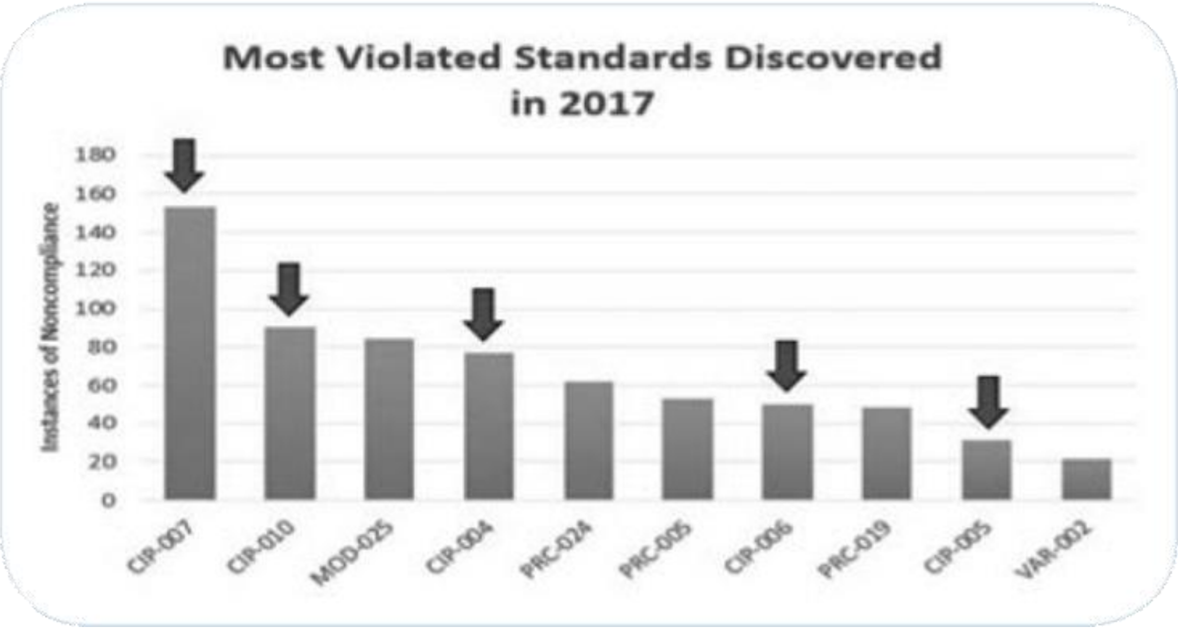


Figure 2.11: Violations of NERC Reliability Standards

Prescriptive cybersecurity regulations tend to provide utilities with the illusion that they are cyber secure. However, "being compliant does not necessarily mean being secure" and combined with the thin margins, significant costs of typically associated with cybersecurity investments, difficulty recouping costs, and a diverse, sometimes conflicting set of Federal and state regulations, many utilities have adopted a culture of minimum compliance [15, p. 5].

Further, current regulatory mechanisms impose fines for failure to achieve resiliency standards. NERC CIP are the most prominent of these mechanisms, but alone, they may not be enough to achieve proper investment because they do not proactively encourage cybersecurity preparation. Instead, NERC CIP requirements contribute to some utilities developing a culture of minimum compliance rather than one which seeks to anticipate and keep pace with threats. Ultimately, utilities that develop a minimum compliance approach to cybersecurity becomes the weakest link in the interdependency of the electricity sector, and every utility and consumer suffers [94].

Finally, information sharing has been widely established as a critical component to the cybersecurity of critical infrastructure and is the subject of much research [95]–[97], [98], [99]. Open sharing laws at the state level threaten proprietary, confidential business cybersecurity information, which could create vulnerabilities in its network, and its customers' privacy information. Both of these liabilities strongly dissuade utilities from promptly sharing relevant information, even though such information could be critical to formulating an adequate response, or even preventing, a cyberattack. Information sharing processes and information sharing and analysis organizations (ISAOs) are discussed in greater detail in sections 2.2.4 and 4.3.3.3, respectively.

2.2.3 Political Factor

Politics play a prominent role in the electricity sector because of the U.S.'s reliance on power for economic growth and public welfare, as addressed in the previous section. Cybersecurity of critical infrastructure, on the other hand, is a less obvious but increasingly recognized aspect of the economy and public welfare. As with other areas of the electricity sector, political influence and PPPs significantly affect the approach to implementing cybersecurity in the electricity sector.

Though implementing new policies and adapting cybersecurity strategy is relatively easy due to the highly regulated nature of the energy sector, neither the state nor the Federal Governments' approaches stimulate the optimal level of investment in cyber resilience.

2.2.3.1 Cybersecurity as a Public Good

Current cybersecurity "doctrines of prevention," "risk management," and "deterrence through accountability" [100] show that cybersecurity has not fully been viewed or managed as a public good. Previous government policies reflect a corresponding inability to protect critical infrastructure. That cybersecurity is a public good is not disputed. It is both non-excludable and non-rivalrous, and as with most public goods, there is compelling evidence that cybersecurity without government intervention is underprovided for in the market [2], [99], [101], [102].

However, there exists a unique intersection of cybersecurity as a private interest and as a national security interest. Indeed, much literature investigates that very dynamic [2], [101], [103], [104]. Cavelty and Suter (2009) put it most succinctly:

> *This creates a situation in which market forces alone are not sufficient to provide security in most of the [Critical Infrastructure] sectors. At the same time, the state is incapable of providing the public good of security on its own, since an overly intrusive market intervention is not a valid option either; the same infrastructures that the state aims to protect due to national security considerations are also the foundation of the competitiveness and prosperity of a nation. Therefore, any policy for [critical infrastructure protection] must absorb the negative outcomes of liberalization, privatization, and globalization, without canceling out the positive effects [105, p. 1].*

Therefore, the Federal Government's approach to cybersecurity in the critical infrastructure sectors focuses on guiding and incentivizing private sector behavior for the benefit of the nation. This approach manifests as collaborative constructs referred to as public-private partnerships (PPP).

2.2.3.2 Overview of U.S. Government and Critical Infrastructure Sectors' Approach to Cybersecurity: Public-Private Partnerships

Since 1996, the U.S. Government designated the energy sector as one of 16 critical infrastructure sectors, defined as:

> [S]*ystems 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 [27, p. 12].*

So designated, the sectors formed the nexus between the government's responsibility to protect the nation's and private sector's ability to operate these industries efficiently.

Beginning with the Clinton Administration, the Government has been wary of the economic impact of overregulation of the critical infrastructure sectors. Due to the implications on state laws, there are untested limits on how much the Federal Government can compel states to enact or enforce laws that uniformly regulate all utilities outside of Federal jurisdiction [90]. Impacts on the critical infrastructure sectors include slower innovation, reduced competition, more costly software, more expensive products, and potentially contradictory effects of enforcing strict cybersecurity measures on private entities, electric utilities included. Additionally, the Government has been unwilling to incur an unfunded mandate to provide cybersecurity for the private sector networks as it would have for national defense, law enforcement, and other emergency services [103], [106]. It asserts that the "Government has neither the responsibility nor the expertise to act like the private sector's system administration" [107, p. 24]. In turn, this implies that the Government has a marginal, potentially passive role in providing cybersecurity and that the private sector is best placed to provide for the security of critical infrastructure networks.

This implication effectively shifts the responsibility and liability for the national security aspect of cybersecurity onto the private sector. However, the private sector seeks to minimize cybersecurity as an expense. Raising expenditures to the level necessary for national security would be significant. Further, the private sector is resistant to accepting the liability for national security in America's litigious society [2]. In other words, what is best for society may not be the most profitable or even sustainable for a utility provider. As a barrier to forming and sustaining effective cyber response mechanisms, private sector participation, and the Government's policies towards it, must be framed with this in mind.

Unfortunately, the Government's approach has not embraced the critical dynamic between national security and business sustainability. The National Infrastructure Advisory Council's *Critical Infrastructure Resilience Final Report and Recommendations* (2009) noted this fact:

> *Current market mechanisms may be inadequate to achieve the level of resilience needed to ensure public health, safety, and security. Even with a strong business case, there are low-probability, high-consequence events for which investments in resilience by private companies cannot be justified. In these cases, stronger government involvement is warranted to ensure adequate functioning of critical infrastructures during disasters [20, p. 10].*

The result has been the formation of partnerships between public entities and private ones. These partnerships manifest in a multitude of ways. The government offers services of law enforcement, technical, security and risk experts, and intelligence, among others (see Chapter 4 for more details). However, it also heavily regulates many of these sectors in order to achieve critical infrastructure sector goals. On the other hand, the private entities within the critical infrastructure sector own and operate their infrastructure, advise on regulations, and in some cases, self-regulate.

For the electricity subsector, in particular, Federal policy on cybersecurity has been a complex political, economic, and technical issue. Strategies have primarily revolved around two main efforts. The first effort has used electricity service reliability and reporting standards enforcement [76] policies administered through NERC (see section 2.2.2 for more information on regulations). Second, the Government encourages participation in information sharing and analysis organizations (ISAOs) consisting of voluntary exchange of cyber-related incident information with energy sector stakeholders [108]. ISAOs participants are better able to prevent, mitigate, and respond to service disruptions as ISAOs consolidate cyber threat information, analyze it, and promulgate mitigation strategies.

Additionally, as a business risk management issue, there are strong indications that the electricity subsector understands the importance of cyber resilience. Its constituent stakeholders have invested in cyber resilience and incorporated cyber risk management into their business models, albeit to varying degrees. The relatively recent development of cybersecurity frameworks specifically for critical infrastructure sectors, such as the NIST's Cybersecurity

Framework, enabled this transformation and aided in the standardization of cyber resilience practices [86].

Twenty years after the U.S. Government designated the Nation's critical infrastructures, the cybersecurity landscape has evolved significantly. In parallel, there have been calls for renewed collaboration in the U.S.'s public-private approaches to managing the critical infrastructure [109]. The Executive Branch has stipulated that new approaches must transcend the previous focus on cybersecurity as a tangential effort to reliability or treatment of cybersecurity as a solely private sector issue [27].

2.2.3.3 Cybersecurity and Energy Security in the Political Domain

As a vital component to national security, economic prosperity, and the environment policies, the discussion of energy security has traditionally been dominated by political interests to gain independence from foreign primary energy sources, such as oil and petroleum products. However, cybersecurity of the electric sector has increasingly moved to the forefront of the conversation [89], [110]. As Figure 2.12 demonstrates, cyber threats dominate the energy security dimension of OECD national energy transition agendas according to the 2018 World Energy Council's Issues Monitor [111, p. 9].

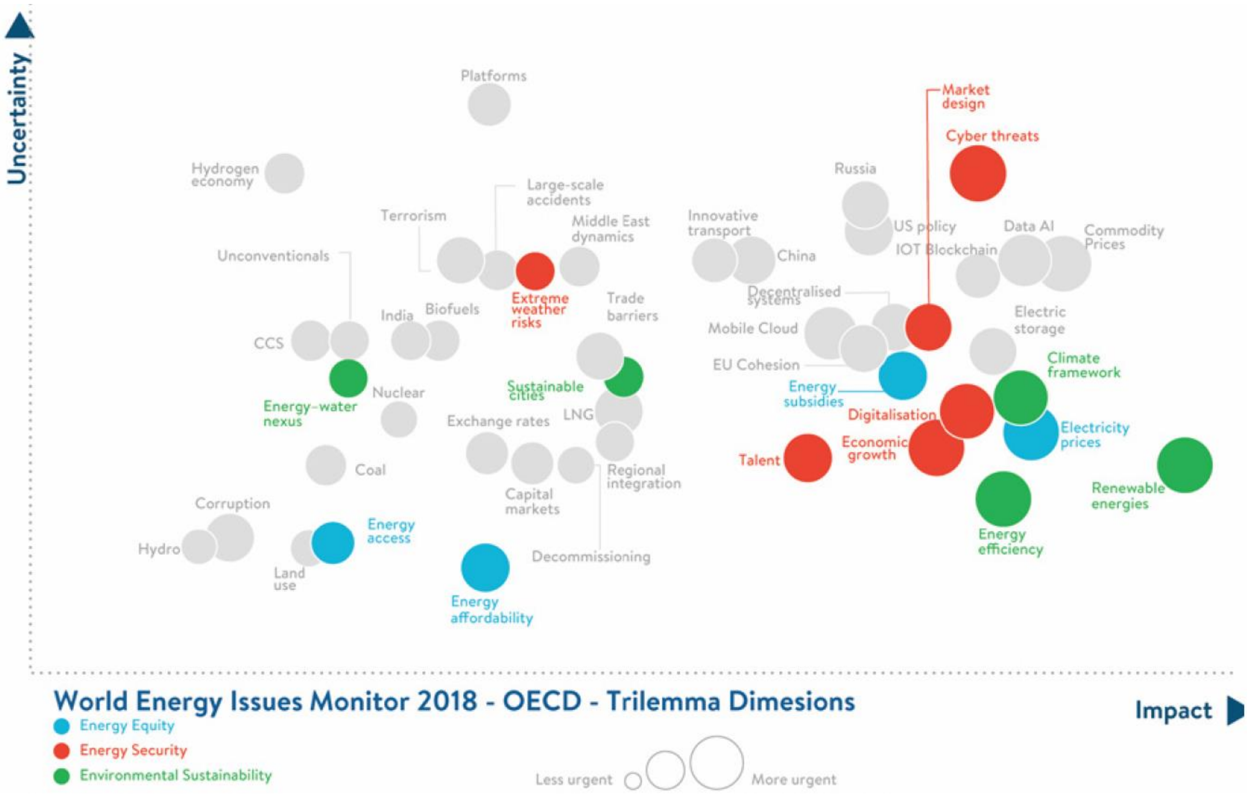


Figure 2.12: Cyber Threats as an Energy Security Issue for OECD Countries

Additionally, the DOE's most recent report on the *Valuation of Energy Security for the United States* (2017) discusses the international redefinition of energy security to incorporate broader energy security paradigm, and it prominently features the cybersecurity of the energy sector with particular emphasis on the electricity subsector [89]. The report indicates the increasing political recognition of the importance of the electricity sector's cyber resilience and future policy direction.

2.2.3.4 State Government Investments in Cybersecurity

Regardless of the level of government, government spending is subject to the priorities of the political parties in power. While Federal Government spending on cybersecurity initiatives for critical infrastructure sectors has picked up in recent years under both parties, state governments have not made it an equal priority. As discussed in section 2.2.2.3, state governments are responsible for an equivalent breadth of cybersecurity challenges as the Federal Government. However, they also have regulatory power over and responsibility for distribution systems which fall outside of the requirement for NERC CIP compliance but make up, by some estimates, 80%-90% of electric power system assets [78].

Despite this fact, only 1%-2% of states' IT budgets on average were spent on cybersecurity measures, and of that, only 21% of the $160 million of the combined IT budgets for 24 states funded initiatives directly related to cyber resilience and the cyber responses of critical infrastructure sectors [112]. A 2018 joint report from Deloitte and the National Association of State Chief Information Officers (NASCIO) also point to a revealing cause: "almost half of states do not have a separate budget line item for cybersecurity" as depicted in Figure 2.13 [113, p. 8]

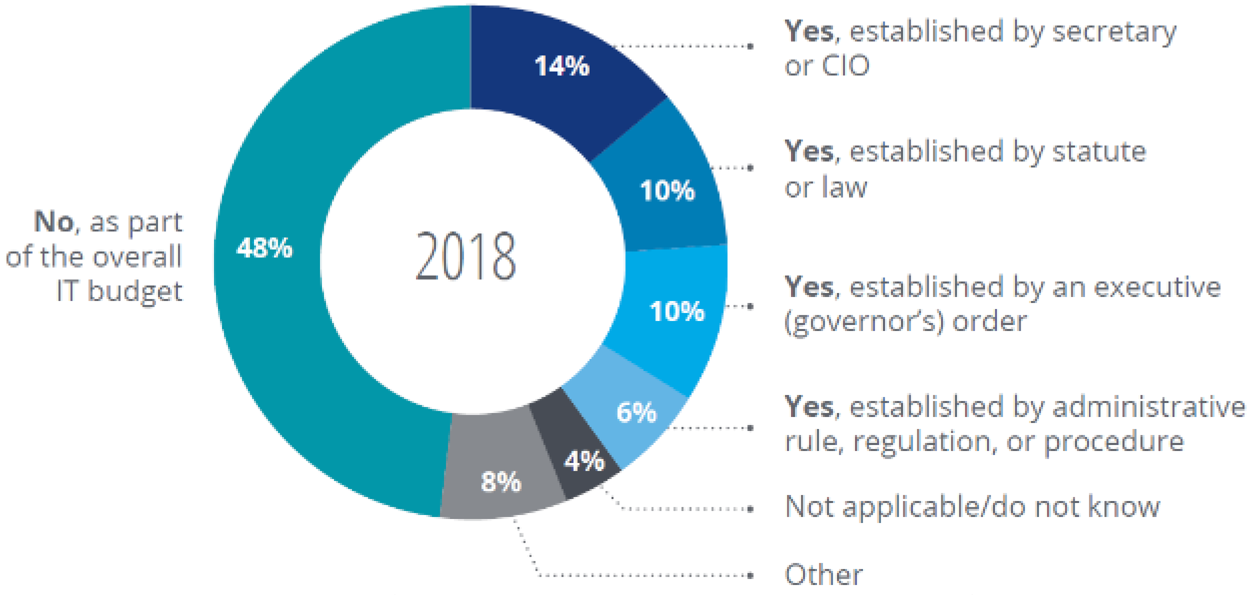


Figure 2.13: Percentage of States with a Separate Budget Line Item for Cybersecurity

(Based on 50 responses from State chief information security officers or equivalent to the question "Does your state have a cybersecurity budget line item. Source: 2018 Deloitte-NASCIO Cybersecurity Study)

Deloitte and NASCIO (2018) also point to stagnant mostly stagnant or marginal increases in cybersecurity budget growth for the same states and have not kept pace with current or anticipated cybersecurity challenges [113]. Similarly, states have difficulties finding and retaining qualified cyber workforce due to noncompetitive pay structures nor have many established career paths for their cyber workforce [113].

2.2.3.5 Political Factor Analysis

With the increasing number of cyberattacks and the likelihood of a significant cyber incident, the Government may have been forced to change its approach, and such a drastic change is not without precedent. As Knake (2017) noted, aviation security was taken over by the Federal Government following the 9/11 attacks [49]. He asserts that Congress would empower the executive branch with increased authority over the electricity sector if a similar event were to occur. While such authority might decrease the efficiency of the grid and open the door for greater Federal Government involvement in other sectors, the political mandate would be met. Geopolitically, the second order consequences to such an attack might include the exposing of a vulnerability that inhibits the U.S. from action abroad.

Thus, the real motivation for the electricity sector should be the maintenance of the status quo, i.e., that cybersecurity is the responsibility of utility owner/operators with support from the Federal Government. In order to do this, the risk profile of cyber resilience investments may need to shift drastically in some cases but might be made harder by the need to appease shareholders and regulators. However, incident response mechanisms, that is the processes, policies, expertise, and technology, that facilitate reaction to a cyber-attack remain some of the most immature capabilities in the cyber resilience spectrum [114].

Fortunately, as of 2018, current Federal Government directives take a strategic approach to cybersecurity and point out the need for the “ability to go across sectors, go across agencies to understand true national risk, set priorities together, plan jointly, train, and exercise alongside each other” [4, p. 38]. These directives affirm that the traditional policies on energy sector cybersecurity are necessary but are no longer sufficient. Among the gaps identified was the lack of capability to consolidate public and private sector resources in response to a malware-based cyberattack on the energy operational technology control systems. To that end, the Department of Energy has sought and obtained increased authority from Congress to regulate the energy sector under the Federal Power Act [115], [116]. The Government's policy on responding to a cyber incident affecting a private entity remains monitoring and offering assistance, and approval of the desired increases in authority remains uncertain [117], [118].

Finally, state CISOs acknowledge that insufficient resourcing presents the most substantial barrier to supporting the cybersecurity of their respective critical infrastructure sectors. The effects of underfunding resound through all facets of the states’ responsibilities towards the electricity sector. Regulations and rate-making suffer from the lack of experience in the workforce, processes, products, and services to support private sector cyber resilience are not in place, and governments tend to struggle with understanding how to foster private sector involvement in cybersecurity to the most efficient degree possible.

2.2.4 Economic Factor

Discussion of the regulatory and political factors have addressed some economic issues affecting the electricity sector as well and are not covered again in this section. Instead, attention must be paid to specific economic attributes of cybersecurity that influence the behavior of the sector. The information asymmetries, that is “where one party has more or better information than another party,” inherent to industries such as the electricity sector create significant barriers to implementing cybersecurity measures [119]. Additionally, both positive and negative externalities arise from cybersecurity’s nature as a public good, as discussed in section 2.2.3.1. This paper will approach those negative factors that have the most significant potential to impede the effectiveness of current and future cyber response mechanisms.

2.2.4.1 Trust and Information Asymmetry

One of the more well-known impediments to building cooperation and collaboration among disparate stakeholders of an industry is the level of trust among them and in the sector's ability to operate effectively and fairly. As applied to critical infrastructure, the importance of trust, mechanisms to instill it, and processes to sustain it, has been exhaustively studied [120], [121], [121]–[124] and are further addressed within the context of the electricity sector in section 4.3.2. However, this section presents the importance of external factors and transactions costs that erode trust and cause trust imbalances between sector stakeholders.

In order to respond to a cyberattack at scale, cyber response mechanisms must make trust a central priority as a high level of information asymmetry characterizes the nature of the problem. Information asymmetries are a significant barrier to the success of the sector’s cyber resilience and exist between multiple parties within the sector, such as between utility operators and cybersecurity vendors, between regulators and utility owners, and even between the sector and cyber-aggressors. These asymmetries may outright deter participation in collaborative public-private efforts because if costs are too high, erode confidence in the organization’s ability to create value, or lead to overconfidence in a provider’s own cyber defenses among others [125].

To better form an organizational structure that effectively mitigates the impact of information asymmetry, it bears clarifying its sources which this paper classifies into three broad categories: quality of information, continuous evolution of the cybersecurity ecosystem, and risks to competitive advantage.

<u>Quality of Information</u>

Asymmetries in this category are those that have both been shown empirically to exist through economic theory and reported by participants in organizations such as ISACs [65], [100], [101], [120], [126], [127]. The following is a brief list of issues with the electricity sector’s cybersecurity caused by the poor quality of information.

- Cyber threat information may be “oversold,” e.g., doomsday cyberattack scenarios, by cybersecurity vendors to utility providers
- Cybersecurity product and services are not verifiably “cybersecure” and lead to overconfidence in cybersecurity or, conversely, mistrust in the ability to achieve an appropriate level of cybersecurity

- Cyber threat information may not be relevant to all vendors and cause information saturation
- Utility providers may not understand the impact of a cyber threat to their business
- Utility providers may not know if a cyber threat applies to their systems
- Utility providers lack the expertise to verify if cyber defenses are adequate
- Utility operators may lack the expertise or technological capability to detect cyberattacks or understand how to mitigate it
- Cyberthreat mitigation may be very technical, affect operation technology, and challenging to put in place
- Information may lack sufficient details to act upon or be classified by the government
- Delay in reporting information
- Governments may not understand their role or the resources required to enable the private sector to invest in cybersecurity properly or, more relevantly, to respond to and recover from a cyberattack

Continuous Evolution of the Cybersecurity Ecosystem

Many aspects of cybersecurity continuously change and an ever more rapid pace. The high rate of change creates significant difficulty for utility providers, ICS vendors, cybersecurity vendors, and other critical infrastructure sector stakeholders to stay ahead of cyber threats. They are as follows:

- Continual development of new digital (OT, IT, IoT, etc.) technologies installed on the electric power system which create new vulnerabilities
- Constant expansion of the electric power system which creates more access points
- Increased focus on smart grid technology and networking architecture of the grid which increases vulnerabilities and access for attackers
- Relentless cyber-aggressors who continuously search for vulnerabilities and create new threat vectors

Risks to Information Security and Competitive Advantage

The interests of the public and private sectors are most divergent in this category of information asymmetry. As a condition of participating in the organization, the government would naturally want the energy sector stakeholders to share their information maximally. Such a practice would improve cybersecurity for all group members by highlighting threats and tangentially act as a source of information it could use to enhance national security in other areas. The government would simultaneously want to retain its classified data to avoid compromise to intelligence activities despite the ability to help mitigate the threat [105].

Conversely, the private energy sector stakeholders would naturally want the government to provide as much intelligence as possible to enable them to respond better. However, they would simultaneously want to retain any information surrounding a cyber incident, which could damage their reputation as a provider or vendor. Further, NERC Critical Infrastructure Protection regulations require a certain level of cybersecurity, and such an incident could also result in a fine. Additionally, sharing information amongst private sectors competitors, a vendor could run afoul of anti-trust laws or divulge valuable intellectual property.

2.2.4.2 Cybersecurity as an Interdependent Security Problem

Moore (2010) posits that externalities stemming from insecurity, interdependent security, and free-riding externalities collectively represent the primary economic barriers that inhibit investment in cybersecurity and much work has been dedicated to understanding cybersecurity investment strategy, [104], [127], [128], [129], [130]. These can be directly translated into barriers to an effective cyber response but must be contextualized.

A variety of authors, including Anderson (2001) and (2002), Varian (2001), Kunreuther and Heal (2003) and Heal and Kunreuther (2004), have framed the problems associated with cybersecurity in terms of economics. In their seminal works on security in networks, such as electrical grid control systems, they classify these externalities into a set called interdependent security problems [129]. Specifically, Varian (2000) first describes the problem of insecurity, as illustrated when a cyberattack using a botnet launched from a university's network attacks a major internet company's network. The university suffers little from the infection, but the company's costs are severe [131]. In later work (2001), he demonstrates that when security is dependent on the weakest link (one who invests least in cybersecurity), that firm determines the security of everyone else. In turn, he shows that the result is that those that do not participate will receive the advantages of everyone else's investments regardless, and a free rider problem results [130].

More generally, Kunreuther and Heal (2003) contend that these problems share a common trait, namely that a utility's decision to invest (or not) in security will impact other utilities' welfare and incentives to invest. They model firms' security investment incentives and apply them to the Prisoner's Dilemma [129]. Later Rowe and Gallaher (2006) provide an empirical analysis that supports the same conclusion [127]. The research shows that for interdependent, complex systems like cybersecurity of the electrical grid, utility's investment in cybersecurity improves others' security and disincentivizes others from investing in their own [128]. The authors do provide more generalized models for a variety of situations where firms cost and benefits are not congruent with a range of implications, including suboptimal investment in cybersecurity rather than a complete lack. Similarly, Gordon et al. (2015) present an economic model that demonstrates that firms' socially optimal cybersecurity investment rises to by no more than 37% of the loss of a cybersecurity breach and that underinvestment is "essentially a given" [132, p. 29]. These researchers conclude that stronger incentives are needed to reach a higher level of investment.

Further, Honeyman, Schwartz, and Van Assche (2007) assert that collaboration between cybersecurity vendors and ICS vendors to provide better products is inherently disadvantageous [94]. The authors show that due to the inability of firms, e.g., electrical utility operator, to quickly identify the source of failures in their control system environment and distinguish between a fault in a control system and a failure in cybersecurity systems, i.e., caused by a cyberattack, results in free-riding problems. Further, utilities may find the financial burden of determining the source of failures or distinguishing it from a cyberattack to be prohibitive. Ultimately, the reliability and security of the utility's control system suffer [94].

2.2.4.3 Economic Factor Analysis

High barriers to trust characterize the cybersecurity industry and, for similar but separate reasons, the electricity sector, [133]. Because of the underlying risks, the severity of consequences, and misinformation, stakeholders have developed skepticism in the processes, products, services, and other stakeholders that make up the sector. Matching cyber response investments with realistic risks, collaboration among stakeholders, prioritization, and pooling of limited resources, and information sharing among others are necessary to effectively mount a response to a widespread attack and rely upon trust.

Likewise, the interdependent security problem, applied to the cyber response mechanisms, indicates that changes to the electricity sector's cyber response mechanisms would have to overcome barriers caused by interdependent security externalities. For example, Gordon, Loeb, and Lucyshyn (2003) apply this concept to ISACs and ISAOs, demonstrate the ineffectiveness of voluntary, collaborative organizations and contend that incentives are needed to reach the optimal level of participation [134]. Thus, the electricity sector is not intrinsically motivated to invest in cyber resilience to an optimal level, and current mechanisms and potential improvements to them must encourage participation through incentivization.

2.2.5 Technology Factor

Technology is both a key enabler of and a hurdle to increased cybersecurity and better response mechanisms in nearly every sector, including electricity. Advances in technology increase the ability to achieve greater cybersecurity because of advancements, such as network monitoring. Conversely, by its nature, new technology, such as smart grid systems, which make the system more efficient to operate and potentially improve the electricity market, introduce new cyber vulnerabilities.

Many critical infrastructure sectors are particularly susceptible to this dynamic because the cybersecurity of their industrial control systems has only relatively recently become the target of cyber-aggressors. Combined with aging systems and electricity grid assets with relatively long lifetimes, the maturity and capabilities of cyber resilience in the electricity sector are behind that of other sectors. Vulnerabilities introduced by a globalized supply chain have also recently come to light and become a source of scrutiny of the sector's cybersecurity posture. The use and impact of cybersecurity technology and tools for utilities also demonstrate the challenges the sector phases when formulating appropriate response mechanisms for a large-scale attack.

2.2.5.1 Physical Infrastructure of the Electric Grid and its Role in Cybersecurity

The electrical grid is geographically dispersed across the entire North American continent and composed of 200,000 miles of high-voltage transmission lines, 55,0000 substations, and 5.5 million miles of distribution lines [49]. Even though these are purely physical components of the power grid, the complexity of the infrastructure and its interdependence with digital systems contributes to the vulnerabilities of the system. Referred to as cyber-physical systems, treating the physical systems separately from the digital is difficult when examining their cybersecurity. However, the physical architecture of the grid is the driver for the creation of its digital systems. It almost exclusively dictates the requirements for digital systems performance, how they are designed and operated, and, consequently, how secure the grid is from cyber threats.

Few grid components are physically supervised or monitored, and the grid operates over a large geographic area. Therefore, electrical grid operation relies upon automation, remote control, and data acquisition technologies. The decentralization of physical components and their control systems create innumerable physical access points for cyber-aggressors to leverage to gain access to networks or exploit the reliance on remote monitoring [110].

At a grid-wide scale, as alluded to in section 2.2.4.2, the interdependent network of power transmission through interconnections and the increasingly networked configuration of generation and distribution systems also represent a vulnerability to the entire grid. Because the grid architecture has been established to enable utilities to support one another, a cyberattack on one utility can have consequences for the supporting utilities. Likewise, an attack on a generation plant can have consequences on transmission and distribution systems [6], [135].

In the past, the components of electrical systems could be treated independently, or at least, constructed, operated, improved, and maintained without the level of planning required of today's complex power grid, and the industry has recognized the need to take a systems of systems approach towards grid architecture [13], [136] [137]. However, traditional mindsets regarding cybersecurity of the complex systems continue to prevail.

Part of the reason for the stall in adopting a better cybersecurity technology is the age and cost of electrical equipment. Seventy percent of transmission systems components, i.e., power lines and transformers, are over 25 years, and the average age of generation plants is over 30 [138]. Naturally, most of the digital systems that operate and support them are of similar ages and come from a time before cyber threats to the grid were capable. Previously, the security of these cyber-physical systems took advantage of their unique, proprietary nature or lack of interconnectivity with other devices and the internet.

Complete replacement of both physical, and consequently their digital systems, before the end of their useful life, was and remains cost prohibitive. Therefore, as control systems have advanced, utilities have added layers to these legacy systems, incrementally increasing efficiency and security [139]. As these systems become increasingly interconnected to more advanced devices added for greater electricity sector efficiency, however, the legacy systems, which may no longer be supported by their manufacturer, become easily exploitable targets for cyber-aggressors [65].

2.2.5.2 Digital Technologies and Their Role in the Electricity Sector Cybersecurity

The cybersecurity of the grid is, obviously, not purely driven by the physical infrastructure, and as its digital systems have advanced in capability, so too has its need for and ability to provide cybersecurity.

The role of digital technologies in the electricity sector almost exclusively follows the evolution of the introduction of automation into the electricity grid. The very first automated systems were installed to control generation and transmission of newly interconnected grids in the 1930s. Over the last 90 years, industrial control systems (ICS) has evolved to include advanced OT such as Supervisory Control & Data Acquisition (SCADA), Energy Management Systems (EMS), and Intelligent Electronic Devices (IEDs). These key technologies managed nearly all aspects of grid operations, including remote control of breakers, monitoring of alarms located distant substations, control generation plants over a wide geographic area, and transmission of electricity between regions [140].

Likewise, the impact of ICS on the cybersecurity of the grid follows the evolution of ICS capability and can be traced to cyberattacks on natural gas plants, electric utilities, and telecommunications systems in the early 2000s. ICS cyber vulnerabilities truly came to the forefront of the electric sector and critical infrastructure protection in 2008. In January of that year, the Federal Government reported that multiple U.S. utility companies had been extorted by the threat of cyberattack from foreign entities and that many non-U.S. utility companies had actually been cyberattacked resulting in power disruptions [140].

In addition to varying ages of equipment and ICS systems within the grid mentioned in the previous section, many ICS vendors typically utilize proprietary software. While initially a benefit to legacy systems' security, proprietary ICS created significant difficulty for the utility operators who had to deploy, operate, maintain multiple variants of ICSs and digital systems operating on the network [141], [140]. As the proprietary ICS proliferated on the network, International Society of Electrical and Electronics Engineers (IEEE) led an effort to standardize the ICS environment to increase interoperability between electricity system components.

However, the standards that IEEE championed still did not mature at a time when cybersecurity was an issue. Due to their low security and commonality among the majority of networks, standard protocols eroded the "unique" nature of proprietary systems and made it easier for cyber-aggressors to exploit [65], [140]. Distributed Network Protocol version 3 (DNP3), International Electrotechnical Commission (IEC) 60870-5-101 and Modbus, for instance, are used widely throughout the power system but could be used to access utilities' ICSs [65]. In aggregate, as ICS reached increased levels of sophistication and integration with the physical systems of industrial plants, they became prime targets for cyber-aggressors.

2.2.5.3 Convergence of Information Technology and Operational Technology

Once separate networks, IT and OT systems have become increasingly connected. Initially, OT systems were purpose-built, proprietary, and highly-specialized to achieve the level of capability required to operate the grid and were characteristics not found in early IT systems. Much like the physical plant equipment, OT systems were the domain of engineers and system operators, not IT professionals, and were used to control all facets of the grid.

However, as IT systems leaped forward in capability, became less expensive, and generally ubiquitous, the value of integrating IT and OT emerged. The convergence of these two networks was initially prompted by the requirement for OT systems to help achieve increased competitiveness in the marketplace. Specifically, utilities wanted to expand capabilities for OT data generation, including "billing, customer service, forecasting, and other responsibilities" [79, p. 9]. Even newer technologies and concepts, such as Smart Grid, have increased the integration of these systems.

IT standards are now being used on OT devices and systems to increase compatibility with less expensive IT hardware integrated into the OT environment [142]. As older proprietary OT system components are phasing out, standard processors, e.g., Intel, and operating systems, e.g., Windows, are being incorporated [143]. In addition to increased efficiency from easily operated and interoperable components, combining the networks also realizes cost savings in bulk pricing from operating and maintaining standardized networks. Nonetheless, the convergence between the systems produces increased attack vectors for cyber-aggressors. Figure 2.14 reveals how threat vectors, shown in gray, have increased as the electricity sector has become more digitized, and the IT and OT systems converge [3, p. 5]. The figure also implies that cybersecurity of the grid will continue to become more complicated and attacks more likely as connected network devices multiply and cultural and human issues more strongly influence the security of systems.

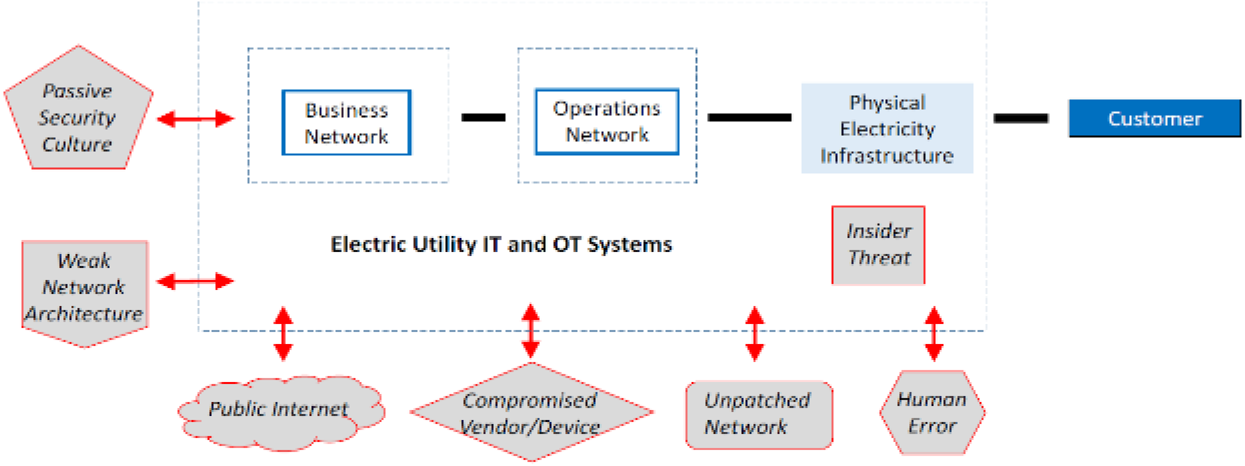


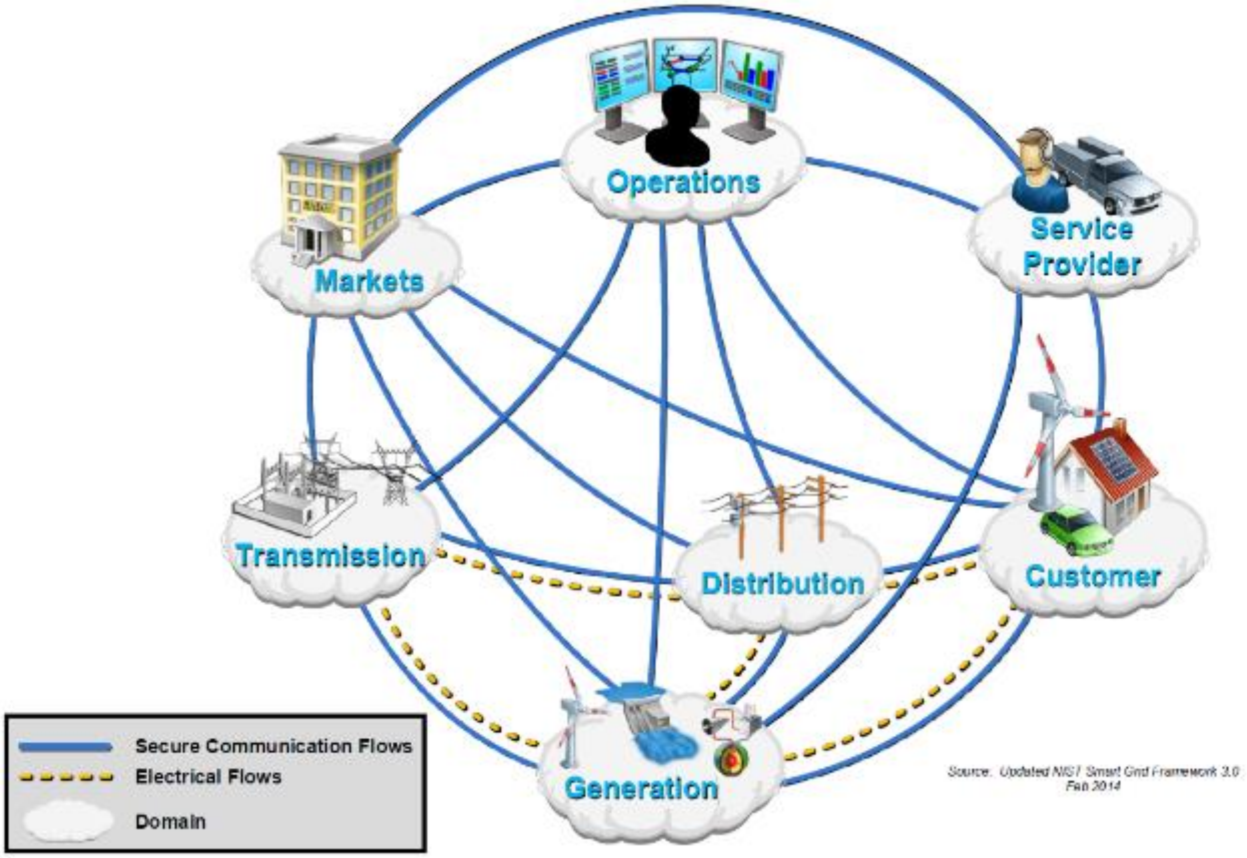
Figure 2.14: Electric Utility Cyberattack Vectors due to IT/OT Convergence

2.2.5.4 The Smart Grid and Cybersecurity

As the IT and OT systems have converged in many electric utilities' operating models, the merger has enabled drastic advancements in the management and capabilities of the grid to provide reliable, renewable, high quality, and less expensive electricity. Collectively, these advancements have become vital components of the Federal Government's initiative to modernize the power grid and are referred to as the smart grid [144].

Under the Energy Independence and Security Act of 2007, NIST is charged with developing the smart grid standards and protocols, including cybersecurity guidelines [85]. NIST defines seven domains, each of which encompasses the roles, services, and requirements that enable the functionality of the smart grid [85], [145]. The seven domains are shown in

Figure 2.15 and demonstrate the interconnected nature of the various systems associated with each domain [85, p. 128].



Source: Updated NIST Smart Grid Framework 3.0 Feb 2014

Figure 2.15: NIST Conceptual Model of the Seven Smart Grid Domains

The implications for cybersecurity are enormous. From the conceptual model, the radical shift in the electricity sector and its cybersecurity may not be apparent. Instead, Figure 2.16 shows more succinctly the required changes to legacy electricity sector systems as the grid becomes smarter [85, p. 139].

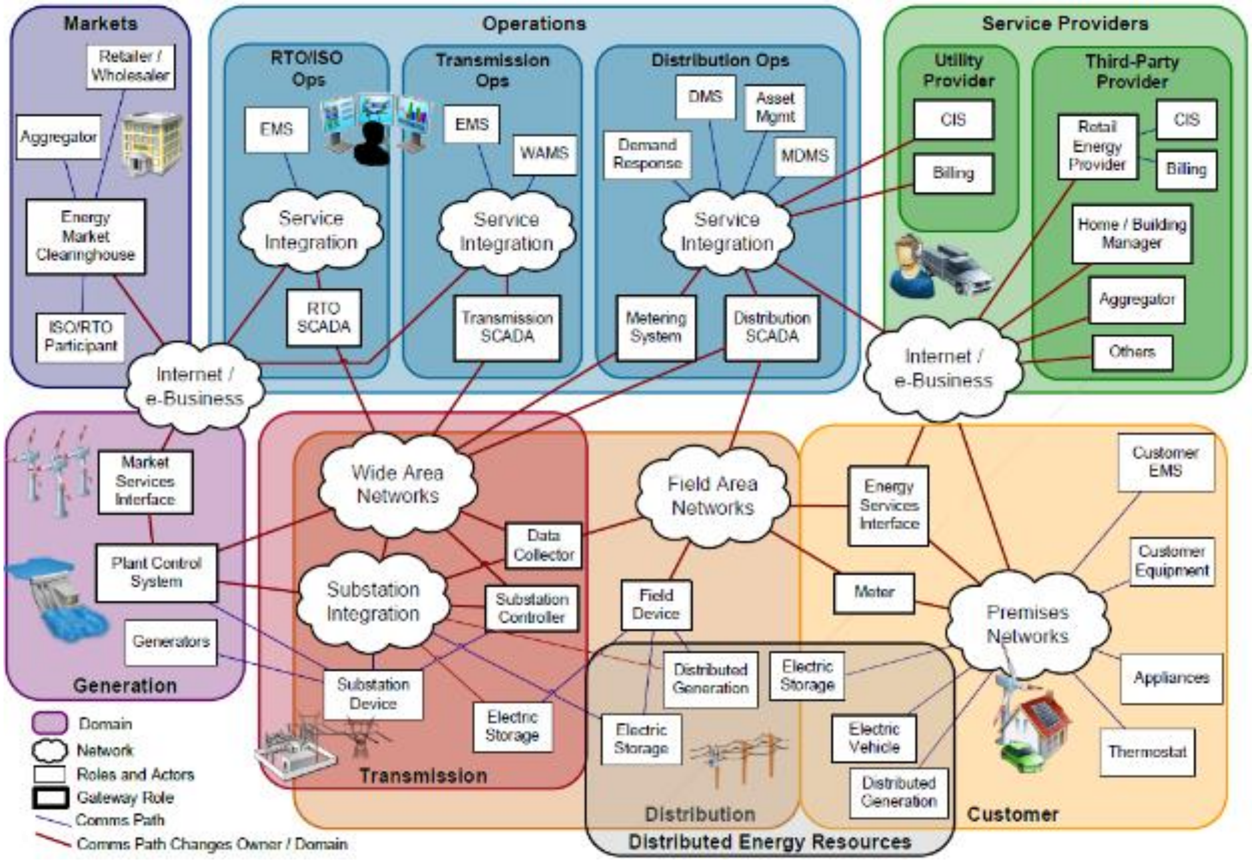


Figure 2.16: Model of Legacy Electricity Sector Systems Mapped onto NIST's Smart Grid Domains

An in-depth description of all smart-grid technologies and systems is outside the scope of this paper, but the summary of critical technologies that follows provides insight into how new are affecting the cybersecurity of the grid [85].

Advanced Metering Infrastructure (AMI)

AMI provides real-time monitoring of energy consumption for commercial, industrial, and residential consumers. These "smart meters" communicate between consumers, utility providers, and other third parties, and using meter data management systems (MDMS), advanced capabilities, such as enable demand response, can be realized.

Demand Response

Programs established between utilities and consumers wherein consumers reduce energy consumption during peak times or when reliability is at risk in exchange for a level of compensation. Demand Response Management Systems (DRMS) ties together AMI, MDMS, and other IT/OT systems to provide levels of automation to control enrolled consumers assets, transmit and collect data on loads, perform measurement and verification to establish compensation, among others.

Distributed Energy Resources (DERs)

DERs in the form of solar, small generators, or combined heat and power (CHP) have existed in as local generation sources in the grid for decades. Due to recent advances in technology and government energy policies, DERs have reached a high level of penetration into power grids, causing utilities to reconsider the most effective means to manage their place within the grid [146]. Benefits of DER penetration include aggregation into virtual power plants, creation of capacity and ancillary service markets to increase grid reliability, and the creation of microgrids that can operate as an island when the larger grid is disrupted [85]. Distribution Energy Resource Management Systems (DERMS) are those automated and digital systems that enable the benefits from DERs to be realized.

Distribution Management System (DMS)

As major physical components of the BPS and distribution systems are upgraded, improved with smart devices, and networked, DMS provides wide-area situational awareness of grid components and performance using data from DERMS, MDMS, Distribution SCADA, and other systems that utilities use to operate their systems and manage their enterprise such as Geographic Information Systems (GIS) and Outage Management Systems (OMS) [85].

All of these systems are increasingly incorporated into electric utilities' operating models, and as technology continues to develop, these systems will likely add capability but also complexity. The requirement for physical infrastructure and network capabilities in order to for them to operate correctly, and as previously explained, the convergence of IT and OT systems, old and new systems, and advanced technologies create significant cyber vulnerabilities.

2.2.5.5 Supply Chain Issues

Past cyber incidents have been perpetrated as utilities installed or connected new devices which were delivered with cyber compromises already installed [140]. In recent years, the risks associated with OT and IT supply chain have come to the forefront as one of the most significant cyber threat vectors to the electricity grid. As these systems increase in complexity, vendors are increasingly reliant upon multiple third-party manufacturers spread across multiple countries to design, assemble, and deliver a single product. Supply chain risk is significant enough that in 2016 FERC issued Order No. 829 for NERC to develop reliability standards that addressed supply chain risk management and approved them in Order No. 850 in October of that same year [147], [148]. FERC cited that cyber supply chain risk could arise from:

> [*I*]*nsertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development processes. Even well-designed products may have malicious components introduced in the supply chain, and it may prove difficult to identify these components before they are deployed [149, p. 1].*

To counter the new threat vector, NERC and the electricity sector have responded with a profusion of best practices and techniques to mitigate the risk posed from the supply chain [142], [148], [149].

2.2.5.6 Cybersecurity Technologies for the Grid

Further adding to the challenge of eliminating malware vulnerabilities and potentially inhibiting effective cyber response is the status of cybersecurity technology in the electricity sector. Investment in cybersecurity technologies for ICS in the electricity sector follows the risk management frameworks outline in section 2.2.2.4. Technologies and tools include data diodes, encryption, firewalls, intrusion detection and prevention systems, malware and anti-virus software, and vulnerability assessment tools. Managed security service providers (MSSP) also provide tiered services that include constant monitoring, evaluation, response, and forensics using these technologies [82].

While the technologies have proven to increase the cybersecurity of ICS, they also contribute to information asymmetries present in the sector. Many utilities must use multiple cybersecurity systems and manufacturers throughout their network. Each of these must be managed, monitored, and updated appropriately. Even with some measures in place, utility owners and operators question if they have sufficient defenses or, conversely, have misplaced confidence in the cybersecurity of their systems [126], [125]. Further analysis of these technologies and their effect on the electricity sector's cyber response is presented in Chapter 4.

2.2.5.7 Technology Factor Analysis

The electricity sector's adoption of new technologies into their ICS environments brings added vulnerabilities and new threat vectors too numerous to go into detail here. In summary, Glenn et al. (2016) put it best:

> *The growing presence of so many peripheral components and expanded interconnectedness and interdependence of systems used by utilities in conjunction with or to add capabilities to their production control systems has contributed to the changing nature of cyber attacks against the energy sector [65, p. 14].*

Further, unlike purely digital or information systems which most often seek to capture data, cyberattacks most frequently target the disruption of the grid's cyber-physical elements. As such, coordinating an attack on complex cyber-physical systems such as the electricity grid is substantially more complicated than one on an IT system, but the severity of the consequences, which can include injury and equipment damage, is also higher. The required sophistication of a cyberattack also means that the cyber response must be equally, or more sophisticated, to be effective [65].

The introduction of standard, non-proprietary components provides cyber-aggressors with commercially available, familiar, and easily exploitable attack vectors. The proliferation of new networked devices on ICS increases the difficulty of keeping track of connectivity, and the use of legacy systems with them compounds the difficulty of determining a system's vulnerabilities, diagnosing cyber incidents, and responding accordingly.

The rapid pace of change in IT systems is asynchronous with capital intensive ICS and OT systems. IT life-cycles are measured in years, whereas OT systems are measured in decades.

Maintaining the compatibility and cybersecurity of OT firmware on perhaps hundreds of devices on a utility's network is all the more difficult and costly.

Additionally, the integration of IT and OT systems has not been followed by equal integration in the career fields. Even as the networks are interconnected and would be difficult to separate, IT and OT professionals may be unfamiliar with the operation and cybersecurity of devices and software on their networks. The lack of familiarity with network configuration is compounded by the relative separation of IT professionals in one department and OT engineers and operators in another. Vulnerabilities "due to misconfiguration, poor administration, lack of perimeter awareness, communication shortcomings, among others," arise as a result [65, p. 12].

Interconnectivity with each other is the foundation of smart grid technologies. While the smart grid capabilities increase efficiencies and provide benefits as outlined above, it also drastically increases the cyber threat surface. Billions of new sensors, most of which will be outside of utilities' firewalls and other cybersecurity measures, will be installed each year to enable smart grid functions and modernize the electric power system. Likewise, as the grid continues to modernize and grow, technology advances, and competition for electricity system components increases, the supply chain risk for the billions of additions will grow as well.

Finally, risk management strategies in the electricity sector favor flexibility to allow utilities to navigate the complicated regulatory environment and tailor investments to their resource and capability constraints. However, the lack of regulations which require utilities to apply tested technologies and continually seek enhancement of their cybersecurity postures leads to degraded security across the sector. No technology or set of technologies can completely mitigate risks, and investments to reduce risk to that degree would be prohibitive. Still, sufficient evidence exists which suggests that the sector chronically underinvests in technologies, such as intrusion detection systems, capabilities, such as whitelisting, and services, such as response and forensic capabilities, that demonstrate the need for clear but mandatory cybersecurity requirements.

2.2.6 Market Factor

2.2.6.1 Wholesale Power Market and Cybersecurity

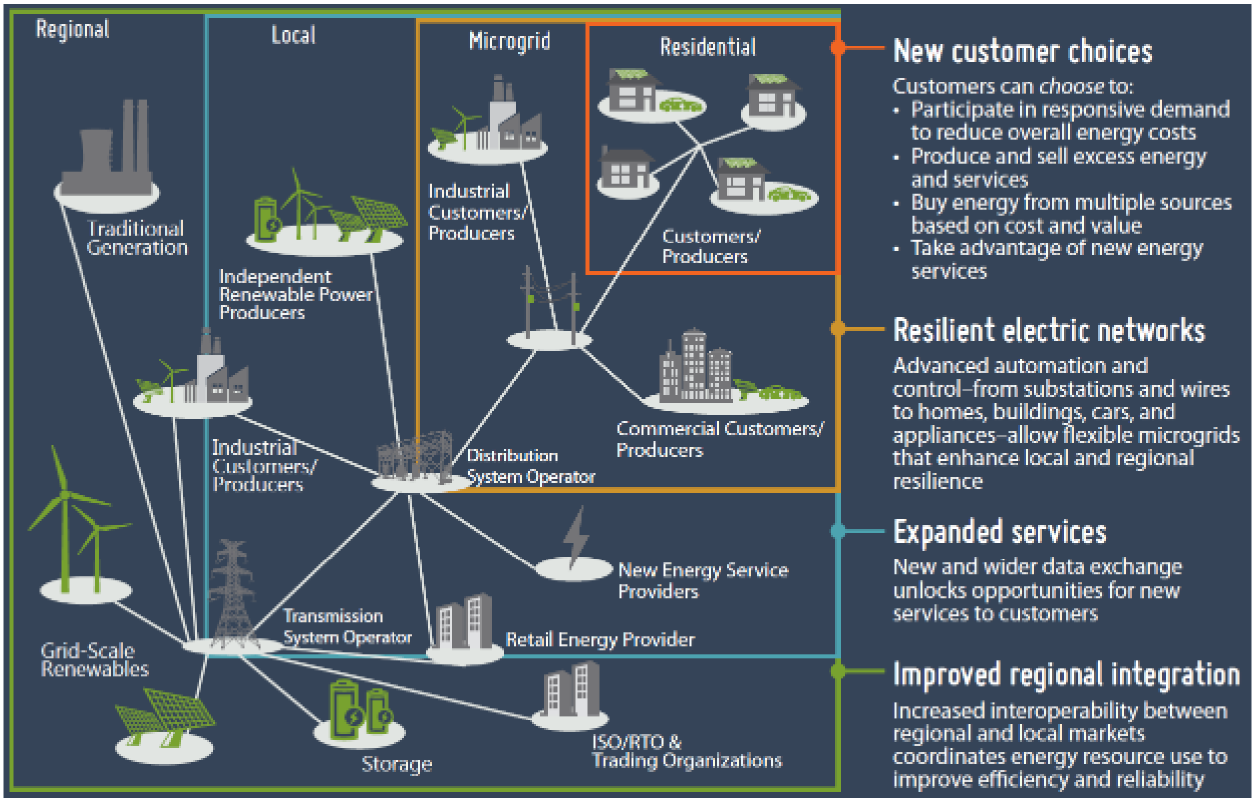
The wholesale power market has already been discussed within the regulatory context in section 2.2.2. However, it is worth noting that while bulk generation of electricity is competitive within market participants, usually overseen by RTOs or ISOs, many other features, particularly distribution and transmission services, are mostly non-competitive due to their natural monopoly over a geographical area. The lack of competition has two main effects on the cybersecurity of the U.S. electricity sector.

First, utilities are generally more willing to work together to address mutual challenges by pooling or exchanging resources, advocating for policy, and sharing best practices. A good example is the ESCC's Cyber Mutual Assistance (CMA) program in which participating utilities agree to share services, personnel, and equipment in response to a cyber incident [150].

Second, as discussed in section 2.2.2.4, the lack of market competition between electricity providers may mean that utilities, particularly ones that do not fall under NERC CIP regulations, are not directly incentivized to invest in cybersecurity. Because consumers cannot switch between utilities due to the electricity companies' natural monopoly, there is no incentive for companies to provide better, more reliable service than other competitors. If competition existed, utilities might fear loss of revenue from customers switching to more reliable and cyber resilient providers [80]. More specifically, a distribution utility might not invest in cybersecurity measures to a level that corresponds to the risks it faces. Regulatory fines or loss of business to a competitor following a cyber incident is not a motivating factor for a distribution utility, and it may even be able to pass along the cost of the attack to its customers through increased electricity rates.

2.2.6.2 Transactive Energy

Smart grid technology, as described in section 2.2.5.4, directly enables transactive energy markets. Unlike the traditional single flow of power from the utility to consumer, transactive energy harnesses DERs, ADMS and other smart grid technologies to enable the buying and selling of electricity and direct control of loads between end consumers and utilities [151]. Figure 2.17 is the transactive energy conceptual model developed by GridWise, the entity that the DOE chartered to "enable all elements of the electric system to interact," that demonstrates the complexity of the transforming electricity market [151, p. v], [152].


Regional
Local
Microgrid
Residential
Traditional Generation
Independent Renewable Power Producers
Industrial Customers/ Producers
Customers/ Producers
Industrial Customers/ Producers
Distribution System Operator
Commercial Customers/ Producers
New Energy Service Providers
Grid-Scale Renewables
Transmission System Operator
Retail Energy Provider
Storage
ISO/RTO & Trading Organizations

New customer choices

Customers can *choose* to:
- Participate in responsive demand to reduce overall energy costs
- Produce and sell excess energy and services
- Buy energy from multiple sources based on cost and value
- Take advantage of new energy services

Resilient electric networks

Advanced automation and control–from substations and wires to homes, buildings, cars, and appliances–allow flexible microgrids that enhance local and regional resilience

Expanded services

New and wider data exchange unlocks opportunities for new services to customers

Improved regional integration

Increased interoperability between regional and local markets coordinates energy resource use to improve efficiency and reliability

Figure 2.17: Interactions of Transactive Energy at the Transmission, Generation, Distribution, and Consumer Levels

The formation of GridWise and the penetration of smart grid devices demonstrates that the commitment towards adopting the transactive energy market is apparent and unavoidable

[151]. The IEEE Power & Energy Society Smart Buildings, Loads and Customer Systems working group called Meshing Smart Grid Interoperability Standards to Enable Transactive Energy Networks is another such example [153].

However, the implications for cybersecurity of the power grid cannot be overstated, and a literature review reveals that most current research focuses on the control systems and infrastructure aspect of the management systems [154]. Krishnan et al. (2018) reviewed multiple approaches for transactive energy to take shape and demonstrated ways for smart devices to encounter a cyberattack. Balda et al. (2017) perform a similar review of transactive energy's impact on the cybersecurity of electronics that support it and make the case that new solutions comprising "both hardware- and software-based mechanisms providing many layers of defense against cyberattack" are required [155, p. 42].

2.2.6.3 Market Factor Analysis

Based on interviews with key stakeholders, the wholesale power market, and specifically, the RTOs and ISOs in it, have started to recognize the role of market mechanisms to encourage proper cybersecurity investments. However, they remain without explicit support from regulatory bodies. In other markets, such as in the U.K., market mechanisms are used to encourage greater cybersecurity investment by allowing cost recovery and providing allowances for cyber resilience investments [156].

Additionally, the cooperative advantages of the non-competitive electricity markets have proven to work well for natural disasters. During Hurricanes Katrina and Sandy, for example, tens of thousands of restoration workers from unaffected utilities were quickly sent to repair downed systems. By nature, however, cyberattacks do not have geographic boundaries, and in those circumstances, it would be difficult for companies to determine if they were under attack or in danger of an imminent. The willingness to commit resources in another utility's response in the face of such uncertainty would likely be very low [157].

Finally, the overwhelming trend towards transactive energy is a complete paradigm shift in the energy market, and the impact will resound through every facet of the electricity subsector. Given the potential for extreme changes in profit, regulations, and investments, cybersecurity might become deprioritized or not properly incorporated as the market develops. Indeed, the GridWise Architecture Council's *Transactive Energy Systems Research, Development and Deployment Roadmap* (2018) fails to mention cybersecurity as a priority issue for its "Physical and Cyber Technologies and Infrastructure" track [158]. The work of Balda et al. (2017) and Krishnan, et al. (2018), however, implies that cybersecurity of these systems cannot be an afterthought, and must happen concurrently with the re-architecting and redesigning of the systems that support transactive energy. Given the shortage of research in the area, it is evident that cyberattacks may be likelier during the initial stages of the shift to transactive energy.

2.3 Motivations for Change

The need for better cyber resilience in the electricity sector is evident from the landscape analysis. However, the need exists to emphasize improved cyber response mechanisms, distinguished from other capabilities in the cybersecurity framework, such as preventative capabilities, which tend to supplant investments in cyber response. This thesis uses force field analysis, first proposed by Lewin (1951) and widely applied across multiple industries, to understand the forces that can drive change in response mechanisms and those drivers that restrain it [159], [160].

2.3.1 Force Field Analysis

The force field analysis depicted in Table 2-1 consolidates the analyses of the factors described in section 2.2 and results from key stakeholder interviews. The drivers are presented without priority and only according to the order in which the factors were explored. The drivers for change identify the problems and opportunities that motivate changing the cyber response mechanisms. Drivers against change are those factors that are barriers to change or indicate that change may not be necessary. Where similar problems existing in both categories, they are juxtaposed in Table 2-1.

Table 2-1: Force Field Analysis of the Drivers For and Against Changing the Cyber Response Mechanisms in the Electricity Sector

Factor	Drivers for Change	Drivers Against Change
Regulatory	Rapidly increasing cyber-aggressor capabilities	Confidence that cyber-aggressor capabilities can be defended against
	Lower requirement for resources as malware increases in capability and becomes more accessible	Confidence that cyber-aggressors require significant resources to attack
	Increased likelihood of an "accidental" cyberattack caused by cyber-aggressor testing in complex ICS environment	Confidence that cyber-aggressors' motivations support nation-state actions and a widespread attack would only be executed as a declaration of war or another major international incident
	Complex regulatory environment that diminishes the ability to achieve consistent cyber resilience standards and drives towards compliance-based cybersecurity	Confidence that regulatory compliance means a system is "cybersecure"
		Lack of experienced, qualified cybersecurity workforce with ICS specialty in both public and private sectors
		Inability to recoup cybersecurity investments
Political	Importance of reliable, resilient power to the U.S. economy and public welfare	
	Increased Federal oversight or partial nationalization of electricity systems	
	Recognition in Federal Government that past strategies are no longer sufficient	Lack of clear insight into the role of the Federal Government to enhance cyber resilience in CI sectors
Economic		High barriers to trust between electricity sector stakeholders
		Lack of incentives to cooperate, collaborate, and invest in cyber resilience and cyber response
		Paradigm shifting in the regulatory environment between risk-based & rules-based cybersecurity approaches
		Unknown costs to increase the cyber resilience of the grid to match risks (assumed to be expensive)
Technology	Product evolution of IEDs, ICS, & IT/OT systems	
	A mix of legacy and new systems in grid that creates unknown vulnerabilities	
	Rapid convergence of IT/OT technologies	
	Proliferation of smart grid technologies	
		Confidence in continually evolving and unverifiable cybersecurity technologies
Market	Recognition by BPS operators of need for market mechanisms to encourage investment in cybersecurity measures	
		Confidence in untested cyber mutual assistance programs based on dissimilar disaster mutual assistance programs
	Confidence in inevitable adoption of transactive energy markets which require orders of magnitude more cyber-physical infrastructure and create corresponding vulnerabilities	Focus on control systems technology to enable transactive energy market without incorporating cybersecurity as a priority

A few trends emerge from studying the force field analysis. First, almost all of the drivers against change can be framed to indirectly create vulnerabilities which, in turn, become a driver for increasing cyber respond mechanisms. For example, a lack of experienced, qualified cybersecurity workforce with ICS specialty in both public and private sectors is a driver against change because it limits the ability of the sectors to identify cyber resilience issues and have advocacy for improving cyber response mechanisms, among others. However, the lack of cybersecurity personnel may also lead to the creation of vulnerabilities in misconfigured IT/OT systems, suboptimal investment in cybersecurity technologies, or a weak culture of cybersecurity, and ultimately, cyber response mechanisms (perhaps even more resource-intensive ones) are needed to counteract the reinforcing behavior of vulnerability creation. To fully explore the impact of this reinforcing behavior on cyber response mechanisms, it is necessary to account for other influences.

Another trend that emerges from the force field analysis is that many of the drivers against change are informational. Specifically, they are based on widely-held (but not universally-held) perceptions on the state of cybersecurity and cyber response in the electricity sector. This further implies that information asymmetries deeply influence the behavior of the sector.

Together, these trends begin to depict critical system dynamic of the electricity sector. Namely, the reinforcing behavior of vulnerability creation caused by differing perspectives, the accuracy of the information, trust among stakeholders, and other information asymmetries. Further examination of the specific effects of this dynamic on current cyber response mechanisms is necessary and is discussed in chapter 4.

2.4 Chapter 2 Summary

Predictably, analysis of the six factors in this chapter confirms that the electricity sector faces the same challenges with cyber resilience as do all other critical infrastructure sectors. Comparably, the same challenges apply to all of the “cybersecurity core functions,” i.e., identify, protect, detect, respond, and recover [24]. However, these factors affect cyber response mechanisms in the electricity sector in unique ways.

First, the cyber threat analysis demonstrates that a large-scale cyberattack may not be an act of war by a nation-state cyber-aggressor. Instead, as threats and capabilities evolve, cyberattacks may become political tools for all types of cyber-aggressors to wield. Thus, the sector must be prepared to respond to a cyberattack as an eventuality.

Even though a large-scale cyberattack is inevitable, the degree to which it impacts the sector is in question. The nature of grid architecture, reliability, and robustness of cyber prevention mechanisms may stymie cyber-aggressors’ ambitions for a catastrophic power failure, but the chore becomes determining what impacts to the sector can reasonably be expected and how to respond and mitigate them.

Second, political and regulatory approaches to governing the electricity sector can be characterized as passive. When threats to the electric grid were largely non-cyber related, such an approach was feasible and even beneficial. As cyber threat vectors rapidly evolve and threat surfaces quickly expand, the same approach has become obsolete and must shift from encouragement of preventive measures to preparation of robust response mechanisms at the regional and sector-wide levels.

Finally, the information asymmetries that plague the sector's ability to build cyber resilient must be addressed authoritatively. The current mode of thinking is to create market mechanisms that govern cybersecurity. However, this premise is built upon the assumption that cybersecurity practices by utility companies will adapt to minimize risk. Unfortunately, the information disparities discussed in section 2.2.4.1 prevents the market from adjusting accordingly. Reinforcing this behavior, the culture of cybersecurity (discussed in greater detail in 4.3.1) has created an environment where stakeholders' perspectives about the likelihood of an attack, definitions of cyber resilience, and proper cybersecurity investments have diverged, entrenched themselves, and obstructed adaptions to present-day threats.

Collectively, these factors reveal the expansive scope of the problem with cyber response in the electricity sector and require a broader interpretation of influences on it. In particular, the definition of electricity sector stakeholders exceeds the bounds of traditional definitions. Thus, a thorough stakeholder analysis is necessary to understand why and how to change the sector's cyber response mechanisms.

3 Stakeholder Analysis

As of 2017, there were over 3,300 utilities which provided generation, transmission, and distribution to consumers across the U.S. As one of the most heavily regulated industries in the nation, Federal, state, and local governments play a significant role in cyber response mechanisms of the electricity subsector. Additionally, the supply chain that provides physical and digital assets and services to utilities make up another critical dimension of the electricity sector. Indeed, there are thousands of stakeholders in the electricity sector most of which have distinct perspectives, risk management strategies, resources, capabilities, and requirements when it comes to appropriate response mechanisms for a cyberattack at scale.

This paper asserts that the underlying gaps in the sector's response mechanisms are primarily born from differing perspectives and interests that need to be more fully aligned. Whether consensus can be reached on the nature of cyber threats or how to best respond to cyberattacks, the fact remains that the diversity of the stakeholder perspectives dramatically inhibits the ability for the sector to be able to respond. Thus, a thorough analysis must be performed in order to bring perspectives into the open, find ways to align interests, and ultimately, formulate the best cyber response mechanisms.

Chapter 3 presents the results from stakeholder interviews and open source research on electricity sector stakeholders to understand their diversity in the industry. It applies techniques to identify and analyze stakeholder needs for competent individual and sector-wide response to a malware attack. It also identifies which stakeholders can influence and change cyber response mechanisms to close any gaps discovered in the analysis.

3.1 Interview Methodology

Key stakeholders were identified as those entities which could represent broad categories of electricity sector stakeholders and could provide insight on behalf of their peers. This thesis used the categories of stakeholders established in REMEDYS research. A minimum of three stakeholders in each category was identified and contacted for interviews. Subsequent stakeholders were identified through interviews and leveraged relationships built through the interview process. National laboratories, universities, and researchers were combined into a single category because they performed the same roles in the electricity sector. A total of 28 interviews were conducted with the breakdown and stakeholder description by category listed in Table 3-1. In all cases, interviewees requested to remain anonymous, so perspective gained from the interviews is not attributed to a single entity herein.

Table 3-1: Initial Categorization for Stakeholder Interviews

Category	Stakeholder Description	Interviews Conducted
ICS Vendors, Manufacturers, and Suppliers	Producers of programs used to operate cyber-physical assets in the electricity sector	2
Utility Companies	Companies involved in the electricity market, including generation, transmission, distribution, and wholesale and retail sales of power	9
Cybersecurity Companies	Companies that supply cyber resilience and cyber response products and services to utility companies	2
National Laboratories, Universities, & Researchers	Organizations that develop frameworks, standards, guidance, technology, and processes to improve electricity sector cyber resilience	5
Government	Federal, state, local, tribal, and territorial government entities who make policy, regulate, and support the electricity sector, particularly those in formal government response plans	10

It is important to note that this thesis does not assert that the stakeholder analysis is complete, and unless tens of thousands of interviews were conducted, a full picture of stakeholders' needs and value propositions could not be formed. Instead, the stakeholder interviews sought to identify trends in the sector that could indicate gaps in its ability to respond to a widespread malware attack and direct the research. Future phases of the REMAED project intend to validate the findings of the stakeholder analysis through multi-stakeholder events and additional interviews.

Interviews generally lasted 45-60 minutes and questions focused on the interviewee's perspectives on limited topics, including:

- Cyber threats to the electricity sector which could have widespread consequences
- Interviewee's (or their organization's) role in electricity sector response mechanisms
- Current cyber response mechanisms
- Perceived adequacy, barriers to improvement of, and gaps in current electricity sector response mechanisms to large scale malware attacks
- Potential solutions to close gaps in the sector's cyber response mechanisms

3.2 Stakeholder Descriptions and Roles

The historically fragmented nature of the electricity sector and its sheer size has produced a convoluted network of stakeholders. Deregulation, while arguably improving market performance, instigated further fragmentation as each state deregulated in different manners, and the effects of deregulation on the industry have yet to arrive at a steady state [161]. As a result, many of the roles that comprise grid operation and regulation, as shown in Figure 3.1, may be consolidated under one organization in a given geographic area while they may be performed by multiple entities in another [13, p. 4.4]. Additionally, past consolidation and the complexity of stakeholders has led to conflicts of interest which remain today [162], [163].

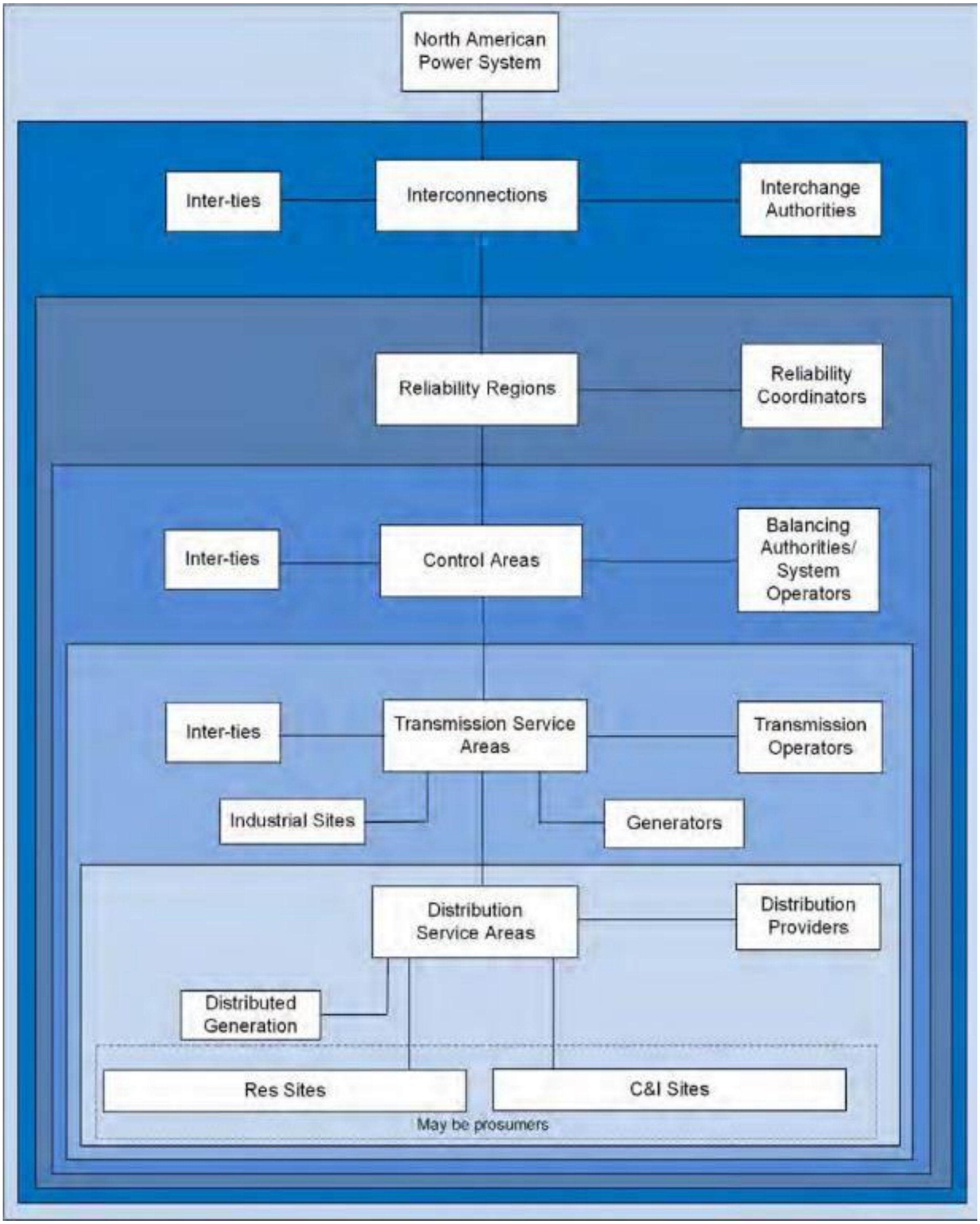


Figure 3.1: Electricity Sector Delivery Functions

What has emerged is a set of electricity sector stakeholders that are broadly characterized as decentralized, redundant, and incoherent with heterogeneous business models, interests, and priorities for cyber resiliency. For example, Figure 3.2 is the Electricity Information Sharing and

Analysis Center's (E-ISAC, see below) Grid Exercise (GridEx) IV communications plan which reveals the complexity of communicating across the electricity sector's stakeholders [164, p. 17].

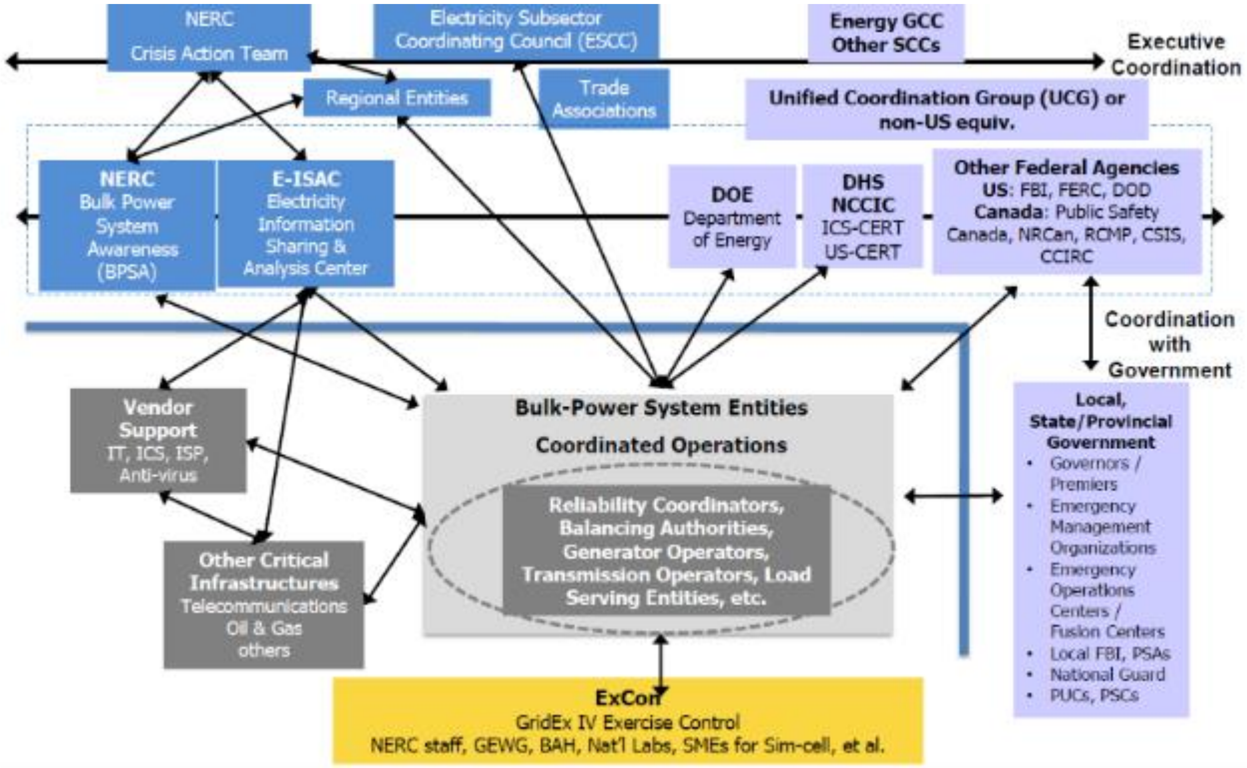

NERC
Crisis Action Team
Electricity Subsector Coordinating Council (ESCC)
Energy GCC
Other SCCs
Executive Coordination
Regional Entities
Trade Associations
Unified Coordination Group (UCG) or non-US equiv.
NERC
Bulk Power System Awareness (BPSA)
E-ISAC
Electricity Information Sharing & Analysis Center
DOE
Department of Energy
DHS
NCCIC
ICS-CERT
US-CERT
Other Federal Agencies
US: FBI, FERC, DOD
Canada: Public Safety Canada, NRCan, RCMP, CSIS, CCIRC
Coordination with Government
Vendor Support
IT, ICS, ISP, Anti-virus
Bulk-Power System Entities
Coordinated Operations
Reliability Coordinators, Balancing Authorities, Generator Operators, Transmission Operators, Load Serving Entities, etc.
Local, State/Provincial Government
• Governors / Premiers
• Emergency Management Organizations
• Emergency Operations Centers / Fusion Centers
• Local FBI, PSAs
• National Guard
• PUCs, PSCs
Other Critical Infrastructures
Telecommunications
Oil & Gas
others
ExCon
GridEx IV Exercise Control
NERC staff, GEWG, BAH, Nat'l Labs, SMEs for Sim-cell, et al.

Figure 3.2: GridEx IV Communications Plan

The impact of such a complex and complicated ecosystem has diluted the ability to achieve industry consensus and form unity of action to increase cybersecurity, particularly cyber response, of the grid. Stakeholder perspectives and their real challenges are central to improving cyber resiliency, and this paper builds upon interviews from representative stakeholders to include both real and perceived challenges to an effective cyber response.

To better understand the relationships between stakeholders, especially as it applies to cyber resilience, it is necessary to catalog the sector's stakeholders. The cataloging begins, somewhat arbitrarily, with the regulatory bodies because they drive many of the cybersecurity-related facets of the other stakeholders. Stakeholders from the initial categories and other stakeholders discovered through interviews and research follow in no particular order.

3.2.1 Federal Energy Regulatory Commission (FERC)

FERC is the independent Federal regulatory agency that:

- *Regulates the transmission and wholesale of electricity in interstate commerce;*
- *Protects the reliability of the high voltage interstate transmission system through mandatory reliability standards;*
- *Monitors and investigates energy markets;*
- *Enforces FERC regulatory requirements through imposition of civil penalties and other means [165]*

The Energy Policy Act of 2005 granted FERC the authority to develop and enforce reliability standards on the BPS inclusive of cybersecurity standards. It develops cybersecurity requirements through the North American Reliability Corporation (NERC). FERC has openly acknowledged that the drivers of change mentioned above, particularly the incorporation of information technologies into grid operations, pose threats to the reliability to the BPS. Through the Energy Independence and Security Act of 2007, FERC coordinates the development and adoption of guidelines and standards to address the drivers [166].

Key Perspectives and Insights:

The process for incorporating regulatory changes tends to be slow, and there is an increasing concern that FERC will not be able to keep pace with how quickly the drivers are evolving and being implemented. Additionally, there is a widely held perception that the electricity sector is overregulated, and support for additional regulations, even for the benefit of cyber resilience, is generally lacking.

3.2.2 North American Energy Reliability Corporation (NERC)

NERC is "a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid" [167]. NERC was initially established as a voluntary organization by the industry itself to promote the reliability of the BPS in Canada, the U.S., and Mexico. Prompted by the Northeast Blackout of 2003, FERC designated NERC as the Electric Reliability Organization (ERO) as called out by the Energy Policy Act of 2005. NERC's status as ERO gave it authority for the following:

- *develops and enforces Reliability Standards;*
- *annually assesses seasonal and long-term reliability;*
- *monitors the bulk power system through system awareness;*
- *and educates, trains, and certifies industry personnel [167]*

NERC's Reliability Standards are broken down into 13 categories, as shown in Table 3-2. These standards include all of the functions necessary to reliably operate the BPS. In particular, the Critical Infrastructure Protection (CIP) standards include stringent regulations on the cybersecurity of assets and infrastructure that form the power grid. CIP standards are the primary mechanism by which cyber resilience is promoted by NERC.

Table 3-2: Categories of NERC Reliability Standards for the Bulk Electric Systems of North America [76]

NERC Reliability Standards	
Resource and Demand Balancing	Critical Infrastructure Protection (CIP)
Communications between BPS entities	Emergency Preparedness and Operations
Facilities Design, Connections, and Maintenance	Interchange Scheduling and Coordination
Interconnection Reliability Operations and Coordination	Modeling, Data, and Analysis
Personnel Performance, Training, and Qualifications	Protection and Control
Transmission Operations	Transmission Planning
Voltage and Reactive Control	

Additionally, NERC has identified 16 reliability functions as part of its Reliability Functional Model [168]. Recently, NERC has added cybersecurity requirements for nearly all of these functions. NERC also assigns the roles of the responsible party for that function. As was previously mentioned in 3.2, many of these roles are performed by the different entities in different areas of the country which adds to the difficulty in identifying consistent requirements for cyber response and existing gaps in the ability to respond. Relevant reliability roles are discussed in subsequent sections of this paper.

Key Perspectives and Insights:

There is a perception that CIP standards enforce only a minimal amount of cybersecurity protocols on electricity assets. CIP standards are prescriptive by nature in order to facilitate enforcement and in response to regulated entities' past actions which have interpreted ambiguity in the standards to avoid the required investment to comply. The prescription has the effect of disincentivizing compliance above those standards or, in some cases, does not permit higher standards of cybersecurity because it does not meet the specific standards. As with FERC, there is a concern that reliability standards will not maintain pace with industry evolution and changes in the cyber threat landscape.

3.2.2.1 Regional Entities

NERC delegates its ERO authorities to seven Regional Entities, as shown in Figure 3.3, which monitor and enforce compliance of reliability standards and, thus, have the mandate to enforce cybersecurity-related CIP standards [169].

Key Perspectives and Insights:

The regional entities work closely with the BPS operators and reliability coordinators within their jurisdiction. Regional Entities have a more intimate understanding of the unique requirements, specific structure of the regional electricity sector, and trusted interpersonal and organizational relationships with regional stakeholders.

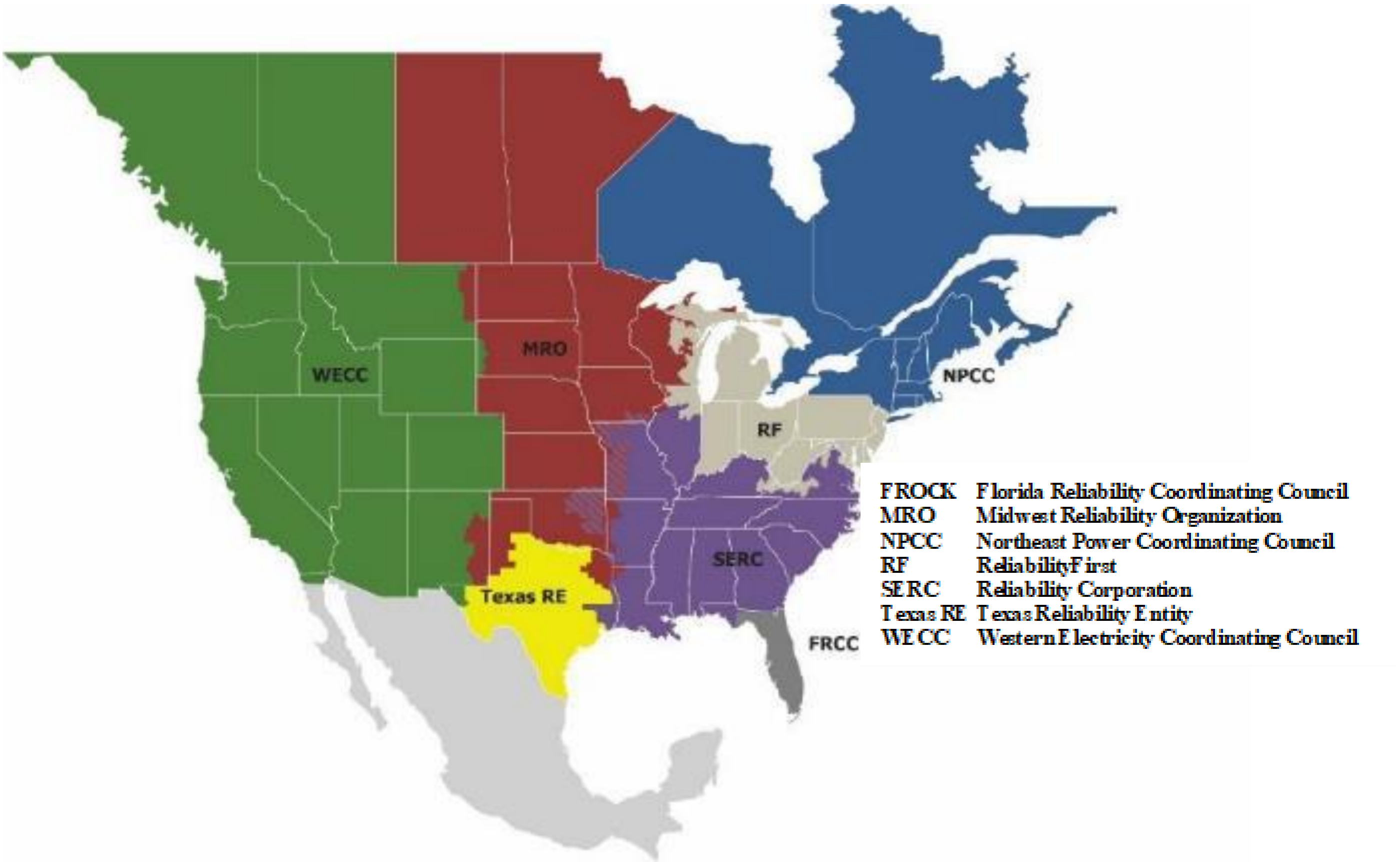

WECC
MRO
NPCC
RF
SERC
Texas RE
FRCC
FROCK Florida Reliability Coordinating Council
MRO Midwest Reliability Organization
NPCC Northeast Power Coordinating Council
RF ReliabilityFirst
SERC Reliability Corporation
Texas RE Texas Reliability Entity
WECC Western Electricity Coordinating Council

Figure 3.3: Seven NERC Regional Entities

3.2.2.2 Electricity Information Sharing and Analysis Center (E-ISAC)

According to the NERC website, the E-ISAC:

- *Gathers, analyzes, and shares cyber and physical threat alerts, warnings, advisories, notices, and vulnerability assessments security information provided by members;*
- *Provides an electronic, secure capability for E-ISAC participants to exchange and share information on all threats to defend critical infrastructure;*
- *Coordinates incident management;*
- *Communicates mitigation strategies with stakeholders across sectors; and*
- *Serves as a central point of coordination and communication for members [170].*

Additionally, it collaborates with the Department of Energy and Electricity Subsector Coordinating Council to serve "as the primary security communications channel for the Electricity Subsector and enhances the subsector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents*"* [108], [170]. While E-ISAC membership is free, it is open only to vetted electricity asset owners and operators and affiliates, government partners, and cross-sector entities. In addition to its stated mission, E-ISAC also conducts the biennial Grid Security Exercise (GridEx) which tests individual response plans and coordination measures in the event of a reliability failure. It provides reports to its members and hosts conferences. It also manages the Cybersecurity Risk Information Sharing Program (CRISP), a subscription-based service that allows Pacific Northwest National Lab to monitor BPS stakeholders' networks for potential cyber intrusions and fuses it with threat intelligence.

Key Perspectives and Insights:

E-ISAC was formed with separation protocols from NERC and chartered in a way so that any information shared with E-ISAC would not be reported to NERC and potentially lead to a violation of CIP requirements. Despite these measures and a concerted effort by E-ISAC, industry stakeholders remained distrustful. This attitude initially slowed E-ISAC participation and the speed of incident reporting and information sharing, severely limiting its effectiveness. Only recently has E-ISAC begun to overcome the stigma of its attachment to NERC, and the dynamic continues to inhibit the speed and effectiveness of information sharing.

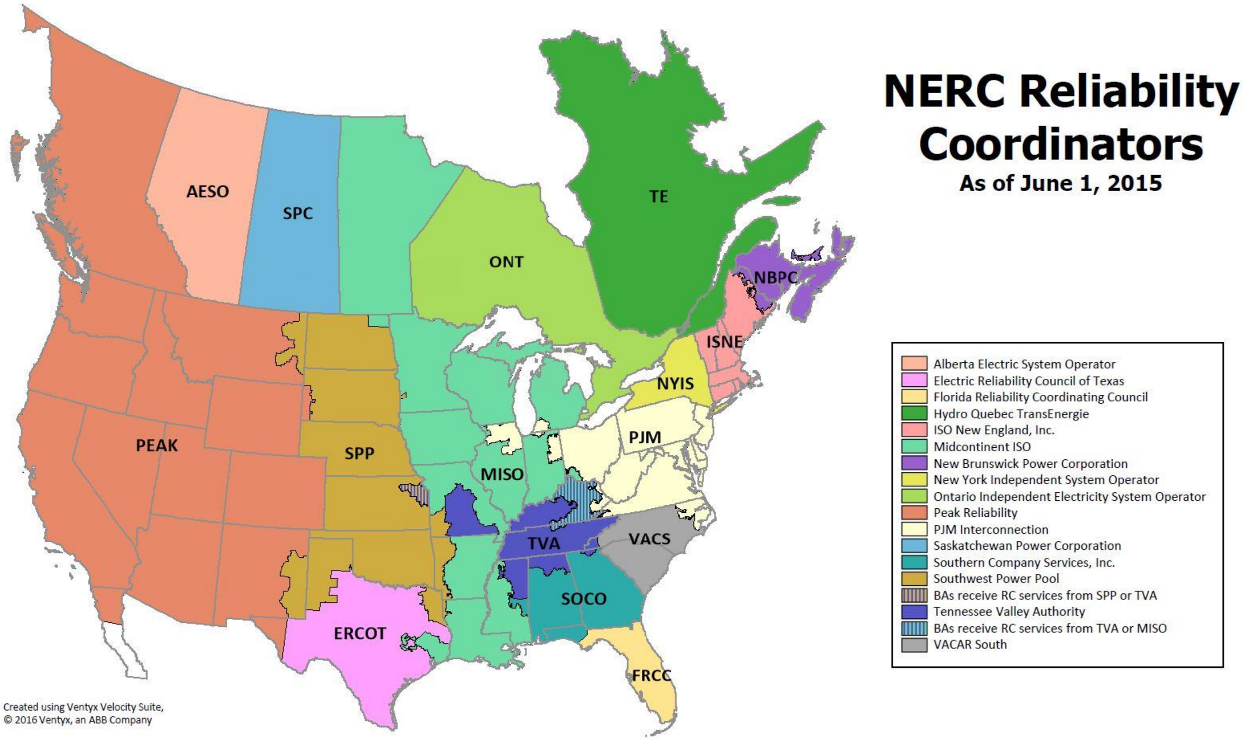
Similarly, GridEx III and IV, held in 2015 and 2017 respectively, revealed capability gaps in this response mechanism involving overwhelmed communications systems, difficulty integrating recovery resources between the public and private sector, and the challenge of prioritizing where to focus recovery efforts [171], [172]. Arguably, these issues arise at the limits of E-ISAC's authority to direct cyber response efforts.

3.2.3 Reliability Coordinators

According to the NERC Glossary of Terms, Reliability Coordinators are defined as:

> *The entity that is the highest level of authority who is responsible for the Reliable Operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations [173, p. 26].*

Per NERC guidelines, they have a requirement to "appropriate security protections for cyber assets and physical assets, and their related support systems and data" [168, p. 13]. There are 16 reliability coordinators for the regions of North America regulated by NERC, as shown in Figure 3.4 [174].


NERC Reliability Coordinators
As of June 1, 2015
AESO
SPC
ONT
TE
NBPC
ISNE
NYIS
PJM
PEAK
SPP
MISO
TVA
VACS
SOCO
ERCOT
FRCC
Alberta Electric System Operator
Electric Reliability Council of Texas
Florida Reliability Coordinating Council
Hydro Quebec TransEnergie
ISO New England, Inc.
Midcontinent ISO
New Brunswick Power Corporation
New York Independent System Operator
Ontario Independent Electricity System Operator
Peak Reliability
PJM Interconnection
Saskatchewan Power Corporation
Southern Company Services, Inc.
Southwest Power Pool
BAs receive RC services from SPP or TVA
Tennessee Valley Authority
BAs receive RC services from TVA or MISO
VACAR South

Created using Ventyx Velocity Suite,
© 2016 Ventyx, an ABB Company

Figure 3.4: NERC Reliability Coordinators

Key Perspectives and Insights:

Reliability coordinators, perhaps more than any other regulatory entity in the ecosystem, can improve cyber resilience and cyber response. Their roles were explicitly created to handle routine, abnormal, and emergency operations of the grid, and during a widespread cyberattack would likely be directing many, or perhaps all, response and recovery efforts.

3.2.4 Regional Transmission Operators / Independent System Operators (RTOs/ISOs)

Among many other stipulations of FERC 888, electric utilities engaged in electricity transmission were required to form operational authority of an electrical power system with the responsibility to monitor, coordinate, and control the electricity within their given grid.

In many cases, ISOs provide open access to their transmission assets independently of financial interests, decision-making, and tariff-setting for the use of their equipment. As shown in Figure 3.5, ISOs tend to administer an electrical grid within a single state but often operate in multiple states [175]. RTOs are similar to ISOs varying only in that they encompass a broader geographic region and have been designated as such by FERC [176], [177]. However, RTOs and ISOs do not exist in every region and serve about two-thirds of U.S. consumers [178]. In the regions they do exist, they may also have roles as interchange coordinator and balancing authority to approve flow of power throughout the grid, as shown in Figure 3.6 [169].

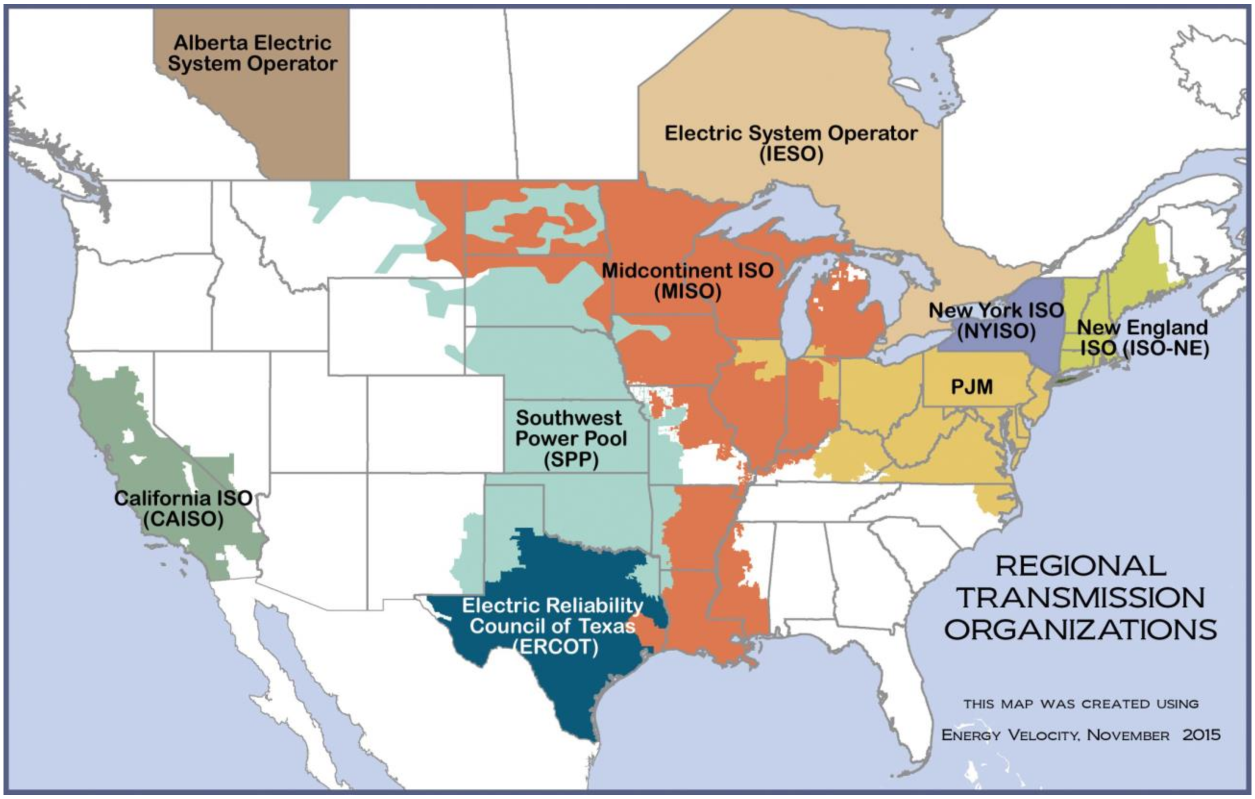

Alberta Electric System Operator
Electric System Operator (IESO)
Midcontinent ISO (MISO)
New York ISO (NYISO)
New England ISO (ISO-NE)
PJM
Southwest Power Pool (SPP)
California ISO (CAISO)
Electric Reliability Council of Texas (ERCOT)
REGIONAL TRANSMISSION ORGANIZATIONS
THIS MAP WAS CREATED USING
ENERGY VELOCITY, NOVEMBER 2015

Figure 3.5: RTOs and ISOs in North America

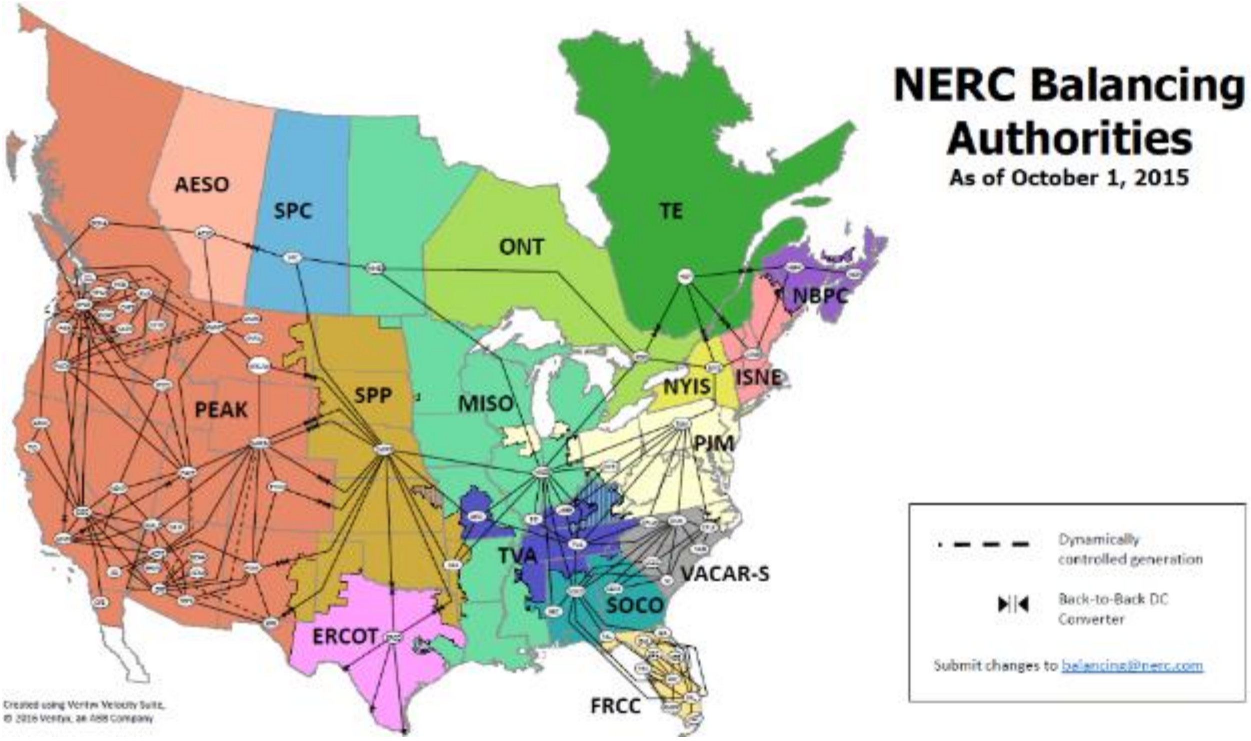

NERC Balancing Authorities
As of October 1, 2015
AESO
SPC
ONT
TE
NBPC
ISNE
NYIS
PJM
MISO
SPP
PEAK
TVA
VACAR-S
SOCO
ERCOT
FRCC
Dynamically controlled generation
Back-to-Back DC Converter
Submit changes to balancing@nerc.com
Created using Ventyx Velocity Suite,
© 2016 Ventyx, an ABB Company

Figure 3.6: NERC Balancing Authorities

Key Perspectives and Insights:

Pertinent to cyber resilience, NERC CIP standards significantly impact ISOs and RTOs approaches to the grid. Figure 3.4 reveals that in many instances, RTOs and ISOs serve as reliability coordinators in their geographical region. As such, RTOs and ISOs are in a unique position to oversee elements cybersecurity within their region. Further, their status as not-for-profit, independent entities and responsibility for grid reliability suggests that their actions are focused on balancing cybersecurity with the market forces.

3.2.5 Investor-Owned Utilities (IOUs)

Investor-owned utilities are privately held by shareholders or investors, and in many cases, these businesses include either or both of the components of electricity distribution and generation. There are approximately 63 investor-owned utilities in the U.S. nearly all of which have subsidiaries that serve over 220 million Americans. Of those 63 utilities, 20 of them provide 80% of the generation and distribution to the population they serve.

Due to IOUs size and interdependence on the BPS, particularly from their power generation, NERC CIP standards also apply to them. However, some investor-owned utilities do not own generation assets or are sufficiently small so as not to need to comply with CIP standards.

Key Perspectives and Insights:

Compared to Publicly Owned Utilities and Cooperative Utilities, IOUs tend to have the resources necessary to invest in cybersecurity measures and are motivated to invest because they profit from the provision of reliable service. In turn, the largest IOUs invest in research and development, have large, dedicated cybersecurity staff, and employ leading-edge cybersecurity measures. They often can extend cyber resilience programs to smaller utilities that engage with them. Nonetheless, cybersecurity investments remain a cost center for their business model, a cost not currently recoverable in electricity rates allowable under FERC and most public utility commissions guidelines [78].

3.2.6 Publicly Owned Utilities (POUs)

In contrast to IOUs, POUs include municipal utilities (munis) and Federal power programs, e.g., Bonneville Power Administration (BPA), and are organized at the local levels along district, city, county, or another service area. POUs are often governed by local government bodies or specially established commissions. They are typically smaller than IOUs serving between 1,800 and 100,000 customers. There are approximately 2,000 POUs that provide power to 49 million people in the U.S.[179], [180]. Ninety percent of the power provided by POUs comes from one-third of the POUs.

Similar to IOUs, many POUs have transmission and generation assets and must comply with NERC reliability and cybersecurity standards. They also foster cyber resilience by extending resources to smaller utilities that might not otherwise be able to afford it.

Key Perspectives and Insights:

A large portion of POUs do not own assets that trigger NERC regulation. While POUs are motivated to provide reliable power, their smaller size usually limits their ability to invest in cyber resilience measures. Trade associations and joint action agencies fill this void by pooling resources between members.

3.2.6.1 Cooperative Utilities

Cooperative utilities, or co-ops, are a subset of POUs that usually exist in rural areas where IOUs or POUs would likely be unable to sustain service because of the limited customer base. There are nearly 900 co-ops in the U.S., most of which provide distribution with limited transmission and generation activities. Co-ops provide power to 42 million people in the U.S., and their mandate is often focused on minimizing the cost of reliable electricity service. Their capital expenditures are usually funded through Federal loans from the Rural Utility Service, and operating costs are paid for by members [181].

<u>Key Perspectives and Insights:</u>

Co-ops represent the least resourced of the types of utilities, which manifests in limited staffing, outreach, and advocacy. These factors inhibit the ability for co-ops to access resources, such as information and cybersecurity professionals. Instead, they rely heavily on pooled resources, mutual assistance programs, and, in particular, the National Rural Electric Cooperative Association to help formulate cyber response [182].

3.2.7 Joint Action Agencies

Joint action agencies "procure and supply wholesale power and a range of advocacy, operational, and business services for groups of POUs, to leverage economies of scale" [179]. There are over 100 joint action agencies, one in almost every state. These agencies are often deeply involved in CIP compliance and other risk management and reliability issues affecting their constituents.

<u>Key Perspectives and Insights:</u>

Joint action agencies enjoy mutual trust and strong relationships with their members, which facilitates development and implementation of effective cybersecurity measures.

3.2.8 Power Marketers

Power marketers obtain status by applying to FERC. By FERC's definition, a power marketer is a "business entity engaged in buying and selling electricity. Power marketers do not usually own generating or transmission facilities. Power marketers, as opposed to brokers, take ownership of the electricity and are involved in interstate trade" [183].

There are hundreds of power marketers engaged in the buying and selling of wholesale electricity, and as of 2018, they supplied approximately 21% of the retail electricity in the U.S. They provide retail buyers with choices in suppliers of electric power by acting as intermediaries, in turn, creating a more competitive marketplace [184], [185].

<u>Key Perspectives and Insights:</u>

While not directly involved in cybersecurity or cyber response, power marketers may have economic incentive to trade electricity from more cyber resilient sources of power, much as they do with renewable energy sources.

3.2.9 Electricity Consumers

Electricity consumers are typically separated into residential and industrial segments based on the amount of power and energy they consume. Herein, they will be treated equivalently since their interests closely align.

Key Perspectives and Insights:

Electricity consumers' roles in the sector as it currently operates is clear. As DERs, such as solar panels and batteries, for example, IoT, and other smart grid technologies mature, the electricity sector will become more transactional. Consumers will become "prosumers" in the transactive energy market, capable of selling energy back to the grid, storing locally, and controlling demand in real-time among other things. The effect is presumed to increase the reliability of the grid as it decentralizes the sources of generation and reduces reliance on the many single points of failure in the larger grid [153]. However, it may simultaneously increase the cyber threat surface for the electricity sector, whereby new access points for malware can be injected, and the physical characteristics of grid operation may be more easily exploited [186].

3.2.10 U.S. Federal Government

In this context, the Federal Government consists of the Executive, Legislative, and Judicial branches, as outlined in the U.S. Constitution. Despite its role as provider for the nation's defense, including critical infrastructure security, the Federal Government has limited authority to direct private sector stakeholders or states' actions during cyber event response. However, the Constitution grants the Federal Government the ability to regulate aspects of the electricity sector involved with interstate commerce. Concerning response to a malware attack on the electricity sector, 16 U.S. Code § 824o-1. *Critical electric infrastructure security* grants the Secretary of Energy authority to direct BPS operators during a declared emergency caused by, in addition to other types of attacks, a cyberattack [91].

More traditionally, the Executive Branch has been charged with and granted significant authority by Congress to enable close partnering with the private sector and deliver significant Federal incident response resources, which it does through the Cabinet Departments, advisory councils, and other mechanisms that are discussed in Chapter 4.

The implications of cyberattacks on the Federal Government and for its responsibilities is significant, and a good indicator of its responsibilities is the number of agencies and their respective cybersecurity roles. Figure 3.7 indicates the complexity of the nation's cybersecurity and an overview of the roles of the different types of agencies. Note that none of the agencies lead response efforts for cyberattacks, but all provide some level of support to private entities or state governments [187].

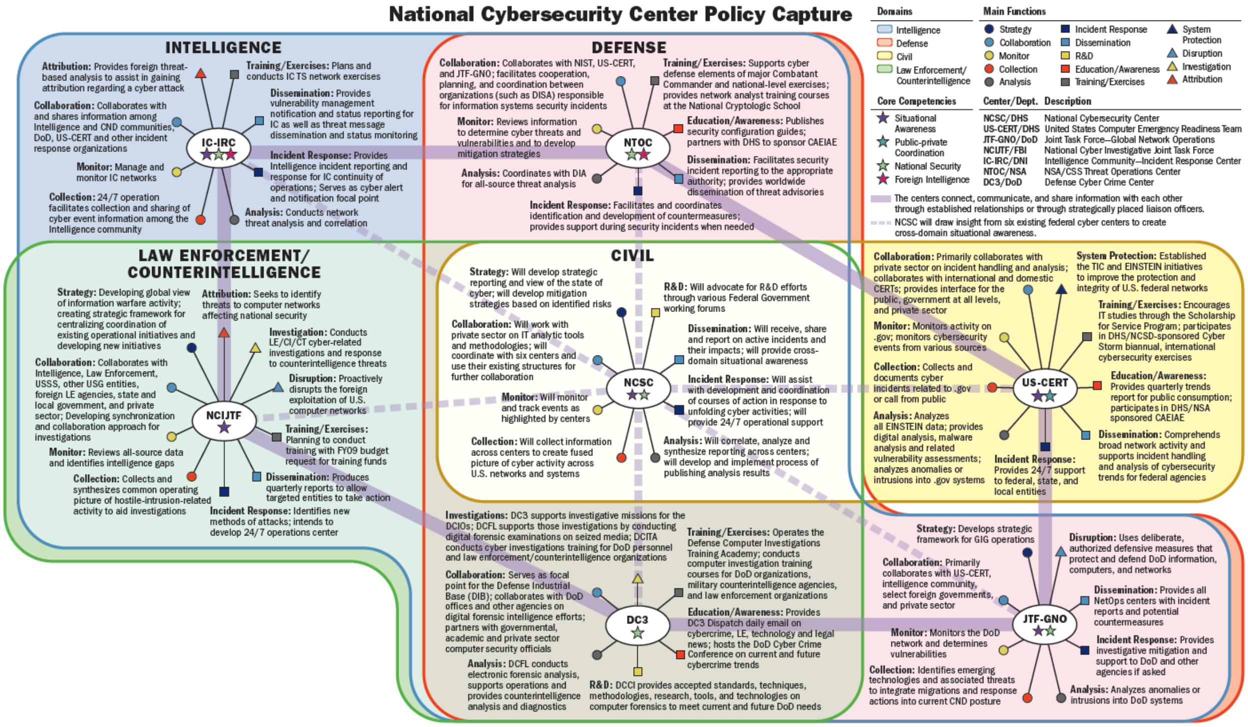

National Cybersecurity Center Policy Capture
INTELLIGENCE
Attribution: Provides foreign threat-based analysis to assist in gaining attribution regarding a cyber attack
Training/Exercises: Plans and conducts IC TS network exercises
Collaboration: Collaborates with and shares information among Intelligence and CND communities, DoD, US-CERT and other incident response organizations
Dissemination: Provides vulnerability management notification and status reporting for IC as well as threat message dissemination and status monitoring
IC-IRC
Incident Response: Provides Intelligence incident reporting and response for IC continuity of operations; Serves as cyber alert and notification focal point
Monitor: Manage and monitor IC networks
Collection: 24/7 operation facilitates collection and sharing of cyber event information among the Intelligence community
Analysis: Conducts network threat analysis and correlation
DEFENSE
Collaboration: Collaborates with NIST, US-CERT, and JTF-GNO; facilitates cooperation, planning, and coordination between organizations (such as DISA) responsible for information systems security incidents
Training/Exercises: Supports cyber defense elements of major Combatant Commander and national-level exercises; provides network analyst training courses at the National Cryptologic School
Monitor: Reviews information to determine cyber threats and vulnerabilities and to develop mitigation strategies
Education/Awareness: Publishes security configuration guides; partners with DHS to sponsor CAEIAE
NTOC
Dissemination: Facilitates security incident reporting to the appropriate authority; provides worldwide dissemination of threat advisories
Analysis: Coordinates with DIA for all-source threat analysis
Incident Response: Facilitates and coordinates identification and development of countermeasures; provides support during security incidents when needed
Domains
Intelligence
Defense
Civil
Law Enforcement/ Counterintelligence
Main Functions
Strategy
Collaboration
Monitor
Collection
Analysis
Incident Response
Dissemination
R&D
Education/Awareness
Training/Exercises
System Protection
Disruption
Investigation
Attribution
Core Competencies
Situational Awareness
Public-private Coordination
National Security
Foreign Intelligence
Center/Dept. Description
NCSC/DHS National Cybersecurity Center
US-CERT/DHS United States Computer Emergency Readiness Team
JTF-GNO/DoD Joint Task Force—Global Network Operations
NCIJTF/FBI National Cyber Investigative Joint Task Force
IC-IRC/DNI Intelligence Community—Incident Response Center
NTOC/NSA NSA/CSS Threat Operations Center
DC3/DoD Defense Cyber Crime Center
The centers connect, communicate, and share information with each other through established relationships or through strategically placed liaison officers.
NCSC will draw insight from six existing federal cyber centers to create cross-domain situational awareness.
LAW ENFORCEMENT/ COUNTERINTELLIGENCE
Strategy: Developing global view of information warfare activity; creating strategic framework for centralizing coordination of existing operational initiatives and developing new initiatives
Attribution: Seeks to identify threats to computer networks affecting national security
Investigation: Conducts LE/CI/CT cyber-related investigations and response to counterintelligence threats
Collaboration: Collaborates with Intelligence, Law Enforcement, USSS, other USG entities, foreign LE agencies, state and local government, and private sector; Developing synchronization and collaboration approach for investigations
Disruption: Proactively disrupts the foreign exploitation of U.S. computer networks
NCIJTF
Training/Exercises: Planning to conduct training with FY09 budget request for training funds
Monitor: Reviews all-source data and identifies intelligence gaps
Collection: Collects and synthesizes common operating picture of hostile-intrusion-related activity to aid investigations
Dissemination: Produces quarterly reports to allow targeted entities to take action
Incident Response: Identifies new methods of attacks; intends to develop 24/7 operations center
CIVIL
Strategy: Will develop strategic reporting and view of the state of cyber; will develop mitigation strategies based on identified risks
R&D: Will advocate for R&D efforts through various Federal Government working forums
Collaboration: Will work with private sector on IT analytic tools and methodologies; will coordinate with six centers and use their existing structures for further collaboration
Dissemination: Will receive, share and report on active incidents and their impacts; will provide cross-domain situational awareness
NCSC
Incident Response: Will assist with development and coordination of courses of action in response to unfolding cyber activities; will provide 24/7 operational support
Monitor: Will monitor and track events as highlighted by centers
Collection: Will collect information across centers to create fused picture of cyber activity across U.S. networks and systems
Analysis: Will correlate, analyze and synthesize reporting across centers; will develop and implement process of publishing analysis results
Collaboration: Primarily collaborates with private sector on incident handling and analysis; collaborates with international and domestic CERTs; provides interface for the public, government at all levels, and private sector
System Protection: Established the TIC and EINSTEIN initiatives to improve the protection and integrity of U.S. federal networks
Training/Exercises: Encourages IT studies through the Scholarship for Service Program; participates in DHS/NCSD-sponsored Cyber Storm biannual, international cybersecurity exercises
Monitor: Monitors activity on .gov; monitors cybersecurity events from various sources
Collection: Collects and documents cyber incidents related to .gov or call from public
US-CERT
Education/Awareness: Provides quarterly trends report for public consumption; participates in DHS/NSA sponsored CAEIAE
Analysis: Analyzes all EINSTEIN data; provides digital analysis, malware analysis and related vulnerability assessments; analyzes anomalies or intrusions into .gov systems
Incident Response: Provides 24/7 support to federal, state, and local entities
Dissemination: Comprehends broad network activity and supports incident handling and analysis of cybersecurity trends for federal agencies
Investigations: DC3 supports investigative missions for the DCIOs; DCFL supports those investigations by conducting digital forensic examinations on seized media; DCITA conducts cyber investigations training for DoD personnel and law enforcement/counterintelligence organizations
Training/Exercises: Operates the Defense Computer Investigations Training Academy; conducts computer investigation training courses for DoD organizations, military counterintelligence agencies, and law enforcement organizations
Collaboration: Serves as focal point for the Defense Industrial Base (DIB); collaborates with DoD offices and other agencies on digital forensic intelligence efforts; partners with governmental, academic and private sector computer security officials
DC3
Education/Awareness: Provides DC3 Dispatch daily email on cybercrime, LE, technology and legal news; hosts the DoD Cyber Crime Conference on current and future cybercrime trends
Analysis: DCFL conducts electronic forensic analysis, supports operations and provides counterintelligence analysis and diagnostics
R&D: DCCI provides accepted standards, techniques, methodologies, research, tools, and technologies on computer forensics to meet current and future DoD needs
Strategy: Develops strategic framework for GIG operations
Disruption: Uses deliberate, authorized defensive measures that protect and defend DoD information, computers, and networks
Collaboration: Primarily collaborates with US-CERT, intelligence community, select foreign governments, and private sector
Dissemination: Provides all NetOps centers with incident reports and potential countermeasures
JTF-GNO
Monitor: Monitors the DoD network and determines vulnerabilities
Incident Response: Provides investigative mitigation and support to DoD and other agencies if asked
Collection: Identifies emerging technologies and associated threats to integrate migrations and response actions into current CND posture
Analysis: Analyzes anomalies or intrusions into DoD systems

Figure 3.7: Federal Responsibilities for Cybersecurity

Key Perspectives and Insights:

Under the War Powers Clause, Congress and the President could exert its authority to direct private enterprise if the cyber event were declared an act of war, i.e., from a nation-state actor [188]. However, this power has not been exercised to date, nor is there any framework that governs what would happen in that event. Subsequently, all subordinate Federal agencies lack authority to direct cyber response efforts of private sector stakeholders short of a national emergency.

3.2.11 National Infrastructure Advisory Council (NIAC)

The NIAC was formed by Presidential order in 2001 to advise the President on the security of the critical infrastructure sectors and is the only executive council to do so. Members consist of up to 30 senior executives from the different sectors and state, local, tribal, and territorial (SLTT) governments who research physical and cyber threats to the critical infrastructure, study the impact across sectors, and advise the President of Federal Government action [189].

3.2.12 Department of Homeland Security (DHS)

Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience*, assigns DHS the lead role for critical infrastructure security and resilience. Specifically, DHS has the following eight overarching responsibilities:

1) *Identify and prioritize critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences, in coordination with SSAs and other Federal departments and agencies;*

2) *Maintain national critical infrastructure centers that shall provide a situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure;*
3) *In coordination with SSAs and other Federal departments and agencies, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure;*
4) *Conduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the SSAs and in collaboration with SLTT entities and critical infrastructure owners and operators;*
5) *Coordinate Federal Government responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities;*
6) *Support the Attorney General and law enforcement agencies with their responsibilities to investigate and prosecute threats to and attacks against critical infrastructure;*
7) *Coordinate with and utilize the expertise of SSAs and other appropriate Federal departments and agencies to map geospatially, image, analyze, and sort critical infrastructure by employing commercial satellite and airborne systems, as well as existing capabilities within other departments and agencies; and*
8) *Report annually on the status of national critical infrastructure efforts as required by statute [27, p. 3].*

In general terms, DHS has the responsibility for national emergency management, including cyberattacks on the electricity sector among other natural and human-made disasters. Its role in response is heavily focused on delivery government resources and coordinating across the government and with the private sector. DHS has created the National Response Framework (NRF), National Incident Management System (NIMS), National Infrastructure Protection Plan (NIPP), the NIPP Energy Sector-Specific Plan, and National Cyber Incident Response Plan (NCIRP) to facilitate understanding and assign clear roles for stakeholders in order to respond to a cyberattack on the electricity sector[117], [190], [191], [192], [32]. DHS executes its responsibilities for electricity sector security and resilience through a variety of subordinate agencies.

3.2.12.1 Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA) is “the Nation’s risk advisor,” replacing the National Protection and Programs Directorate (NPPD) in 2018 [193]. CISA reduces risk to critical infrastructure by identifying risks; disseminating threat, vulnerability, and consequence information; developing risk mitigation strategies, and overseeing the development of the NIPP [194]. CISA provides support to the electricity through two centers described below.

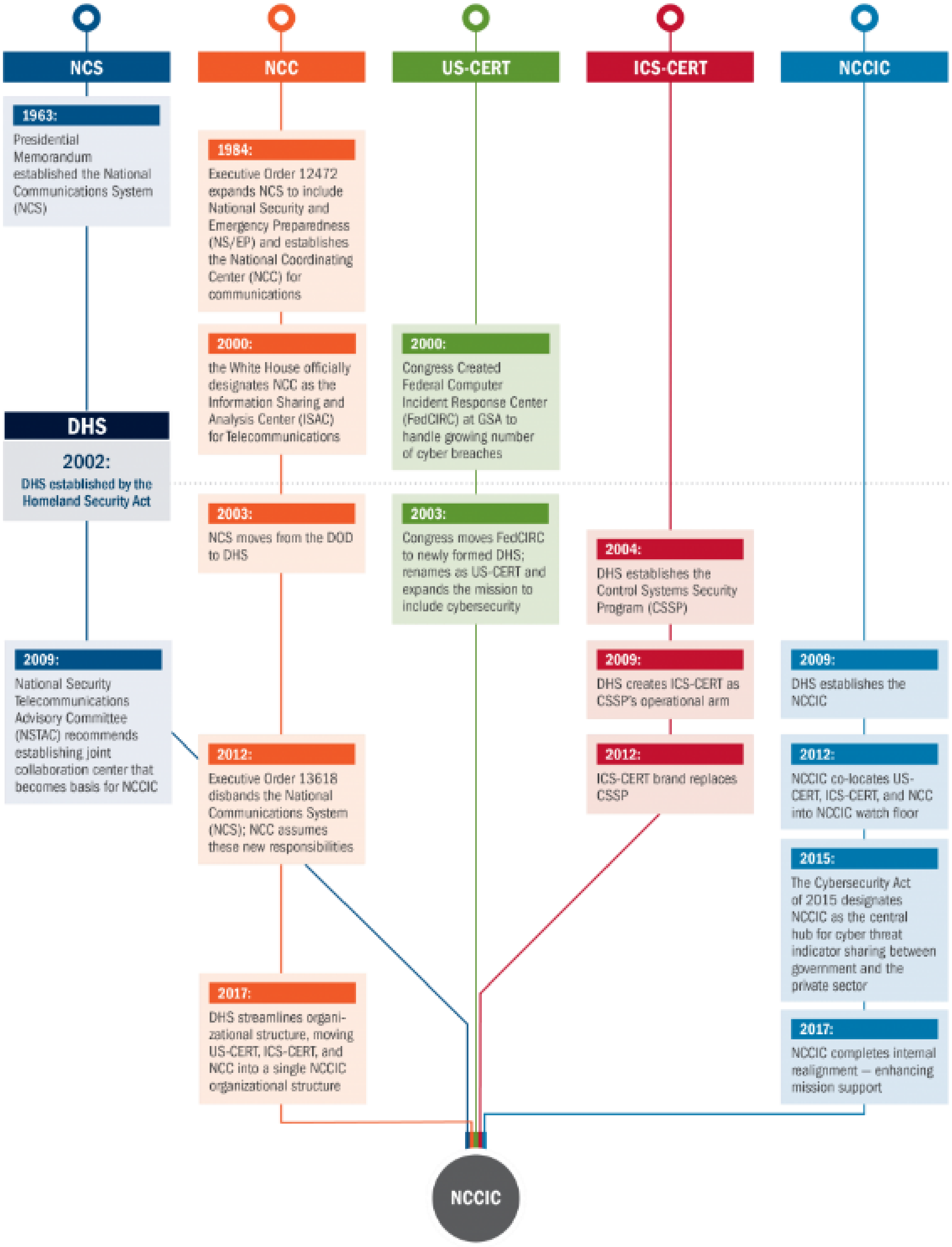
3.2.12.2 National Cybersecurity and Communications Integration Center (NCCIC)

As part of CISA, NCCIC acts as a communications and coordination hub between law enforcement agencies, the intelligence community, Federal, state, local, tribal, and territorial (FSLTT) governments, and private sector owners, operators, and vendors in critical infrastructure industries for cyber-related issues. The NCCIC was created under PPD-21 and operates a continuously monitored watch floor to perform the roles of:

- *Responding to and analyzing control systems related incidents*
- *Conducting vulnerability, malware, and digital media analysis*
- *Providing onsite incident response services*
- *Providing situational awareness in the form of actionable intelligence*
- *Coordinating the responsible disclosure of vulnerabilities and associated mitigations*
- *Sharing and coordinating vulnerability information and threat analysis through information products and alerts [195, p. 1].*

Key Perspectives and Insights:

The evolution of cybersecurity and communications security in the U.S. can be traced back to NCCIC's origins. This evolution not only parallels the advent of the internet and information technology but also corresponds to the increasing integration of public and private concerns with the need for cybersecurity. Figure 3.8 shows the path from the National Communications Systems in 1963 to the NCCIC in present-day [196].



1963: Presidential Memorandum established the National Communications System (NCS)

1984: Executive Order 12472 expands NCS to include National Security and Emergency Preparedness (NS/EP) and establishes the National Coordinating Center (NCC) for communications

2000: the White House officially designates NCC as the Information Sharing and Analysis Center (ISAC) for Telecommunications

2000: Congress Created Federal Computer Incident Response Center (FedCIRC) at GSA to handle growing number of cyber breaches

2002: DHS established by the Homeland Security Act

2003: NCS moves from the DOD to DHS

2003: Congress moves FedCIRC to newly formed DHS; renames as US-CERT and expands the mission to include cybersecurity

2004: DHS establishes the Control Systems Security Program (CSSP)

2009: National Security Telecommunications Advisory Committee (NSTAC) recommends establishing joint collaboration center that becomes basis for NCCIC

2009: DHS creates ICS-CERT as CSSP's operational arm

2009: DHS establishes the NCCIC

2012: Executive Order 13618 disbands the National Communications System (NCS); NCC assumes these new responsibilities

2012: ICS-CERT brand replaces CSSP

2012: NCCIC co-locates US-CERT, ICS-CERT, and NCC into NCCIC watch floor

2015: The Cybersecurity Act of 2015 designates NCCIC as the central hub for cyber threat indicator sharing between government and the private sector

2017: DHS streamlines organizational structure, moving US-CERT, ICS-CERT, and NCC into a single NCCIC organizational structure

2017: NCCIC completes internal realignment – enhancing mission support

Figure 3.8: Evolution of Communications and Cybersecurity in the U.S.

NCCIC's incident response capabilities, while essential to an effective cyber response, remain untested particularly for cyber events at scale. There is also a perception that NCCIC will have a limited role in any real-time response. While it is charged with maintaining a common operating picture of a cyber event, the data that NCCIC collects during a cyber-attack is limited and unlikely to enable a focused and coordinated Federal response.

3.2.12.3 NCCIC Hunt and Incident Response Team (HIRT)

HIRT provides free, onsite incident response services to organizations that need them. As Figure 3.8 implies, US-CERT and ICS-CERT functions were combined into NCCIC, and HIRTs were formed under NCCIC purview. HIRTs are fly-away teams that can meet with affected organizations to respond to cyber events. HIRTs are perceived to be valuable, particularly to under-resourced utilities, but potentially under-skilled to assist with more advanced and sophisticated systems that larger utilities operate.

<u>Key Perspectives and Insights:</u>

During a large-scale event, HIRTs' unique resources and capabilities will be in high demand, but its capacity to respond to all affected organizations may not be sufficient. A prioritization mechanism is necessary, which the industry presumes will place the utilities with the most extensive affected customer base first, regardless of the internal capability of the organization to respond.

3.2.12.4 National Infrastructure Coordination Center (NICC)

In addition to the NCCIC, PPD-21 created the NICC to serve as a "clearinghouse of information to receive and synthesize critical infrastructure information and provide that information back to decision-makers at all levels to enable rapid, informed decisions in steady state, heightened alert, and during incident response" [192, p. 39]. The NICC, in contrast to the NCCIC, focuses on physical threats to critical infrastructure, but PPD-21 created an integration function between the two centers to ensure proper coordination [192].

3.2.12.5 National Operations Center (NOC)

The NOC functions like the integrated operations center for DHS and comprises five sub-entities: NOC Watch, Intelligence Watch and Warning, FEMA's National Watch Center and National Response Coordination Center, and the NICC. It is the central hub for the Federal Government and SLTT entities in the event of natural or human-made disasters and ensures critical terrorism and disaster-related information is communicated to appropriate government officials.

3.2.12.6 National Risk Management Center (NRMC)

As part of the CISA, the NRMC plans, analyzes, and collaborates to identify and address risks to critical infrastructure [197]. Compared to the NCCIC, the NRMC focuses on future threats to critical infrastructure [198]. It partners with DHS, DOE, and the Department of the Treasury to work closely with the financial services sector, the communications sector, and the electricity sub-sector through the Tri-Sector Executive Working Group.

The NRMC plays a critical role in the *Joint National Priorities for Critical Infrastructure Security and Resilience* and aims to advance reduction of risk to national critical functions, enhance incident response and recovery capabilities, improve information sharing, and protect critical infrastructure against nation-state cyber threats [199].

Key Perspectives and Insights:

The NRMC has a stated goal of turning identified risks into collective action by leveraging PPP. However, the relatively new organization, which stood up in mid-2018, has unproven value but demonstrates a promising capability for the electricity sector [200].

3.2.12.7 Federal Emergency Management Agency (FEMA)

As an agency within the DHS, FEMA is commonly associated with emergency and disaster response, and collateral damage and secondary threats to the public from a cyberattack would FEMA's primary concern. It would also be a key enabler for cyber incident response, for instance, by providing backup power to operational facilities, from issues that would arise from a prolonged and widespread outage regardless of cause. However, CISA would maintain the lead role for a cyber response that FEMA would typically provide in other types of physical disasters and human-made emergencies.

3.2.13 Department of Energy (DOE)

The DOE is the sector specific-agency (SSA) for the electricity subsector per PPD-21. As such, PPD-21 sets out the DOE's role regarding critical infrastructure protection:

1) *As part of the broader national effort to strengthen the security and resilience of critical infrastructure, coordinate with the Department of Homeland Security (DHS) and other relevant Federal departments and agencies and collaborate with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with SLTT entities, as appropriate, to implement this directive;*
2) *Serve as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities;*
3) *Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations;*
4) *Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate; and*
5) *Support the Secretary of Homeland Security's statutorily required reporting requirements by providing on an annual basis sector-specific critical infrastructure information [27, p. 4].*

The DOE executes its SSA mission by investing in cybersecurity initiatives, such as REMEDYS, partnering with industry to formulate legislation and standards of practice, hosting preparedness and response exercises, such as Liberty Eclipse, and participating in information and intelligence fusion with other agencies.

3.2.13.1 Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

CESER "leads the Department of Energy's emergency preparedness and coordinated response to disruptions to the energy sector, including physical and cyberattacks, natural disasters, and man-made events" [201]. CESER's role in cyber incident response is limited to coordination across the government and with the electricity sector and provision of Federal resources consistent with the NIPP, NRF, NIMS, and NCIRP [117], [190], [191], [192], [32]. Specifically, CESER is responsible for Emergency Support Function #12 of the NRF and maintains trained emergency responders with technical expertise who can rapidly deploy to locations where the electricity sector is being compromised.

CESER also maintains dedicated personnel at each of FEMA's regional officers to facilitate rapid response and coordinate activities on behalf of the DOE [202]. Along with other Federal agencies, CESER conducts training with the private sector to facilitate preparedness and communication in the event of a cyber event on the electricity sector.

Key Perspectives and Insights:

Because CESER recently emerged from a DOE restructuring, its role in the sector may not be fully formed. However, CESER recently established standing request documents between industry partners to facilitate rapid access to critical electrical infrastructure components in the event of the response and indicates their increased prioritization of cyber response.

3.2.13.2 National Laboratories & Federally Funded Research and Development Centers (FFRDCs)

Supported by the government, national laboratories and FFRDCs fuse Federal resources, particularly funding and intelligence, with dedicated facilities to advance science and technology. The DOE leverages its 17 national labs to directly address the requirements for EDS cybersecurity, including performing research on the technical and organizational requirements for increasing cyber response capability in the electricity sector. The National Infrastructure Simulation and Analysis Center, for instance, is a combined effort between three of the national labs and the DHS to advance research into critical infrastructure issues [203].

3.2.14 Federal Bureau of Investigation (FBI)

Through its Cyber Division and specially trained cyber squads located at each of the 56 FBI field offices, the FBI heads the national effort "to address cybercrime in a coordinated and cohesive manner" [204]. Within the electricity sector, the FBI strictly performs a law enforcement role. It typically requires forensic analysis of systems immediately following a cyber event in order to investigate the crime.

Key Perspectives and Insights:

Many in the industry maintain reluctance to partner with the FBI because their investigative authorities permit intrusive control of private businesses systems. Some perceive that the FBI might override the need to destroy forensic data in order to respond quickly to a cyber event. While this is likely accurate when systems need to be erased, rebooted, and restored, the industry understands the priority to restore system operation as quickly as possible regardless of the potential for evidence destruction.

Additionally, some electricity sector stakeholders perceive that each FBI field office prioritizes cybercrime differently and have varying levels of ability with cyber systems. These perceptions leave stakeholders reluctant to notify the FBI and ask for assistance in response to a cyber event.

3.2.14.1 Cyber Action Team (CAT)

CATs are the primary unit of action for the FBI to provide a rapid incident response in major cyber-related emergencies. Members of the CAT are located throughout the field offices and have specialized training to perform malware analysis and forensic investigations. Their primary focus remains on attributing crimes and catching cybercriminals [204].

3.2.14.2 National Cyber Investigative Joint Task Force (NCIJTF)

NCIJTF is the primary U.S. government agency responsible for coordinating cyber threat investigations and liaisons with the intelligence community, DHS, and DOD [117], [205]. Since information sharing and intelligence fusion remain one of the most substantial gaps in the EDS, the NCIJTF performs a valuable role in the electricity sector. However, it remains focused on "placing cybercriminals behind bars and removing them from the nation's networks" and reinforces the perception that the FBI's incident response may not prioritize restoration of electricity service [204].

3.2.14.3 InfraGard

InfraGard is a partnership between the FBI and members of the private sector that promotes public-private information sharing relevant to the protection of critical infrastructure, including the electricity sector. It also provides access to FBI and DHS threat advisories, vulnerability assessments, and analytical reports [206], [207].

3.2.15 Federal Trade Commission (FTC)

The FTC is an independent agency of the Federal Government that protects consumers and promotes competition. The FTC has increasingly focused on electricity sector competition as deregulation and technology advances have eroded its monopolistic nature. It also has prosecuted companies for failing to maintain reasonable cybersecurity protections for data.

Key Perspectives and Insights:

With the new technologies, such as DERs and IoT, driving the electricity sector towards a revolutionary change in the marketplace, i.e., transactive energy, the FTC's role in protecting consumers may grow to encompass cyber resilience [208], [209].

3.2.16 Department of Defense (DOD)

Through its various units, the DoD monitors cyber threat intelligence and performs defensive and offensive cyber operations. The EDS has been designated one the primary targets of nation-state actors, and through NCIJTF and other platforms, the DoD partners with the electricity sector to provide information, intelligence, and defensive cyber capabilities.

Key Perspectives and Insights:

However, some in the industry view partnering with the DoD as provoking adversaries and increasing the likelihood of cyber-attack.

3.2.17 State governments

Similar to the U.S. Federal Government, some state governments retain authority to regulate segments of the electricity sector, typically the distribution systems, within their jurisdiction, and state constitutions may grant the state governor and legislatures powers like those the Federal Government has to regulate the sector.

State and local governments' approaches to incident response and cyber resilience are too numerous and heterogeneous to describe in sufficient detail, and the variety of the approaches and inconsistency of regulation between states contributes to dynamics which negatively affect the sector's cyber response capability. However, states share many common issues with cybersecurity and cyber response [113]. There are a few organizations that all states maintain that are relevant to cyber response.

3.2.17.1 State Chief Information Security Officers (CISO)

Each of the 50 states has a CISO by statute or executive order. These professionals advocate for cyber resilience measures at the state level. Disconcertingly, a 2018 study found that state cyber resilience programs, both internal government operational and external regulatory and support functions, are insufficiently resourced and organized to comply with Federal and their state regulations [113].

Key Perspectives and Insights:

Evidence suggests state CISO concerns reflect an increased focus on state-level cybersecurity measures inclusive of electricity sector cyber response [113]. However, their concerns are not being prioritized, or resources do not exist to implement the measures.

3.2.17.2 State and Major Urban Area Fusion Centers

According to Masse and Rollins (2007), a fusion center's value proposition is to integrate:

> *various streams of information and intelligence, including that flowing from the Federal Government, state, local, and tribal governments, as well as the private sector, a more accurate picture of risks to people economic infrastructure, and communities can be developed and translated into protective action [210, p. ii].*

In other words, they act as a hub to receive threat information from FSLTT and private entities within their area, synthesize it through the lens of their specific environment, and disseminate back to the FSLTT and private communities. The fusion center concept was established in the wake of the 9/11 terrorist attack as a formalization of the functions that many state's criminal intelligence bureaus conducted which were considered key to combating foreign and domestic terrorism [210]. As of 2017, 78 fusion centers exist and provide cyber threat information analysis and dissemination throughout their jurisdictions. However, each state has taken individualized approaches to establish and run the fusion centers, and given the variation in each state's resources, criminal focus, physical environment, and political landscape, no two fusion centers are alike [210].

Key Perspectives and Insights:

Fusion centers provide an invaluable resource to the electricity sector but have incurred significant criticism since their inception in the early 2000s. Critics have cited ineffectiveness in sharing information, abuse of privacy, civil rights, and civil liberties, and ambiguity of authority [211], [212], [213].

3.2.17.3 National Guard

National Guard units remain at the disposal of state governors and typically train for responding to state-wide disasters. While some maintain extremely robust cyber defensive and offensive capabilities, other states have not invested in their Guards' personnel, training, and resources to develop the capability to respond to a widespread cyberattack.

3.2.17.4 Public Utility Commissions / Utility Regulatory Commissions / Public Service Commissions (PUCs)

PUCs are governing bodies that regulate the rates and services of electric utilities (almost exclusively distribution systems) within their service areas, typically at the state level. Each state and the District of Columbia have a PUC or equivalent. PUC set many regulations which influence the behavior of the electric sector in their state, including cyber resilience and response measures. These regulations vary from state to state and are enforced inconsistently even then [214]

Key Perspectives and Insights:

Since distribution systems are outside the purview of NERC, state utility commissions provide oversight and regulation for the distribution system within their borders. In this way, they function much like NERC by providing reliability and cybersecurity standards for utilities within the state. However, as one study shows, the perception that PUCs have inadvertently put in place barriers to increasing cyber resilience and response measures, specifically in the areas of information sharing, cost recovery options, and improvements to system performance. In total, these actions are considered to increase the risk of a cyber event rather than minimize it [215].

3.2.17.5 State and Territory Energy Office (SEO)

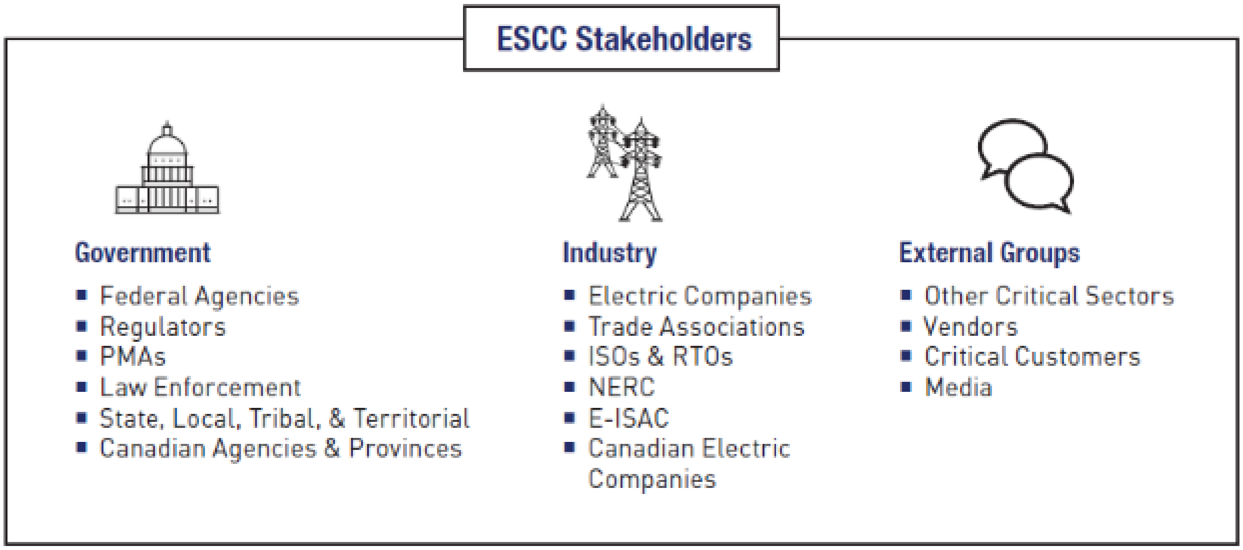
The 56 State and Territory Energy Offices generally advise on and advocate for state-related energy issues, emphasizing energy education; economic development; energy research, innovation, and demonstration; and energy legislation and policy [216]. There is no standard model for SEOs, and in many cases, they are subsumed in state utility commissions and regulators, environmental quality and protection agencies, or more extensive state government departments. However, they partner closely with DOE and, through state Energy Emergency and Assurance Coordinators (EEACs), help respond to energy disruptions or emergencies in their respective states. SEOs work with their respective State Offices of Emergency Management to create and execute State Energy Assurance plans to prepare for and enable a response to energy emergencies.

3.2.17.6 State Office Emergency Management (OEM)

A state OEMs, alternatively named Emergency Management Department, Division, or Agency, is the state entity responsible for planning for, responding to, and recovering from human-made and natural disasters. All states, territories, and commonwealths in the U.S. have some variant of an OEM. Unlike FEMA, which is primarily focused on the response to physical disasters and emergencies and taking a secondary role to other Federal agencies to respond to cyber threats, OEMs are at an appropriate level to combine both cyber and physical emergency response. However, like other government agencies, OEMs focus on providing the necessary support to the utility providers rather than outright disaster response as in an emergency with physical consequences. Thus, most OEMs have a critical role in cyber response in the electricity sector.

3.2.18 Electricity Subsector Coordinating Council (ESCC)

The ESCC was formed at the recommendation of the National Infrastructure Advisory Council (NIAC), DOE, and DHS with support from a group of electricity industry CEOs. Along with the Oil and Natural Gas Subsector Coordinating Council, the ESCC is a component of the Energy Sector Coordinating Council that is part of the Sector Partnership Structure (see Chapter 4). It includes electricity company CEOs and trade association leaders to represent every segment of the industry. Its stated mission is to serve “as the principal liaison between the Federal Government and the Electricity Subsector with the mission of coordinating efforts to prepare for and respond to national-level disasters or threats to critical infrastructure” [217, p. 1]. The ESCC coordinates directly with the Energy Sector Government Coordinating Council (EGCC) and other stakeholders, as shown in Figure 3.9 [217, p. 3].



ESCC Stakeholders

Government

- Federal Agencies
- Regulators
- PMAs
- Law Enforcement
- State, Local, Tribal, & Territorial
- Canadian Agencies & Provinces

Industry

- Electric Companies
- Trade Associations
- ISOs & RTOs
- NERC
- E-ISAC
- Canadian Electric Companies

External Groups

- Other Critical Sectors
- Vendors
- Critical Customers
- Media

Figure 3.9: ESCC Stakeholders

The ESCC focus has been to communicate the industry's perspectives and requirements to the dozens of disparate organizations in all branches the Federal Government that handle the national response to threats to critical infrastructure. It does this mostly through outreach and coordination in the following areas:

- *Threat Information Sharing: Improve and institutionalize the flow of, and access to, actionable information among public- and private-sector stakeholders.*
- *Industry-Government Coordination: Establish unity of effort and unity of messaging between industry and government partners to support the missions of the ESCC both during crises and in steady state.*
- *Research & Development: Coordinate government and industry efforts on strategic infrastructure investments and R&D for resilience and national security related products and processes.*
- *Cross-Sector Liaisons: Develop strong partnerships at all levels of the Electricity, Communications (Telecommunications), Oil and Natural Gas (Downstream Gas), Financial Services, Transportation Systems, and Water and Wastewater Systems (Water) sectors to plan and respond to major incidents, to better understand and protect our mutual dependencies, and to share information effectively and efficiently to improve cross-sector situational awareness. [217, p. 2]*

Additionally, the ESCC formed the Cyber Mutual Assistance Program (CMA) to bring together industry partners and cybersecurity experts to share resources during a cyber event.

Key Perspectives and Insights:

ESCC is highly regarded within the industry because of the influence it has been able to bring to bear with the Federal Government. However, there is a perception that ESCC initiatives and information, while valuable to cyber response, take too long to consolidate, gain momentum, and trickle down to the industry.

3.2.19 Energy Sector Government Coordinating Council (EGCC)

The EGCC is the Federal Government's counterpart to the ESCC under the Sector Partnership Structure. It serves to "address initiatives to include policy considerations, program goals, and communication across government as well as between the government and the private sector to support the Nation's energy security and resilience mission" [218, p. 1]. More pointedly, its membership of public power administrators, state energy officials, and ten of the Cabinet Departments seek to serve as the single touchpoint between government and private sector to address threats to the energy sector.

3.2.20 Critical Infrastructure Cross-Sector Council

The Critical Infrastructure Cross-Sector Council is one of four cross-sector councils. It is comprised of the chairs and vice chairs of the Sector Coordinating Councils and serves as a way to identifying common and cross-cutting critical infrastructure issues, disseminating best practices, and collaborating to enhance the security of their sectors [192].

3.2.21 Federal Senior Leadership Council (FSLC)

The FSLC is the Federal Government's counterpart to the Critical Infrastructure Cross-Sector Council. It comprises officials from the SSAs and other agencies who together develop and promote Federal Government programs, policies, and goals within and across sectors [192].

3.2.22 State, Local, Tribal, & Territorial Government Coordinating Council (SLTTGCC)

The SLTTGCC serves as a forum to promote SLTT entities participation in the Federal Government's Sector Partnership Structure. It coordinates across the different levels of government to advance critical infrastructure issues of mutual concern between the Federal government and other SLTT entities [192].

3.2.23 Regional Consortium Coordinating Council (RC3)

Much like the SLTTGCC, the RC3 unites existing regional organizations to assist with the protection of critical infrastructure across sectors but at the regional level. It focuses fostering awareness and promoting the importance of critical infrastructure protection through collaborative activities among its members including, education and communication, incorporating incident response and recovery exercises into their outreach programs, identifying and disseminating best practices for infrastructure protection [192]. The RC3 currently has 34 member organizations coming from 47 states and major urban areas [219].

3.2.24 Cybersecurity Platforms

Cybersecurity platforms provide a wide variety of services to the electric sector, including threat intelligence, network monitoring, vulnerability assessments, and threat modeling, compliance consultation, incident response, forensics, and threat hunting [220], [221]. Utilities typically hold cybersecurity companies on retainer to provide regular services, or in case a cyber incident exceeds internal capacity or expertise.

Key Perspectives and Insights:

There are a limited number of platforms that specialize in industrial control systems and the electricity sector. During a widespread cyberattack, many in the industry expect that the platforms will not have the reserve capacity to respond to all affected utilities. Similar to HIRTs, many believe the platforms will respond to the utilities with the most extensive affected customer base or the company with the best likelihood of being able to execute a rapid recovery.

3.2.25 Electrical Equipment Manufacturers & Industrial Control System (ICS) Vendors

Electrical equipment manufacturers and ICS vendors are limited in number in the U.S. Only a few specialized companies provide the majority of equipment to the electricity sector, and they have made concerted efforts to upgrade software with innovative cybersecurity features. While their equipment includes ICS, they are rarely responsible for installation and configuration of the physical and digital networks.

Key Perspectives and Insights:

As network malfunctions are usually caused by operational error or physical damage to equipment, and network monitoring is not prevalent in the sector, installers and integrators – not cybersecurity experts or equipment manufacturers – are the first to respond. When a cyber-attack is finally suspected, equipment manufacturers and ICS vendors are typically the last to be notified. Not only does this delay the response and potentially allow attackers to continue network penetration, but it also prolongs the diagnosis of the actual cause. For instance, the TRITON attack was caused, in part, by the integration of original equipment manufacturer ICS with a safety system [222].

In sum, electrical equipment manufacturers and ICS vendors believe that not being included in network configuration or incident response activities creates vulnerabilities and slows the response process. Further, they are motivated to assist in both efforts because their involvement might limit reputational damage from cyber events. Given the current number of noncyber-related incidents, however, such involvement would be cost-prohibitive.

3.2.26 American Public Power Association (APPA)

The APPA is a service organization that represents over 2,000 POUs that serve over 49 million consumers. Their members also include joint action agencies, rural electric cooperatives, and other public power utilizes in the U.S. and Canada. The APPA provides a venue to leverage POUs collectively to support mutual interests and share best practices. For instance, the association offers a variety of programs tailored to their unique needs that they might otherwise not be able to afford. The APPA's services include employee education and certification, reliability, safety, and disaster preparation programs, and news and information publications [223], [161].

Key Perspectives and Insights:

The APPA prioritizes Federal advocacy on legislation that supports its members. Specifically, the association routinely advocates before government and regulatory agencies against “one-size-fits-all” policies which are typically focused on larger utilities and fights for inclusion in reliability standards development. The Association perceives federally mandated, blanket regulations as obstacles to its members’ abilities to achieve cyber resiliency.

3.2.27 National Rural Electric Cooperatives Association (NRECA)

NRECA is another membership organization that “represents over 900 co-ops, public power districts, and public utility districts in the United States” [224]. Much like the APPA, NRECA offers educational, business, reliability, safety, and disaster preparedness programs in addition to serving as a hub to share best practices and leverage common interests for unity of action. Nearly identical associations supporting energy cooperatives exist at the state level.

Additionally, NRECA created the Rural Cooperative Cybersecurity Capabilities Program (RC3) to support cybersecurity among its members. RC3’s goal is to provide cybersecurity tools and resources to co-ops, which typically have few or no information technology or cybersecurity personnel and limited access to cybersecurity technology [225].

Key Perspectives and Insights:

NRECA shares APPA concerns about Federal policies that inhibit co-ops ability to tailor their risk management and cybersecurity measures to its unique geographic, resource, and business constraints. Additionally, it advocates for legislative change to Federal funding initiatives on which its members rely for research and development, cyber resilience, and recovery efforts [182], [226].

3.2.28 Touchstone Energy Cooperative

Touchstone was created as a national branding organization to improve recognition for co-ops [227]. Over time, their services have grown to include much of what NRECA does with greater emphasis on business strategies that enable the provision of cost-effective, reliable electrical service [228].

3.2.29 State and Regional Public Power Associations

State and regional public power associations are local variants of the APPA and NRECA which advocate for local and state public power issues, including cyber resilience measures, with SLTT government entities. They also offer training and education and other ancillary services to their member utilities. As of 2019, there are 61 of these associations [179].

3.2.30 Large Public Power Council (LPPC)

The LPPC is a non-profit organization formed in 1987 consisting of 27 of the largest public power systems in the U.S. It advocates for policies surrounding reliability, including cyber resilience, affordability, and environmental stewardship on behalf of the 30 million consumers.

3.2.31 National Governors Association (NGA)

The NGA is a public policy organization whose members include the governors from the 55 states, territories, and commonwealths. It advocates on behalf of states for policies at the state, national, and international levels. It Resource Center for State Cybersecurity helps states “address the consequences of the rapidly evolving and expanding technological threats now faced by law enforcement agencies, public works and energy agencies, private financial and communications sectors and the general public" [229]. The NGA advocates for national and state policies that support cyber resilience of critical infrastructure and provide resources, tools, and strategic recommendations to the government and private sector to that end [229]. NGA is a participant in the DOE's Energy Emergency Assurance Coordinators' (EEAC) Agreement that enables mutual assistance to energy disruptions such as an outage caused by a cyberattack [230].

3.2.32 National Association of State Energy Officials (NASEO)

NASEO is the non-profit association composed of each of the 56 states and territories energy officials who are designated by their respective governors. Their stated mission is to "facilitate peer learning among state energy officials, serve as a resource for and about state energy offices, and advocate the interests of the state energy offices to Congress and Federal agencies" [231]. NASEO maintains multiple committees, including one for energy security which covers cybersecurity of the state energy critical infrastructure.

Of note, NASEO and DOE first implemented the EEAC program in 1996 before expanding it to include NGA, NARUC, and NEMA [230]. NASEO also maintains a formal role in national cyber response plans for the energy sector [23].

3.2.33 National Association of Regulatory Utility Commissioners (NARUC)

NARUC is a national association that represents PUCs from all 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands before the Federal Government, particularly FERC. As with other associations, they provide a venue for their members to pool resources and share best practices, and it provides access to a variety of operational, educational, research, and business programs to its members [232]. NARUC also hosts conferences which discuss, among other topics, issues of recoverable costs and rate design. Through its Cybersecurity Strategy Guide and other publications, NARUC promotes utility commissioner integration in the state utilities' cyber resilience measures [233]. NARUC is a participant in the DOE's EEAC Agreement and has formal roles in national cyber response plans and has formal roles in national response plans for electricity outages [230], [23].

Key Perspectives and Insights:

NARUC provides training for utility commissioners including rate setting and cybersecurity. This organization's training of personnel is uniquely essential, given the relatively higher turnover due to the many officials who are elected or appointed by the state. Due to the different states' approaches to rate recovery, NARUC is positioned to increase awareness of cost recovery barriers to cyber response measures.

3.2.34 National Association of State Chief Information Officers (NASCIO)

NASCIO is a national association that represents each state's Chief Information Officer or equivalent. According to their website, NASCIO:

> [*P*]*rovides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of*

> *information and promote the adoption of IT best practices and innovations. From national conferences, peer networking, research and publications, briefings and government affairs, NASCIO is the premier network and resource for state CIOs [234]*

They heavily advocate for CIO-related interests, and primarily, for more significant resources to support cybersecurity initiatives within state governments' IT systems and for programs to support private entities.

Key Perspectives and Insights:

Unlike NARUC and NASEO, NASCIO is not included in the EEAC or formal national electricity sector cyber response plans [23].

3.2.35 National Emergency Management Association (NEMA)

NEMA is a professional association of the emergency management directors for 59 states and territories. Like many other professional associations, NEMA is a forum for state emergency managers to exchange best practices and educate the wider public, advocating on public policy on levels that supports improved emergency management, and sponsor research and development of solutions to emergency management issues [235]. NEMA is also a participant in the DOE's EEAC Agreement [230].

3.2.36 Edison Electric Institute (EEI)

EEI is a trade association that represents all IOUs in the U.S. and some international utilities. It provides "public policy leadership, strategic business intelligence, and essential conferences and forums" similar to APPA and NRECA [236]. Relevant to cybersecurity, EEI promotes industry involvement and investment in cyber resilience measures, advocates for pertinent legislation, and facilitates the integration of government cybersecurity stakeholders, primarily through the ESCC which was formed out of EEI initiatives.

3.2.37 Information Sharing and Analysis Organizations (ISAOs)

In response to Executive Order 13691, DHS through NPPD (now CISA) encouraged the formation of ISAOs to share information related to cybersecurity risks among both critical infrastructure to all other types of organizations [193]. Before EO 13691, industries and organizations found it difficult to develop adequate information sharing organizations. DHS has helped establish the ISAO Standards Organization (ISAO SO) to combat this and encourage the growth of ISAOs.

Further, sector-based ISAOs are referred to as Information Sharing and Analysis Centers. The E-ISAC is one such ISAO.

Key Perspectives and Insights:

Currently, there are over 60 registered ISAOs, all of which provide access to each other's cyber information and can collectively participate in Federal information sharing programs to enhance their cybersecurity [237]. E-ISAC, for example, is one of many registered ISAOs that collects and analyzes threat information relevant to the electricity sector and aids in mitigation and response o threats. Not all ISAOs have the same functions or capability, but they are evolving into significant cyber response resources.

3.2.38 National Council of ISACs (NCI)

The NCI was formed in 2003 to coordinate and encourage collaboration between the sector-based ISACs and FSLTT entities. According to its mission statement, the NCI is "true cross-sector partnership, providing a forum for sharing cyber and physical threats and mitigation strategies among ISACs and with government and private sector partners during both steady-state conditions and incidents requiring cross-sector response" [238]. Outside of incident response, NCI is integrated into the Sector Partnership Structure and coordinates with the SLTTGCC and other councils. During significant incidents, NCI members are integrated into the NCCIC watch floor and can be deployed to national, regional, and SLTT response centers [238].

3.2.39 Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC is a division of the non-profit Center for Internet Security. Much like E-ISAC, it aims to function as a hub for "cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial (SLTT) governments" [239]. Its stated mission is to provide "real-time network monitoring, dissemination of early cyber threat warnings, vulnerability identification and mitigation, along with education and outreach aimed at reducing risk to the nation's SLTT government cyber domain" [239]. MS-ISAC focuses on building, trusted relationship among its members and can provide direct assistance for cyber incident response.

MS-ISAC maintains a security operations center in New York City and field offices in select cities across the country. It organizes around engagement teams of 8 to 10 people each that are assigned to stakeholders within defined geographical regions of the U.S.

Key Perspectives and Insights:

Unlike the risk management trend within the electricity sector, which focuses on the largest utilities and customer bases, MS-ISAC focuses on the inclusion of as many stakeholders as possible. It makes a concerted effort to include smaller utilities, i.e., municipal and rural cooperatives, to ensure they can reach the broadest possible area and mitigate threats and attacks accordingly.

3.2.40 Electric Power Research Institute (EPRI)

EPRI is an independent non-profit organization that focuses on research, development, and demonstration projects supporting electricity generation, delivery, and use. Its members include 90% of the U.S. utility market and 35 other countries, government agencies and regulators, and other ELECTRICITY SECTOR stakeholders. Through its Cyber Security Program, EPRI conducts research supporting industry resilience, including developing security metrics, risk assessment techniques, and incident management tools. Its guidelines for creating an Integrated Security Operations Center focus on and enable incident management within a single business.

Key Perspectives and Insights:

Following trends in cybersecurity, EPRI's research and development focuses on technical and technological approaches to managing cyber events. However, there is a concern that such solutions fail to address the cultural and organizational issues that are required to realize improved cyber response and may even provide a false sense of progress.

3.2.41 National Institute of Science and Technology (NIST)

NIST is part of the Department of Commerce and focuses on measurement science and standards development [240]. NIST's Cyber Security Framework is a foundational process by which many electricity sector stakeholders formulate their approaches to cybersecurity [24]. Additionally, the Cybersecurity Enhancement Act of 2014 charges NIST with "developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators" [24, p. v].

3.2.42 Cyber-aggressors

Hackers are malign actors who perpetrate cyberattacks. Their goals and capabilities are varied but greatly influence cybersecurity and cyber response approaches, particularly in the energy delivery sector. This thesis uses Fischer et al.'s (2014) classification of cyber-aggressors in addition to the motivations described in section 2.2.1.1 to understand the motivations and capabilities of different actors. It is important to note that these classifications are not mutually exclusive, i.e., an actor may be motivated by goals that fall into more than one category [56].

3.2.42.1 Cyberwarriors

State-sponsored agents who conduct cyberattacks to advance a country's strategic objectives are currently the likeliest source of a cyber threat to the U.S. EDS. The complex grid and control system architecture requires significant resources and expertise that few other types of hackers possess.

Key Perspectives and Insights:

Presumably, the resources, planning, and long-time horizon of a widespread attack would pre-empt or be part of a more comprehensive act of war. Thus, the industry is reasonably assured that, unless an actor wants to declare war on the U.S., such an attack will not occur. However, as the threat surface increases and grid architecture changes with the incorporation of new technologies, the barrier to accessing operational networks will lower.

3.2.42.2 Cyberterrorists

Open source threat intelligence suggests that terrorist groups do not possess the ability to successfully attack the electricity sector at scale due to capability and resource constraints. However, should the threat surface or the groups' expertise sufficiently increase, electricity delivery disruption would be a primary way of attacking the U.S.

3.2.42.3 Cyberspies

This class of cyber-aggressor engages in espionage to gain a competitive advantage over its victim. Whether motivated by corporate, national policy, or financial goals, they aim to steal information. Cyber-spies present a direct threat to utility companies' business systems but only an indirect threat to grid operations in that they can collect information on grid configuration or operations to be used to develop cyberattack capability.

3.2.42.4 Cyberthieves

As with the terrorist groups, cyberthieves cannot cause widespread electrical service disruption. More commonly referred to as cybercriminals, these organizations are most numerous in the cyber threat landscape and often target utilities' business IT systems. Again, as the hacker capabilities and sector's technology evolve, these actors may become more significant threats to the electrical system.

3.2.42.5 Cyberhacktivists

These cyber-aggressors execute cyberattacks "for pleasure, or for philosophical, or other nonmonetary reasons" [56, p. 4]. Cyberhacktivists also cannot attack the electrical system and cause a widespread outage but could develop it in the future.

3.3 Stakeholder Salience

Having identified 68 stakeholders, determining their abilities to improve cyber response mechanism is useful for two reasons. First, such an analysis permits future resources and effort to build cyber response mechanisms around stakeholders with the appropriate power, legitimacy, and urgency to create and sustain an effective mechanism. Second, it also reveals to other stakeholders where they are limited or empowered to make changes in the sector's response mechanisms and drive collectively towards consensus on gaps and solutions. To this end, stakeholder saliency can be assessed, which then informs the stakeholders with the authority and ability to develop and implement cyber response mechanisms.

3.3.1 Salience Methodology

Salience can be determined using Mitchell et al.'s approach to stakeholder saliency. In their work, the authors classify stakeholders according to three attributes, i.e., power, legitimacy, and urgency [35]. For this evaluation, the three attributes of power, legitimacy, and urgency must be defined. Rhodes provides clear explanations of each:

- *Powerful stakeholders possess power in their relationship to the* [sector]*, and may be capable of imposing their will on the* [sector]
- *Legitimacy is the perception that the actions of a stakeholder are desirable, proper, or appropriate within norms, values, and beliefs of the enterprise.*
- *Urgency exists when the stakeholder's relationship with the* [sector] *is time-sensitive in nature, and/or is of importance to strategy and operations [241, p. 49]*

In order to apply these definitions correctly, the stakeholders must first be considered in the context of their ability to improve the electricity sector stakeholders' abilities to respond to a cyber event at scale. In that context, the definitions become:

- Power – the ability to hold sector entities accountable to develop and implement cyber response preparations in both the public and private sectors and the ability to direct and prioritize public and private response efforts and resources at the sector-wide level during a cyber event
- Legitimacy – the legal authority or legal obligation to provide for reliable electricity delivery and cyber resilience, including cyber response, of the electricity sector
- Urgency – the desire to improve cyber response by nature of a stakeholder's underlying mission or responsibility

Given these definitions, saliency may be analyzed using Mitchell et al.'s typology for describing stakeholders, as shown in Figure 3.10 [35, p. 874].

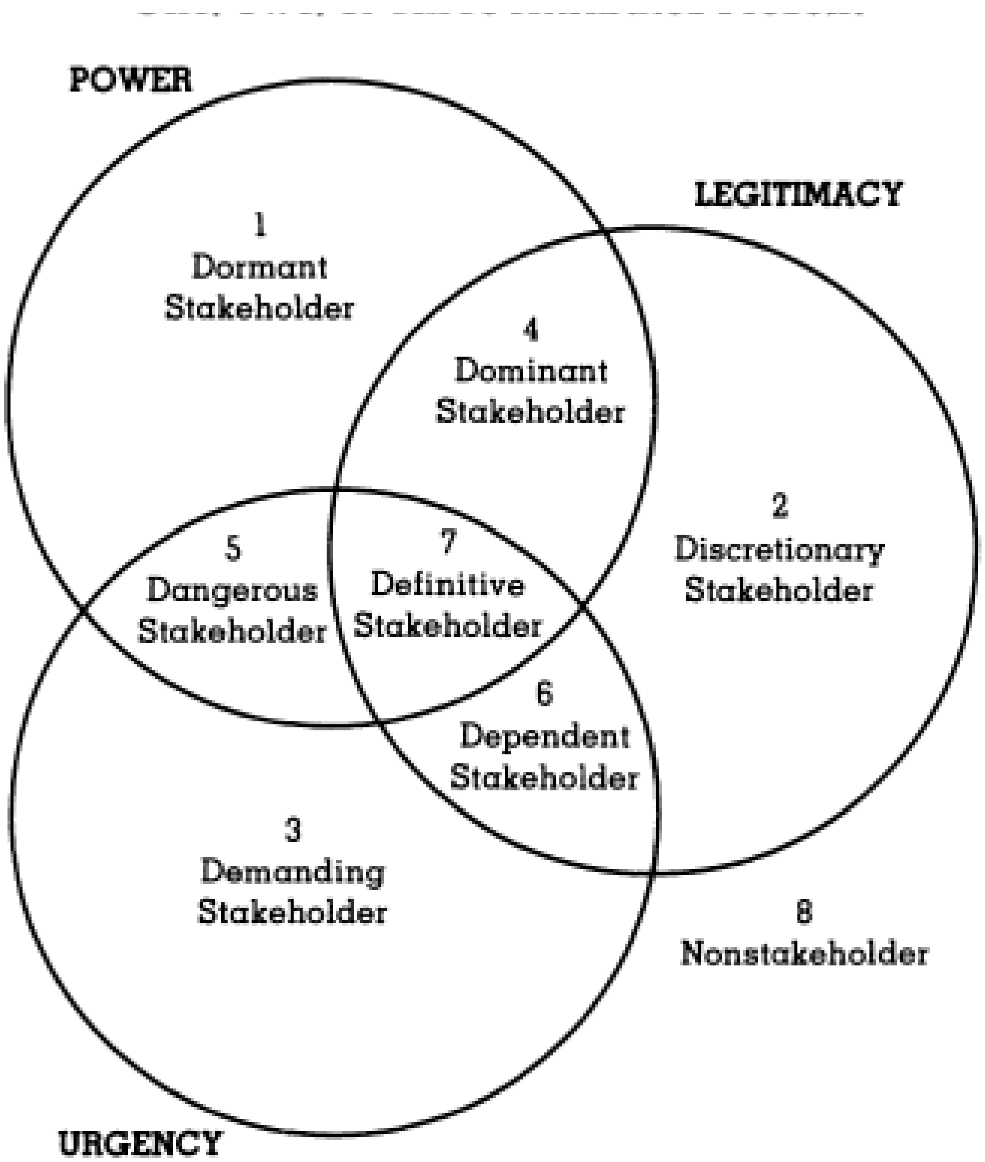


Figure 3.10: Stakeholder Typology

3.3.2 Stakeholder Salience Analysis and Results

Applying the refined definitions of the three attributes and typology reveals stakeholder saliency, as shown in Figure 3.11 with an accompanying key in Table 3-3.

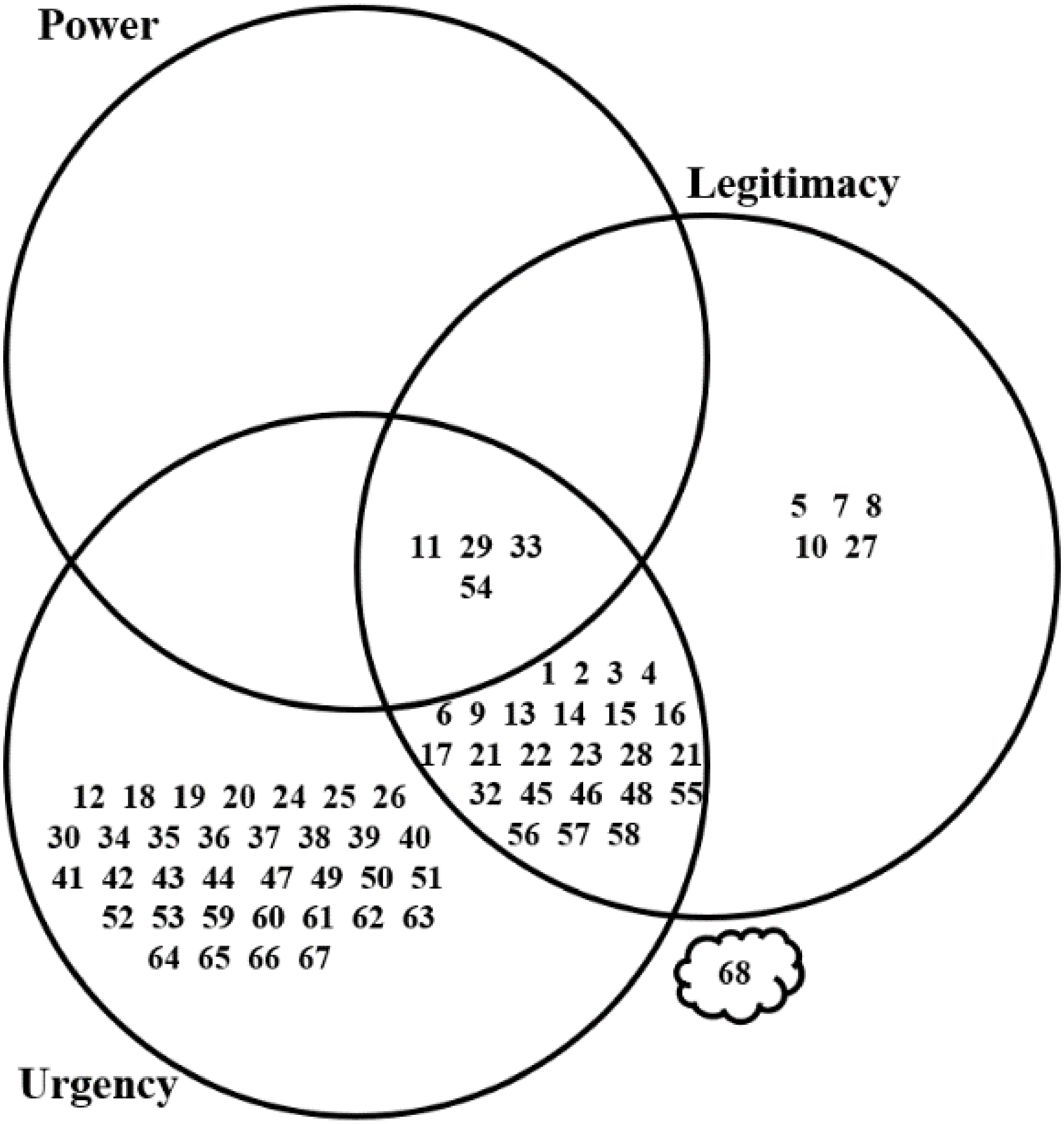


Figure 3.11: Electricity Sector Stakeholder Salience Analysis

From this, only four types of stakeholders emerged: demanding, dependent, discretionary, and definitive. Cyber-aggressors, though influential in the electricity sector, obviously do not directly contribute to the improvement of cyber response in the industry.

Table 3-3: Stakeholder Key for Figure 3.11

#	Stakeholder	#	Stakeholder
1	Investor-Owned Utilities	35	National Rural Electric Cooperative Association (NRECA)
2	Publicly-Owned Utilities	36	Touchstone Energy Cooperative
3	Cooperative Utilities	37	American Public Power Association (APPA)
4	Regional Transmission Operators Independent Systems Operators	38	
5	Joint Action Agencies	39	State and Regional Public Power Associations
6	Balancing Authorities	40	National Association of State Chief Information Officers (NASCIO)
7	Regional Entities	41	National Governors Association (NGA)
8	Power marketers	42	National Association of State Energy Officials (NASEO)
9	Reliability Coordinators	43	National Emergency Management Association (NEMA)
10	Consumers	44	Large Public Power Council (LPPC)
11	U.S. Federal Government	45	Electricity Information Sharing & Analysis Center (E-ISAC)
12	National Infrastructure Advisory Council (NIAC)	46	Multi-State Information Sharing & Analysis Center (MS-ISAC)
13	Department of Homeland Security (DHS)	47	Information Sharing & Analysis Organizations (ISAOs)
14	Cybersecurity & Infrastructure Security Agency (CISA)	48	InfraGard
15	National Cybersecurity & Communications Integration Center (NCCIC)	49	State Fusion Centers
16	NCCIC Hunt & Incident Response Teams (HIRT)	50	Federally Funded Research & Development Centers (FFRDCs)
17	National Infrastructure Coordination Center (NICC)	51	Electric Power Research Institute (EPRI)
18	National Operations Center (NOC)	52	SANS Institute
19	National Risk Management Center (NRMC)	53	National Institute of Science & Technology (NIST)
20	Federal Emergency Management Agency (FEMA)	54	State Governments
21	Department of Energy (DOE)	55	State Chief Information Security Officers (CISO)
22	Office of Cybersecurity, Energy Security, & Emergency Response (CESER)	56	National Guard
23	Energy Sector Government Coordinating Council (EGCC)	57	State and Territory Energy Office (SEO)
24	Federal Senior Leadership Council (FSLC)	58	State Office of Emergency Management
25	State, Local, Tribal, & Territorial Government Coordinating Council (SLTTGCC)	59	Federal Bureau of Investigation (FBI)
26	Regional Consortium Coordinating Council (RC3)	60	Cyber Action Team
27	Federal Trade Commission (FTC)	61	National Cyber Investigative Joint Task Force (NCIJTF)
28	Department of Defense (DoD)	62	Threat Analysts
29	Electricity Subsector Coordinating Council (ESCC)	63	Monitoring Platform Vendors
30	Critical Infrastructure Cross-Sector Council	64	Response & Forensics Vendors
31	Federal Energy Regulatory Commission (FERC)	65	Cybersecurity Software & Other Product Vendors
32	North American Energy Reliability Corporation (NERC)	66	Electrical Equipment Manufacturers
33	Public Utilities Commissions (PUCs)	67	Operational Technology (OT) Producers
34	National Association of Regulatory Utility Commissioners (NARUC)	68	Cyber-aggressors

3.3.2.1 Demanding Stakeholders

Demanding stakeholders are characterized by the attribute of urgency and are the most numerous. In this context, they are characterized by the desire to improve electricity sector response mechanisms because of their stated mission, inherent interest, or direct liability for cyber incidents, but they simultaneously lack authority and are not in a place to effect any changes. They fall into five categories:

- Advisory bodies who are formally established within government constructs to advise on policy and government action
- Law enforcement or security agencies whose responsibility it is to protect national interests but do not have a direct responsibility to the electricity sector
- Trade associations and advocacy groups which provide cybersecurity programs to members for reliability and compliance purposes and advocate for government policies on behalf of their members
- Research and Development entities charged with developing technology and process to increase cyber resilience and cyber response in the electricity sector
- Business interests who sell cybersecurity products and services and facilitate cyber response

3.3.2.2 Dependent Stakeholders

Dependent stakeholders are characterized by both urgency and legitimacy and fall into two categories:

- Electricity market entities include generation, transmission, and distribution entities and electricity market participants, charged with providing reliable power to consumers
- FSLTT Government critical infrastructure support agencies who are charged with executing its policies for sector support and providing incident response resources
- Energy and electricity regulatory agencies at Federal, regional, and state levels who are responsible for enforcing compliance with reliability, i.e., cybersecurity standards.

3.3.2.3 Discretionary Stakeholders

Discretionary stakeholders are characterized by their legitimate concern in the cyber response process. They are removed from any direct control over cyber response mechanisms and are only focused on access to electricity, not necessarily how cyber secure it is.

3.3.2.4 Definitive Stakeholders

Definitive stakeholders are fewest in number. This paper asserts that the only definitive stakeholder is the one with power, legitimacy, and urgency: the U.S. Federal Government, i.e., the Executive and Legislative Branches. Though the U.S. Constitution grants the Federal Government power to regulate the electricity sector under the commerce clause and charges it with providing for the national defense, it has yet to establish primacy for a cyber response. Currently, the Federal Government only has authority to direct utilities in instances of “grid security emergencies,” and even then, it is limited to the BPS [91].

State utility commissions, unlike, FERC, have more consolidated power and can influence the utilities under their jurisdiction to a higher degree. Likewise, state governments have power similar to the Federal Government within their borders, especially over distribution systems. However, the BPS crosses state lines and remains mainly under the purview of the Federal Government, so state governments lack power over the entire sector.

Finally, the ESCC is increasingly influential in that it has earned expert, referent, and informational power, not based on positional authority, as the liaison between the government and industry [242]. Given its unique and influential position in the electricity sector, the ESCC likely has the potential, however indirect, to direct response preparations and efforts.

3.3.3 Stakeholder Salience and Cyber Response

With a more detailed understanding of the salience of the stakeholder categories, it is clear that the definitive stakeholders must play an active role in the creation and sustainment of any response mechanisms. However, the landscape analysis in chapter 2 reveals a lack of willingness on the part of the government to assert their authority and take a more active role in cyber response mechanisms. Similarly, most of the sector lacks any meaningful authority to make changes or improvements where they see fit. Thus, either the definitive stakeholders need to assert their authority prudently or delegate it to stakeholders that have a higher degree of urgency.

3.4 Stakeholder Value Exchange

3.4.1 Stakeholder Value Exchange Methodology

Another essential step in the stakeholder analysis process is the identification of stakeholder value exchange [33]. This process includes classifying stakeholders and then examining their needs from the sector to enable cyber response and their contributions to the sector's response mechanisms. Finally, the stakeholder values are examined to identify disparities between the importance of needs and how well they are being fulfilled. The insight gained from this process is used to develop the value proposition necessary for crafting a cyber response mechanism that meets stakeholders' needs for responding to a large scale malware attack [33].

3.4.2 Stakeholder Classification

Next, it is necessary to categorize the stakeholders in order to simplify value exchange analysis and align it with a whole-of-sector perspective. The stakeholder salience analysis produces a feasible way of classifying stakeholders using their salience typology because it groups stakeholders according to their functions and interests in the electricity sector's cyber response mechanisms.

For instance, many of the stakeholders perform the same roles in the ecosystem in different locations, e.g., state public utilities commissions, investor-owned utilities, and can be presumed to share similar interests. Specific entities are enumerated because they occupy a unique role within the ecosystem, separate from any other organization. Many of these are Federal Government agencies which, by their nature, are the only bodies granted appropriate authority relevant to the analysis. Similarly, there are few trade associations and research & development organizations which should be discussed together.

Because of the size of the sector under analysis, the process of classification in this instance also had the effect of quasi-prioritization. The categorization generalizes the stakeholders into the critical functions necessary for responding to a malware attack, and it diluted the effects such as an organization's size or resources which tended to overweight their importance to the sector's mechanisms. For instance, state governments, arguably, have more critical infrastructure within their jurisdiction, yet they lack the resources of the Federal Government to regulate them adequately [113]. Thus, observers might weigh the contributions of the Federal Governments more heavily and potentially focus the improving response mechanisms by empowering it to a higher degree. However, the classification process is informed by the saliency analysis, which suggests that state governments are equal or near equal stakeholders to the Federal Government.

In many instances, the stakeholders fall into more than one classification based on their functions. In order to simplify the analysis, they are categorized by their explicit authority or the category by which they exert the most considerable influence on the sector. Appendix B shows the classification of stakeholders, but a list of the ten identified classifications follows:

- Electricity Market Entities
- Federal Government Critical Infrastructure Advisory Bodies & Support Agencies
- State, Local, Tribal, and Territorial Government Critical Infrastructure Support Agencies
- Regulatory Bodies
- Trade Associations & Advocacy Groups
- Information Sharing Entities
- Standards, Research, & Development Organizations
- Law Enforcement
- Cybersecurity Vendors
- Electricity Cyber-Physical Asset Manufacturers
- Cyber-Aggressors (omitted in value analysis)

3.4.3 Stakeholder Value Exchange Assessment

A value exchange analysis identifies what each category of stakeholder needs or expects from an enterprise. The ultimate goal of the analysis is to identify gaps and create a value proposition for potential mechanism improvements [241]. In this case, the analysis determined what the electricity sector stakeholders needed to respond to a large-scale malware attack. Concurrently, it identified the value each stakeholder provides to cyber response mechanisms in the sector.

Stakeholder value was determined through interviews with representative members in each category and augmented with open source analysis of stated missions and values. The interviews and research yielded the value exchange shown in Table 3-4.

Table 3-4: Stakeholder Value Exchanges

Value EXPECTED FROM Sector Cyber Response Mechanisms	Stakeholder Classification	Value CONTRIBUTED TO Sector Cyber Response Mechanisms
• Response frameworks, processes, and prioritization from FSLTT support agencies • Threat information and intelligence to support investment and risk management • Clear roles for public and private entities • Trusted relationships with supporting stakeholders • Autonomy to manage risk and incident response measures • Malware mitigations • Clarity on cyber resilience best practices and metrics • Support for cybersecurity investment recoupment	**Electricity Market Entities**	• Expertise on grid and equipment operations • Mutual assistance to peer stakeholders • Local leadership of response efforts • Trusted relationships with business partners • Advising FSLTT policy formation
• Integration into private sector response plans and efforts • Compliance to legislation, regulation, and policies • Information sharing from private sector entities • Recommendations and advice on cyber response policy, frameworks, and government action • Trusted relationships with local public and private partners	**Federal Government Critical Infrastructure Advisory Bodies & Support Agencies**	• Valuable national and regional response resources • Research & development funding • Legislation and regulation that supports cybersecurity investment • Intelligence collection, fusion, and sharing • Large-scale risk assessments and management frameworks • Offensive and defensive cyber capabilities targeted at cyber threats
• Information and intelligence sharing • Coordination between public and private entities • Consensus and support of membership for cybersecurity initiatives	**SLTT Government Critical Infrastructure Support Agencies**	• Valuable regional and local response resources • Research & development funding • Legislation and regulation that supports cybersecurity investment • Trusted relationships with local public and private partners
• Compliance with incident reporting, response preparations, and other CIP measures as required by regulations • Recommendations for rule-making of new and updated regulations	**Regulatory Bodies**	• Regulations that support compliance with critical infrastructure protection standards • Support to rate cases that allow for recoupment of prudent cybersecurity investments
• Information and intelligence sharing • Integration into private sector response plans and efforts • Consensus and support of membership for cybersecurity initiatives • Trusted relationships with supported and supporting stakeholders	**Trade Associations & Advocacy Groups**	• Pooled resources for investment in research and development and shared cyber technologies • Coordination of mutual assistance programs • Consensus building for cyber response mechanisms among members • Advocacy for regulatory and legislative changes that permit better cybersecurity investment and improved processes • Coordination of industry-government incident response plans at all levels

Value EXPECTED FROM Sector Cyber Response Mechanisms	Stakeholder Classification	Value CONTRIBUTED TO Sector Cyber Response Mechanisms
• Timely cyber incident reporting from utilities • Collaborative participation in information sharing programs • Funding to support information sharing organization	**Information Sharing Entities**	• Incident notification processes and anonymization • Limited coordination of relevant entities for cyber response
• Information sharing from electricity market entities and government agencies • Investment in organizations' cybersecurity projects	**Standards, Research, & Development Organizations**	• Long term cyber threat, vulnerability, and technology analysis to feed policy decisions and inform the sector • Innovative cybersecurity tools, processes, frameworks, guidelines, and technologies that keep pace with cyber threats, vulnerabilities, and technology
• Timely cyber incident reporting from utilities • Preservation of evidence and facilitation of investigation, forensic analysis	**Law Enforcement**	• Cyber forensic analysis capability through fly away teams or local field office support
• Intelligence and information sharing • Trusted relationships with supporting and supported stakeholders • Business opportunities to provide cyber incident response services	**Cybersecurity Vendors**	• Specialized cybersecurity expertise • Information sharing with public and private stakeholders • Cyber incident response services tailored to supported customers
• Business opportunities/feedback to provide cutting edge cyber technologies that increase cyber resilience and ability to respond • Integration into response plans	**Electricity Cyber-Physical Asset Manufacturers**	• Development and sales of ICS-tailored cyber technologies and increasingly hardened cyber-physical assets • Specialized equipment and software expertise to identify and mitigate cyber threats

3.4.4 Stakeholder Value Map

Following a value exchange assessment, stakeholder value mapping can identify disparities between the needs of stakeholders and the sector's current ability to deliver or perform to fulfill them. Thus, the results of individual stakeholder value mapping may indicate where gaps in sector-wide cyber response mechanisms may exist. In this instance, value mapping identified the importance of each value to the stakeholder's ability to respond or support a response to a large-scale cyber event. Then the sector's current quality of value delivery or performance was measured. The examination was performed qualitatively based on interview responses and existing studies. Both the importance and delivery were measured for each classification of stakeholder, as shown in Appendix C. The corresponding results were plotted on a stakeholder value map in Figure 3.12. On the value map, every point represents a need listed in the "Expected From" column of Table 3-4.

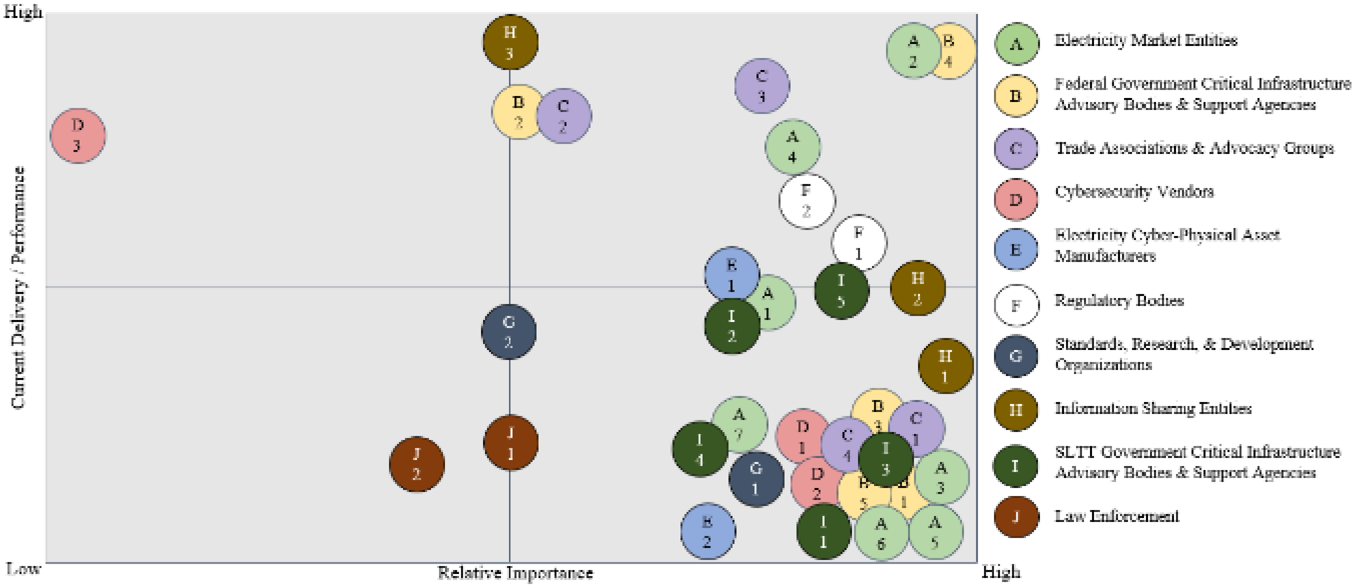


Figure 3.12: Current Stakeholder Value Map for the Electricity Sector

Despite the number of stakeholders and their diverse values and perspectives, common interests emerged. Pointedly, the bottom right quadrant of Figure 3.12 shows the values for each category of stakeholder, which are of high importance but which the sector struggles to deliver or perform. The needs for stakeholders had in common that appeared in the bottom right quadrant were:

- Trusted relationships between stakeholders, especially from different categories
- Clear roles for response processes
- Integration of external entities into Electricity Market Entities response plans
- Information sharing and access to intelligence

Collectively, these four shared needs indicate gaps in the sector's ability to respond to a large-scale malware attack.

3.5 Chapter 3 Summary

In summary, because the electricity sector is large and fragmented, stakeholder analysis is essential to identifying the gaps in cyberattack response mechanisms. The number of roles and responsibilities needed to respond to a widespread cyber incident is significant. However, that realization provides only a small indication of the complexity of the environment and the mechanisms required to reach the goal of improved cyber response. As demonstrated by the stakeholder saliency analysis, the electricity sector has many stakeholders who perform the same function, has many interested but disempower parties, and lacks definitive stakeholders at the right locations within the sector who capable of making critical incident response decisions.

The looming threat of consistently evolving hackers and a growing threat surface indicate the sector must make preparations to rapidly respond and recover from a cyberattack that affects more than one utility. As is evident from the stakeholder analysis, there are four areas for future work: establishing trusted relationships between sector stakeholders, clearly defining roles and responsibilities for a coordinated response, maturing integrated incident response plans, and sharing information and intelligence across the sector.

4 Current Architecture of Electricity Sector Cyber Response

The NIST Cybersecurity Framework's definition described in sections 1.3.5 and 1.3.6 broadly capture the functions required to respond to a cybersecurity event; identify protect, detect, respond, and recover. They are useful to simplify complex response mechanisms that must be planned for, resourced, and executed throughout an entire sector, at all levels of government, and across an entire continent. Chapter 4 endeavors to offer a thorough analysis of these complex functions using the ARIES Enterprise Element Model discussed in section 1.6.3. Additionally, this chapter assesses the current state of the sector's ability to respond to a large-scale malware attack informed by the landscape analysis and electricity sector's drivers for changing cybersecurity in Chapter 2 and analysis of the stakeholder value exchange in Chapter 3.

Chapter 4 analyzes the sector's cyber response mechanisms using the six of the ten ARIES "view elements." Table 1-2 is presented below again with the six view elements discussed in Chapter 4 emphasized.

Table 4-1: ARIES Framework Enterprise Elements Adapted to the Electricity Sector

Element	Description
Ecosystem	The external cyber threat, regulatory, political, economic, and market environment in which the electricity sector operates with other subsectors and critical infrastructure sectors
Stakeholders	Organizations who contribute to, benefit from, and/or are affected by the electricity sector's ability to provide reliable, cyber resilient power to the U.S.
Strategy	The strategic vision and key strategic thrusts and goals of electricity market stakeholders and the governments who regulate and provide existing incident response mechanisms
Information	Information that electricity sector needs to measure, prepare for, and respond to widespread malware attacks
Infrastructure	Physical and technological systems that enable cyber response mechanisms to operate efficiently and effectively
Products	Products that the electricity sector develops and uses to enhance cyber resiliency and cyber incident response capabilities
Services	Services that the electricity sector develops and uses to enhance cyber resiliency and cyber incident response capabilities
Process	Processes through which the electricity sector manages cyber risk and communicates, coordinates, mitigates, and evaluates cyber response mechanisms
Organization	Organizational structure, cybersecurity cultural and relational values of the electricity sector that influence its cyber response mechanisms
Knowledge	Competencies, expertise, and explicit and tacit knowledge that the electricity sector stakeholders contribute to or require from the sector in order to enable cyber incident response

Products and services are combined because their roles in the sector's response mechanisms are nearly identical to one another. Knowledge has been omitted because preliminary analysis revealed the only knowledge deficiency relevant to electricity sector cyber response mechanisms was a shortage of qualified personnel. This shortage affects all industries, has been widely documented, and is currently being addressed [32], [133], [3], [243]. Infrastructure is omitted because, at this level of analysis, the infrastructure that enables large-scale cyber response falls into another critical infrastructure sector, e.g., telecommunications, transportation, which is beyond the scope of this thesis. However, further study of the cross-sector implications of a large-scale malware attack is necessary to identify other gaps in the electricity sectors response mechanisms.

Another critical aspect of the ARIES Element Model is the concept of entanglement. Nightingale and Rhodes (2015) assert that the view elements cannot be viewed in isolation because they are inherently connected and changes to the one element may propagate to others in varying degrees [33], [244]. The authors point to the element of strategy as being a "key driver of the architecture of the process, organization, knowledge, and information elements," and in the case of the electricity sector, this observation holds [33, p. 18]. Strategy, process, organization, and information elements of the sector's response mechanisms are deeply entangled, and often, the interactions bidirectionally influence one another. Each section in this chapter identifies these interconnected relationships in the context of the existing response mechanism and determines how the relationships contribute to gaps in the electricity sector's cyber response mechanisms. The elements are presented in order of the amount of influence they have over the sector's response mechanisms.

Finally, each element is broadly assessed according to the five parts of its anatomy (structure, behavior, artifacts, measures, periodicity) as shown in Table 1-3, and the more prominent parts of the element anatomy are described and analyzed.

4.1 Strategy

The electricity sector's strategy for cyber response most closely reflects the influences of the regulatory and political factors described in Chapter 2. The need for energy security in the U.S. and cybersecurity's position as a public good require significant involvement from FLSTT governments, and the PPP approach drives many of the other elements of a cyber response. Within the cyber response mechanism itself, strategy directs the processes used for response, the way information is created and disseminated, and the empowerment of entities and organizations to manage response efforts. Strategy also indirectly influences the ability of the sector to acquire, develop, and maintain knowledge and expertise in cybersecurity. In the same manner, national cybersecurity standards and organizational interests drive strategy development and implementation.

The strength and influence of these interactions emerge when one examines the element anatomy of the sector's cyber response mechanism strategy. In particular, the structure of the strategy dominates the other parts of the anatomy and drives variation in how segments of the electricity sector develop and implement their strategies. Notably, the structure of the response mechanism strategies can be generalized into three groups: the electricity market entities' approaches to cyber response, the state's policy on the sector's cyber response, and equivalently, the Federal Government's policy on critical infrastructure incident response. The remaining subsections in section 4.1 explore the strategy element anatomy within the three groups using the policy artifacts as evidence and highlight the other element anatomy parts that contribute to gaps in the response mechanism.

Additionally, because response functions to a malware attack are process-oriented and focused on quick action, the strategy is difficult to distinguish from the process, and many of the artifacts are the same for both elements. In this analysis, the strategy element conveys the general approach that stakeholders and the sector take towards cybersecurity and cyber response. Conversely, processes refer more to the procedures that the sector takes to respond or enable a response to a cyberattack. Often, strategy and processes are captured in the same artifact, such as a response plan, rather than separate documents, making the distinction even more challenging.

4.1.1 Electricity Market Entities Approaches

Industry surveys have shown that utilities and other energy industry entities place cyber risk in their top five business concerns[110], [245]. A 2018 survey conducted by Ernst and Young, however, revealed that cyber incident response remained a critical weakness in investment priorities for private companies from all sectors [114]. The same survey showed that half of the companies polled are not confident in their ability to conduct forensics on a cyber incident, i.e., determine the nature of the cyberattack in order to develop and apply mitigations [114, p. 17]. What the survey does not call out is the impact on operations and exigency with which utilities must be able to react, contain, and mitigate a malware attack. However, it does report that the sector recognizes the growing cyber threat and has made investments and taken steps to protect themselves, though at levels far lower than the researchers recommend [114].

Another trend that emerged from both the Ernst and Young survey and stakeholder interviews was that of the divide between utility companies' approaches to cyber response based on their size. Smaller utilities, such as municipal utilities and cooperatives, lack the resources that large IOUs have to invest in cyber resilience measures, including response mechanisms. Because of their small size, they are also generally excluded from regulatory requirements that demand formal incident response programs. These dynamics can drive small utilities to seek to reduce the burden of investments in cyber response mechanisms to the lowest level practicable. Such an approach cannot keep pace with threat evolution or provide adequate cyber incident response.

On the other hand, large utilities, especially IOUs and RTOs/ISOs, can afford a robust investment in cyber response capabilities, like full-time cybersecurity staff or retainers with MSSPs. For IOUs, cyberattacks pose a threat to the business and, ultimately, shareholders, so cyber resilience and cyber response are business risk mitigation strategies. While they are compelled to excel and innovate cyber response methods that can efficiently and effectively mitigate risks, they are also heavily regulated under NERC CIP and must also focus on compliance with relatively precise response requirements.

Regardless of the size of utilities, their individual strategies are often not codified or fall into an all-encompassing cyber resilience strategy and incident response plan. These strategies and plans follow standardized cybersecurity approaches, typically using the NIST Cybersecurity Framework, and few discuss how to address emerging threats, adapt their organization to new cyber response practices, articulate metrics by which the company measures its cybersecurity posture, or, importantly, how the company differentiates its response based on the scale of the cyberattack.

4.1.2 State Policy

Even though state governments regulate nearly all companies involved in electrical distribution, they rely heavily on Federal guidance for critical infrastructure management. In turn, state critical infrastructure strategies directly influence local incident management policy.

Unsurprisingly, with 56 state and territorial governments, state policy and strategies uniquely reflect the electricity concerns within their jurisdiction and can be influenced by political administration changes and priorities. For instance, one NGA (2017) memorandum reviewed 32 cybersecurity incidents and disruption response plans within 26 states and found no two the same [246]. Thus, state-level policies and strategies have little uniformity between them.

Consistent with the political approach of intergovernmental and PPP, the concept of cooperation between the states and between states and the Federal government emerges as the main thrust of state and territorial cyber response strategies. These strategies are formalized through the Energy Emergency Assurance Coordinators (EEAC) program.

4.1.2.1 Energy Assurance Plans and Incident Response Plans

In 1996, the DOE and NASEO, and later followed by NGA, NARUC, and NEMA, created the EEAC program in order to drive standardization of states' processes governing all types of energy-related emergencies, including cyber incidents [230]. In addition to cyber incident or disruption response plans, states use energy assurance guidelines to develop adaptive strategies to respond to economic factors, natural and human-made disasters, and malicious threats to the energy supply.

For PUCs, strategies for increasing cyber resilience and cyber response mimic the actions of FERC and NERC within the regulatory scheme. PUCs' strategies revolve around incentivizing the right level of investment in cybersecurity measures and compliance with critical infrastructure protection mechanisms to enhance cyber resilience. However, they face the same challenges outlined in section 2.2.2.3 of this thesis.

4.1.3 Federal Policy

The Federal Government strategy to cyber response in the electricity sector is heavily influenced by its historical approach of PPPs with electricity market entities. Indeed, partnering with the private sector by facilitating information exchange, providing intelligence, investing in research and development, and communicating with sector representatives remains the overarching strategy of the Federal Government. The emphasis on each of these features may vacillate depending on leadership changes within the various Federal stakeholder agencies.

Current strategic cybersecurity and critical infrastructure-related imperatives are captured in policies like Presidential Policy Directives (PPDs) 8, 21 and 41, various Executive Orders (EOs). These PPDs and EOs recognize that cyber incidents require unique response capabilities and so have augmented traditional emergency management and response mechanisms, outlined in the National Preparedness and National Planning Systems products and other cyber-specific plans. These remain the critical documents by which the Federal Government communicates its strategy. Although recent changes to the authority of the President and Secretary of Energy under the Federal Power Act (2018) to direct private sector entities' response actions may signal a potential shift to increased involvement in the cyber resilience of the sector [116].

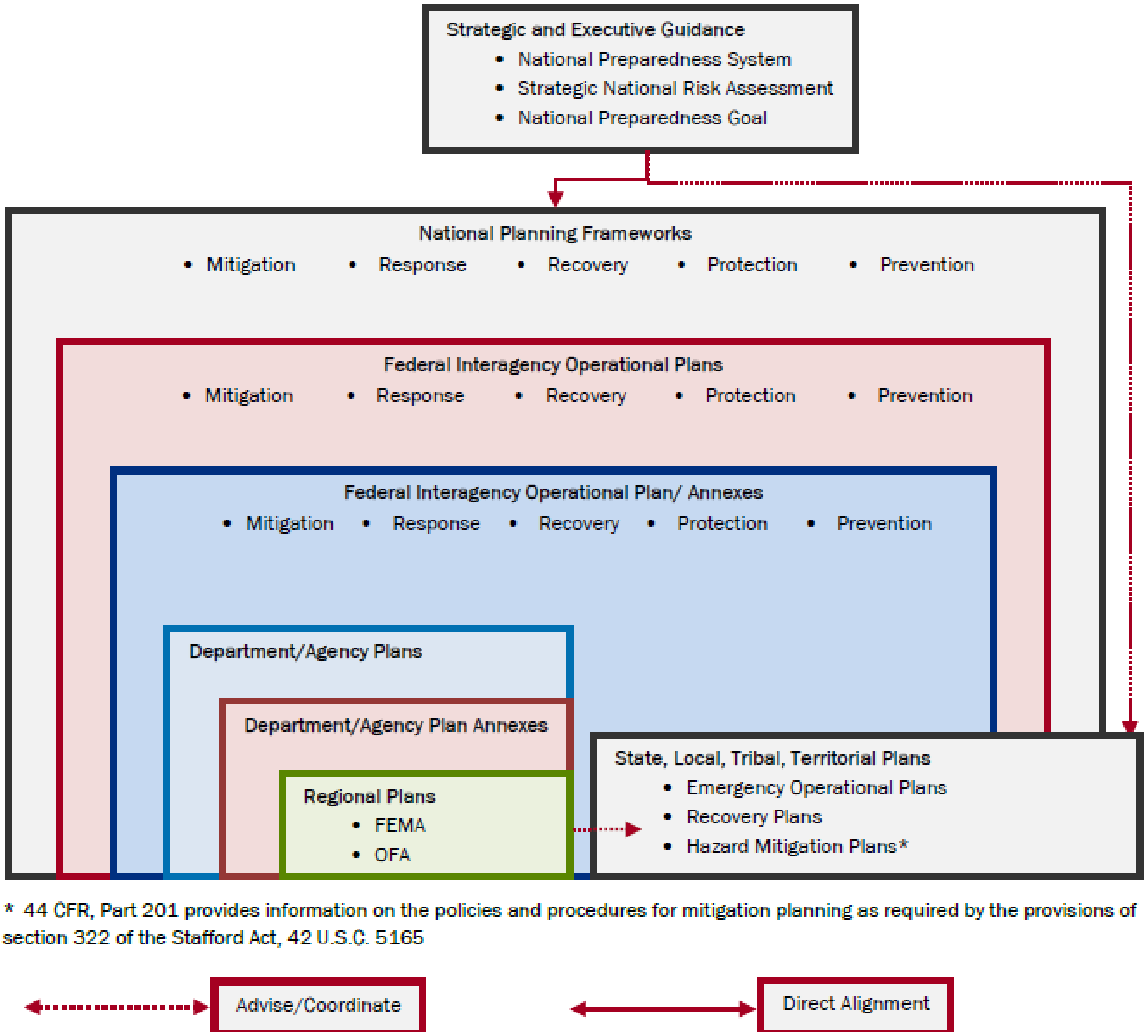
The following subsection describes the strategic imperatives of the national government by analyzing PPDs, EOs, components of the National Planning System. More detailed plans and processes are more closely aligned with the cyber response processes of the Federal Government and are discussed in the next section.

4.1.3.1 Presidential Policy Directive – 8: National Preparedness

PPD – 8 issued by President Obama in 2011 initiated the development of a "national preparedness goal" and the National Preparedness System to strengthen the nation's resilience against the most significant national security risks, including cyberattacks. Under the auspices of the Secretary of Homeland Security, the PPD directs an "all-of-nation, capabilities-based approach to preparedness" [247, p. 1].

The national preparedness goal is a synthesis of the National Security Strategy, applicable PPDs, Homeland Security Presidential Directives, National Security Presidential Directives, and national strategies. These documents define the core capabilities necessary to prepare for "the specific types of incidents that pose the greatest risk to the security of the Nation, and shall emphasize actions aimed at achieving an integrated, layered, and all-of-Nation preparedness approach that optimizes the use of available resources" [247, pp. 2–3].

The outcome of the PPD-8 pertinent to the Federal Government's approach to cyber incident response can be understood by examining the planning efforts in Figure 4.1 [190, p. 49]. The cyber incident response strategies and plans that subsequently emerge from PPD-8 are described below, and the processes that are relevant to a cyber incident response are discussed in the next section.


Strategic and Executive Guidance
National Preparedness System
Strategic National Risk Assessment
National Preparedness Goal
National Planning Frameworks
Mitigation
Response
Recovery
Protection
Prevention
Federal Interagency Operational Plans
Mitigation
Response
Recovery
Protection
Prevention
Federal Interagency Operational Plan/ Annexes
Mitigation
Response
Recovery
Protection
Prevention
Department/Agency Plans
Department/Agency Plan Annexes
Regional Plans
FEMA
OFA
State, Local, Tribal, Territorial Plans
Emergency Operational Plans
Recovery Plans
Hazard Mitigation Plans*
Advise/Coordinate
Direct Alignment

* 44 CFR, Part 201 provides information on the policies and procedures for mitigation planning as required by the provisions of section 322 of the Stafford Act, 42 U.S.C. 5165

Figure 4.1: Alignment of Planning Efforts with PPD-8

4.1.3.2 Strategic National Risk Assessment (SNRA)

The SNRA is another byproduct of PPD-8, which was led by the Secretary of Homeland Security to identify the risks that pose a threat to homeland security [248]. In order to achieve preparedness goals set out by PPD-8, the SNRA evaluated known threats and hazards and categorized them into national-level events. The SNRA's evaluation categorized a "Cyber Attack against Physical Infrastructure," i.e., the electricity sector, under the Adversarial/Human-Caused Hazard/Threat Group and defined a "National-level Event" as:

> *An incident in which a cyber attack is used as a vector to achieve effects which are —beyond the computer‖ (i.e., kinetic or other effects) resulting in one fatality or greater or economic losses of $100 Million or greater [248, p. 3]*

The SNRA also calls out cyberattacks within one of only five overarching themes revealed in the analysis. Its emergence as an overarching theme indicates the cyberattacks have posed a significant risk, a combination of likelihood, consequences, and uncertainty, to the Nation and must be addressed as a national imperative. Specifically, it states:

> *Cyber attacks can have their own catastrophic consequences and can also initiate other hazards, such as power grid failures or financial system failures, which amplify the potential impact of cyber incidents [248, p. 5].*

The classification of a cyberattack against the electricity sector and its emergence as "theme" in this way provides a good indication of the Federal Government's recognition of the seriousness of the attack and, perhaps, under what circumstances it might intervene in the private sector. While the SNRA informs the response mechanisms in the Federal Government, it nonetheless is only used to create a high-level strategy, not develop specific actions for a cyberattack.

4.1.3.3 National Preparedness System

The National Preparedness System is an "integrated set of guidance, programs, and processes that…enable the Nation to meet the national preparedness goal" and comprises five planning frameworks that govern prevention, protection, response, mitigation, and recovery to the Nation's most significant security risk [247, p. 2], [249]. The National Preparedness System also created the National Planning System, which has four components:

> *(1) a set of National Planning Frameworks that describe the key roles and responsibilities to deliver the core capabilities required to prevent, protect, mitigate, respond, and recover;*
> *(2) a set of Federal Interagency Operational Plans (FIOP)—one for each mission area—that provides further detail regarding roles and responsibilities, specifies the critical tasks, and identifies resourcing and sourcing requirements for delivering core capabilities;*
> *(3) Federal department and agency operational plans to implement the FIOPs; and*
> *(4) comprehensive planning guidance to support planning by local, state, tribal, territorial, and insular area governments, nongovernmental organizations (NGO), and the private sector [250, p. 1]*

Among other things, it establishes the Nation's approach to all-hazards response under the National Response Framework (NRF) as outlined below.

4.1.3.4 National Incident Management System (NIMS)

NIMS was born out of the need to have a "common, interoperable approach to sharing resources, coordinating and managing incidents, and communicating information" to address threats, hazards, and events across the nation at all levels of government and in both the public and private sectors [191, p. 1]. NIMS outlines the standard mechanisms to manage resources before and during incidents, describes leadership roles and organizational structures for incident management, and describes systems and methods that help incident response stakeholders communicate and make decisions. It operates on three guiding principles of flexibility, standardization, and unity of effort to achieve priorities of "saving lives, stabilizing the incident, and protecting property and the environment" [191, p. 3]. NIMS provides the "shared vocabulary, systems, and processes to deliver the capabilities described in the National Preparedness System," but is deliberately broad and does not contain cyber incident-specific guidance [191, p. 1].

4.1.3.5 National Response Framework (NRF)

The NRF "describes structures for implementing nationwide response policy and operational coordination for all types of domestic incidents" [190, p. 4]. The Framework further clarifies how the nation applies an all-hazards approach to incident response management. The all-hazards approach describes a capability-based approach to dealing with any "incident, natural or manmade, that warrants action to protect life, property, environment, and public health or safety, and to minimize disruptions of government, social, or economic activities" [251, p. 1]. The definition also implies that an all-hazards approaches are independent of scale and location of the incident but also recognizes that many incidents may occur simultaneously and with little warning. Therefore, the NRF "focuses on core capabilities that can be applied to deal with cascading effects. Since many incidents occur with little or no warning, these capabilities must be able to be delivered in a no-notice environment" [190, p. 7].

The NRF is one of five National Planning Frameworks that fall under the National Preparedness System established in PPD-8. Since NIMS is intrinsically linked to the response function, the NRF is closely aligned with the system's guiding principles, priorities, and standardization protocols. The NRF includes a base document, multiple Emergency Support Function (ESF) Annexes, and Support Annexes that detail the response process and mechanisms that the Federal Government would take in the event of specific incidents. Relevant to the electricity sector's response mechanism, the NRF contains ESF #12 and the Critical Infrastructure and Key Resources (CIKR) Support Annex. The NRF also feeds the Response Federal Interagency Operational Plan (FIOP) which provides a more detailed concept of operations and tasks. The relationship between the National Planning Frameworks, ESFs, Support Annexes, and FIOPs is shown in Figure 4.2 [190, p. 3]. Because ESFs, FIOPS, and Support Annexes provide significant detail on response actions, they will be covered in the following section: 4.2 Processes.

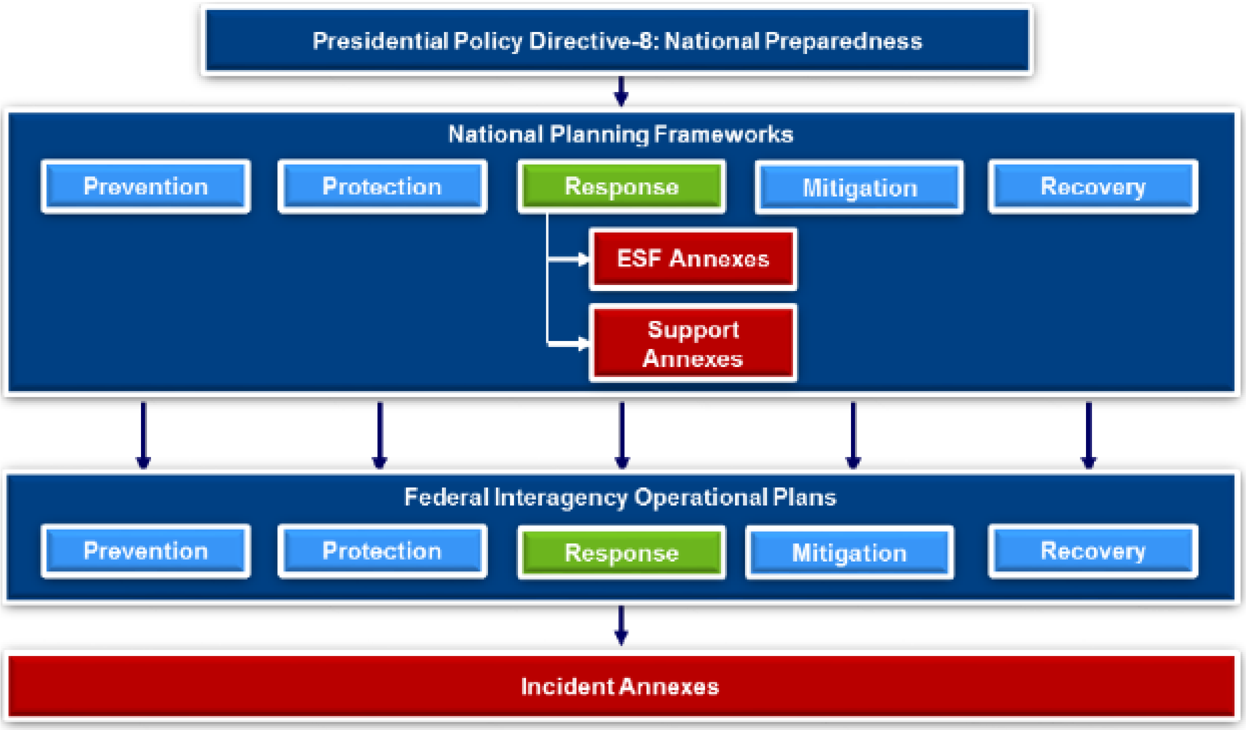


Figure 4.2: NRF, ESF, Support Annex, and FIOP Relationship

4.1.3.6 Presidential Policy Directive – 21: Critical Infrastructure Security and Resilience

Building on PPD – 8, President Obama outlines the national strategy for critical infrastructure protection with PPD – 21. The Directive reaffirmed the Federal Government's approach to the cybersecurity of the electricity sector by stating that CIP is the responsibility of both the public and private sectors. It identified the energy and communications sectors as "uniquely critical due to the enabling functions they provide across all critical infrastructure sectors" and outline three strategic imperatives [27, p. 2]:

1) *Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;*
2) *Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and*
3) *Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure [27, p. 2].*

PPD-21 also calls for an update to the NIPP and refines the roles of the Federal Government in critical infrastructure protection by assigning roles and responsibilities to the SSAs, i.e., the DOE, as stated in section 3.2.13. These roles and responsibilities broadly indicate the strategic approach of the Federal Government to serve as a collaborator with the private sector, other Federal agencies, and SLTT entities.

4.1.3.7 Presidential Policy Directive – 41: United States Cyber Incident Coordination

PPD-41 defines the Federal Government's response to cyber incidents [252]. The Directive assigns lead agencies and establishes an architecture for coordinating with the Federal Government. It provides for five crucial strategic elements of the Federal Government regarding a cyberattack on the private sector. First, it establishes a national definition of a significant cyber event as:

> *A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people [252, p. 2].*

Second, it reiterates the Government's partnering approach to responding to a cyber incident by adopting a risk-based approach that intervenes only when necessary for national security and even then, works to protect privacy and civil liberties. Third, it establishes three concurrent lines of effort, threat response, asset response, and intelligence support, which dictate broad actions it will undertake during a cyber incident. Fourth, it sets out five principles for guiding Federal Government incident response activities: share responsibility between individuals, the private sector, and government agencies; risk-based response; respecting affected entities' privacy and civil liberties to the extent it can; unity of governmental effort to coordinate Federal agencies' efforts; and enabling restoration and recovery by facilitating transition from response actions. These five guiding principles are echoed throughout all Federal guidance on cyber incident response and focus on the strategy and efforts of its agencies. Finally, PPD-41 provides an annex that outlines the structure of the Cyber Unified Coordination Group, the entity that coordinates Federal Government efforts with SLTT and private entities for during a cyber incident [253].

4.1.3.8 Executive Order 13636: Improving Critical Infrastructure Cybersecurity

EO13636 again reinforces the Federal Government's partnership philosophy by focusing on barriers to information sharing, such as the timeliness of intelligence reports, granting of security clearances to critical infrastructure owners and operators, and expand other information sharing programs. Perhaps more importantly, it was the instrument that initiated the development of the NIST Cybersecurity Framework and began the process of the developing frameworks, guidelines, and standards that dominates much of the sector's response mechanism resources [24], [84], [85].

4.1.3.9 Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

EO13800 ordered an in-depth review of critical infrastructure sectors by the DHS with attention paid to the authorities and capabilities that the Federal Government could bring to bear to support the cybersecurity of critical infrastructure sectors. More relevant to the electricity sector, the Order required a detailed examination of:

> *the potential scope and duration of a prolonged power outage associated with a significant cyber incident…; the readiness of the United States to manage the consequences of such an incident; and any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident [254].*

The subsequent subsector report, Assessment of Electricity Disruption Response Capabilities, issued by the DOE in 2017 presents seven, high-level gaps in capabilities of the electricity subsector to respond to a cyber-induced power outage and drive the current Federal Government strategy [3]. The seven gaps align with much of the analysis stated herein and are detailed as follows:

1) *Cyber Situational Awareness and Incident Impact Analysis*
2) *Roles and Responsibilities under Cyber Response Frameworks*
3) *Cybersecurity Integration into State Energy Assurance Planning*
4) *Electric Cybersecurity Workforce and Expertise*
5) *Supply Chain and Trusted Partners*
6) *Public-Private Cybersecurity Information Sharing*
7) *Resources for National Cybersecurity Preparedness [3, p. ix]*

However, the recommendations to close these gaps as outlined in the report take an approach, as can be expected, that is Federal Government-centric. The recommendations focus on what the Federal Government can do not necessarily what the private sector needs, which does not align with its approach to partnering with the sector.

4.1.3.10 National Infrastructure Protection Plan

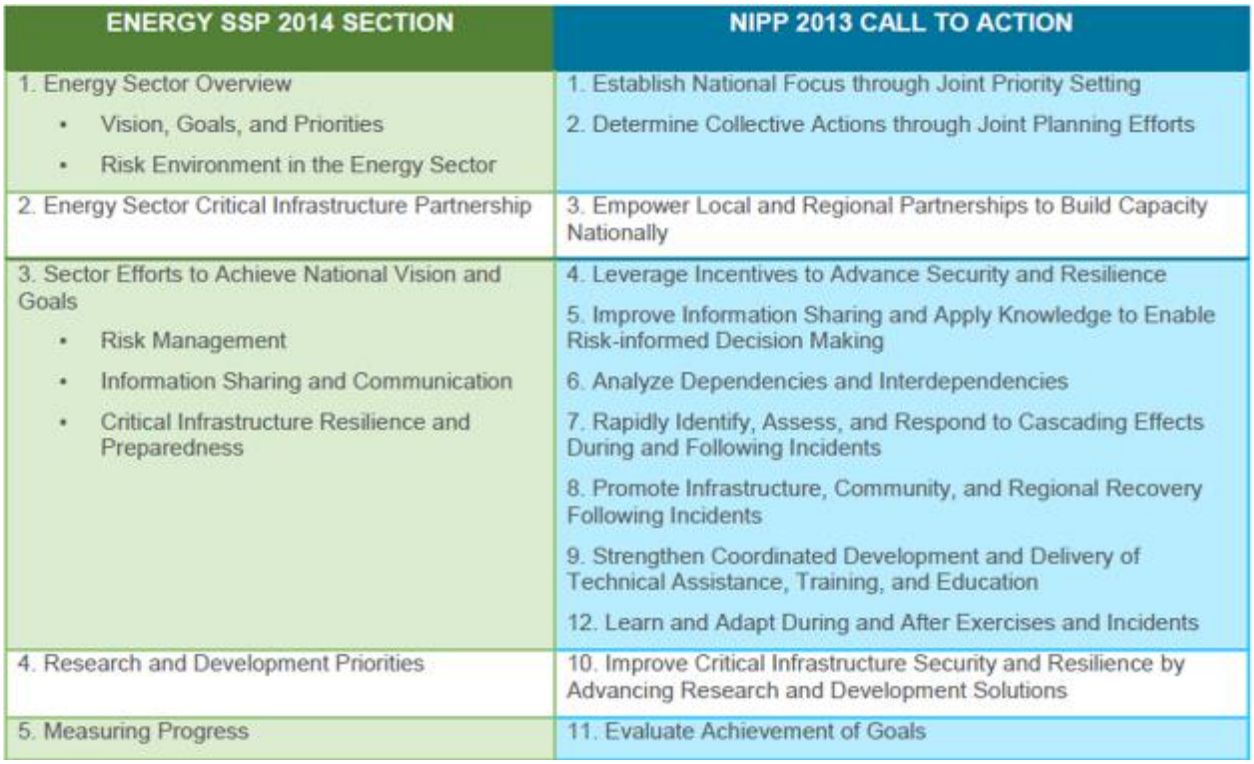
The NIPP is the outcome of the PPD-8, PPD-21, EO 13636, and other national policy and strategy documents governing critical infrastructure protection. It outlines the mission, vision, and goals of the Federal Government towards managing the risk to the Nation's critical infrastructure in an all-hazards context. The Plan provides seven core tenets "representing the values and assumptions the critical infrastructure community should consider (at the national, regional, SLTT, and owner and operator levels) when planning for critical infrastructure security and resilience" [192, p. 13]. Additionally, it provides three sets of activities, builds upon partnership efforts, innovates in managing risk, and focus on outcomes, that are aimed at guiding collaborative efforts within the critical infrastructure sectors. Germane to the electricity sector response mechanism, the PPD-21 and NIPP require the all SSAs to develop Sector-Specific Plans (SSP), and the DOE release the Energy SSP in 2015 accordingly.

The NIPP also lays out a framework, the Sector Partnership Structure, through which the Federal Government approaches working with the private sector for critical infrastructure protection. The Sector Partnership Structure will be discussed further in section 4.3.3.1, but the Structure reinforces the paternalistic, Federal Government-centric view of its role in the cyber response in the electricity sector.

4.1.3.11 Energy Sector-Specific Plan (ESSP)

The ESSP provides the most concise description of the Federal Government’s strategic approach to managing risk and providing for “protection, security and resilience” to the electricity sector because it reflects the consolidation of threats to the sector informed by the DOE [32, p. 1]. Its contents directly map to the NIPP 2013 Call to Action, as shown in Table 4-2, [32, pp. 1–2].

Table 4-2: ESSP Mapping to NIPP 2013 Call to Action

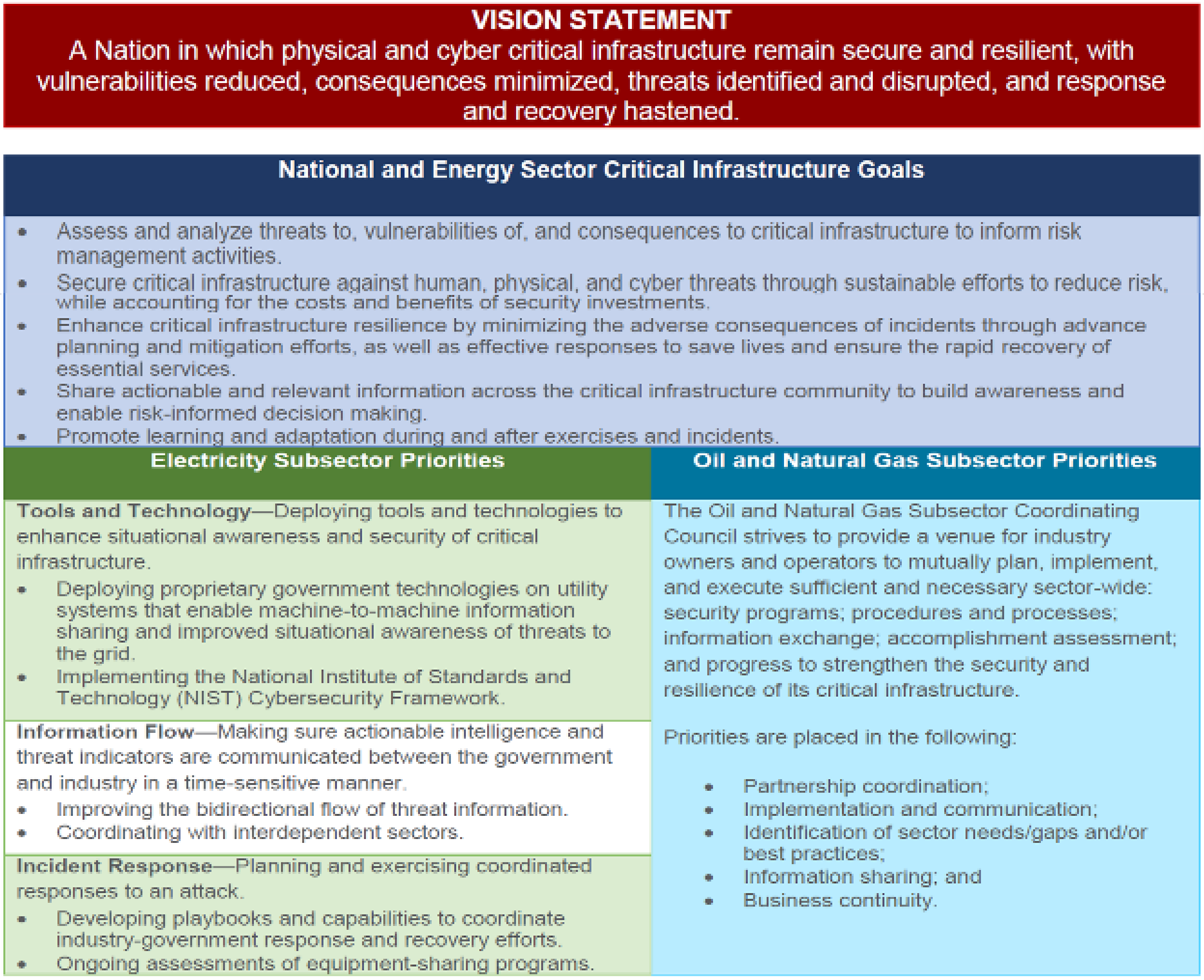


ENERGY SSP 2014 SECTION	NIPP 2013 CALL TO ACTION
1. Energy Sector Overview • Vision, Goals, and Priorities • Risk Environment in the Energy Sector	1. Establish National Focus through Joint Priority Setting 2. Determine Collective Actions through Joint Planning Efforts
2. Energy Sector Critical Infrastructure Partnership	3. Empower Local and Regional Partnerships to Build Capacity Nationally
3. Sector Efforts to Achieve National Vision and Goals • Risk Management • Information Sharing and Communication • Critical Infrastructure Resilience and Preparedness	4. Leverage Incentives to Advance Security and Resilience 5. Improve Information Sharing and Apply Knowledge to Enable Risk-informed Decision Making 6. Analyze Dependencies and Interdependencies 7. Rapidly Identify, Assess, and Respond to Cascading Effects During and Following Incidents 8. Promote Infrastructure, Community, and Regional Recovery Following Incidents 9. Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education 12. Learn and Adapt During and After Exercises and Incidents
4. Research and Development Priorities	10. Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions
5. Measuring Progress	11. Evaluate Achievement of Goals

The mapping provides critical insight into the strategic cybersecurity approach of the DOE as the SSA, namely, that it directly reflects the Federal Government’s PPP approach, risk management, information sharing, and investment in R&D. While not a cyber incident-specific strategy, the ESSP defines the Government’s steady state efforts to support critical infrastructure resilience.

The vision, goals, and priorities of the ESSP, on the other hand, directly addresses the priority and approach to all-hazards incident response for the electricity sector. The ESSP cites incident response planning and exercise as the means to achieve resilience through preparedness. Even though it concentrates on ESF #12 as the Federal Government’s response mechanism, it merely indicates that electricity market entities “have their own company- and facility-level response plans” and does not provide strategic approach or significant detail on their composition [32, p. 25]. Discussion of the current role of exercises as a cyber response mechanism appears in section 4.2.7. The ESSP vision, goals, and priorities are shown in Table 4-3 [32, pp. 3–4].

Table 4-3: ESSP Vision, Goals, and Priorities for the Energy Sector



VISION STATEMENT

A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.

National and Energy Sector Critical Infrastructure Goals

- Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities.
- Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments.
- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, as well as effective responses to save lives and ensure the rapid recovery of essential services.
- Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making.
- Promote learning and adaptation during and after exercises and incidents.

Electricity Subsector Priorities	Oil and Natural Gas Subsector Priorities
Tools and Technology—Deploying tools and technologies to enhance situational awareness and security of critical infrastructure. • Deploying proprietary government technologies on utility systems that enable machine-to-machine information sharing and improved situational awareness of threats to the grid. • Implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework.	The Oil and Natural Gas Subsector Coordinating Council strives to provide a venue for industry owners and operators to mutually plan, implement, and execute sufficient and necessary sector-wide: security programs; procedures and processes; information exchange; accomplishment assessment; and progress to strengthen the security and resilience of its critical infrastructure. Priorities are placed in the following: • Partnership coordination; • Implementation and communication; • Identification of sector needs/gaps and/or best practices; • Information sharing; and • Business continuity.
Information Flow—Making sure actionable intelligence and threat indicators are communicated between the government and industry in a time-sensitive manner. • Improving the bidirectional flow of threat information. • Coordinating with interdependent sectors.	
Incident Response—Planning and exercising coordinated responses to an attack. • Developing playbooks and capabilities to coordinate industry-government response and recovery efforts. • Ongoing assessments of equipment-sharing programs.	

4.1.3.12 Cybersecurity Enhancement Act of 2014

The National Cybersecurity Protection Act of 2014 further codifies the strategy of the Federal Government and emphasizes its role to establish "to provide for an ongoing, voluntary PPP to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes" [255, p. 2971].

4.1.3.13 National Cybersecurity Protection Act of 2014 (NCPA)

Similar to the Cybersecurity Enhancement Act, the NCPA reinforces the role of the Federal Government as an agent to facilitate information exchange. The Act charges NCCIC with specific tasks to provide timely, relevant information to potentially affected sectors, especially the Federal Government to SLTT government and private sector entities and across sectors. Additionally, it charges DHS with the creation of a cyber incident response plan to address cybersecurity risks to critical infrastructure [256].

4.1.3.14 National Cyber Incident Response Plan (NCIRP)

The NCIRP is the Incident Annex to the Response Federal Interagency Operational Plan (FIOP)(see section 4.2.6.2) and acts as the Federal Government's strategic framework that "outlines the roles and responsibilities, capabilities, and coordinating structures that support how the Nation responds to and recovers from significant cyber incidents posing risks to critical infrastructure" [117, p. 4]. It communicates how the Federal agencies provide resources for cyber incident response, provides the structure and substance of response plans that all electricity sector stakeholders can draw upon, and dictates roles and responsibilities of the private sector, SLTT entities, and Federal Government that are critical to understanding the electricity sector's cyber response mechanisms.

The NCIRP also enumerates core capabilities and critical tasks that must be executed to respond to a cyber incident in alignment with the core capabilities of National Preparedness Goal, NRF, and Response FIOP [117, Sec. Annex F]. The core capabilities and critical tasks are associated with specific response processes in the event of the cyber incident and are discussed in section 4.2.6.2.

The NCIRP focuses on "building mechanisms need to respond to a significant cyber incident" as defined by PPD-41 [117, p. 8]. The NCIRP also provides a standard Cyber Incident Severity Schema (CISS) to measure cyber incidents and provide a common framework to evaluate, assess, and communicate the severity, urgency, and response efforts required of the incidents.

Perhaps most importantly, the NCIRP dictates the roles and responsibilities of the private sector, SLTT entities, and Federal Government within the three concurrent lines of effort during cyber response activities stated in PPD-41:

1. Threat Response
2. Asset Response
3. Intelligence Support

The implications of the NCIRP's roles and responsibilities are far-reaching and reinforce the observations made in the political factor and stakeholder analyses in Chapters 2 and 3, respectively. Specifically, the threat response is led by the Department of Justice through the FBI and NCIJTF, and they "use criminal and national security authorities to investigate, prosecute, and disrupt cyber threats and to apprehend cyber threat actors" [117, p. 13]. The role of the private sector in threat response is to promptly report the incident to the appropriate authorities with relevant information. However, the roles are reversed for asset response where the Federal Government becomes a passive provider of resources and a conduit for information exchange, and in the case of the electricity sector, utilities become the primary responders. This dynamic naturally puts the onus on the private sector to respond to any effects of cyberattacks on their systems.

For SLTT and private sector entities, the NCIRP provides recommendations of formulating cyber incident response plans in accordance with NIST Special Publication 800-61:

Computer Incident Handling Guide and points to the NRF, Comprehensive Preparedness Guide 101, and Response FIOP as references for their own operational planning and understanding the Federal Government's approach to incident response [257], [258].

Finally, the NCIRP elaborates on PPD-41's establishment of the Cyber Unified Coordination Group. It outlines the authorities, circumstances for formation, responsibilities, and participants of the group, which coordinates the whole-of-nation cyber incident response [253]. Further, section 4.3.3.2 describes the importance of the Cyber UCG and provides greater detail of its function.

4.1.3.15 Federal Power Act

The Federal Power Act as amended in 2018 grants the President and Secretary of Energy the authority to "issue such orders for emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability of critical electric infrastructure or of defense critical electric infrastructure during such emergency" [116, p. 73]. The authority granted to the President and Secretary of Energy is expansive and unprecedented but, simultaneously, untested. However, the authority has never been asserted under the conditions of a cyberattack. What actions the Federal Government could take to enable a more effective response compared to utility owners and operators is a significant gap.

4.1.4 Strategy Gap Analysis

While electricity market entities' response strategies are regularly tested at the scale of the individual company, they remain mostly untested for effectiveness in responding to a large-scale malware attack on the grid. For instance, while the Ernst and Young surveys suggest that utilities are confident in their own ability to respond to a cyberattack, the results reflect a degree of overconfidence because the sector lacks an objective measure of cybersecurity or response preparedness [32].

Likewise, neither the results nor the sum of the incident response plans cannot be interpreted as a comment on how prepared the entire sector is for a large-scale attack. For those private sector entities that face resource constraints on cyber response mechanisms, the lack of metrics or authoritative guidance from FLSTT entities inhibits the ability to articulate deficiencies to policymakers or PUCs that can close funding gaps. Despite this, the aggregate of Federal policies places asset response squarely on the shoulders of the private sector entities that may not be able to afford to respond.

The dynamic that manifests from a lack of testing response strategies also emerges with the state and Federal Governments because their cyber incident strategies, much like the private sector, have not been adequately tested. Simultaneously, electricity market entities, particularly POUs, openly state that they do they know how the government would or could provide assistance during an attack nor do they want government support, with less expertise, involved in a cyber response.

The lack of trust that is created by low confidence stakeholders' reactions during an incident is compounded by the conflicting and ambiguous definitions of a "cyber incident" between the SNRA and PPD-41. The SNRA is very clear in what constitutes a national-level cyberattack, and the PPD-41 provides a broader but not contradictory definition. Yet, neither openly state at what point the Federal Government would step in or to what degree they might engage in private sector response actions. The signing of the Federal Power Act makes that point all the murkier through its definition of grid security emergency which is broad to the point of being vague, but it still grants the Federal Government explicit authority to step in when they so deem. These conflicting definitions and subsequent lack of clarity on the Federal Government's roles reveal the source of some of the private sector's mistrust but also point to government action that direct contravenes its stated partnering strategy.

Analysis of the cybersecurity and cyber response strategies collectively supports the existence of the gap between private sector expectation and public sector response strategy. The aim of the Energy Emergency Assistance Coordinator program and NIPP is to integrate public and private response efforts and resources. However, the dearth of large-scale cyber response strategies at the state and electricity market entity-level and the inversely large number of Federal policies indicates that the sector is not capable, or vested in, providing for a response that goes beyond individual electricity assets. This gap is not unexpected as the analysis in sections 2.2.4 and 2.2.3 shows, but it can no longer be ignored. The government has very clearly articulated its actions during a widespread cyber-related outage, but now it must incentivize a higher degree of preparedness, stipulate private sector actions during such an event, and provide easier access to resources.

Separately, the structure of the electricity sector's cyber response mechanisms is more nebulous than analysis of the structure of strategy would reveal. Electricity sector response strategies generally revolve around individual utilities' IRPs. Despite the governments' wealth of response strategies and processes, there is no overarching strategy or plan that ties individual response plans and actions to sector-wide ones, and the lack of an *integrated* plan is one of the primary gaps in the response mechanisms. The EEAC program has, in theory, addressed this deficiency by outlining the interfaces between FLSTT and private sector plans as shown in Figure 4.3 [259, p. 5], but the degree of integration between plan, which is only recommended by the EEAC program, is questionable.

The National Planning Frameworks compounds the lack of integration because it creates opacity in the ability to understand and navigate governmental response mechanisms. The Frameworks documents have multiple, sometimes redundant reference documents for various incident types and lack cyber incident-specific response for all critical infrastructure sectors. Nevertheless, individual IRPs and government plans reveal much about the sector's ability to respond.

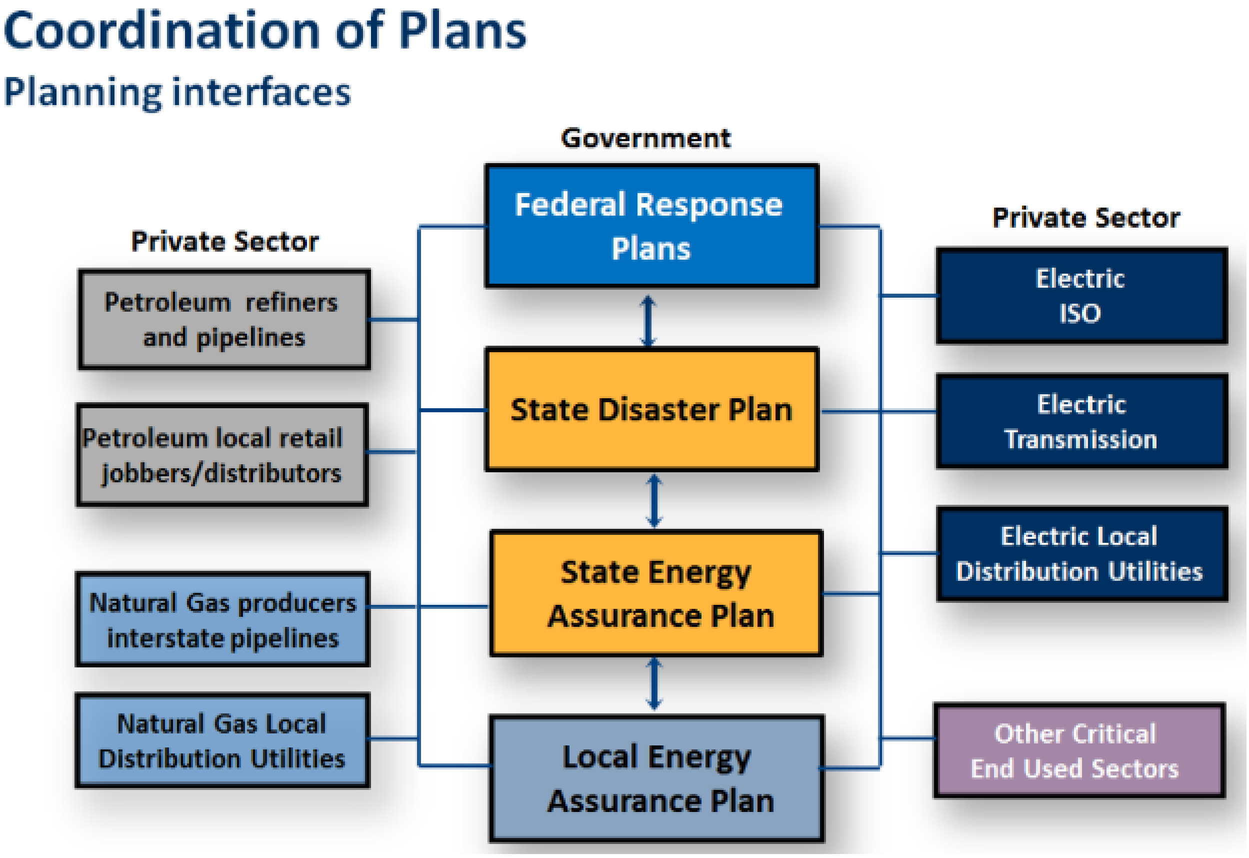

Coordination of Plans
Planning interfaces
Government
Federal Response Plans
State Disaster Plan
State Energy Assurance Plan
Local Energy Assurance Plan
Private Sector
Petroleum refiners and pipelines
Petroleum local retail jobbers/distributors
Natural Gas producers interstate pipelines
Natural Gas Local Distribution Utilities
Private Sector
Electric ISO
Electric Transmission
Electric Local Distribution Utilities
Other Critical End Used Sectors

Figure 4.3: Public-Private Planning Interfaces According to the EEAC Program

The NRF, much like NIMS, drives a top-down approach from the Federal Government to SLTT entities and notes the importance of private sector entities, especially critical infrastructure sector owners and operators, in providing for a response to incidents. However, beyond charging them with the role to promote resilience, it offers little in the way of incentivizing participation in incident response efforts that exceed business continuity. The SNRA's projected risk assessment for a cyberattack on the U.S. and the designated role of electricity market entities in the NRF are mismatched. Business continuity should not be the aim of the electricity sector response strategies. Instead, mitigation of the effects of a cyberattack on its infrastructure must be the key objective.

This approach should not be confused with advocating for nationalization of the grid, and in the case of the Federal Power Act, ceding control over to the government during a cyber incident. However, stakeholder interviews and current research suggest that gaps are created by an imbalance between national security and public interest on one side and economic impact on the other. More explicit and more stringent guidelines for and incentives to invest in cyber response mechanism that strikes such a balance must be sought after and included in the sector's cyber response strategy to combat.

Additionally, PPD-41 and NCIRP stipulate three concurrent lines of effort for the whole-of-nation approach during a response to a cyber incident. At face value, the clear division of roles and responsibilities and assignment of lead agencies and primary responders suggests that incident response tasks not suffer from significant redundancy or miscoordination. However, both documents fail to prioritize the lines of effort when their goals and the goals of the leading responders' conflict.

With OT and ICS in the electricity sector, in particular, there is a conflict between the actions of threat response, which include preservation of evidence, and asset response and regulatory requirements, which include the restoration of reliable power as quickly as possible. Often, steps to restore power involve the destruction of forensic evidence, e.g., wiping infected computers and restoring back-up versions. This conflict is also interestingly reinforced by the NCIRP's "Key Federal Points of Contact," which suggest affected entities contact both threat response agencies, i.e., the FBI, U.S. Secret Service, NCIJTF, or US Immigration and Customs Enforcement / Homeland Security Investigations, and NCCIC for asset response [117, p. 41]. In another reported case, the Federal Government prevented ICS vendors from alerting system users of a critical vulnerability because it was in the process of investigating and did not want to alert the cyber aggressor exploiting it. Therefore, there is a clear gap in the priority of effort for the electricity sector that also contributes to a low level of trust between the public and private sector [126].

Moreover, the division of roles and responsibilities in the NCIRP also neglects to treat cybersecurity as a public good as described in section 2.2.3.1. The Plan indicates that the threat response is to be fulfilled with resources commensurate with national security interests. Federal law enforcement agencies with the requisite legal authorities and jurisdictions are subsequently charged with providing that support. Simultaneously, the NCIRP asserts that the role of asset response, which also has national security implications, falls to the private sector but without the resources, interests, or authorities of the provided to threat responders. Many electricity market entities are neither resourced to provide cyber resilience or large-scale malware attack response capabilities, nor is it within their business interest to make such an investment.

NCIRP relegates states' roles to that of information conduit and facilitator of access to Federal resources. The states' response resources generally do fall behind those of the Federal Government, but the NCIRP's approach does not entertain any measures to identify minimum levels of resources need for SLTT entities to be prepared. This lack exists even though the 2018 National Preparedness Report cited many instances of resource shortfalls and mismanagement during incidents, extreme funding shortfalls in the investment of critical infrastructure resilience, and an inherent complication of resilience efforts with the Federal Government [117].

Optimistically, the NCIRP's recognition of the importance of local governments roles as conduits of information and response resources is an indication that the Federal Government understands the need for greater access to response resources. However, the Government does not and cannot require SLTT entities to formally act in that role which creates issues with information asymmetry in the sector and incidentally breeds high barriers to trust, which are described in 4.3.2.

Finally, while Federal policies provide for many, much-needed inclusive mechanism to continually refine cyber response in the electricity sector, the strategy of the Federal Government allows for partnering to the degree that may detract from the ability to achieve optimal cybersecurity. The Federal Governments dependence on input and guidance from the private sector to increase cybersecurity neglects a more objective point of view and may empower the sector to place their interests over those of the public. The FLSTT PPP strategies rely on the feedback from the electricity sector to develop its policy which, if not objectively measured, perpetuates a cycle that reinforces the illusion of preparedness for an attack. Thus, there should be a mechanism that removes the influence of the private sector and incorporates a "non-partnership" mentality into the development of Federal Government strategy.

4.2 Processes

The processes that surround responding to a large-scale malware attack on the electricity sector remain some of the most underdeveloped relative to other FSLTT and private sector response plans, such as those for major storms and other natural disasters. Processes are arguably the core of cyber response mechanisms where effective processes directly translate to an effective response. In limited cases, these processes, e.g., a utility's incident response plan (IRP), outline the exact steps to be taken to respond to a cyberattack. More often, incident response plans cover broad functions, resources, and capabilities to address any incidents that disrupt reliable electricity delivery. Still, in other cases, there are processes which described enabling functions that facilitate response to an attack or disruption, as in risk management application and incident reporting. Thus, the process element of the cyber response mechanism must be thoroughly examined for gaps and for improvements that can better support response processes.

Additionally, unlike the other elements being examined, the process element of electricity sector cyber response mechanism influences and is influenced by all other elements. These bidirectional relationships expose a high degree of connectivity between the mechanisms, which indicates that changing processes will propagate changes to all other elements – that is, to strategy, information, products and services, and organization. In turn, this implies that identifying and fixing gaps in processes is extremely important to improving the sector-wide response mechanisms and that changes in processes will likely need be considered first to determine the impact on the sector's mechanisms.

As gaps in processes are identified and improvements considered, the degree to which the other elements change is unlikely to be consistent. Therefore, analysis of the elements' interactions is necessary to provide insight into the sensitivity of the other elements to changes in the process [244]. Currently, strategy drives many of the processes in the response mechanisms, but the policy and regulations by which strategies are enacted may also limit the processes to a narrower set of suboptimal mechanisms. The same dynamic between strategy and process also emerges between processes and information elements because of the industry frameworks, guidelines, and standards that the sector uses to establish cybersecurity practices. These documents consist of a variety of management-related and technical processes, and some of the more prominent standards for cybersecurity in the electricity sector include:

- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology, [24]
- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, National Institute of Standards and Technology, [260]
- Guidelines for Smart Grid Cybersecurity, National Institute of Standards and Technology, [145]
- Framework and Roadmap for Smart Grid Interoperability Standards, National Institute of Standards and Technology, [85]
- Guide to Industrial Control Systems Security, National Institute of Standards and Technology, [82]
- Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, [257]
- Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, National Institute of Standards and Technology, [84]
- ISO/IEC 27000-series standards, International Standards Organization/International Electrotechnical Commission, [261]
- NERC Critical Infrastructure Protection, North American Electricity Reliability Corporation, [76]
- State Energy Assurance Guidelines, Version 3.1, National Association of State Energy Officers, [262]
- Electricity Subsector Cybersecurity Risk Management Process, Department of Energy, [83]
- Electricity Subsector Cybersecurity Capability Maturity Model, Department of Energy [87]

Countless other cybersecurity standards exist or are in development. They drive, if not directly dictate, the processes that stakeholders must follow during a cyber response and are reinforced by regulation that mandate compliance with them. As a result, cyber response processes may be overly constrained to the mandated processes and unable or disincentivized to innovate better mechanisms. Since Federal Government policy often charges institutions, like NIST, to create these frameworks and standards, strategy and organizations also become drivers of the process element.

Products and services are slightly less influential to process than the other three elements and again emerge as originators of information asymmetry in the sector. Products and services are incorporated into the response processes, e.g., MSSPs, as a way to compensate for known deficiencies in response plans. Despite this, both elements can contribute to under and overconfidence in the ability for utilities and the sector as a whole to effectively respond to a large-scale malware attack.

An assessment of the process element anatomy has many similarities to that of strategy because response functions are mainly process-oriented. For instance, the artifacts of strategy, e.g., Federal Government response plans, state energy assurance plans, are the same as those of the process element. Likewise, the structure of the process element can be analyzed with the same three categories used to examine the strategy element (section 4.1) with the addition of supporting and enabling process categories.

The remainder of this section reviews four enabling cyber response processes: cyber risk management, incident reporting, malware mitigation, and response plan exercises, and their implications on the response processes. Additionally, the response plans for electricity market entities, states, and the Federal Government are examined. An examination of response processes to second or third order effects of a cyberattack on the electricity sector, e.g., the response processes for coordinating critical transportation during a power outage, is limited to the impact on responding to the cyber incident.

4.2.1 Implications of Risk Management on Cyber Response

The Federal Government drives the electricity sector's approach to cybersecurity, which, at its core, is based on risk management practices. Cyber risk management frameworks, such as the NIST Risk Management and Cybersecurity Frameworks, encourage electricity market entities to apply business practices that weigh the cost of consequences of a cyberattack with the cost of mitigation. In theory, risk management allows them to provide adequate security of the grid within the fiscal constraints of their operating model based on the understanding of risk and performance of mitigation measures. However, Langner and Pederson (2013) suggest that electricity market entities do not fully understand cyber threats, the criticality of their assets, or the vulnerabilities of their systems to the degree required to make risk management decisions. Therefore, utilities are not appropriately incentivized to invest in cybersecurity to the levels required of national security [1].

4.2.2 Incident Reporting Process

A similar electricity sector effort for cyber response is the process of incident reporting. This process is a realization of the Federal Governments emphasis on information sharing, and how it manifests in the sector reveals much about the dynamic that may emerge during a response to a cyber incident.

Cyber incident reporting is required of electricity market entities that fall under NERC authority. Specifically, NERC CIP 008: Incident Reporting and Response Planning requires that they report specific cyber incidents within specified timeframes [76]. Despite the guidelines, the CIP standards were open for sufficient interpretation, and affected utilities were found more likely to construe the terms of the regulations to delay or completely ignore the requirement to notify government agencies.

Not unexpectedly, utility companies' motivations to postpone notification to the last possible moment was to avoid scrutiny of their response processes, avoid potential fines for non-compliance that the cyberattack exposed, or demonstrate competency to handle the incidents and thereby eliminate any chance of government intervention. In turn, the government agencies lost advantages of reporting timeliness that is essential for developing situational awareness and common operating picture during a widespread cyber event.

In response, FERC and NERC recently updated CIP 008 with revision six that very clearly defines reportable incidents and timelines and removes any room for interpretation [263]. The regulatory adjustment by FERC indicates some of the issues with risk management approaches and underscores the issues of trust between stakeholders in the sector.

For unregulated utilities and many regulated ones, interviews conducted for this thesis demonstrated that they might have the opposite issue and not understand whom to notify, how to notify them, and under what circumstances they should be notified. One of the chief complaints uncovered during REMEDYS research was confusion over whom to call to report an incident. Some utilities stated that there were too many entities with redundant reporting requirements and resources, and others stated that they would not know whom to turn to in the event a cyber incident. Some of this challenge can be traced back to the top-down, Federal Government-centric approach that Federal agencies take. While they are all charged with working together, they each have different reporting requirements, e.g., threat response, asset response, or intelligence support, and provide different resources to the sector. However, at the individual company-level or even the state level, where many of the Federal functions are combined into one entity, the reporting requirements could be overwhelming. The adverse effects of unclear and complicated communications channels on cyber response mechanisms would only be amplified in a widespread cyberattack.

4.2.3 Malware Mitigation Process

Currently, the electricity sector has no single entity responsible for developing malware mitigations. Mitigations steps include identification of exploited vulnerabilities and actions needs to eliminate them as well as the removal of malware from affected systems. For OT and ICS in the electricity sector, mitigations can have impacts on the ability for systems to operate reliability and must often be tested to ensure that there is no loss of performance or reliability. For cyberattacks in the electricity sector, the difficulty in coordinating operational considerations, such as plant downtime or electricity provision, with the need to provide safe and tested mitigations is reflected in delays in steady-state patching of ICS software vulnerabilities. Under non-urgent circumstances, patching can take months to develop and release and still longer to be installed [264], [265].

4.2.4 Electricity Market Entities Response Processes

Electricity market entities have limited roles in sector-wide cyber response mechanisms, but they are essential roles nonetheless. The main contribution to the cyber response of the sector is incident reporting and timely notification, which feeds situational awareness at a higher level and allows regional, state, and national entities to respond. Hence, the importance of timely reporting mentioned in the previous section.

These roles are codified by NERC CIP 008-6: Incident Reporting and Response Planning for federally regulated utilities and by their respective state's incident response plan requirements, if any, for state-regulated utilities [214], [263]. Incident response plan regulations generally require market entities to be able "to identify, classify, and response to cybersecurity incidents" including attempts to compromise electricity system assets, to report the incidents to higher level authorities, to identify roles and responsibilities of cyber incident response personnel, and to outline steps necessary to contain, eradicate, and recover from the incident [263, p. 7]. Notably, the response plans are subject to broad interpretation and do vary based on risk assessments, size, and resources of the market entity, its role within the electricity sector, and the geographic area it covers.

Informally, electricity market entities such as large IOUs, regional and national trade associations, RTOs/ISOs, and joint action agencies also play critical sector-wide roles by extending cyber response programs. These programs bolster the response capabilities of participants and interdependent stakeholders who would not otherwise be able to afford the investments. The natural emergence of support for large electricity market entities may indicate an opportunity to empower them with expanded authority to govern and provide for a cyber response.

4.2.4.1 Cybersecurity Mutual Assistance (CMA) Program

Similar to the informal assistance for larger utility companies, the CMA was built to emulate other electricity industry programs and leverage the culture of mutual assistance which has formed around them. The CMA is a free program wherein participants agree to share cyber resources, such as services, personnel, and equipment, for a short-term in response to a cyber event. It currently includes more than 150 participants across the entire electricity sector [150].

Industry representatives view the CMA as a benefit to the electricity sector and valuable. Where other mutual assistance programs are built around responding to events with geographical borders, the nature of cyberattacks is not constrained to distinct locations. Therefore, many stakeholders maintain that during a widespread event or when threats are imminent, participants will be disinclined to share resources they might need if they are attacked. Additionally, the CMA has never been activated during a widespread cyber event, and its effectiveness remains untested.

4.2.5 State Response Processes

As with state and territorial strategies, the cyber incident response plans vary widely. PUCs and SEOs generally work with state law enforcement agencies, emergency management agencies, and the utilities within state lines to develop their energy assurance and incident response plans. However, as the EO 13800 Section 2(e) Report (2017) noted, state energy assurance plans “do not fully incorporate cybersecurity concerns, including planning for long-term disruption event” [254, Sec. 2(e)].

At the same time, most state cyber incident response plans do not take specifically mention the unique requirements for responding to cyberattacks on the electricity sector or other critical infrastructure sectors [246]. However, they consistently identify lead and supporting agency roles and responsibilities in the state’s response to a cyber incident, address the response protocol, and frequently articulate threat level and response definitions. Most states create ad hoc or permanent organizations for cyber incident response expertise and capability. However, many reports note that despite recognition of the risk of cyberattack and planning efforts, as shown in Figure 4.4, states repeatedly underfund expansion of cybersecurity capabilities [266, p. 45].

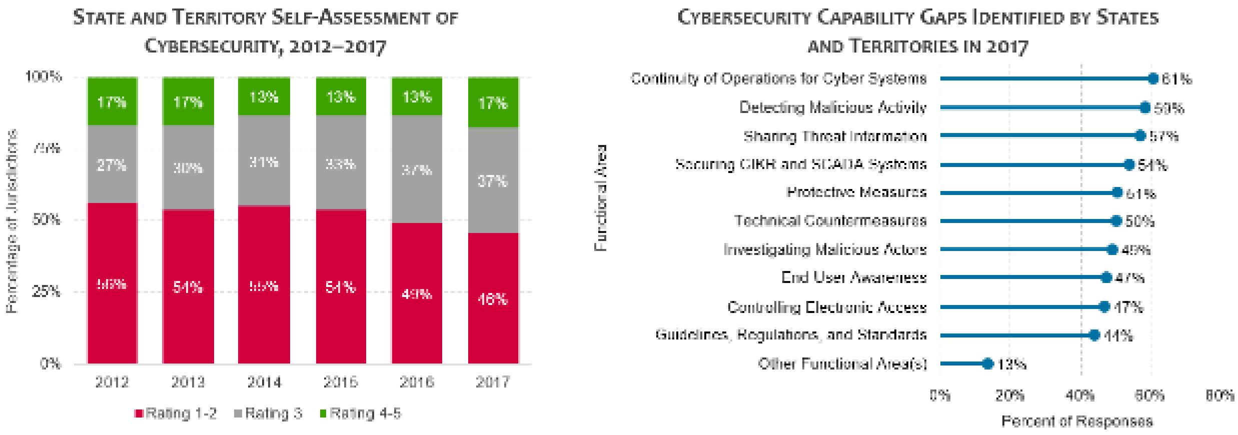


Figure 4.4: State and Territory Cybersecurity Assessment Data from the 2018 National Preparedness Report

Nonetheless, during a large-scale malware attack on the electricity sector, state governments will likely be on the frontline of response efforts. Many have made concerted efforts to partner with their utilities, regional and national organizations, and Federal agencies to understand how to access resources when incidents expand beyond their resources [262]. In that event, the states provide a vital conduit to regional resources and Federal resources by declaring a statewide emergency under the Stafford Act [267].

4.2.5.1 Emergency Management Assistance Compact (EMAC)

Much like the CMA, the EMAC is an agreement between state governments to provide reimbursable mutual assistance during times of state or regional emergencies and when local resources have been exhausted. All 50 states and four territories are members of the EMAC which was developed by NEMA and subsequently ratified by Congress. It is meant to complement Federal Government response functions aligned with FEMA and the National Response Framework. The EMAC construct takes an “all hazards – all disciplines” approach to rendering needed personnel, equipment, commodities, and services during a state emergency of any type [268].

Also, like CMA, the EMAC has never been used to respond to a cyber incident. A review of their mission response package templates, which are formulated for states to determine how to respond and calculate reimbursement costs, and after-action reports, which capture lessons learned after an emergency, indicates a focus on natural disaster response [269]. Typically, the state closest to the affected state is requested to respond, but one of the other tenets of EMAC is that states are not required to send resources to another state if it deems the risk of an incident within its borders is too high. Under the conditions of a cyberattack which lack geographical limits, it may be unlikely that states render assistance to affected states in anticipation of being attacked themselves.

4.2.6 National Response Processes

The Federal Government's cyber incident response processes are exclusively driven by the high-level policy, frameworks, and plans that define the National Preparedness System and cyber incident coordination strategies. From these sources, the Government further documents the support it will provide, the conditions for activating response actions, the roles and responsibilities of stakeholders, and the method for providing it during a cyber incident through five essential plans.

4.2.6.1 Emergency Support Function (ESF) and Support Annexes

The NRF's base document is augmented with two types of annexes that provide greater detail to its vision and mission, ESFs and Support Annexes. In general, ESFs "describe the Federal coordinating structures that group resources and capabilities into functional areas that are most frequently needed in a national response" [190, p. 8]. In other words, ESFs designate Federal Agencies with specific response functions, resources, and required capabilities aligned with their inherent missions, statutory authorities, and the National Planning Framework components. Capabilities required by ESFs can be called upon alone or combined with the capabilities of other ESFs to fulfill an incident response requirement. ESF #12 covers the response functions that would likely be needed to respond to a disruption in electricity delivery caused by a malware attack. Other ESFs may be activated in combination with ESF #12, but it provides the most detail on the Federal Government's response efforts and resources during a cyber incident on the electricity sector [270].

Similarly, Support Annexes describe "essential supporting aspects that are common to all incidents" [270, p. 1]. Where ESFs communicate functions and resources needed for response, Support Annexes describe how Federal agencies, SLTT entities, and the private sector coordinate to execute those functions for specific activities that arise during most national-level incidents. Of the eight Support Annexes, the Critical Infrastructure and Key Resources (CIKR) Support Annex is most relevant to cyber incident response.

<u>Emergency Support Function #12 – Energy Annex</u>

ESF #12 is dedicated to those national response functions that require support from the energy sector to meet the Nation's energy needs in an all-hazards response context. Under the NRF protocol, ESF #12:

> *ESF #12 collects, evaluates, and shares information on energy system damage and estimations on the impact of energy system outages within affected areas. Additionally, it provides information concerning the energy restoration process such as projected schedules, percent completion of restoration, and geographic information on the restoration. ESF #12 facilitates the restoration of energy systems through legal authorities and waivers. ESF #12 also provides technical expertise to the utilities, conducts field assessments, and assists government and private-sector stakeholders to overcome challenges in restoring the energy system [270, p. 35].*

Even though ESF #12 is not specific to cyber incident response, it provides two critical indications of the Federal Governments role in such an event. First, it reiterates the authority that the Federal Power Act grants the Secretary of Energy to direct electricity utilities to alter their operation of the grid that "will best serve the public interest and alleviate the emergency" [271, pp. 12–5]. Second, it empowers the DOE to identify the prioritization of Federal resources during response operations, essentially dictating which utilities receive the means to respond to disruption over other utilities.

Critical Infrastructure and Key Resources (CIKR) Support Annex

The CIKR Support Annex consolidates existing incident response functions, resources, and authorities from other Federal policies and plans into a single reference. More specifically, it provides a clear concept of operations that:

> [*D*]*escribes specific organizational approaches, processes, coordinating structures, and incident-related actions required for the protection and restoration of CIKR assets, systems, networks, or functions within the impacted area and outside the impacted area at the local, regional, and national levels [272, p. CIKR-5]*

The concept of operations concentrates on four functions that are aligned with the NRF, NIPP, and Federal Government's approach to critical infrastructure protection: "situational awareness, impact assessment and analysis, information sharing, and requests for assistance or information from private-sector CIKR owners and operators" [272, p. CIKR-5-6]. Given the emphasis on communicating within those four functions, the CIKR Support Annex is primarily dedicated to describing what and how information flows during a CIKR-related incident.

4.2.6.2 Response Federal Interagency Operational Plan (FIOP)

The Response FIOP builds upon the NRF and its annexes to provide:

> *the concept of operations for integrating and synchronizing existing national-level Federal capabilities to support local, state, tribal, territorial, insular area, and Federal plans and is supported by Federal department-level operational plans, where appropriate [250, p. 1].*

The Plan translates the core capabilities in the NRF into a plan for Federal agencies to deliver them during incident response and helps SLTT and private sector entities to anticipate how the Federal Government will respond to an incident. It focuses on coordination of Federal Government efforts to "save lives, protect property and the environment, and meet basic human need" within 24 to 72 hours of an incident [250, p. 1].

Just like the NRF, the Response FIOP has a base document with functional annexes with the addition of incident-specific annexes that address specific situations that require the specialized application of its strategy and processes.

The base plan places the existing processes for accessing, organizing, and requesting into the context of incident response. More critically, it provides insight into the Federal

Government's response planning assumptions about how incidents will occur, how non-Federal entities will react, and what impacts incidents will have on the Nation. Its functional annexes describe the planning, operational coordination, logistics and supply chain management, and communications aspects of organizing the response, and the appendices within each annex provide the concept of operations and tasks for the NRF core capabilities. Similarly, incident-specific annexes describe the Federal Government's approach for incidents that require specialized approaches to a response.

The Response FIOP's Appendix 5: Infrastructure Systems of Annex C: Operational Coordination is the most relevant functional annex to the electricity sector. The NCIRP serves as the Cyber Incident Annex and outlines specialized core capabilities and critical tasks, among other more strategic approaches, that the Federal Government has deemed necessary to respond to a cyber incident. Additionally, the Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans serves as another incident-specific annex for the electricity sector.

4.2.6.3 Appendix 5: Infrastructure Systems of Annex C: Operational Coordination of the Response Federal Interagency Operational Plan

The Infrastructure Systems Appendix of the Response FIOP is a comprehensive process that breaks the Federal Government's response efforts for both critical and non-critical infrastructure into three phases. Each phase has distinct tasks further divided by ESFs. The Appendix spells out the tasks and functions independently of the type of incident.

4.2.6.4 National Cyber Incident Response Plan (NCIRP) Core Capabilities and Critical Tasks

Much of the guidance found in the NCIRP relates to the Federal Government's strategic approach to handling cyber incident response. However, Annex F: Core Capabilities and Critical Tasks outlines all of "tasks that are essential to achieving the desired outcome of the capability. Critical tasks inform mission objectives, which allow planners to identify resourcing and sourcing requirements prior to an incident" [117, p. 45].

4.2.6.5 Power Outage Incident Annex (POIA) to the Response and Recovery Federal Interagency Operational Plans

The POIA establishes the guidelines for the provision of Federal resources to SLTT entities in the event of a long-term power outage and is organized into phases identical to NCIRP. Unlike the NCIRP, the organizational structures, planning assumptions, required capabilities and tasks, and logistics and supply guidance are independent of the incident type. Nonetheless, the POIA make critical distinctions between the effects of a cyberattack and other natural disasters. Notably, that organizational structures would be governed by PPD-41 and NCIRP and that "[p]hysical damage to electricity infrastructure may not be the primary hindrance to the restoration of power (e.g., power generation capabilities may be impaired due to a cyber incident)" [23, p. 8].

4.2.7 Response Plan Exercises

The final enabling process is the electricity sector’s mechanism for exercising its response plans. In order to validate process and procedures to ensure that incident response plans are valid, it is necessary to test them under conditions that emulate real-world conditions. NIST, cybersecurity vendors, and other research and development institutes provide significant guidance to electricity market entities on how to formulate incident response plan testing, evaluation, and exercise, and also create opportunities to test them [260]. For BPS, NERC CIP 008-6 dictates that federally regulated utilities must test its cybersecurity incident response plan at least once every 15 months [166, p. 468], and some state PUCs have imposed mandatory testing requirements on the utilities that they regulate.

However, only two existing exercises exist which test the electricity sector’s ability to respond to a large-scale malware attack: Grid Security Exercise (GridEx), conducted by E-ISAC, and Liberty Eclipse, hosted by DOE. GridEx is a centrally managed communications exercise that enables BPS members to test their IRPs ability to respond to both cyber and physical threats and incidents [273]. In essence, E-ISAC fulfills its role as a central communications hub during a cyber incident it designs to test the sector’s response. It provides routine scenario injections to evolve the scenario and test different aspects of plans. Participants typically use the opportunity to test and self-audit their IRPs while communicating externally through E-ISAC and other pre-established guidance. Figure 4.5 is a sample communications plan that demonstrates the purpose of GridEx [164, p. 17].

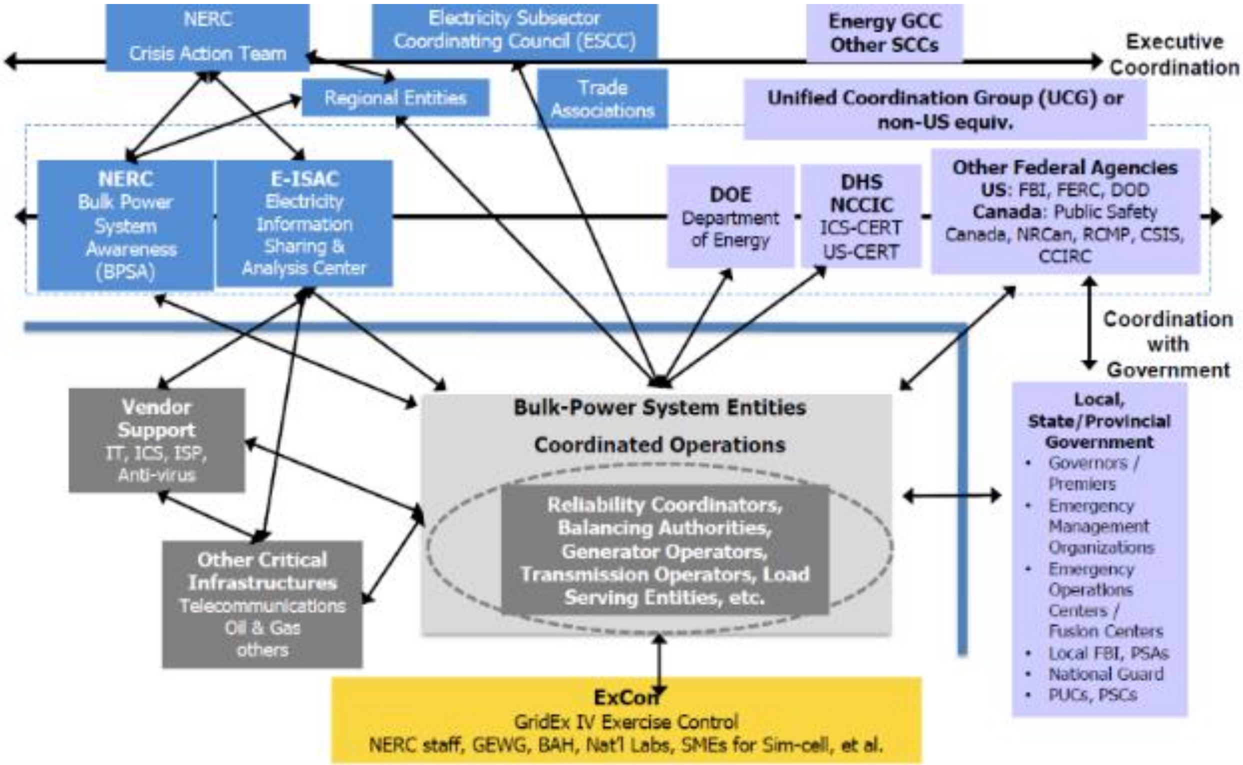

NERC Crisis Action Team
Electricity Subsector Coordinating Council (ESCC)
Energy GCC Other SCCs
Executive Coordination
Regional Entities
Trade Associations
Unified Coordination Group (UCG) or non-US equiv.
NERC Bulk Power System Awareness (BPSA)
E-ISAC Electricity Information Sharing & Analysis Center
DOE Department of Energy
DHS NCCIC ICS-CERT US-CERT
Other Federal Agencies US: FBI, FERC, DOD Canada: Public Safety Canada, NRCan, RCMP, CSIS, CCIRC
Coordination with Government
Vendor Support IT, ICS, ISP, Anti-virus
Bulk-Power System Entities
Coordinated Operations
Reliability Coordinators, Balancing Authorities, Generator Operators, Transmission Operators, Load Serving Entities, etc.
Other Critical Infrastructures Telecommunications Oil & Gas others
Local, State/Provincial Government
• Governors / Premiers
• Emergency Management Organizations
• Emergency Operations Centers / Fusion Centers
• Local FBI, PSAs
• National Guard
• PUCs, PSCs
ExCon
GridEx IV Exercise Control
NERC staff, GEWG, BAH, Nat'l Labs, SMEs for Sim-cell, et al.

Figure 4.5: GridEx IV Communications Plan

Conversely, Liberty Eclipse is an exercise series that rotates its focus iteration, but its purpose is to test the effects of cyberattack scenarios on various components of the electrical grid and analyze the ability to respond and recover. The most recent Liberty Eclipse to test cyber incident response at the sector level was held in 2017. It was conducted as a tabletop exercise of a simulated cyberattack on the electricity grid in the northeastern U.S., and multiple FLSTT entities, energy sector companies, and trade associations participated. While it founded some of the gaps enumerated herein and might even be considered a necessary first step towards exercising response mechanisms, the 2017 exercise did not require more real-time, detailed response actions from participants. At the time this thesis was written, the DOE has no plans to hold a subsequent Liberty Eclipse exercise to stress test the EDS response mechanisms further.

4.2.8 Processes Gap Analysis

While much criticism of the deemphasizing cyber risk management focuses on the implication of "spending unbounded amounts of time and money on [cyber]security measures," preparing for a cyberattack, regardless of threat vector, is always prudent and consistent with the all-hazards model in contemporary emergency management philosophies [88, p. 4], [192]. Because of the dynamic of risk management and the culture of cybersecurity presented in section 4.3.1, resources tend to focus on preventive measures, rather than on mitigations for an inevitable attack. Thus, the current process of risk management does not enable adequate cyber response mechanism investment or development.

Likewise, the current mechanism for reporting cyber incidents does not enable optimal response for a malware attack at scale. The system disincentivizes early and detailed reporting from the private sector and provision of classified, actionable intelligence from the Federal Government. Despite legislation like the National Cybersecurity Protection Act and regulations like NERC CIP 008-6 that requires information and intelligence exchange, communication of remains suboptimal due to cultural and trust issues [256], [263].

Another gap in the electricity sector's response mechanism is the immature malware mitigation development mechanism. Without a robust process to identify, develop, test, and disseminate mitigation, the electricity sector will be unable to respond as quickly as needed and prolong a large-scale malware attack. Given the number of different resources available to electricity market utilities and the complex communications external plan noted in section 4.2.2, malware mitigation efforts would likely be redundant and drastically slow the process of containing and removing it from affected systems.

In the case of the electricity market entities, interdependent security theories suggest that cyber resilience will increase as the number of utility incident response plans and their response capabilities increase. However, the aggregate of these individual incident response plans does not create a sector-wide response mechanism. To wit, there is no requirement for response plans to incorporate differences in response procedures in the event of a large-malware attack. Most of the steps of individual incident response plans would likely remain during such an event, but for utilities that plan to rely on external resources, such as NCCIC HIRT teams or MSSPs, a large-scale event might rapidly drain the capacity of those supporting organizations.

Additionally, both public and private sectors conflate the effects of natural disaster with cyberattacks. Cyberattacks do not have the geographical or temporal boundaries that physical disaster has causes. The public or private sector would be unlikely to share resources under mutual assistance agreements because malware has persistence and nearly unlimited potential to spread that natural disasters do not. While some Federal Government plans recognize the need for specialized treatment of cyber incidents, they still rely on capabilities, tasks, and organizational structures built to handle a natural or human-made disaster. Thus, the majority of cyber incident response processes are formed from overconfidence in current response mechanisms, which are suboptimal even for less dynamic natural disaster responses [266].

The complexity of the National Planning Framework that affects the sector's response strategy also affects its response process. Despite the thorough documentation and clear organization of the response planning guidance, greater transparency is needed in several areas. First, FLSTT response plans deliberately incorporate flexibility and adaptability that is traditionally required for an all-hazards-like approach to a cyber incident. However, the differences between natural disasters and cyber incidents are such that flexibility and adaptability manifest as ambiguity and needless complexity in the response process. Too often in the electricity sector, there is no authoritative standard by which to measure a response process, nor is there a central authority accountable for providing complete incident response. Instead, the sector spreads authorities and responsibilities across the public sector, which is concerned for national security and welfare, and the private sector, which is concerned for business continuity. Unless these interests can be more closely aligned, incident response plans will continue, however subtly, to reflect the divergent interests.

Second, the planning assumptions that inform Federal plans also create gaps in the sector's response mechanism. The Response FIOP assumes that only one catastrophic incident would occur at a time, which is a reasonable assumption given the precedent of natural disasters. However, cyber threat intelligence suggests that not only would a coordinated attack be exponentially more damaging to the nation but also the likely course of action for cyber-aggressors [10], [65].

Third, electricity sector stakeholders routinely criticize the system for the inability to access resources before or during an event. Such criticism is particularly prevalent in the case of the substantial Federal resources that have been created for increasing cyber resilience and cyber response. Despite aggressive Federal agency outreach campaigns, the confusion comes from a combination the passive approach it takes during incident response, i.e., waiting for requests for assistance during an incident, and the dense, redundant, and sometimes conflicting National Planning Framework documents.

Another critical process element gap that arose from stakeholder analysis was the lack of a consolidated, meaningful common operating picture (COP) for the sector during a cyber incident. The complexity of monitoring the performance of a single utility network is technically challenging for its operators under normal conditions. During a widespread cyberattack, no current system provides a way to consolidate multiple system statuses into a single picture.

Despite the need for a consolidated, real-time COP to enhance decision making, no process exists to create one. Many Federal government centers, agencies, and working groups each have the responsibility for assembling a piece of the picture according to the Response FIOP, CIKR Annex, and POIA, but no entity has the responsibility to consolidate [23], [117], [250], [272].

Finally, current cyber incident response exercises for the electricity grid have shown to mature response processes and build awareness of threats to critical infrastructure. However, most exercises only test the aggregate of individual IRPs through a non-real time, tabletop exercise, and do not place sufficient stress on the system to identify where it might not respond. Stakeholder analysis consistently revealed that self-audited IRP exercises failed to simulate an actual cyber event and take into account resource and personnel constraints. When external auditors tested the same response plans and exposed personnel shortages or longer response timeframes than had been assumed, only then did individual organizations understand the deficiencies in their IRP. Further stakeholder analysis and literature review exposed an absence of research on the effectiveness of self-audited response plans and identification and maturity of private sector critical tasks and capabilities.

4.3 Organization

Like the process element, the organization element of the electricity sector's cyber response mechanisms is characterized by significant interconnectivity with the other ARIES view elements. The electricity sector's organization is driven mainly by the response strategy and processes of the sector. The effect of the organization is best understood by examining its element anatomy.

The organizational structure of the sector's response organization is definitively hierarchical and functionally aligned as revealed by the stakeholder classification in section 3.4.2 and implied by the governance in the National Preparedness System [249]. Figure 4.6 provides a simplified model of the organizational structure that exists for incident response in the U.S. electricity sector.

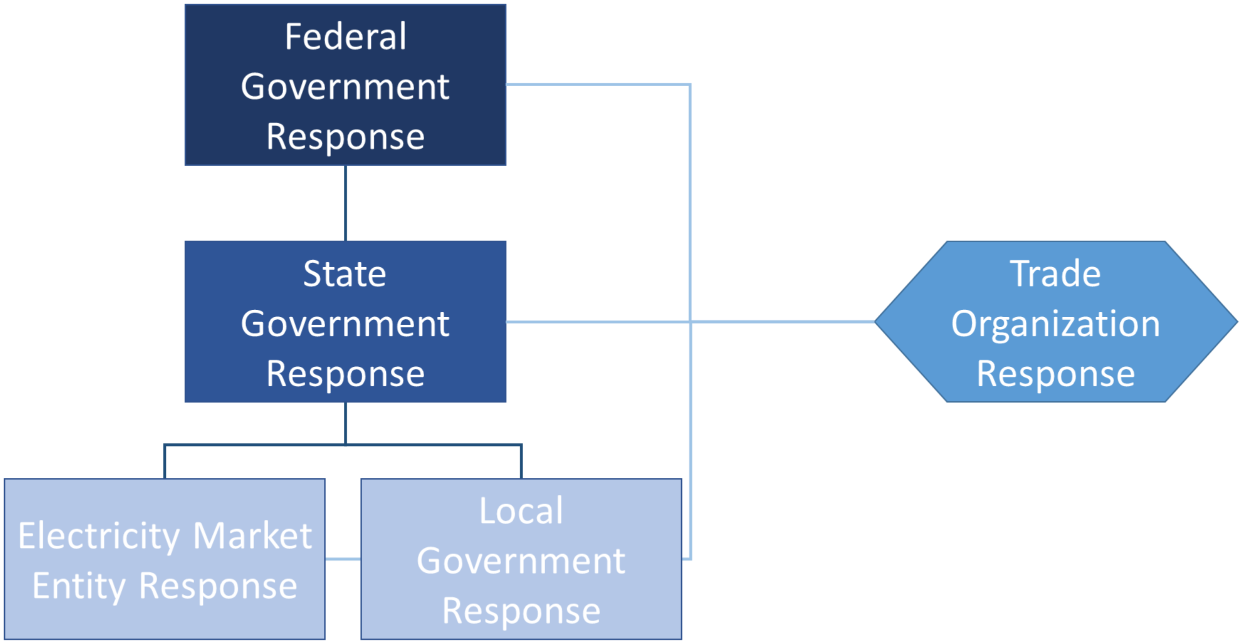

Federal Government Response
State Government Response
Trade Organization Response
Electricity Market Entity Response
Local Government Response

Figure 4.6: Conceptual Organizational Structure of Electricity Sector Response Mechanisms

Conceptually, the electricity market entities make up the lowest tier of the hierarchy. That is, they operate the grid and are closest to the point of execution for cyber incident response. Many utilities cover areas larger than town and city government, so local government response organizations are rare and usually have fewer, if any resources. However, local governments' may be involved in a sector-wide cyber incident response as an extension of the state government and can be categorized at the lowest tier as well.

State response organizations make up the second tier because of their proximity to the sector's operators. Federal response organizations comprise the top tier of the sector's response organization. Trade associations and advocacy groups are woven through all tiers and hold formal and informal roles in the response organizations at all levels.

Electricity market entities and state response organizational effects vary greatly, are too numerous for the scope of this thesis, and are omitted from further analysis. Further supporting the non-inclusion of the electricity market entities and state governments is the dominance of the Federal Government's formal and informal role in the sector's response mechanisms. As the strategy and process reveal, the substantial resources and efficiencies that Federal agencies can bring to bear during an incident incentivize alignment with national policies.

The remainder of this chapter examines the behavior of the organization of the electricity sector cyber incident response mechanisms by assessing the culture of cybersecurity within the sector and the substantial role that trust plays in the health of its cyber response. The structure of the Federal Government is presented in greater detail to understand how it contributes to the sector's response mechanism and the gaps they inherently create in it.

4.3.1 Culture of Cybersecurity

Analysis of the strategy and process elements have demonstrated that the electricity sector has a deeply ingrained culture of cybersecurity that heavily influences its approach to a cyber incident. Therefore, it is necessary to understand the electricity's organizational cybersecurity culture to identify how it reinforces the current cyber response mechanisms, understand how it creates gaps and keeps others closed, and determine what must change to improve the ability for the sector to respond to a large-scale malware attack.

Huang and Pearlson provide an apt definition of organizational cybersecurity culture as a synthesis of organizational culture, national culture, and information security culture models and their analysis [274], [275], [276], [277]. Their definition is given as "the beliefs, values, and attitudes that drive employee behaviors to protect and defend the organization from cyber attacks" [278, p. 1]. Additionally, the authors provide a useful model of organizational cybersecurity culture model to analyze the effects of different influences on the culture. The complete model is shown in Figure 4.7 [278, p. 7].

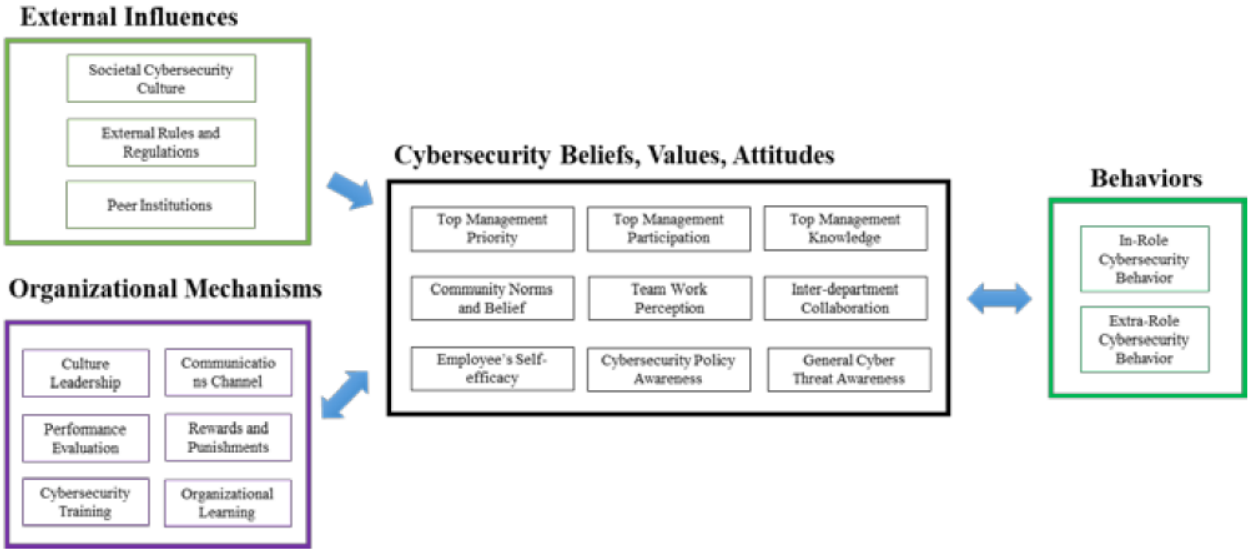
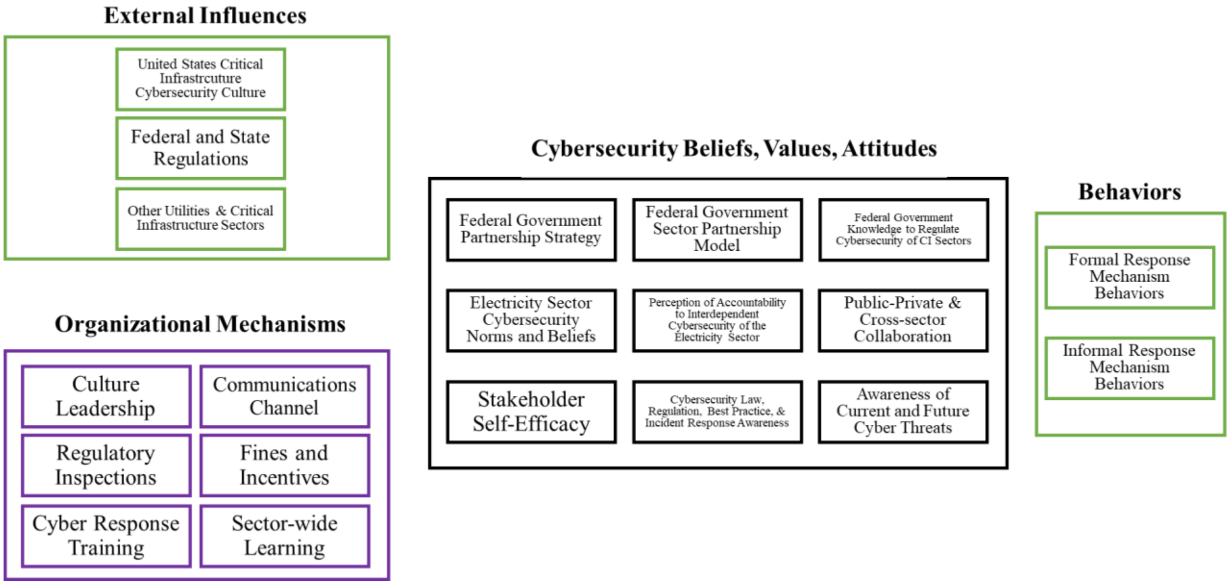

External Influences
Societal Cybersecurity Culture
External Rules and Regulations
Peer Institutions
Organizational Mechanisms
Culture Leadership
Communications Channel
Performance Evaluation
Rewards and Punishments
Cybersecurity Training
Organizational Learning
Cybersecurity Beliefs, Values, Attitudes
Top Management Priority
Top Management Participation
Top Management Knowledge
Community Norms and Belief
Team Work Perception
Inter-department Collaboration
Employee's Self-efficacy
Cybersecurity Policy Awareness
General Cyber Threat Awareness
Behaviors
In-Role Cybersecurity Behavior
Extra-Role Cybersecurity Behavior

Figure 4.7: Huang and Pearlson's Organizational Cybersecurity Culture Model

With minor modifications, both the definition and model can be adapted to describe the electricity sector's cybersecurity culture. In that case, the modified definition becomes: the beliefs, values, and attitudes that drive stakeholders to protect and defend the electricity sector from cyberattacks. The substitution of stakeholder for employee and organization for the electricity sector applies to the model as well. Further, we can interpret "top management" as the Federal Government consistent with previous assertions.

A full application of their model is not necessary to reveal the gaps in the response mechanism but an adaptation of the model, as shown in Figure 4.8, can be used to understand the most relevant points. Most elements of the model would reveal the same gaps that have already been exposed by previous analysis. For example, the "Top Management Priority" would reflect the effects of the Federal Government's emphasis on information sharing and research and development on cybersecurity. "Top Management Participation" would exhibit the influence of the PPP approach and passive response role that Federal agencies use. However, the two elements of the model have not been explored: “Societal Cybersecurity Culture” and “General Cyber Threat Awareness.”



External Influences
United States Critical Infrastrcuture Cybersecurity Culture
Federal and State Regulations
Other Utilities & Critical Infrastructure Sectors
Organizational Mechanisms
Culture Leadership
Communications Channel
Regulatory Inspections
Fines and Incentives
Cyber Response Training
Sector-wide Learning
Cybersecurity Beliefs, Values, Attitudes
Federal Government Partnership Strategy
Federal Government Sector Partnership Model
Federal Government Knowledge to Regulate Cybersecurity of CI Sectors
Electricity Sector Cybersecurity Norms and Beliefs
Perception of Accountability to Interdependent Cybersecurity of the Electricity Sector
Public-Private & Cross-sector Collaboration
Stakeholder Self-Efficacy
Cybersecurity Law, Regulation, Best Practice, & Incident Response Awareness
Awareness of Current and Future Cyber Threats
Behaviors
Formal Response Mechanism Behaviors
Informal Response Mechanism Behaviors

Figure 4.8: Huang and Pearlson’s Organizational Cybersecurity Culture Model Applied to the U.S. Electricity Sector

Huang and Pearslon define Societal Cybersecurity Culture as “the societal norms, beliefs, attitudes and values in which an organization lives” [279, p. 9]. In the case of the U.S. electricity sector, the societal cybersecurity culture can be characterized as closely tied to the dominance of America’s military and economy. The authors define General Cyber Threat Awareness refers to “the [stakeholder’s] knowledge and understanding of threats.” As alluded to in this thesis definition of a cyberattack, each stakeholder has a different perspective on the threats to the electricity sector.

The association between national preeminence and the U.S. electricity sector’s cybersecurity perpetuates the belief that cyber-aggressors would not attack for fear of provoking military retaliation. Despite policy and evidence to the contrary, stakeholder analysis revealed almost unanimous agreement that a large-scale cyberattack on the electricity grid would constitute an act of war. Combined with inconsistent awareness of evolving cyber threats, the cybersecurity culture has become overconfident in a low likelihood of large-scale cyberattack. This paper does not asses a *high* likelihood of an attack, only a *higher* likelihood than is currently presumed.

One important consequence of the electricity sector’s cybersecurity culture is the emphasis on investment in preventive activities rather than response preparedness. The former is typically easier to quantify, and risk management strategies enable an easy justification by comparing mitigated and unmitigated consequences. On top of that, the cybersecurity culture suggests that preventive mitigations are can mitigate risks so that response preparedness becomes seemingly unnecessary.

Compare the U.S. electricity sector's culture with that of Israel. Israel's critical infrastructure protection and cybersecurity strategies are also tightly aligned with their military, but they are also grounded in the belief that it is numerically inferior to and faces a constant existential threat from its neighbors [280]. Thus, its policies reflect a culture that must be continually evolving and have the ability to respond to an inevitable cyberattack on its critical infrastructure. The central government asserts higher authority over the cybersecurity of its networks and critical infrastructure and provides stricter regulations for all functions of cyber resilience [280].

4.3.2 Trust and Cyber Response in the Electricity Sector

Closely related to cybersecurity culture, the dynamics of interorganizational trust is another important organizational component of the electricity's sector response mechanism. Stakeholder analysis revealed numerous challenges with establishing and maintaining trust in the sector, and an analysis of the economic factors influencing the electricity sector in section 2.2.4.1 revealed barriers to trust as a function of information asymmetry. Stakeholders from both sides recognized that issues with trusted relationships were impeding cyber response mechanism performance. Thus, an examination of interorganizational trust within the electricity sector as an organizational element is necessary to understand what gaps exist and how they have been created.

Since the 1980s, interorganizational cooperation and trust have been studied comprehensively for their positive benefits on organizational performance but has recently gained even greater importance as the global commons becomes increasingly interconnected [281], [282], [283]. Relevant to the electricity sector's response mechanism challenges, three primary trust-related factors contribute to a gap in interorganizational trust in the sector.

First, Zaheer et al. (1998) assert that trust is inherently relational and concluded that interpersonal trust between members of organizations is the origin of interorganizational trust rather than "being faceless and monolithic" [284, p. 143]. The authors contend that "individual boundary spanners" were members from organizations who actively fostered trust with members from other organizations [284, p. 143]. Stakeholder analysis suggests that many Federal agencies lack the recognition of the nature of interorganizational trust or capacity to actively foster the trust among the thousands of SLTT and private sector stakeholders in the sector.

Second, Moorman et al. (1993) establish that trust has separate dimensions based on competence, i.e., skills and experience, and on integrity, i.e., motives and character, of the members involved in a relationship [285]. Connelly et al. (2018) compared both aspects and found that, while competence is importance, integrity-based trust significantly increases the performance of both members in the relationship [286]. Stakeholder analysis indicates that there are low levels of trust in the technical ability of the Federal agencies to provide for effective response and integrity of its politically influenced motive. Similar levels of trust in the electricity market entities integrity to meet incident reporting timelines or invest in cybersecurity exist on the government side.

Finally, Inkpen and Currall (2004) state that several interorganizational trust propositions are relevant to the sector. The authors argue that common objectives, clear responsibilities and performance expectations, and learning about other member foster trust and power asymmetries and dependence on formal control mechanisms decrease trust [287]. This paper has already shown that common response objectives, responsibilities, and expectations, if they exist, are at least challenging to discern, and the statutory power imbalance and regulatory requirements of the Federal Government create significant barriers to trust. Therefore, the current response mechanisms do not enable trusted relationships to form easily at any level in the electricity sector, and cybersecurity and response preparedness suffers

4.3.3 Federal Response Organization

An in-depth discussion of the Federal incident and emergency response agencies would only serve to reiterate the complexity of national response mechanisms in an organizational context and present no unique issues. For example, Figure 4.9 shows a simplified yet still complex representation of the coordinating mechanisms between the incident response and power restoration functions [23, p. 25]. During a malware attack, cyber response groups and operational centers would also be activated as well. All of these entities bring to bear significant resources and response capabilities, but as current history has shown, the management of resources and ability to respond to the needs of affected areas struggles because of the complex organizational structure [266]. However, three organizational structures, the functions they serve to perform, and their membership create unique gaps in the electricity sector's ability to coordinate a response to a cyberattack as outline below.

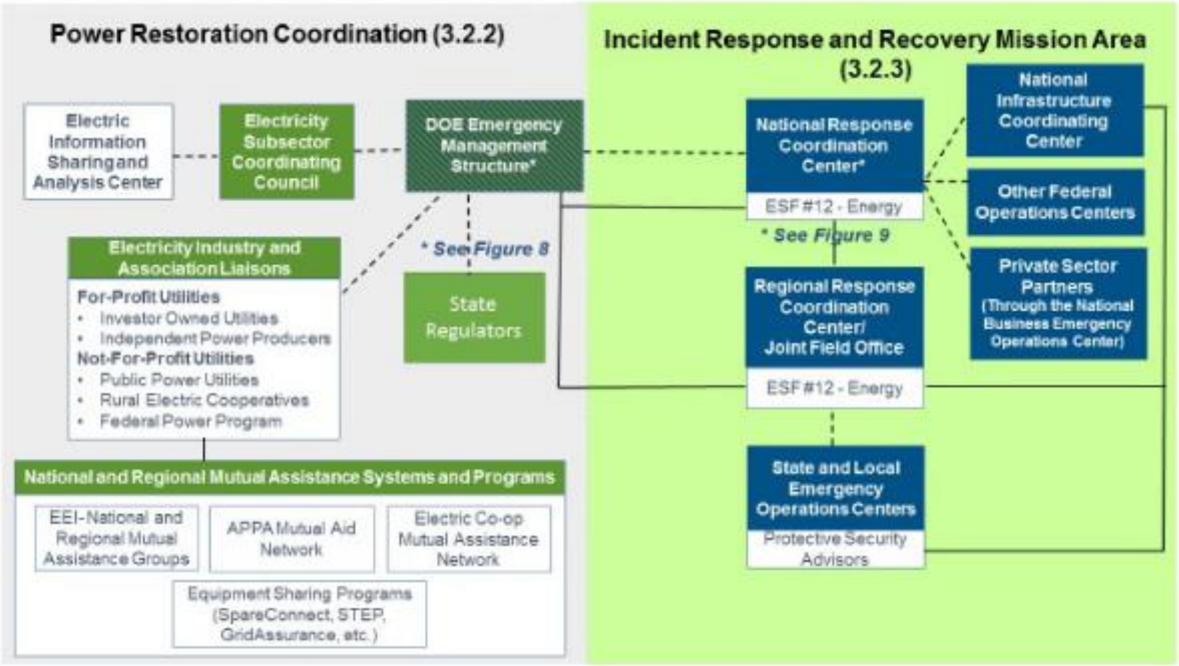

Power Restoration Coordination (3.2.2)
Incident Response and Recovery Mission Area (3.2.3)
Electric Information Sharing and Analysis Center
Electricity Subsector Coordinating Council
DOE Emergency Management Structure*
National Response Coordination Center*
ESF #12 - Energy
National Infrastructure Coordinating Center
Other Federal Operations Centers
Private Sector Partners (Through the National Business Emergency Operations Center)
* See Figure 8
* See Figure 9
State Regulators
Electricity Industry and Association Liaisons
For-Profit Utilities
Investor Owned Utilities
Independent Power Producers
Not-For-Profit Utilities
Public Power Utilities
Rural Electric Cooperatives
Federal Power Program
Regional Response Coordination Center/ Joint Field Office
ESF #12 - Energy
State and Local Emergency Operations Centers
Protective Security Advisors
National and Regional Mutual Assistance Systems and Programs
EEI-National and Regional Mutual Assistance Groups
APPA Mutual Aid Network
Electric Co-op Mutual Assistance Network
Equipment Sharing Programs (SpareConnect, STEP, GridAssurance, etc.)

Figure 4.9: Unified Coordination Between Power Restoration and Incident Response and Recovery Mission Area

4.3.3.1 Critical Infrastructure Sector Partnership Organizations

The Critical Infrastructure Sector Partnership Model was created by the NIPP to encourage collaboration on CIKR issues between Federal, SLTT, and private sector stakeholders. The concept of the organization, shown in Figure 4.10, is comprehensive and provides the legal framework and coordination mechanisms for the stakeholders to collaborate on mutual issues, including incident preparedness and response [192], [288, p. 2].

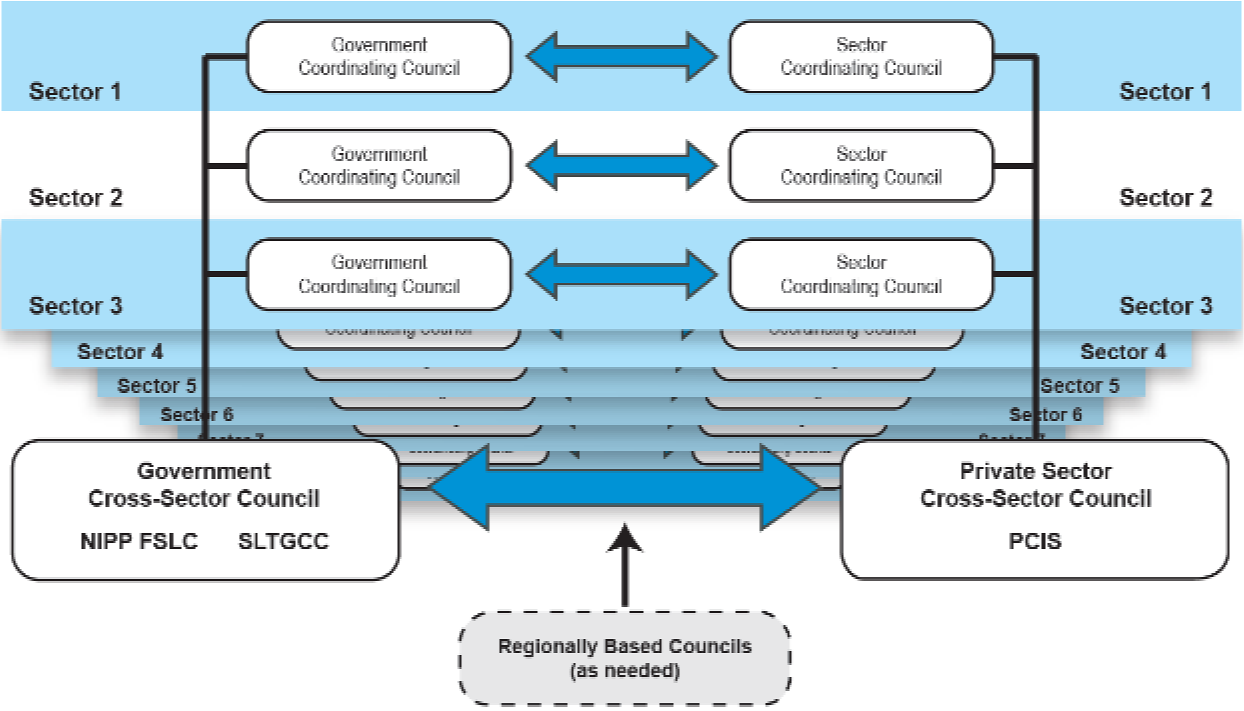

Sector 1
Government Coordinating Council
Sector Coordinating Council
Sector 1
Sector 2
Government Coordinating Council
Sector Coordinating Council
Sector 2
Sector 3
Government Coordinating Council
Sector Coordinating Council
Sector 3
Sector 4
Sector 4
Sector 5
Sector 5
Sector 6
Sector 6
Government Cross-Sector Council
NIPP FSLC
SLTGCC
Private Sector Cross-Sector Council
PCIS
Regionally Based Councils (as needed)

Figure 4.10: Sector Partnership Model

In the electricity sector, the Sector Partnership Model empowers the ESCC to represent multiple stakeholders throughout the sector, as shown in Figure 4.11, and comprises three co-chairs, a nine-member steering committee, and 19 other representatives of electricity market entities [217, p. 3]. The ESCC is the primary mechanism that the Federal Government receives input from the electricity sector and how the private sector advocates for Federal Government policy. During a response to an incident in the sector, the ESCC serves as “the mechanism for executive coordination and communication between the electric power industry and government” yet it lacks authority to direct response actions in the sector [23, pp. 26–27].

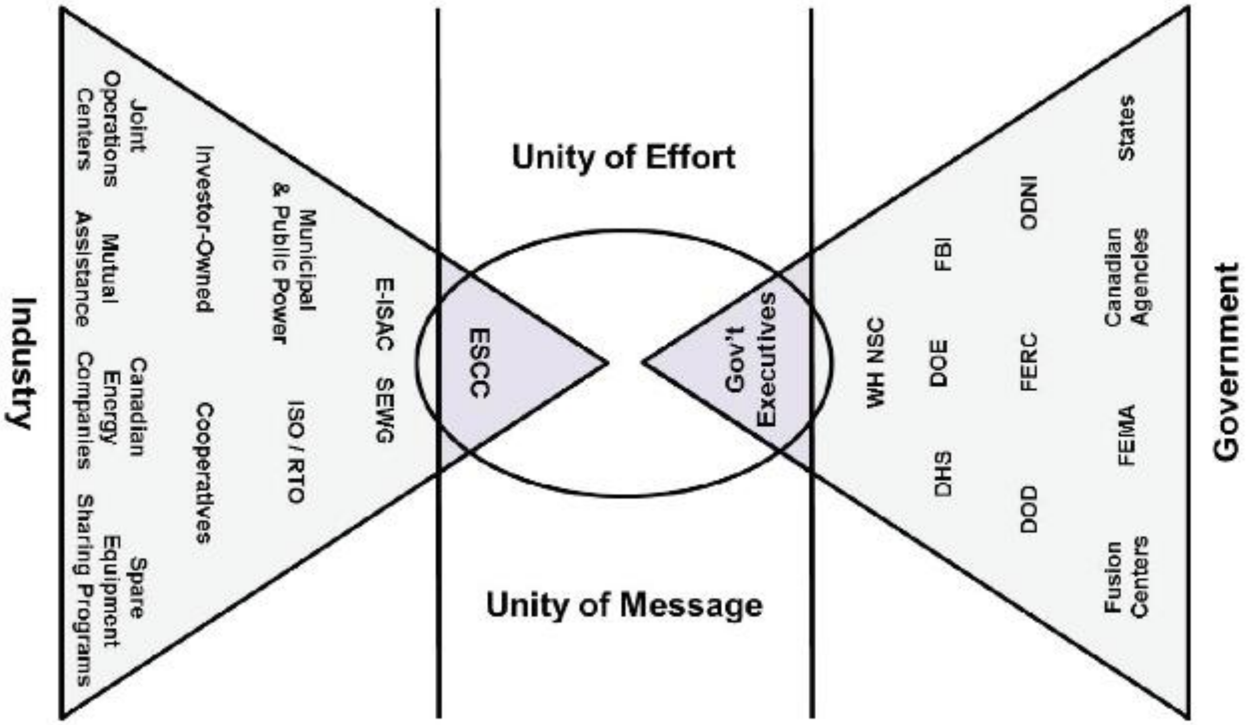


Figure 4.11: Sector Partnership Model in the Electricity Subsector

4.3.3.2 Cyber Unified Coordination Group (UCG)

PPD-41 created the Cyber UCG in the event of a significant cyber incident to coordinate across Federal agencies and externally to SLTT and private sector entities. Per the PPD, a Cyber UCG:

> *serves as the primary national operational coordination mechanism between and among federal agencies responsible for identifying and developing operational response plans and activities during a significant cyber incident, as well as for integrating private sector partners and the SLTT communities into incident response efforts, as appropriate [117, p. 31]*

When a Cyber UCG is established, PPD-41's three concurrent lines of effort are assigned to Federal agencies. The DOJ through the FBI and NCJITF act as threat response. DHS takes on asset response through the NCCIC, and the Office of the Director of National Intelligence (ODNI) takes on intelligence support through the Cyber Threat Intelligence Integration Center (CTIIC). The Cyber UCG also has other intelligence agency operations centers at its disposal to support coordination, communication, and situational awareness.

4.3.3.3 ISACs and ISAOs

ISACs and ISAOs remain the centerpieces of the Federal priorities for critical infrastructure protection. Further, the benefits of information sharing and the framework for establishing productive information sharing environments in the cybersecurity domain has been well documented [96], [97], [121], [289], [290], [291]. Many ISAOs and ISACs have been established to, and been successful in, facilitating knowledge exchange. They represent the primary collaborative organizations in critical infrastructure sectors with the intent to share threat indicators, vulnerabilities, and lessons learned from cyber incidents throughout their respective sectors [95], [292].

O'Halloran (2017) and stakeholder interviews conducted as part of this thesis suggested that participation in these ISACs and ISAOs may breed the misperception that they are capable of coordinating a timely and effective response to a malware attack [103]. The confusion may be natural as the charter of many ISACs is to aid in the coordination of response efforts. ISACs act as forums to develop and vet critical requirements such as emergency response plans, playbooks, and communications plans. However, a survey of ISAC-related literature revealed a general lack of fully developed capability for incident response in these organizations. Nonetheless, analysis of cyberattack response mechanisms assumed that ISACs would act as the coordinating authority for the response [293].

Indeed, the Electricity Information Sharing and Analysis Center (E-ISAC), an entity under NERC, "coordinates incident management" and provides services for "malware analysis and indicator extraction" which at first appear to provide a venue for coordinating malware response [108]. While E-ISAC retains those incident coordination and malware analysis mechanisms and could deploy them on a limited basis, it more explicitly uses them to act as an information sharing platform that facilitates communications between stakeholders. A recent NERC cybersecurity exercise, GridEx III, revealed capability gaps in this response mechanism involving overwhelmed communications systems, difficulty integrating recovery resources between the public and private sector, and the challenge of prioritizing where to focus recovery efforts [171].

Similarly, polls ISAO participants reveal that the multitude of information sharing organizations, including government entities, can obscure the communications process, slow down response times, and obfuscate the cyber threat [103], [126], [290]. Energy sector ISAO participants and stakeholders have reported that the lack of standardized reporting procedures makes it difficult to obtain relevant threat and mitigation data. These same stakeholders also noted that ISAOs often complicated the process of accessing cyber incident response resources by adding another entity between the utility and response resource provider.

Further, ISACs have mostly be organized around a specific sector and cannot address the cross-sector dependencies stated above. To that point, the Under Secretary of Homeland Security for National Protection and Programs Directorate, Christopher Krebs, recently stated that:

> *Those [ISACs} focus on information sharing—in some cases on a sector-specific basis. ¬ The ability to go across sectors, go across agencies to understand true national risk, set priorities together, plan jointly, train, and exercise alongside each other was lacking* [4, p. 38].

ISAC participation is not comprehensive, either. The E-ISAC, for instance, does not include over 3,000 unregulated utilities. The lack of participation from all utilities challenges any malware attack responders, which necessarily must have industry-wide reach [126].

4.3.4 Organization Gap Analysis

While the U.S. and its electricity sector do not face the existential challenges of Israel, the sector does face a more significant threat from cyberattack than its culture will allow it to acknowledge. For those entities that do acknowledge the higher likelihood of a large-scale cyberattack, they are faced with governmental response mechanisms that direct its attention towards preventive measures. Further, the influence of cybersecurity culture focuses on traditional all-hazards approaches for cyber incidents and do not make planning and resource assumptions on the nature of the cyber threat. In order to increase cyber resilience in the electricity sector, its culture must change to openly recognize that a large-scale cyberattack is inevitable – though not necessarily catastrophic or an act of war – and rebalance investments across all cyber resilience functions.

For a culture of cybersecurity to exist in the energy sector, interorganizational trust must also exist. The current organizational structure does not foster the development of trust been boundary spanning members as noted above, particularly between the public and private sectors. Additionally, SLTT and private sector entities limited access to heavily centralized Federal Government response resources creates a high barrier to developing and maintaining trusted relationships. While it is relatively easy to deploy those resources during an incident, it is far more difficult to spread awareness, develop technical knowledge, or create trusted relationships that are needed in crises.

Analysis has also shown the limitations of the Sector Partnership Model. The ESCC's benefits for enhancing the cyber resilience of the electricity sector is indisputable. However, its lack of objectivity inhibits the adoption of better response mechanisms. The Council is inherently interested in protecting its members from government policies that have an adverse impact on their performance. Since electricity market entities are only inclined to invest when risk management frameworks suggest its prudent, they are not incentivized to advocate for or adopt better cyber response mechanism. In turn, the Federal Government relies almost exclusively on the ESCC for cyber resilience policy and are unlikely to think outside of the proverbial box.

Despite the situational awareness and resources that the UCG can obtain, cyber incident response exercises have repeatedly revealed issues with the concept. Primarily, after action reports spanning exercises from multiple years demonstrate a lack of understanding of the UCG by the private sector, and the UCG lacks authority to make an appropriate decision given its awareness and resources [294], [295].

ISACs have helped sectors recognize the importance of sharing information to mitigate cyberattack and working with other stakeholders to coordinate a response. As sectors' realization of ISACs as valuable tools has grown, so has its recognition that increased collaboration between private and public sectors [4], [171], [125]. Thus, cybersecurity coordination previously driven by ISACs has evolved and now requires a dedicated organization to bring together stakeholders from all sectors, coordinate public and private entities, and form a timely response to threats.

4.4 Information

The information element of the electricity sector's cyber response mechanism captures many of the current stakeholder priorities for cyber incident response. Because information is so profoundly entangled throughout the ecosystem, this thesis has already covered many gaps that would have otherwise fallen into the information element category. Specifically, the gaps stemming from issues timeliness of incident reporting; volume and quality of threat notifications; and frameworks, guidelines, and standards have been discussed as functions of economics, strategy, and organization. The gaps arising evolving grid architecture, control systems, and convergence of IT and OT were discussed as functions of technology. Classification of incidents, deployment of response resources, and formation of a common operating picture, have created gaps as well and were discussed as functions of strategy and process. However, the lack of industry-standard resiliency metrics is a critical gap in the sector's response mechanism. The remainder of this section highlights the need for standardized cyber response metrics and the barriers to adopting sector-wide metrics.

4.4.1 Cyber Response Metrics

The 2015 ESSP and 2017 EO13800 Electricity Subsector report both noted a critical lack of cybersecurity metrics to "help support making risk-informed decisions, enabling prioritization of issues, and aligning resources to address them" [32, p. 31]. James et al. (2019) provide a full analysis of current resilience metrics for the electricity sector [214]. The authors draw several conclusions that expose the underdeveloped state of metrics and critical gaps they create. First, they assert that, despite broad recognition of a need for cyber resilience metrics and many available options, there is no consensus on which metrics are essential to effectively measuring cybersecurity. Second, they emphasize the need for cyber resilience-specific metrics as distinguished from the reliability metrics because of fundamental differences in risk calculations. Moreover, they contend that metrics need to be created for each of the four resiliency phases used by NERC, i.e., robustness, resourcefulness, recovery, and adaptability, and that each phase has different complexity from the others [214]. While the authors do not extrapolate their assertions to a sector-wide scale, the absence of any public or private sector metrics for measuring the electricity sector's cyber resilience is a significant gap.

4.4.2 Information Gap Analysis

The emphasis that the current electricity cyber response mechanism places on preventive measures over response preparedness has already been discussed in the context of political and regulatory factors and its elements of process and organization. However, the inability to quantify cyber response investments and evaluate them as a risk and business decision has contributed to asymmetrical investment in preventive measures. Further, federally sponsored research has focused on the development of organizational-level metrics but omitted any for sector-wide or national-level cyber resilience metrics [214].

4.5 Products and Services

Products and services, like those described in section 2.2.5.6, play a relatively small but essential role in the electricity sector's response mechanism. In essence, cybersecurity products and services provide technological solutions to the cyber resilience issues that the sector encounters. There are three categories of cybersecurity products and services relevant to sector response mechanisms:

- Cybersecurity products, such as firewalls, network monitoring, and antivirus tool
- Cybersecurity vendors and services, such as threat analysts, network monitoring, incident response, and forensic services
- Cybersecurity insurance which protects businesses from losses caused by cyberattacks

The structure, or types, of these products and services, are primarily driven by the strategy and information elements of the sector. Both elements emphasize private market participation in the industry's cybersecurity and establish frameworks, guidelines, and standards that dictate requirements for cybersecurity products. Additionally, the information and organizational elements, i.e., the expertise and its location within the sector, create product and service demand, such as network monitoring and incident response services.

4.5.1 Cyber Insurance

Cyber Insurance has been come to the forefront as one of the leading cybersecurity mechanisms for all sectors and can improve all cyber resilience functions by reducing liability and incentivizing investment. Cyber insurers would drive improvements in all areas of the electricity sector's cybersecurity – prevention, response, and recovery – in order to mitigate the likelihood and costs of any claims. For example, insurers would lower rates for utilities that had network monitoring and in-house employees trained to diagnose and respond to malware threats.

DHS, through CISA, has pursued cyber insurance development and outreach to critical infrastructure sector stakeholders to improve robust insurance mechanisms and facilitate a clear understanding of what services are offered [296]. Specific priorities for CISA to engage with the insurance market include, building better incident information sharing and data repository, incident consequence analysis, and enterprise risk management capabilities [297], [298].

4.5.2 Products and Services Gap Analysis

The behavior of the products and services in the industry can be naturally characterized as competitive. Cybersecurity manufacturers, ICS vendors, and insurers compete with one another to attract business within the electricity sector. For utilities, in particular, this creates many of the information asymmetries mentioned in section 2.2.4.1 and is compounded by the lack of metrics for the quality and effectiveness of the products and services. The ambiguity created by the information asymmetry obscures the sector's ability to identify the gaps in sector-wide response mechanisms.

On the other hand, insurance has tremendous potential to improve cyber response mechanisms in the electricity sector. However, CISA's implies that preventative measures should be the primary driver for reducing insurance premiums. Such a conjecture is reflective of the culture of cybersecurity in the U.S. electricity sector and the Federal Government's strategic approach to cybersecurity, but it again neglects the importance of cyber response capabilities. With CISA as one of the main drivers in developing the market, the cyber insurance market may disproportionately focus on prevention compared to response and recovery, and cyber insurance may not realize its full potential as an instrument to collectively increase electricity sector cyber resilience.

4.6 Chapter 4 Summary

Application of the ARIES Framework view elements reveals several gaps in the electricity sector's cyber response mechanisms. Dense, inconsistent, and suboptimally integrated response strategies appear at the private sector, SLTT, and Federal levels of the cyber response mechanism. Response processes and organization reflect issues created by the sector's strategy are reinforced by its cybersecurity culture, low levels of trust, and lack of a mechanism to test or measure the effectiveness sector-wide response. As a result of the existing response mechanisms, few electricity sector stakeholders are in a position to recognize the gaps that exist and doubtless will struggle to close them.

5 Conclusion

This thesis analyzes the current state of the U.S. electricity sector's response mechanism to a large-scale malware attack. Using the ARIES Framework to perform a comprehensive analysis of the sector's landscape, stakeholders, and attributes of the response mechanisms, multiple gaps, and areas for improvement were identified. Table 5-1 shows a summary of the gaps in the electricity sector's response mechanism discussed in this thesis.

Table 5-1: Summary of Gaps in the Electricity Sector Cyber Incident Response Mechanism

ARIES View Element	Gap in Electricity Sector Cyber Incident Response Mechanism
Strategy, Organization	Lack of a culture of cybersecurity that embraces current and future cyber vulnerabilities and threats and emphasizes adequate preparation
Strategy, Information	Lack of objective measure of preparedness and response capability
Strategy	Lack of singular, authoritative guidance on cyber incident response requirements for electricity market entities
Strategy	Lack of clear and consistent cyber incident response roles and responsibilities for the utilities, Federal, state, tribal, and territorial entities
Strategy	Lack of clear Federal definition of significant cyber incident and point at which the Federal Government will intervene on private sector response to a cyber incident under the Federal Power Act, et al.
Strategy, Process	Lack of cyber incident response-specific plans for government entities with clear integration of private sector entities
Strategy, Process	Lack of large-scale cyber incident response-specific plans for government and private entities
Strategy	Lack of incentives and resources for businesses to invest in cyber response measures commensurate with known risks and threats
Strategy	Conflict between threat response and asset response priorities for Federal Government
Strategy, Organization	Lack of objective feedback mechanism that has resources and knowledge of the electricity sector and cybersecurity to advise to provide policy guidance in the Nation's best interest
Process	Institutionalized overinvestment in and overemphasis on preventive measures, rather than response measures
Process	Strong disincentives for participating in information sharing programs, i.e. ISAOs
Process	Immature malware mitigation development, testing, implementation, and dissemination apparatus
Process	Lack of understanding and response mechanisms for cyber incidents' secondary and third order effects on public welfare and the economy
Process	Difficulty in incident reporting and accessing incident response resources
Process	Lack of an accessible, consolidated common operating picture of the electricity grid in the event of a cyber incident
Process	Lack of exercises that "stress test" electricity sector response plans to evaluate adequacy and identify gaps
Organization	Lack of trust between sector stakeholders, particularly between public and private sectors
Organization	Increased need for collaborative forums beyond ISAOs
Products & Services	Lack of cyber insurance market mechanism that encourages investment in cyber response measures

Chief among these gaps, and perhaps the systemic cause of the rest, is the sector's culture of cybersecurity. The culture of cybersecurity leads public and private sectors to believe that the electricity sector is unlikely to suffer a malware attack and, therefore, should invest little to prepare for one. This thesis demonstrated that current and future cyber threats are not well-understood in the sector and many structural and cultural reasons that electricity market entities are not appropriately incentivized to invest appropriately.

The ramifications of the culture are reinforced by the Federal Government's long-standing PPP approach to critical infrastructure protection and its existing, all-hazards approach to incident response. The Federal Government's centrality to large-scale incident response in the U.S. drives cyber incident response investments and preparations at lower levels of government and in the private sector. Although other stakeholder groups had significant influence, the Federal Government was shown to be the only entity with authority to change the current cyber incident response at the sector-level. However, it may lack the technical capability, objectivity, or motivation to make the necessary and challenging changes required to improve cyber resilience in the electricity sector.

5.1 Next Steps

In order to validate this research, REMAED researchers will develop a case study built around discovered gaps. The case study is intended to be delivered to a representative cross-section of the electricity sector stakeholders, to highlight the discovered gaps, expose any unidentified gaps, and build consensus among stakeholders on how to close the gaps. The REMAED team anticipates that the process of identifying the gaps, validating, and building consensus on them will be iterative, but ultimately, it intends to lay the foundation to determine and implement mechanisms that will increase the ability for the entire energy delivery sector to respond to a large-scale malware attack.

5.2 Future Work

In addition to refining the gap analysis presented herein, the findings in this thesis were intended to support the broader goal of strengthening response mechanisms in the energy delivery critical infrastructure. This thesis revealed potential areas for improvement that applied strictly to the electricity subsector. However, further research should include the oil and natural gas sector due to their strong interdependencies.

Simultaneously, the stakeholder interviews captured only a small portion of perspectives from the electricity sector. Future efforts should be dedicated to performing more interviews with the same types of stakeholders and in different geographical areas. Mainly, interviews should target state and Federal Government entities, especially DHS, PUCs, SEOs, research and development institutions, and POUs which were not adequately represented in this study.

Through these interviews, perspectives on cybersecurity culture, interorganizational trust, and the effects of technological and cyber threat evolution should be obtained. While this thesis used past research to understand the influence of factors on the electricity sector's response mechanisms, stakeholder interviews reveal perceptions that must be overcome to move the electricity sector towards consensus.

5.3 Call to Action

The objective of this work was to do a deep analysis of the energy delivery subsector with an eye towards finding ways to mitigate malware in the energy delivery subsector. The key findings of this work suggest that the U.S. energy sector is under-prepared for a large-scale malware attack. Many gaps exist in the ability for the country to respond to such an attack, and we are now at a point that a major transformation of response mechanisms is necessary to achieve protection of our critical infrastructure.

However, it is highly unlikely that we will be able to identify, create, implement, and sustain such a paradigm shift without first adjusting the culture of cybersecurity in the electricity sector. As a country, we don't want our energy executives and government to be caught unprepared when the welfare of our people and stability of our economy are on the line, nor do we want to count on cybersecurity vendors or mutual assistance agreements when they will likely not be available. In many ways, we are lucky that our country has not experienced a cyberattack that resulted in widespread damage, injury, and economic loss. But some say it's just a matter of time before this is reality. This thesis lays the foundation for building the unity of action in the energy delivery sector that is necessary to rethink our approach to cyber incident response, identify gaps, and work together to continually adapt response mechanisms to maintain cybersecurity of the Nation's critical infrastructure.

Appendix A. Value Streams for Various Markets

All figures are taken from [13].

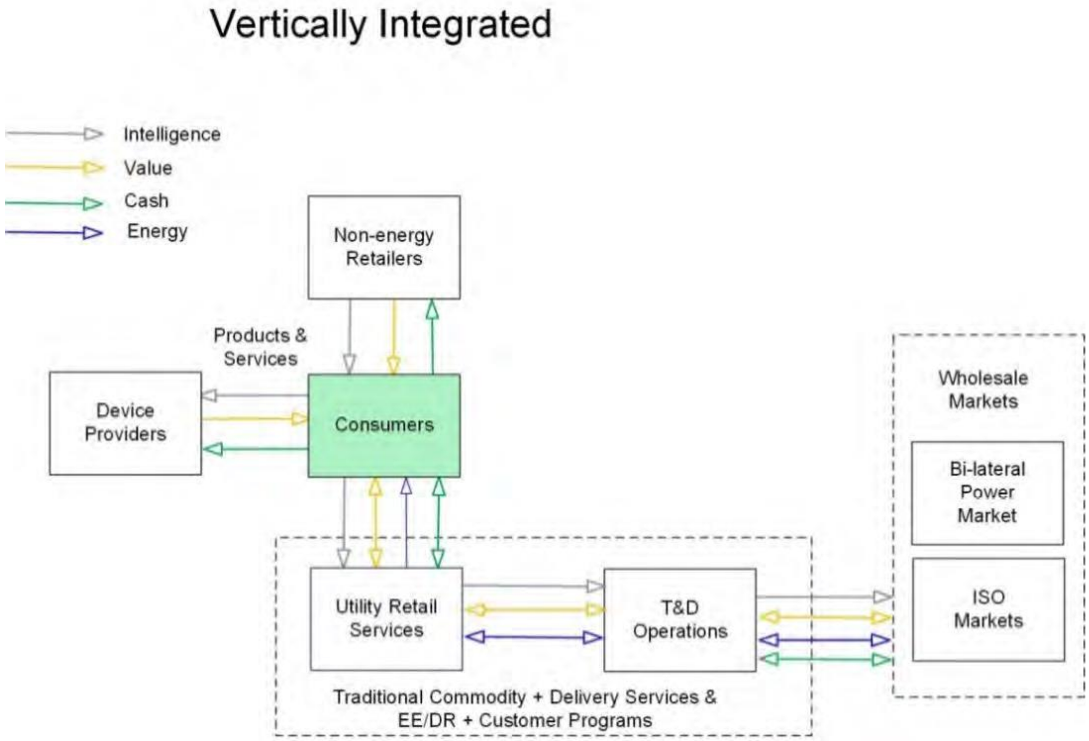


Figure 5.1: Vertical Integration Value Stream Structure

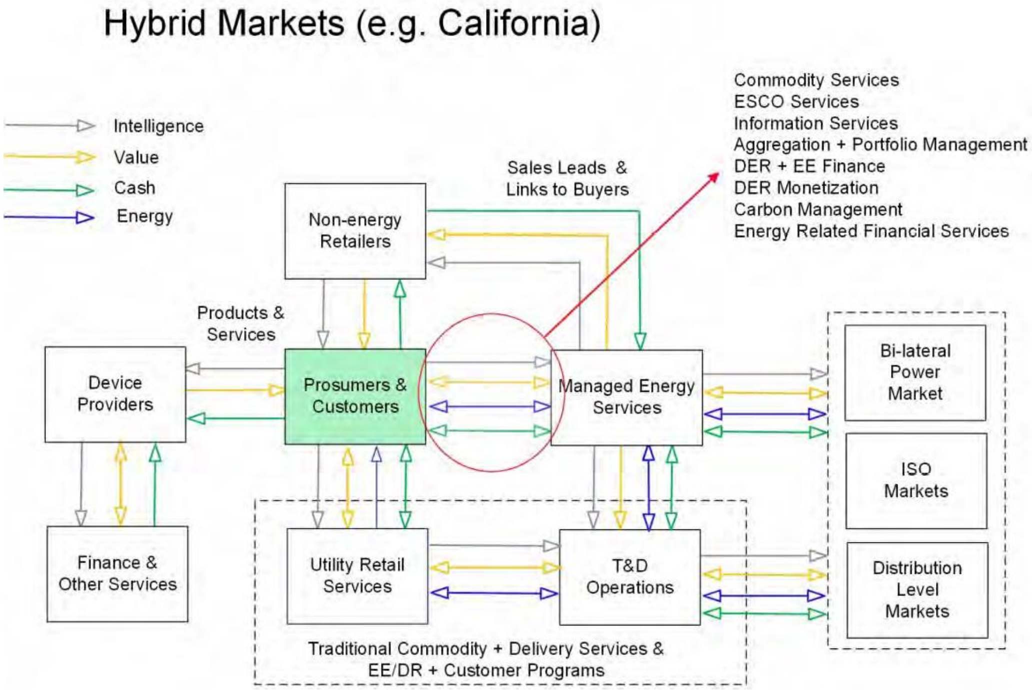


Figure 5.2: Hybrid Markets Value Stream Structure

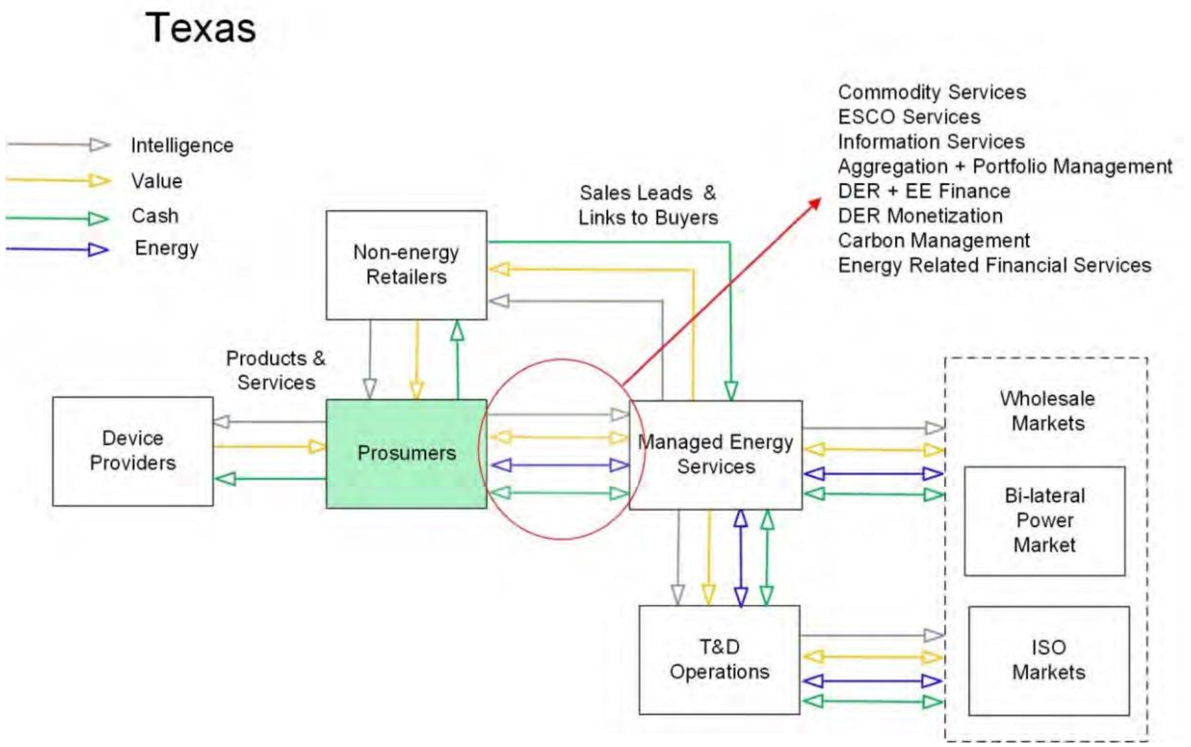


Figure 5.3: Texas Value Stream Structure

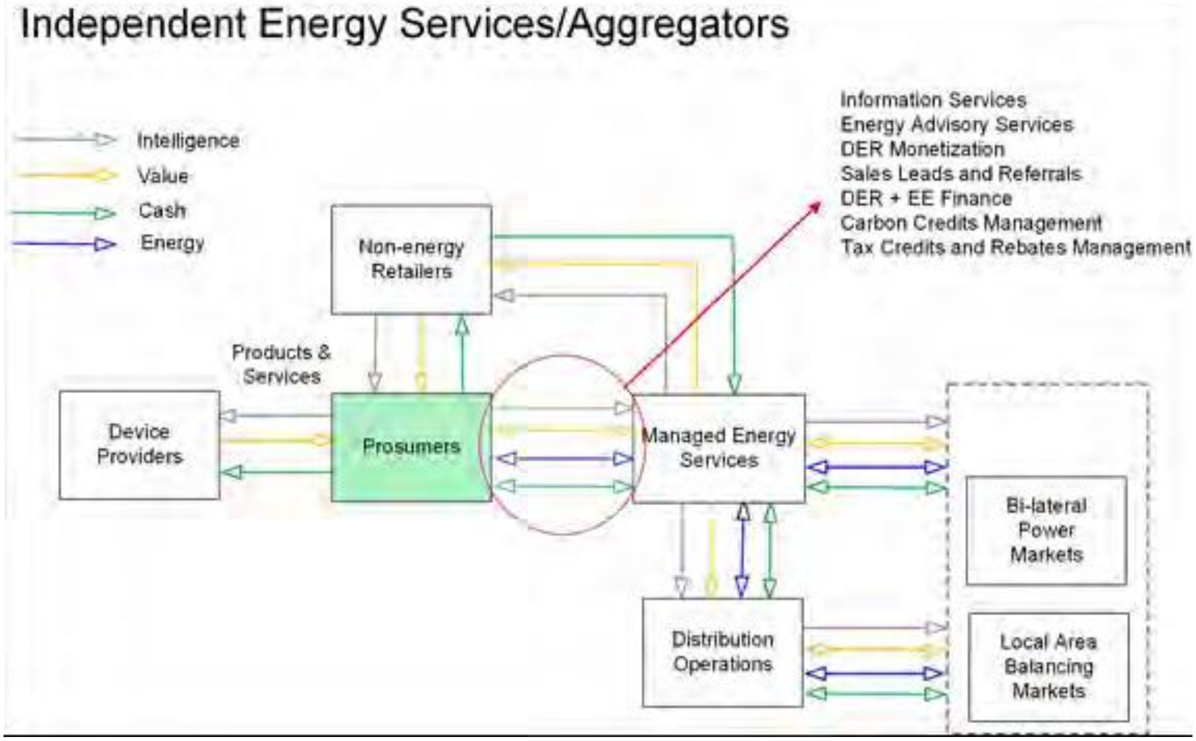


Figure 5.4: Energy Services/Aggregator Value Stream Structure[13]

Appendix B. Stakeholder Classification

Electricity Market Entities	Federal Government Critical Infrastructure Advisory Bodies & Support Agencies	Trade Associations & Advocacy Groups	Information Sharing Entities
Investor-Owned Utilities	National Infrastructure Advisory Council (NIAC)	Electricity Subsector Coordinating Council (ESCC)	Electricity Information Sharing and Analysis Center (E-ISAC)
Consumer-Owned Utilities	Department of Homeland Security (DHS)	Critical Infrastructure Cross-Sector Council	Multi-State Information Sharing and Analysis Center (MS-ISAC)
Cooperative Utilities	Cybersecurity and Infrastructure Security Agency (CISA)	National Association of Regulatory Utility Commissioners (NARUC)	Information Sharing and Analysis Organizations (ISAOs)
Regional Transmission Operators Independent Systems Operators	National Cybersecurity and Communications Integration Center (NCCIC)	National Rural Electric Cooperative Association (NRECA)	InfraGard
Joint Action Agencies	NCCIC Hunt and Incident Response Teams (HIRT)	Touchstone Energy Cooperative	State Fusion Centers
Balancing Authorities	National Infrastructure Coordination Center (NICC)	American Public Power Association (APPA)	
Regional Entities	National Operations Center (NOC)	Edison Electric Institute (EEI)	
Power marketers	National Risk Management Center (NRMC)	Cybersecurity Mutual Assistance (CMA) Program	
Reliability Coordinators	Federal Emergency Management Agency (FEMA)	State and Regional Public Power Associations	
Consumers	Department of Energy (DOE)	Large Public Power Council (LPPC)	
	Office of Cybersecurity, Energy Security, and Emergency Response (CESER)	National Governors Association (NGA)	
	Energy Sector Government Coordinating Council (EGCC)	National Association of State Energy Officials (NASEO)	
	Federal Senior Leadership Council (FSLC)	National Emergency Management Association (NEMA)	
	State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)	National Association of State Chief Information Officers (NASCIO)	
	Regional Consortium Coordinating Council (RC3)		
	Federal Trade Commission (FTC)		
	Department of Defense (DoD)		

Attackers	Standards, Research, & Development Organizations	State, Local, Tribal and Territorial Government Critical Infrastructure Support Agencies	Law Enforcement
Cyberwarriors	Electric Power Research Institute (EPRI)	State Chief Information Security Officers (CISO)	Federal Bureau of Investigation (FBI)
Cyberterrorists	National Laboratories Federally Funded Research & Development Centers (FFRDCs)	National Guard	Cyber Action Team
Cyberspies	SANS Institute	State and Territory Energy Office (SEO)	National Cyber Investigative Joint Task Force (NCIJTF)
Cyberthieves	National Institute of Science and Technology (NIST)	State Office of Emergency Management	
Cyberhacktivists			

Regulatory Bodies	Cybersecurity Vendors	Electricity Cyber-Physical Asset Manufacturers	
Federal Energy Regulatory Commission (FERC)	Threat Analysts	Electrical Equipment Manufacturers	
North American Energy Reliability Corporation (NERC)	Monitoring Platform Vendors	Industrial Control System (ICS) & Operational Technology (OT) Producers	
Public Utilities Commissions	Response and Forensics Vendors		
	Cybersecurity Software and Other Product Vendors		

Appendix C. Stakeholder Needs Analysis

Stakeholder: Electricity Market Entities		
Need	How important?	How well is need being met?
A1 - Information and intelligence sharing	H	L
A2 - Assistance developing frameworks, processes, and other tools for enabling optimal cyber response mechanisms	H	H
A3 - Expectations for response process and clear roles and lines of authority	H	L
A4 - Autonomy to manage risk and incident response measures	H	H
A5 - Trusted relationships with supporting stakeholders	H	L
A6 - Consistent, universal standards to define cyber resilience and cyber response for entire sector	H	L
A7 - Support for cybersecurity investment recoupment	H	L

Stakeholder: Federal Government, National Regulatory Bodies, & Law Enforcement		
Need	How important?	How well is need being met?
B1 - Integration into private sector response plans and efforts	H	L
B2 - Compliance with legislation, regulation, and policies	M	H
B3 - Information sharing and reporting from the private sector	H	L
B4 - Recommendations and advice on cyber response policy, frameworks, and government action	H	H
B5 - Trusted relationships with regional and local public and private partners	H	L

Stakeholder: Regional & Local Government & Regulatory Bodies		
Need	How important?	How well is need being met?
C1 - Information and intelligence sharing	H	L
C2 - Integration into private sector response plans and efforts	M	H
C3 - Consensus and support of membership for cybersecurity initiatives	H	H
C4 - Trusted relationships with supported and supporting stakeholders	H	L

Stakeholder: Cybersecurity Vendors		
Need	How important?	How well is need being met?
D1 - Information and intelligence sharing	H	L
D2 - Trusted relationships with supporting and supported stakeholders	H	M
D3 - Business opportunities to provide cyber incident response services	L	H

Stakeholder: Electricity Cyber-Physical Asset Manufacturers		
Need	How important?	How well is need being met?
E1 - Business opportunities/feedback to provide cutting edge cyber technologies that increase cyber resilience	H	M
E2 - Integration into response plans	H	L

Stakeholder: Regulatory Bodies		
Need	How important?	How well is need being met?
F1 - Compliance with legislation, regulation, and policies	H	M
F2 - Recommendations for rule-making of new and updated regulations	H	M

Stakeholder: Standards, Research, & Development Organizations		
Need	How important?	How well is need being met?
G1 - Information and intelligence sharing	H	L
G2 - Investment in cybersecurity projects	M	M

Stakeholder: Information Sharing Entities		
Need	How important?	How well is need being met?
H1 - Timely cyber incident reporting from electricity market entities	H	L
H2 - Collaborative participation in information sharing programs	H	M
H3 - Funding to support information sharing organization	M	H

Stakeholder: Standards, Research, & Development Organizations		
Need	How important?	How well is need being met?
I1 - Integration into private sector response plans and efforts	H	L
I2 - Compliance with legislation, regulation, and policies	H	M
I3 - Information sharing and reporting from the private sector	H	L
I4 - Recommendations and advice on cyber response policy, frameworks, and government action	H	L
I5 - Trusted relationships with regional and local public and private partners	H	M

Stakeholder: Law Enforcement		
Need	How important?	How well is need being met?
J1 - Timely cyber incident reporting from electricity market entities	M	L
J2 - Preservation of evidence and facilitation of investigation, forensic analysis to prosecute cybercrime	L	L

Appendix D. Acronyms

AMI	Advanced Metering Infrastructure
APPA	American Public Power Association
ARIES	Architecting Innovative Enterprise Strategy
BPA	Bonneville Power Administration
BPS	Bulk Power System
CAMS	Cybersecurity at MIT Sloan
CAT	Cyber Action Team
CESER	Office of Cybersecurity, Energy Security, and Emergency Response
CIKR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Protection Advisory Council
CISA	Cybersecurity and Infrastructure Security Agency
CISS	Cyber Incident Severity Schema
CMA	Cyber Mutual Assistance
CNIO	Critical National Infrastructure Operator
COP	Common Operating Picture
COU	Consumer-Owned Utility
CRISP	Cybersecurity Risk Information Sharing Program
CTIIC	Cyber Threat Intelligence Integration Center
DCS	Distributed Control System
DER	Distributed Energy Resources
DERMS	Distributed Energy Resource Management System
DHS	Department of Homeland Security
DMS	Distribution Management System
DNP3	Distributed Network Protocol version 3
DoD	Department of Defense
DOE	Department of Energy
DRMS	Demand Response Management System
EDS	Energy Delivery Sector
EEAC	Energy Emergency Assurance Coordinator
EEI	Edison Electric Institute
E-ISAC	Electricity Information Sharing and Analysis Center
EMAC	Emergency Management Assistance Compact
EMS	Energy Management System
EO	Executive Order
EPRI	Electric Power Research Institute
ERO	Electric Reliability Organization
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
ESCC	Electricity Subsector Coordinating Council

ESF	Emergency Support Function
ESSP	Energy Sector-Specific Plan
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FFRDC	Federally Funded Research and Development Centers
FIOP	Federal Interagency Operational Plan
FLSTT	Federal, State, Local, Tribal and Territorial
FSLC	Federal Senior Leadership Council
FTC	Federal Trade Commission
GIS	Geographic Information System
GridEx	Grid Exercise
HIRT	Hunt and Incident Response Team
ICS	Industrial Control System
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	International Society of Electrical and Electronics Engineers
IOU	Investor-Owned Utility
IRP	Incident Response Plan
ISAC	Information and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISO	Independent System Operator
IT	Internet of Things
LPPC	Large Public Power Council
MDMS	Meter Data Management System
MS-ISAC	Multi-State Information Sharing and Analysis Center
MSSP	Managed Support Service Provider
NARUC	National Association of Regulatory Utility Commissioners
NASEO	National Association of State Energy Offices
NCCIC	National Cybersecurity and Communications Integration Center
NCI	National Council of ISACs
NCIJTF	National Cyber Investigative Joint Task Force
NCIRP	National Cyber Incident Response Plan
NEMA	National Emergency Management Association
NERC	North American Electricity Reliability Corporation
NGA	National Governors Association
NIAC	National Infrastructure Advisory Council
NICC	National Infrastructure Coordinating Council
NIMS	National Incident Management System

NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NIST	National Institute of Science and Technology
NOC	National Operations Center
NRECA	National Rural Electric Cooperatives Association
NRF	National Response Framework
NRMC	National Risk Management Center
ODNI	Office of the Director of National Intelligence
OEM	Office of Emergency Management
OMS	Outage Management System
OT	Operational Technology
POIA	Power Outage Incident Annex
PPD	Presidential Policy Directive
PPP	Public-Private Partnership
PUC	Public Utility Commissions
RC3	Regional Consortium Coordinating Council
REMAED	Response Examination of Malware Attacks on the Energy Delivery sector
REMEDYS	Research Exploring Malware in the Energy Delivery Sector
RTO	Regional Transmission Operator
SCADA	Supervisory Control & Data Acquisition
SEO	State Energy Office
SIS	Safety Instrument System
SLTT	State, Local, Territorial, and Tribal
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
UCG	Unified Coordination Group

References

[1] R. Langner and P. Pederson, "Bound to Fail: Why Cyber Security Risk Cannot Simply Be 'Managed' Away," *Cent. 21st Century Secur. Intell.*, p. 16, Feb. 2013.

[2] M. Carr, "Public-private partnerships in national cyber-security strategies," *Int. Aff.*, vol. 92, no. 1, pp. 43–62, Jan. 2016.

[3] "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," *Fed. Regist.*, vol. 82, no. 93, p. 7, May 2017.

[4] C. Krebs, "A Case for Collective Defense," *Electric Perspectives*, vol. 43, no. 5, Oct-2018.

[5] S. Madnick, "Preparing for the Cyberattack That Will Knock Out U.S. Power Grids," p. 6, May 2017.

[6] "Business Blackout," Lloyd's of London and the University of Cambridge Centre for Risk Studies, 2015.

[7] "Crash Override Malware Took Down Ukraine's Power Grid Last December | WIRED." [Online]. Available: https://www.wired.com/story/crash-override-malware/. [Accessed: 16-May-2019].

[8] "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations," Dragos, Inc., Jun. 2017.

[9] R. Lee M., M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," SANS ICS, E-ISAC, Defense Use Case, Mar. 2019.

[10] R. J. Campbell, "Electric Grid Cybersecurity," Congressional Research Service, R45312, Sep. 2018.

[11] "Annual Cybersecurity Report," Cisco, 2018.

[12] "The GrayMatter Cyber Tracker," GrayMatter Systems, 2017.

[13] "Grid Architecture," Pacific Northwest National Laboratory, Richland, Washington, Nov. 2014.

[14] M. S. Jalali, J. P. Kaiser, M. Siegel, and S. Madnick, "The Internet of Things (IoT) Promises New Benefits and Risks: A Systematic Analysis of Adoption Dynamics of IoT Products," *SSRN Electron. J.*, 2017.

[15] "Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards," Centre for Cybersecurity and Electricity Industry Community, World Economic Forum, Geneva, Switzerland, Jan. 2019.

[16] A. Clark-Ginsberg, "What's the Difference between Reliability and Resilience," p. 3, Mar. 2016.

[17] "Essential Reliability Services: Whitepaper on Sufficiency Guidelines," North American Electric Reliability Corporation, Atlanta, GA, Dec. 2016.

[18] Reishus Consulting LLC, "Electricity Ancillary Services Primer," New England States Committee on Electricity, Aug. 2017.

[19] "Understanding the Grid," North American Electric Reliability Corporation, Atlanta, GA, Dec. 2012.

[20] "Critical Infrastructure Resilience Final Report and Recommendations," National Infrastructure Advisory Council, Sep. 2009.

[21] A. R. I. Berkeley and M. Wallace, "A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council," Oct. 2010.

[22] B. R. Lindsay, "Federal Emergency Management: A Brief Introduction," Congressional Research Service, R42845, Nov. 2012.

[23] “Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans: Managing the Cascading Impacts from a Long-Term Power Outage,” Department of Homeland Security, Jun. 2017.

[24] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” National Institute of Standards and Technology, Gaithersburg, MD, NIST Cybersecurity White Paper, Apr. 2018.

[25] P. Paganini, “Introduction to the NIST CyberSecurity Framework for a Landscape of Cyber Menaces,” *Security Affairs*, 20-Apr-2017. [Online]. Available: https://securityaffairs.co/wordpress/58163/laws-and-regulations/nist-cybersecurity-framework-2.html. [Accessed: 18-May-2019].

[26] “NIST Cybersecurity Framework FAQs -.” [Online]. Available: https://foresite.com/nist-cybersecurity-framework-faqs/. [Accessed: 23-Jun-2019].

[27] B. Obama, “Presidential Policy Directive 21: Critical Infrastructure Security and Resilience,” PPD 21, Feb. 2013.

[28] “Cybersecurity and Cross-Sector Coordination: A Conversation with Keith Alexander,” *Fletcher Forum World Aff.*, vol. 40, no. 2, Summer 2016.

[29] M. Korkali, J. G. Veneman, B. F. Tivnan, J. P. Bagrow, and P. D. H. Hines, “Reducing Cascading Failure Risk by Increasing Infrastructure Network Interdependence,” *Sci. Rep.*, vol. 7, no. 1, Dec. 2017.

[30] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, G. Lykou, and D. Gritzalis, “Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures,” *Int. J. Crit. Infrastruct. Prot.*, vol. 12, pp. 46–60, Mar. 2016.

[31] I. B. Utne, P. Hokstad, and J. Vatn, “A method for risk modeling of interdependencies in critical infrastructures,” *Reliab. Eng. Syst. Saf.*, vol. 96, no. 6, pp. 671–678, Jun. 2011.

[32] “2015 Energy Sector-Specific Plan,” Department of Homeland Security, 2015.

[33] D. J. Nightingale and D. H. Rhodes, *Architecting the Future Enterprise*. Cambridge, MA: The MIT Press, 2015.

[34] D. H. Rhodes, “Systems Architecting Applied to Enterprises Class 3, Spring 2019,” presented at the Class 3, Massachusetts Institute of Technology, 25-Feb-2019.

[35] R. K. Mitchell, B. R. Agle, and D. J. Wood, “Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts,” *Acad. Manage. Rev.*, vol. 22, no. 4, pp. 853–886, Oct. 1997.

[36] M. Keenan, “Force-field analysis,” *Salem Press Encyclopedia*. Salem Press, 2018.

[37] J. J. Messerly, “Final Report on the August 14, 2003 Blackout in the United States and Canada,” U.S. Department of Energy, Apr. 2004.

[38] “How the Electricity Grid Works,” *Union of Concerned Scientists*. [Online]. Available: https://www.ucsusa.org/clean-energy/how-electricity-grid-works. [Accessed: 17-May-2019].

[39] “Report on “Energy for Sustainable Development",” United Nations Economic Commission for Africa, Progress Review, Apr. 2006.

[40] G. S. S. Gopinath and M. V. K. Meher, “Electricity a basic need for the human beings,” presented at the INTERNATIONAL CONFERENCE ON RENEWABLE ENERGY RESEARCH AND EDUCATION (RERE-2018), Andhra Pradesh, India, 2018, p. 5.

[41] L. B. R. L. http://www.lbresearch.com, “The Increasing Importance of Energy Security in an Unpredictable World - The Latest Legal Features, Research and Legal Profiles,” *Who’s Who Legal*, Jul-2015. [Online]. Available:

https://whoswholegal.com/news/features/article/32363/increasing-importance-energy-security-unpredictable-world. [Accessed: 28-May-2019].

[42] "Use of Electricity - Energy Explained, Your Guide to Understanding Energy - Energy Information Administration." [Online]. Available: https://www.eia.gov/energyexplained/index.php?page=electricity_use. [Accessed: 29-May-2019].

[43] "IEA Energy Atlas." [Online]. Available: http://energyatlas.iea.org/#!/tellmap/-1118783123/1. [Accessed: 28-May-2019].

[44] K. H. LaCommare, J. H. Eto, L. N. Dunn, and M. D. Sohn, "Improving the estimated cost of sustained power interruptions to electricity customers," *Energy*, vol. 153, pp. 1038–1047, Jun. 2018.

[45] R. J. Campbell, "Weather-Related Power Outages and Electric System Resiliency," Congressional Research Service, R42696, Aug. 2012.

[46] P. J. Feldman, "A Huge Distribution Opportunity," Electricity Policy, Feb. 2015.

[47] A. Azzuni and C. Breyer, "Definitions and dimensions of energy security: a literature review," *Wiley Interdiscip. Rev. Energy Environ.*, vol. 7, no. 1, p. e268, Jan. 2018.

[48] "Transcript: Dan Coats Warns the Lights Are 'Blinking Red' on Russian Cyberattacks," *NPR.org*, 18-Jul-2018. [Online]. Available: https://www.npr.org/2018/07/18/630164914/transcript-dan-coats-warns-of-continuing-russian-cyberattacks. [Accessed: 06-May-2019].

[49] R. K. Knake, "A Cyberattack on the U.S. Power Grid," Center for Preventive Action, Council on Foreign Relations, Contingency Planning Memorandum 31, Apr. 2017.

[50] M. J. Assante and R. M. Lee, "The Industrial Control System Cyber Kill Chain," SANS Institute, Oct. 2015.

[51] J. Martindale, "From pranks to nuclear sabotage, this is the history of malware," *Digital Trends*, 29-Mar-2018. [Online]. Available: https://www.digitaltrends.com/computing/history-of-malware/. [Accessed: 08-Dec-2018].

[52] M. Landesman, "A Brief History of Malware on the Internet (the First 25 Years)," *Lifewire*, 02-Sep-2018. [Online]. Available: https://www.lifewire.com/brief-history-of-malware-153616. [Accessed: 08-Dec-2018].

[53] S. Morgan, "Global Ransomware Damage Costs Predicted to Hit $11.5 Billion By 2019," *Cybercrime Magazine*, 14-Nov-2017.

[54] D. E. Denning, "Stuxnet: What Has Changed?," *Future Internet*, vol. 4, no. 3, pp. 672–687, Jul. 2012.

[55] M. Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *Int. Stud. Rev.*, vol. 15, no. 1, pp. 105–122, Mar. 2013.

[56] S. Hakim and R. M. Clark, Eds., *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, vol. 3. New York, NY: Springer Berlin Heidelberg, 2016.

[57] J. Petters, "What is an Advanced Persistent Threat (APT)?," *Varonis Blog*, 26-Nov-2018. [Online]. Available: https://www.varonis.com/blog/advanced-persistent-threat/. [Accessed: 09-Dec-2018].

[58] "What Is an Advanced Persistent Threat (APT)? - Cisco." [Online]. Available: https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html. [Accessed: 09-Dec-2018].

[59] “What is an Advanced Persistent Threat (APT)? | APT Definition,” *Carbon Black*. [Online]. Available: https://www.carbonblack.com/resources/definitions/what-is-advanced-persistent-threat/. [Accessed: 09-Dec-2018].

[60] “Anatomy of an APT (Advanced Persistent Threat) Attack | FireEye.” [Online]. Available: https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html. [Accessed: 09-Dec-2018].

[61] “TRISIS Malware: Analysis of Safety System Targeted Malware,” Dragos, Inc., Dec. 2017.

[62] “Triton/Trisis Attack Was More Widespread Than Publicly Known,” *Dark Reading*. [Online]. Available: https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known/d/d-id/1333661. [Accessed: 01-Jun-2019].

[63] T. Rid and B. Buchanan, “Attributing Cyber Attacks,” *J. Strateg. Stud.*, vol. 38, no. 1–2, pp. 4–37, Jan. 2015.

[64] “WannaCry Ransomware: 6 Implications for the Insurance Industry.” [Online]. Available: http://www.symantec.com/connect/blogs/wannacry-ransomware-6-implications-insurance-industry. [Accessed: 23-Jun-2019].

[65] C. Glenn, D. Sterbentz, and A. Wright, “Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector,” INL/EXT--16-40692, 1337873, Dec. 2016.

[66] “Tripwire Study: Energy Sector Sees Dramatic Rise in Successful Cyber Attacks.” [Online]. Available: http://www.tripwire.com/company/press-releases/2016/04/tripwire-study-energy-sector-sees-dramatic-rise-in-successful-cyber-attacks/. [Accessed: 09-Dec-2018].

[67] “2018 Department of Defense Cyber Strategy: Summary,” Department of Defense, 2018.

[68] “Electricity Regulation in the US: A Guide,” Montpelier, Vermont, Mar. 2011.

[69] “Timeline and History of Energy Deregulation in the United States,” *Electric Choice*. [Online]. Available: https://www.electricchoice.com/blog/timeline-history-energy-deregulation/. [Accessed: 02-Jun-2019].

[70] “Regulated & Deregulated Energy Markets,” *CustomerFirst Renewables*, 02-Jun-2019. [Online]. Available: https://www.customerfirstrenewables.com/resources/regulated-deregulated-energy-markets/. [Accessed: 02-Jun-2019].

[71] “History of NERC,” North American Electric Reliability Corporation, Atlanta, GA, Aug. 2013.

[72] “North American Electric Reliability Corporation,” *Wikipedia*. 27-Nov-2018.

[73] D. H. Meyer and N. Kamel, “The August 14, 2003 Blackout One Year Later: Actions Taken in the United States and Canada To Reduce Blackout Risk,” U.S. Department of Energy, Ministry of Natural Resources Canada, Aug. 2004.

[74] “Improving Coordinated Operations Across the Electric Reliability Organization Enterprise,” North American Electric Reliability Corporation, Atlanta, GA, Feb. 2014.

[75] E. Currens, “What You Need to Know about NERC CIP Cybersecurity Standards,” *Trustwave*, 28-Nov-2018. [Online]. Available: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/what-you-need-to-know-about-nerc-cip-cybersecurity-standards/. [Accessed: 03-Jun-2019].

[76] “Reliability Standards for the Bulk Electric Systems of North America.” North American Electric Reliability Corporation, 03-Jul-2018.

[77] “FERC v. Mississippi, 456 U.S. 742 (1982),” *Justia Law*. [Online]. Available: https://supreme.justia.com/cases/federal/us/456/742/. [Accessed: 04-Jun-2019].

[78] D. Phelan, “A Summary of State Regulators’ Responsibilities Regarding Cybersecurity Issues,” National Regulatory Research Institute, Silver Spring, MD, 14–12, Dec. 2014.

[79] L. Holt and M. Galligan, “State Public Utility Commissions’ Role in Cybersecurity and Physical Security Issues: Trade-Offs and Challenges,” Public Utilities Research Center, University of Florida Warrington, Dec. 2017.

[80] F. Massacci, R. Ruprai, M. Collinson, and J. Williams, “Economic Impacts of Rules- versus Risk-Based Cybersecurity Regulations for Critical Infrastructure Providers,” *IEEE Secur. Priv.*, vol. 14, no. 3, pp. 52–60, May 2016.

[81] E. A. Fischer, E. C. Liu, J. W. Rollins, and C. A. Theohary, “The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress,” Congressional Research Service, Dec. 2014.

[82] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to Industrial Control Systems (ICS) Security,” National Institute of Standards and Technology, NIST SP 800-82r2, Jun. 2015.

[83] “Electricity Subsector Cybersecurity Risk Management Process,” Department of Energy, DOE/OE-0003, May 2012.

[84] Joint Task Force Transformation Initiative, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-37r2, Dec. 2018.

[85] C. Greer *et al.*, “NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0,” National Institute of Standards and Technology, NIST SP 1108r3, Oct. 2014.

[86] “Framework for Improving Critical Infrastructure Cybersecurity,” National Institute of Standards and Technology, v1.0, Feb. 2014.

[87] “Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2),” *Energy.gov*. [Online]. Available: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-1. [Accessed: 06-Jun-2019].

[88] S. B. Lipner and B. W. Lampson, “Risk Management and the Cybersecurity of the U.S. Government,” *Input Comm. Enhancing Natl. Cybersecurity*, p. 7, 2016.

[89] “Valuation of Energy Security for the United States,” *Energy.gov*. [Online]. Available: https://www.energy.gov/policy/articles/valuation-energy-security-united-states. [Accessed: 28-May-2019].

[90] “Tenth Amendment to the United States Constitution,” *Wikipedia*, 16-Apr-2019. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Tenth_Amendment_to_the_United_States_Constitution&oldid=892767393. [Accessed: 04-Jun-2019].

[91] “16 U.S. Code § 824o–1 - Critical electric infrastructure security,” *LII / Legal Information Institute*. [Online]. Available: https://www.law.cornell.edu/uscode/text/16/824o-1. [Accessed: 12-Jun-2019].

[92] “10 CFR Subpart W - Electric Power System Permits and Reports; Applications; Administrative Procedures and Sanctions; Grid Security Emergency Orders,” *LII / Legal Information Institute*. [Online]. Available: https://www.law.cornell.edu/cfr/text/10/part-205/subpart-W. [Accessed: 12-Jun-2019].

[93] D. W. Hilt, “Critical Infrastructure Protection Required on Electric Grid Continually Changing,” *Nat. Gas Electr.*, vol. 34, no. 8, pp. 9–15, Mar. 2018.

[94] P. Honeyman, G. A. Schwartz, and A. Van Assche, “Interdependence of Reliability and Security,” in *Proceedings of 6th Workshop on Economics of Information Security*, Pittsburgh, PA, 2007, p. 22.

[95] R. F. Dacey, “Critical Infrastructure Protection - Establishing Effective Information with Infrastructure Sectors,” U.S. General Accounting Office, Testimony before the Subcommittees on Cybersecurity, Science, and Research & Development and Infrastructure and Border Security, Select Committee on Homeland Security, House of Representatives, Apr. 2004.

[96] C. Goodwin and J. P. Nicholas, “A Framework for Cybersecurity Information Sharing and Risk Reduction,” Microsoft Corporation, 2015.

[97] W. Zhao and G. White, “A collaborative information sharing framework for Community Cyber Security,” in *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA, USA, 2012, pp. 457–462.

[98] K. Harrison and G. White, “Information sharing requirements and framework needed for community cyber incident detection and response,” in *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA, USA, 2012, pp. 463–469.

[99] “Cybersecurity - National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented,” Government Accountability Office, GAO-13-187, Feb. 2013.

[100] D. K. Mulligan and F. B. Schneider, “Doctrine for Cybersecurity,” *Daedalus*, vol. 140, no. 4, pp. 70–92, Oct. 2011.

[101] R. Anderson, “Why information security is hard - an economic perspective,” in *Seventeenth Annual Computer Security Applications Conference*, New Orleans, LA, USA, 2001, pp. 358–365.

[102] A. Etzioni, “The Private Sector: A Reluctant Partner in Cybersecurity,” *Georget. J. Int. Aff.*, p. 11, 2014.

[103] J. O’Halloran, “Challenges of Public-Private Partnerships in Cybersecurity,” Utica College, 2017.

[104] T. Moore, “Introducing the Economics of Cybersecurity: Principles and Policy Options,” *Natl. Acad. Sci.*, p. 21, 2010.

[105] M. Dunn-Cavelty and M. Suter, “Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection,” *Int. J. Crit. Infrastruct. Prot.*, vol. 2, no. 4, pp. 179–187, Aug. 2009.

[106] B. Powell, “Is Cybersecurity a Public Good? Evidence from the Financial Services Industry,” San Jose State University & The Independent Institute, Independent Institute Working Paper 57, Mar. 2001.

[107] *Internet Security*. Washington, DC: U.S. Government Printing Office, 2000, p. 68.

[108] “Understanding Your E-ISAC.” Electricity Information Sharing and Analysis Center, Jun-2016.

[109] “Public Private Partnerships and the Cybersecurity Challenge of Protecting Critical Infrastructure,” *Forbes*. [Online]. Available: https://www.forbes.com/sites/cognitiveworld/2019/05/06/public-private-partnerships-and-the-cybersecurity-challenge-of-protecting-critical-infrastructure/. [Accessed: 06-May-2019].

[110] L. Nottingham *et al.*, “The Road to Resilience: Managing Cyber Risks,” World Energy Council, 2016.

[111] “Perspectives on the Grand Energy Transition,” World Energy Council, 2018.

[112] “Memo on State Cybersecurity Budgets,” Resource Center for State Cybersecurity, National Governors Association, Mar. 2017.

[113] S. Subramanian and D. Robinson, “2018 Deloitte-NASCIO Cybersecurity Study: States at risk: Bold Plays for Change,” NASCIO and Deloitte Insight, 2018.

[114] “EY Global Information Security Survey 2018–19,” Ernst & Young, 2018.

[115] “Summary for Policymakers,” Department of Energy, Jan. 2017.

[116] *Federal Power Act*. 2018, p. 102.

[117] “National Cyber Incident Response Plan - December 2016.” Department of Homeland Security, Dec-2016.

[118] *Presidential Policy Directive 41: United States Cyber Incident Coordination*. 2016.

[119] “Adverse selection | economics,” *Encyclopedia Britannica*. [Online]. Available: https://www.britannica.com/topic/adverse-selection. [Accessed: 05-Jul-2019].

[120] L. C. Abrams, R. Cross, E. Lesser, and D. Z. Levin, “Nurturing interpersonal trust in knowledge-sharing networks,” *Acad. Manag. Perspect.*, vol. 17, no. 4, pp. 64–77, Nov. 2003.

[121] F. Skopik and Qin Li, “Trustworthy incident information sharing in social cyber defense alliances,” in *2013 IEEE Symposium on Computers and Communications (ISCC)*, Split, Croatia, 2013, pp. 000233–000239.

[122] C. Burnett, T. J. Norman, and K. Sycara, “Bootstrapping Trust Evaluations through Stereotypes,” in *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems*, Toronto, Canada, 2010, vol. 1, pp. 241–248.

[123] Ö. Özer, U. Subramanian, and Y. Wang, “Information Sharing, Advice Provision, or Delegation: What Leads to Higher Trust and Trustworthiness?,” *Manag. Sci.*, vol. 64, no. 1, pp. 474–493, Jan. 2018.

[124] C. E. Porter and N. Donthu, “Cultivating Trust and Harvesting Value in Virtual Communities,” *Manag. Sci.*, vol. 54, no. 1, pp. 113–128, Jan. 2008.

[125] “Critical Infrastructure Readiness Report: Holding the Line Against Cyberthreats,” The Aspen Institute, 2015.

[126] “Malware Mitigation Challenges (Draft),” Pacific Northwest National Laboratory, PNNL-SA-139835, Nov. 2018.

[127] B. R. Rowe and M. P. Gallaher, “Private Sector Cyber Security Investment Strategies: An Empirical Analysis,” p. 23, Mar. 2006.

[128] G. Heal and H. Kunreuther, “Interdependent Security: A General Model,” National Bureau of Economic Research, Cambridge, MA, w10706, Aug. 2004.

[129] H. Kunreuther and G. Heal, “Interdependent Security,” in *The Risks of Terrorism*, W. K. Viscusi, Ed. Boston, MA: Springer US, 2003, pp. 133–151.

[130] H. Varian, “System Reliability and Free Riding,” in *Economics of Information Security*, vol. 12, L. J. Camp and S. Lewis, Eds. Boston: Kluwer Academic Publishers, 2004, pp. 1–15.

[131] H. R. Varian, “Managing Online Security Risks,” *The New York Times*, p. 3, 01-Jun-2000.

[132] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, “Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model,” *J. Inf. Secur.*, vol. 06, no. 01, pp. 24–30, 2015.

[133] A. J. Mathew and C. Cheshire, “A Fragmented Whole: Cooperation and Learning in the Practice of Information Security,” Center for Long-Term Cybersecurity, UC Berkeley, Feb. 2018.

[134] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, “Sharing information on computer systems security: An economic analysis,” *J. Account. Public Policy*, vol. 22, no. 6, pp. 461–485, Nov. 2003.

[135] “Aurora Generator Test,” *Wikipedia*. 13-Jan-2019.

[136] “Transforming the Nation’s Electricity System: The Second Installment of the Quadrennial Energy Review,” Department of Energy, Summary for Policymakers, 2017.

[137] “Pre-read Materials,” in *The Future of the Grid: Evolving to Meet America’s Need*, GridWise Alliance and DOE National Summit, 2014.

[138] “INFOGRAPHIC: Understanding the Grid,” *Energy.gov*. [Online]. Available: https://www.energy.gov/articles/infographic-understanding-grid. [Accessed: 07-Jun-2019].

[139] “Replacing the US electric grid could cost $5 trillion - Business Insider.” [Online]. Available: https://www.businessinsider.com/replacing-the-us-electric-grid-could-cost-5-trillion-2017-3. [Accessed: 07-Jun-2019].

[140] E. Hayden, M. J. Assante, and T. Conway, “An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity,” SANS Institute, Analyst Whitepaper, Aug. 2014.

[141] “Convergence of IT and OT in Energy and Manufacturing.” [Online]. Available: https://www.digitalistmag.com/cio-knowledge/2018/11/05/convergence-of-it-ot-in-energy-manufacturing-06192743. [Accessed: 07-Jun-2019].

[142] J. Corell *et al.*, “Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions,” The Public-Private Analytic Exchange Program, 2017.

[143] “Ensuring Cybersecurity in the Electric Utility Industry,” *https://www.bcg.com*. [Online]. Available: https://www.bcg.com/publications/2017/power-utilities-technology-digital-ensuring-cybersecurity-electric-utility-industry.aspx. [Accessed: 08-Jun-2019].

[144] *Energy Independence and Security Act of 2007*, vol. 42 USC 17001. 2007, p. 311.

[145] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, “Guidelines for Smart Grid Cybersecurity,” National Institute of Standards and Technology, NIST IR 7628r1, Sep. 2014.

[146] “Distributed Energy Resources: Technical Considerations for the Bulk Power System,” Federal Energy Regulatory Commission, Staff Report Docket No. AD18-10-000 1, Feb. 2018.

[147] Federal Energy Regulatory Commission, “Revised Critical Infrastructure Protection Reliability Standards [Docket No. RM15-14-002; Order No. 829],” Jul. 2016.

[148] Federal Energy Regulatory Commission, “Supply Chain Risk Management Reliability Standards [Docket No. RM17-13-000; Order No. 850],” Oct. 2018.

[149] “Draft Cybersecurity Supply Chain Risks,” North American Electric Reliability Corporation, Atlanta, GA, Staff Report and Recommended Actions, Feb. 2019.

[150] “The ESCC’s Cyber Mutual Assistance Program,” Electricity Subsector Coordinating Council, Jan. 2019.

[151] GWAC, “GridWise Transactive Energy Framework, Version 1.0,” GridWise Architecture Council, Richland, Washington, Jan. 2015.

[152] GWAC, “GridWise Architecture Council - Transactive Energy Flyer,” GridWise Architecture Council, Richland, Washington, 2014.

[153] “A Transactive Energy Future: The Inevitable Rise of Economic-based Grid Control.” [Online]. Available: https://www.renewableenergyworld.com/articles/print/volume-20/issue-5/features/solar-wind-storage-finance/a-transactive-energy-future-the-inevitable-rise-of-economic-based-grid-control.html. [Accessed: 18-May-2019].

[154] Z. Liu, Q. Wu, S. Huang, and H. Zhao, “Transactive energy: A review of state of the art and implementation,” in *2017 IEEE Manchester PowerTech*, Manchester, United Kingdom, 2017, pp. 1–6.

[155] J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, “Cybersecurity and Power Electronics: Addressing the Security Vulnerabilities of the Internet of Things,” *IEEE Power Electron. Mag.*, vol. 4, no. 4, pp. 37–43, Dec. 2017.

[156] Office of Gas and Electricity Markets, “RIIO-2 Sector Specific Methodology,” London, England, 2018.

[157] M. Keogh and S. Thomas, “Regional Mutual Assistance Groups: A Primer,” National Association of Regulatory Utility Commissioners, Nov. 2015.

[158] GWAC, “Transactive Energy Systems Research, Development and Deployment Roadmap,” GridWise Architecture Council, Richland, Washington, Dec. 2018.

[159] K. Lewin, *Field Theory in Social Science: Selected Theoretical Papers*. New York, NY: Harper & Brothers, 1951.

[160] R. L. Daft and D. Marcic, *Understanding Management*, 6th ed. Mason, OH: South-Western Cengage Learning, 2009.

[161] “Grid Security,” American Public Power Association, Jan. 2019.

[162] “WECC Moves to Restructure Organization into Two Distinct Entities,” *Washington Energy Report*, 14-Sep-2012. [Online]. Available: https://www.troutmansandersenergyreport.com/2012/09/wecc-moves-to-restructure-organization-into-two-distinct-entities/. [Accessed: 18-May-2019].

[163] O. Aaltomaa, “Conflicts of Interests between Different Market Players in Smart Grid Environment,” Master’s Thesis, Aalto University, Helsinki, Finland, 2012.

[164] B. Lawrence, C. de Siebert, and P. Daigle, “E-ISAC Update,” presented at the Critical Infrastructure Protection Committee, Jacksonville, FL, Mar-2018.

[165] “FERC: About FERC - What FERC Does.” [Online]. Available: https://www.ferc.gov/about/ferc-does.asp. [Accessed: 18-May-2019].

[166] “FERC: Electric Reliability: Cyber & Grid Security.” [Online]. Available: https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp. [Accessed: 18-May-2019].

[167] “About NERC.” [Online]. Available: https://www.nerc.com/AboutNERC/Pages/default.aspx. [Accessed: 18-May-2019].

[168] “Reliability Functional Model,” North American Electric Reliability Corporation, Version 6 (Draft), Jun. 2016.

[169] “Key Players.” [Online]. Available: https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx. [Accessed: 17-May-2019].

[170] “Electricity Information Sharing and Analysis Center.” [Online]. Available: https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx. [Accessed: 18-May-2019].

[171] P. Behr, “Grid attack exercise exposes threat-sharing issues,” *E&E News*, 01-Apr-2016. [Online]. Available: https://www.eenews.net/stories/1060034924. [Accessed: 09-Dec-2018].

[172] “Grid Security Exercise GridEx IV: Lessons Learned,” North American Electric Reliability Corporation, Mar. 2018.

[173] “Glossary of Terms Used in NERC Reliability Standards,” North American Electric Reliability Corporation, May 2019.

[174] “Reliability Coordinators.” [Online]. Available: https://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx. [Accessed: 05-Jul-2019].

[175] “FERC: Industries - RTO/ISO.” [Online]. Available: https://www.ferc.gov/industries/electric/indus-act/rto.asp. [Accessed: 17-May-2019].

[176] “Regional transmission organization (North America),” *Wikipedia*. 06-Apr-2019.

[177] *Promoting Wholesale Competition Through Open Access Non-discriminatory Transmission Services by Public Utilities and Recovery of Stranded Costs by Public Utilities and Transmitting Utilities*. 1996.

[178] F. Flores-Espino, T. Tian, I. Chernyakhovskiy, and M. Miller, “Competitive Electricity Market Regulation in the United States: A Primer,” North American Electric Reliability Corporation, Atlanta, GA, NREL/TP--6A20-67106, 1336561, Dec. 2016.

[179] “Our Members | American Public Power Association.” [Online]. Available: https://www.publicpower.org/our-members. [Accessed: 18-May-2019].

[180] “Differences Between Publicly and Investor-Owned Utilities.” [Online]. Available: https://www.energy.ca.gov/pou_reporting/background/difference_pou_iou.html. [Accessed: 18-May-2019].

[181] “Rural Utilities Service | USDA Rural Development.” [Online]. Available: https://www.rd.usda.gov/about-rd/agencies/rural-utilities-service. [Accessed: 18-May-2019].

[182] “Reliability and Security,” *America’s Electric Cooperatives*, 26-Apr-2019. [Online]. Available: https://www.electric.coop/issues-and-policy/reliability-and-security/. [Accessed: 18-May-2019].

[183] “FERC: Guide to Market Oversight - Glossary.” [Online]. Available: https://www.ferc.gov/market-oversight/guide/glossary.asp. [Accessed: 18-May-2019].

[184] “Power Marketer | Practical Law.” [Online]. Available: https://content.next.westlaw.com/Document/I4cf87056ef2a11e28578f7ccc38dcbee/View/FullText.html?transitionType=Default&contextData=(sc.Default). [Accessed: 18-May-2019].

[185] “Power marketers are increasing their share of U.S. retail electricity sales - Today in Energy - U.S. Energy Information Administration (EIA).” [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=36415. [Accessed: 18-May-2019].

[186] V. V. G. Krishnan, Y. Zhang, K. Kaur, A. Hahn, A. Srivastava, and S. Sindhu, “Cyber-Security Analysis of Transactive Energy Systems,” in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, Denver, CO, USA, 2018, pp. 1–9.

[187] B. Obama, “National Cybersecurity Center Policy Capture,” U.S. White House.

[188] M. R. Strasser, “War Powers,” *LII / Legal Information Institute*, 02-Jul-2008. [Online]. Available: https://www.law.cornell.edu/wex/war_powers. [Accessed: 18-May-2019].

[189] “NIAC Fact Sheet,” Department of Homeland Security, Dec. 2018.

[190] “National Response Framework, Third Edition,” Department of Homeland Security, Jun. 2016.

[191] “National Incident Management System, Third Edition,” Department of Homeland Security, Oct. 2017.

[192] “National Infrastructure Protection Plan,” Department of Homeland Security, 2013.

[193] “About CISA,” *Department of Homeland Security*, 18-Jun-2015. [Online]. Available: https://www.dhs.gov/cisa/about-cisa. [Accessed: 18-May-2019].

[194] “DHS National Protection and Programs Directorate,” *Wikipedia*. 23-Mar-2019.

[195] “NCCIC ICS Fact Sheet,” Department of Homeland Security, National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team.

[196] “About Us | US-CERT.” [Online]. Available: https://www.us-cert.gov/about-us. [Accessed: 18-May-2019].

[197] “National Risk Management Center Fact Sheet,” Department of Homeland Security, Nov. 2018.

[198] “NPPD’s Krebs: NCCIC Focus is ‘Today’ and NRMC ‘Tomorrow,’” *MeriTalk*, 05-Oct-2018. [Online]. Available: https://www.meritalk.com/articles/nppds-krebs-nccic-focus-is-today-and-nrmc-tomorrow/. [Accessed: 18-May-2019].

[199] “Joint National Priorities Fact Sheet,” Department of Homeland Security, Sep. 2018.

[200] J. Lynch, “Homeland Security announces new first response cyber center,” *Fifth Domain*, 01-Aug-2018. [Online]. Available: https://www.fifthdomain.com/critical-infrastructure/2018/07/31/homeland-security-announces-new-risk-management-center/. [Accessed: 18-May-2019].

[201] “CESER Mission,” *Energy.gov*. [Online]. Available: https://www.energy.gov/ceser/ceser-mission. [Accessed: 18-May-2019].

[202] “ESF 12 Events,” *Energy.gov*. [Online]. Available: https://www.energy.gov/ceser/esf-12-events. [Accessed: 18-May-2019].

[203] “NISAC Fact Sheet,” Sandia National Laboratories, 2016.

[204] “Cyber Crime,” *Federal Bureau of Investigation*. [Online]. Available: https://www.fbi.gov/investigate/cyber. [Accessed: 18-May-2019].

[205] “FBI Cyber Division,” *Wikipedia*. 31-Oct-2018.

[206] “Mission & Vision – InfraGard National.” [Online]. Available: https://www.infragardnational.org/about/mission/. [Accessed: 18-May-2019].

[207] “Home.” [Online]. Available: https://www.infragard.org/. [Accessed: 18-May-2019].

[208] *Reform of Generator Interconnection Procedures and Agreements: Comment of the Staff of the Federal Trade Commission*. Federal Energy Regulatory Commission, 2017.

[209] C. C. 400 7th S. S. Washington and D. 20024 U. States, “Something New Under the Sun: Competition & Consumer Protection Issues in Solar Energy,” *Federal Trade Commission*, 07-Apr-2016. [Online]. Available: https://www.ftc.gov/news-events/events-calendar/2016/06/something-new-under-sun-competition-consumer-protection-issues. [Accessed: 18-May-2019].

[210] T. Masse and J. Rollins, “A Summary of Fusion Centers: Core Issues and Options for Congress,” Congressional Research Service, RL34177, Sep. 2007.

[211] S. A. Salvatore, “Fusion center challenges: why fusion centers have failed to meet intelligence sharing expectations,” Naval Postgraduate School, Monterey, CA, 2018.

[212] N. Klem, “Elements Impacting the Integration of the National Network of Fusion Centers with the U.S. National Security Strategy,” Walden University, 2017.

[213] T. Coburn, “Federal Support for and Involvement in State and Local Fusion Centers,” United States Senate, Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, Majority and Minority Staff Report, Oct. 2012.

[214] M. James, A. McGovern, J. Somelofske, C. Valentine-Fossum, and K. Zweifel, “Improving the Cybersecurity of the Electric Distribution Grid,” Institute for Energy and the Environment, Vermont Law School, Phase 1, 2019.

[215] “Cyber-securing the grid: Best practices for state utility commissions,” *Utility Dive*. [Online]. Available: https://www.utilitydive.com/news/cyber-securing-the-grid-best-practices-for-state-utility-commissions/553389/. [Accessed: 18-May-2019].

[216] “State Energy Offices | NASEO.” [Online]. Available: https://www.naseo.org/state-energy-offices. [Accessed: 02-Jun-2019].

[217] “Electricity Subsector Coordinating Council Brochure,” Electricity Subsector Coordinating Council, Jan. 2018.

[218] “Energy Sector Government Coordinating Council Charter,” p. 4, Nov. 2014.

[219] “About,” *Regional Consortium Coordinating Council (RC3)*, 10-Oct-2011. [Online]. Available: https://rtriplec.wordpress.com/about/. [Accessed: 30-May-2019].

[220] “Incident Response, Forensics & Threat Hunting,” *CyberX*. [Online]. Available: https://cyberx-labs.com/incident-response-forensics-threat-hunting/. [Accessed: 18-May-2019].

[221] “Dragos | Industrial (ICS/OT) Cyber Security.” [Online]. Available: https://dragos.com/. [Accessed: 18-May-2019].

[222] “Attackers Deploy New ICS Attack Framework ‘TRITON’ and Cause Operational Disruption to Critical Infrastructure « Attackers Deploy New ICS Attack Framework ‘TRITON’ and Cause Operational Disruption to Critical Infrastructure,” *FireEye*. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html. [Accessed: 18-May-2019].

[223] “About the Association | American Public Power Association.” [Online]. Available: https://www.publicpower.org/about. [Accessed: 19-May-2019].

[224] “Our Organization,” *America’s Electric Cooperatives*, 26-Feb-2016. [Online]. Available: https://www.electric.coop/our-organization/. [Accessed: 19-May-2019].

[225] “Rural Cooperative Cybersecurity Capabilities Program (RC3),” *America’s Electric Cooperatives*, 02-May-2017. [Online]. Available: https://www.electric.coop/rural-cooperative-cybersecurity-capabilities-program-rc3/. [Accessed: 19-May-2019].

[226] “NRECA CEO to Promote Electric Co-op Cybersecurity Efforts in Senate Testimony,” *America’s Electric Cooperatives*, 28-Feb-2018. [Online]. Available: https://www.electric.coop/nreca-ceo-promote-electric-co-op-cybersecurity-efforts-senate-testimony/. [Accessed: 19-May-2019].

[227] “Affiliates | Union Rural Electric Cooperative, Inc.” [Online]. Available: https://www.ure.com/affiliates. [Accessed: 19-May-2019].

[228] “NRECA CEO Jim Matheson Affirms Support for Touchstone Energy - Touchstone Energy.” [Online]. Available: https://www.touchstoneenergy.com/co-op-business-resources/brand-news/nreca-ceo-jim-matheson-affirms-support-touchstone-energy/. [Accessed: 19-May-2019].

[229] "Resource Center for State Cybersecurity," *National Governors Association*. [Online]. Available: https://www.nga.org/bestpractices/divisions/hsps/statecyber/. [Accessed: 02-Jun-2019].

[230] "Coordinator Roles | NASEO." [Online]. Available: https://www.naseo.org/eeac. [Accessed: 12-Jun-2019].

[231] "National Association of State Energy Officials (NASEO) In Brief," National Association of State Energy Officials, Arlington, VA.

[232] "NARUC Services to Members," *NARUC*. [Online]. Available: https://www.naruc.org/memberbenefits/. [Accessed: 19-May-2019].

[233] Cadmus Group LLC, "Cybersecurity Strategy Development Guide," National Association of Regulatory Utility Commissioners, version 5, Oct. 2018.

[234] "About NASCIO." [Online]. Available: https://www.nascio.org/AboutNASCIO. [Accessed: 12-Jun-2019].

[235] "What is NEMA?" [Online]. Available: https://www.nemaweb.org/index.php/about/what-is-nema. [Accessed: 02-Jun-2019].

[236] "Mission & Vision." [Online]. Available: http://www.eei.org/about/mission/Pages/default.aspx. [Accessed: 19-May-2019].

[237] "Frequently Asked Questions – ISAO Standards Organization." [Online]. Available: https://www.isao.org/faq/. [Accessed: 18-May-2019].

[238] "National Council of ISACs | About NCI," *National Council of ISACs*. [Online]. Available: https://www.nationalisacs.org/about-nci. [Accessed: 27-May-2019].

[239] "MS-ISAC® Charter," *CIS*. [Online]. Available: https://www.cisecurity.org/ms-isac/ms-isac-charter/. [Accessed: 19-May-2019].

[240] R. Materese, "NIST History," *NIST*, 23-Feb-2019. [Online]. Available: https://www.nist.gov/nist-history. [Accessed: 19-May-2019].

[241] D. H. Rhodes, "Systems Architecting Applied to Enterprises Class 4, Spring 2019," presented at the Class 4, Massachusetts Institute of Technology, 04-Mar-2019.

[242] "French and Raven's bases of power," *Wikipedia*. 08-May-2019.

[243] S. Cobb, "Mind This Gap: Criminal Hacking and the Global Cybersecurity Skills Shortage, a Critical Analysis," presented at the Virus Bulletin Conference, 2016, p. 8.

[244] E. Crawley, B. Cameron, and D. Selva, *System Architecture*. Hoboken, NJ: Pearson Higher Education, Inc., 2016.

[245] "Could Energy Industry Dynamics Be Creating an Impending Cyber Storm?," Marsh & McLennan Companies, Briefing, 2018.

[246] "Memo on State Cybersecurity Response Plans," National Governor's Association, Memorandum, 2017.

[247] O. Barack, "Presidential Policy Directive-8: National Preparedness," United States. White House Office, Mar. 2011.

[248] "The Strategic National Risk Assessment in Support of PPD 8," United States. Department of Homeland Security, Dec. 2011.

[249] "National Preparedness System," United States. Department of Homeland Security, Nov. 2011.

[250] "Response Federal Interagency Operational Plan, Second Edition," United States. Department of Homeland Security, Jul. 2014.

[251] "National Response Framework Resource Center: Glossary/Acronyms," United States. Federal Emergency Management Agency, 2010.

[252] B. Obama, “Presidential Policy Directive 41: United States Cyber Incident Coordination,” United States. White House Office, Jul. 2016.

[253] Obama, Barack, “Annex to the Directive on United States Cyber Incident Coordination,” United States. White House Office, Jul. 2016.

[254] D. Trump, “Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” United States. Office of the Federal Register, May 2017.

[255] *Cybersecurity Enhancement Act of 2014*, vol. 15 USC 7421. 2014, p. 17.

[256] *National Cybersecurity Protection Act of 2014*, vol. 6 USC 101. 2014, p. 8.

[257] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology,” National Institute of Standards and Technology, NIST SP 800-61r2, Aug. 2012.

[258] “Comprehensive Preparedness Guide 101,” United States. Federal Emergency Management Agency, Nov. 2010.

[259] “Agreement for Enhanced Federal and State Energy Emergency Coordination, Communications, and Information Sharing,” National Association of State Energy Officials, Jun. 2015.

[260] T. Grance, T. Nolan, K. Burke, R. Dudley, G. White, and T. Good, “Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-84, Sep. 2006.

[261] *ISO/IED 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary*, 5th ed. Switzerland: International Standards Organization, 2018.

[262] NASEO, “State Energy Assurance Guidelines Version 3.1,” National Association of State Energy Officials, Dec. 2009.

[263] NERC, “CIP-008-6 — Cyber Security — Incident Reporting and Response Planning Final,” North American Electric Reliability Corporation, Jan. 2019.

[264] B. Wang, X. Li, L. P. de Aguiar, D. S. Menasche, and Z. Shafiq, “Measurement and Analysis of Patching Practices for Industrial Control Systems,” in *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 2017, vol. 1, p. 18.

[265] R. Rademacher, “Patch Management for ICS: Lifecycle and Compliance,” FoxGuard Solutions, Inc, Jan. 2018.

[266] “2018 National Preparedness Report,” Department of Homeland Security, Federal Emergency Management Agency, 2018.

[267] *Robert T. Stafford Disaster Relief and Emergency Assistance Act*. 1988, p. 180.

[268] “What Is EMAC?” [Online]. Available: https://www.emacweb.org/index.php/learn-about-emac/what-is-emac. [Accessed: 21-Jun-2019].

[269] “Mission Ready Packages.” [Online]. Available: https://www.emacweb.org/index.php/mutualaidresources/emac-library/mission-ready-packages. [Accessed: 21-Jun-2019].

[270] “Overview: ESF and Support Annexes: Coordinating Federal Assistance in Support of the National Response Framework,” United States. Department of Homeland Security, January 2008.

[271] “Emergency Support Function #12 – Energy Annex,” 2016.

[272] “Critical Infrastructure and Key Resource Support Annex,” United States. Department of Homeland Security, Jan. 2008.

[273] "GridEx." [Online]. Available: https://www.nerc.com/pa/ci/cipoutreach/pages/gridex.aspx. [Accessed: 23-Jun-2019].

[274] G. Hofstede, "Cultural Dimensions in Management and Planning," *Asia Pac. J. Manag.*, vol. 1, no. 2, pp. 81–99, Jan. 1984.

[275] A. D. Veiga, "A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument," in *2016 SAI Computing Conference (SAI)*, London, United Kingdom, 2016, pp. 1006–1015.

[276] E. H. Schein, *Organizational Culture and Leadership*. San Francisco, CA: Jossey-Bass, 2004.

[277] J. J. van Muijen *et al.*, "Organizational Culture: The Focus Questionnaire," *Eur. J. Work Organ. Psychol.*, vol. 8, no. 4, pp. 551–568, Dec. 1999.

[278] K. Huang and K. Pearlson, "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture," presented at the Hawaii International Conference on System Sciences, 2019.

[279] K. Huang and K. Pearlson, "Profiling the Organizational Cybersecurity Culture: Toward a Cybersecurity Culture Framework." 24-Jan-2018.

[280] L. Tabansky and I. Ben Israel, *Cybersecurity in Israel*. Cham: Springer International Publishing, 2015.

[281] B. D. Adams, C. Flear, T. E. Taylor, and C. D. Hall, "Review of Interorganizational Trust Models," Humansystems Incorporated, Guelph, ON, Jun. 2010.

[282] A. Zaheer and J. Harris, "Interorganizational Trust," in *Handbook of Strategic Alliances*, 2455 Teller Road, Thousand Oaks, CA: SAGE Publications, Inc., 2006, pp. 169–198.

[283] M. E. Graebner, F. Lumineau, and D. Fudge Kamal, "Unrequited: Asymmetry in Interorganizational Trust," *Strateg. Organ.*, p. 26, Nov. 2018.

[284] A. Zaheer, B. McEvily, and V. Perrone, "Does Trust Matter? Exploring the Effects of Interorganizational and Interpersonal Trust on Performance," *Organ. Sci.*, vol. 9, no. 2, pp. 141–159, Apr. 1998.

[285] C. Moorman, R. Deshpande, and G. Zaltman, "Factors Affecting Trust in Market Research Relationships," *J. Mark.*, vol. 57, no. 1, p. 81, Jan. 1993.

[286] B. L. Connelly, T. R. Crook, J. G. Combs, D. J. Ketchen, and H. Aguinis, "Competence- and Integrity-Based Trust in Interorganizational Relationships: Which Matters More?," *J. Manag.*, vol. 44, no. 3, pp. 919–945, Mar. 2018.

[287] A. C. Inkpen and S. C. Currall, "The Coevolution of Trust, Control, and Learning in Joint Ventures," *Organ. Sci.*, vol. 15, no. 5, pp. 586–599, Oct. 2004.

[288] "National Infrastructure Protection Plan Sector Partnership Model." [Online]. Available: https://emilms.fema.gov/IS0913a/groups/488.html. [Accessed: 30-May-2019].

[289] Jorge. Hernandez-Ardieta, J. Tapiador, and G. Suarez-Tangil, "Information Sharing Models for Cooperative Cyber Defence," in *2013 5th International Conference on Cyber Conflict*, Tallinn, Estonia, 2013, p. 28.

[290] P. Koepke, "Cybersecurity Information Sharing Incentives and Barriers," Cybersecurity at MIT Sloan, Cambridge, MA, Working Paper CISL# 2017-13, Jun. 2017.

[291] J. Korte, "Mitigating cyber risks through information sharing," *J. Paym. Strategy Syst.*, vol. 11, no. 3, pp. 203–214, Jul. 2017.

[292] C. McCarthy, K. Harnett, A. Carter, and C. Hatipoglu, "Assessment of the Information Sharing and Analysis Center Model," National Highway Traffic Safety Administration, Washington, DC, DOT HS 812 076, Oct. 2014.

[293] “Developing a Community Cyber Security Incident Response Capability,” in *2009 42nd Hawaii International Conference on System Sciences*, Waikoloa, Hawaii, USA, 2009, pp. 1–9.

[294] “Cyber Storm III Final Report,” United States. Department of Homeland Security, Jul. 2011.

[295] “Cyber Storm V: After Action Report,” United States. Department of Homeland Security, Jul. 2016.

[296] “Cybersecurity Insurance,” *Department of Homeland Security*, 22-Jun-2015. [Online]. Available: https://www.dhs.gov/cisa/cybersecurity-insurance. [Accessed: 13-Jun-2019].

[297] R. Bohme and G. Schwartz, “Modeling Cyber-Insurance: Towards A Unifying Framework,” presented at the Workshop on the Economics of Information Security, 2010, p. 36.

[298] “Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues,” United States. Department of Homeland Security. National Protection and Programs Directorate, Insurance Industry Working Session Readout Report, Jul. 2014.