ABSTRACT

Title of Dissertation:	ISSUES MANAGEMENT OF COMPOUNDING WICKED PROBLEMS BY CRITICAL INFRASTRUCTURE UTILITIES: CYBERSECURITY AND COVID-19
	Gareth Thomas Williams, Doctor of Philosophy, 2022
Dissertation directed by:	Associate Professor Erich Sommerfeldt, Department of Communication

"Wicked problems" present issues managers in public relations with complex challenges and no definitive resolutions. Multiple concurrent wicked problems may compound these challenges. This study extends understanding of how issues managers address compounding wicked problems with a multiple-case study. The multiple-case study focuses on the experiences of issues managers at public cooperative electric distribution utilities and includes interviews with issues management personnel at multiple levels of oversight and influence, including regional, national, and federal organizations. Interviews with issues managers explore strategies for identifying and addressing wicked problems and reactions to messaging from other organizations. Examination of publicly available organizational communications and media triangulate conclusions. This study illustrated that compounding wicked problems require issues management, issues managers do not

directly address the wicked problem(s), education alone or enforced by policy did not produce lasting changes in behavior advocated to publics, that study of compounding problems requires the problems also have common publics; and issues management by critical infrastructure seeks cocreation. Specific observations include that cultivated networks of communication improved perceptions of legitimacy in sources of information and guidance, attempts to convey legitimacy from the cultivated network to other publics were not successful, utilities were subject to and responded to power imposed upon them by state authorities, and that utilities relied heavily on establishing organizational legitimacy with member/owner publics when communicating about changes resulting from external influences of either legitimacy or power. In addition, this study illustrated that resilience is the overwhelming priority of critical infrastructure utilities when responding to wicked problems, and both supply chain and utility personnel play indispensable roles in organizational resilience. This study extends existing issues management literature of critical infrastructure utilities, which are currently under-represented in issues management literature.

ISSUES MANAGEMENT OF COMPOUNDING WICKED PROBLEMS BY CRITICAL INFRASTRUCTURE UTILITIES: CYBERSECURITY AND COVID-19

by

Gareth Thomas Williams

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2022

Advisory Committee:
Associate Professor Erich Sommerfeldt, Chair
Professor Jennifer Golbeck
Associate Professor Damien Pfister
Assistant Professor Catherine Knight Steele
Professor Emerita Elizabeth Toth

Dedication

For Amy, Catrin, and Hannah: Thank you for your love, patience, sacrifice, and support in making this dream come true.

To Mom and Dad: Thank you for your faith in me and encouragement. Mom, your support helped me through the toughest times. Dad, you were and continue to be an inspiration in my academic career and personal life. I miss you.

Acknowledgements

Dr. Erich Sommerfeldt: Thank you for all your guidance, counsel, and encouragement over the past six years. It is not hyperbole to say that you have shaped me as a scholar more than anyone else. I am honored to have worked with you, and grateful for your generosity in time and collaboration. Your scholarship and dedication to the field have been an inspiration and a goal toward which I have striven and continue to strive.

To the members of my committee: Thank you for the time you spent considering my exams, prospectus, and dissertation, as well as the numerous amendments to the dissertation. I have always felt supported by you and have appreciated your encouragement.

- Dr. Elizabeth Toth: Your seminar was engaging and enlightening and enhanced my enthusiasm for scholarship in the field of public relations. It was an honor to study with you. Thank you for all the time you took to review my writing with care, and your insightful comments that improved my subsequent work.
- Dr. Damien Pfister: Your seminar opened entire areas of theory that I continue to explore today. I appreciate all the time you took for hallway conversations, as I'm sure my nascent enthusiasm dug into your time for other obligations.
- Dr. Catherine Knight Steele: Thank you for welcoming me to the department and encouraging my enthusiasm in digital humanities. One of my very few regrets at Maryland is that I never had the opportunity to take

a seminar of yours. You are an inspiring scholar, and I am grateful to have had your input on my work.

- Dr. Jen Golbeck: Thank you for being willing to serve on my committee. I was introduced to your work in the first seminar for digital humanities, and your class on social media analysis was inspiring. I am grateful for your input at many stages of my time at Maryland.

To the 15 participants in this study: Thank you for taking the time to discuss your experiences with me. You showed faith in me in being willing to discuss some difficult and sensitive topics, and I hope that you find this document valuable. I learned so much during the course of our interviews and came away from our conversations inspired by your work and overwhelmed by your generosity of time and forthright discussion of your perspectives. I literally could not have done this without you, and your input is what makes this document insightful and valuable.

Table of Contents

Table of Tables

Chapter 1: Introduction

"Wicked problems" are intractable social dilemmas (Rittel & Webber, 1973). Wicked problems are not solvable in the conventional sense and are often defined through their nature and the priority of the need(s) to be addressed (Rittel & Webber, 1973; Roper & Hurst, 2019). Comprehensive definition of a wicked problem requires definition of all possible attendant solutions, which include conflicting social influences and societal priorities (Rittel & Webber, 1973). Proposed solutions to wicked problems must consider compounding "social, political, psychological and economic factors" (Willis, 2016, p. 308). While wicked problems offer no discrete solution, better understanding of them and of their nature improves the ability to parse the available means to address the challenges they produce (Peters, 2017).

Public relations practitioners and issues managers address wicked problems (Willis, 2016). The public relations issues management function is responsible for engaging publics in discourse about an organization's stance on a wicked problem and influencing the societal approach to that problem (Coombs & Holladay, 2012). Because actions seeking to address wicked problems will be incomplete (i.e., not a solution, *per se*) and involve additional consequences, addressing wicked problems requires reciprocal relationships to iterate and verify what are the best acceptable impacts and consequences (Roper & Hurst, 2019). This collective decision-making demands public relations practitioners within organizations establish collaborative engagements with publics and engage in symmetrical problem solving (Willis et al., 2018). Organizational efforts to

address wicked problems benefit from these ongoing collaborations with key publics (Roper & Hurst, 2019; Willis, 2016; Willis et al., 2018).

Two wicked problems currently faced by public relations practitioners are the COVID-19 pandemic and cybersecurity (Cohen & Cromwell, 2020; Kerr & Glantz, 2020; Malone & Malone, 2013; Singer & Friedman, 2014). These two wicked problems mutually compound: cybersecurity presents additional problems in addressing the pandemic, and the pandemic complicates efforts to maintain or improve cybersecurity (Khan et al., 2020; Naidoo, 2020). Examining how public relations practitioners as issues managers approach mutually compounding wicked problems extends wicked problems literature and expands the issues management literature on cybersecurity and the COVID-19 pandemic. This study improves issues managers' understanding of effective means to approach wicked problems and academic understanding of the role of public relations in defining and prioritizing issues attending wicked problems. This study will also explore how simultaneous and compounding wicked problems affect organizational strategy or publics' understanding of and attendance to the problems.

Public Relations as Issues Management

The public relations function builds relationships with key stakeholders and publics (Grunig, 2009). By the mid-20th century, public relations scholarship recognized the profession's persuasive influence on society in its molding of both the attitudes of publics to the organization's needs and projecting an image of the organization fitting the publics' expectations (Bernays, 1952). Since the 1950s, public relations has played an increasingly significant role in the formation of

public opinion and influence of public dialogue (Ramsey, 2016). Relationships with multiple publics necessitate the curation of multiple organizational identities to address the priorities or power of each public (Coombs & Holladay, 2012). Public relations scholarship addresses monitoring of environmental issues, strategic planning to address those issues, and managing public opinion regarding societal expectations and policies that could affect an organization's operations (Heath & Palenchar, 2008).

The issues management function of public relations includes organizational management and communicative roles and responsibilities. Issues management evolved in business and industrial organizational communication beginning in the late 19th century and was further developed following the engagement of communication specialists by commercial and industrial management in the early to mid-20th century (Heath & Palenchar, 2008, p. 6). As the "strategic core" of public relations, issues management addresses "political, health, risk, and crisis" issues (Botan & Taylor, 2004, p. 654). Public relations and its issues management function can be undertaken by any organization, including corporations, activist groups, and NGOs (Smith & Ferguson, 2010) as well as governments and affiliated organizations (Wu & Yang, 2017). Issue management communications, as a conduit for organizational management, can help "bring order and control to uncertainty," affording public relations a socially beneficial role amplified by the challenges posed by wicked problems (Heath, 2006, p. 100). Issues managers—those involved in conducting organizational issues management—necessarily include public relations practitioners but may

also include organizational leadership and other personnel who contribute to "...an organization's efforts to monitor its environment, analyze potential threats and opportunities, and communicate with publics about disputes or matters of public contention" (Sommerfeldt & Yang, 2017, p. 831).

Society is open to definition by all who participate (and communicate) in it (Carey, 2009). Organizations engaging in issues management must recognize ethical impacts of their advocacy at local, national, and global levels of influence (Kent et al., 2011). Affording voice to dominant and marginalized groups alike allows public relations to enhance pluralism and inclusiveness in deliberative democracy (Edwards, 2016). While public relations scholarship has considered how many types of public and private sector organizations collaborate to influence society, consideration of critical infrastructure organizations—upon which rests the stability and function of society—are notably absent.

Issues Management and Critical Infrastructure

Public relations issues management literature addresses commercial and industrial corporations (Heath & Palenchar, 2008; Jaques, 2006; Smith & Ferguson, 2013; Veil et al., 2015), activist and nonprofit groups (Jaques, 2006; Kim & Dutta, 2009; Smith & Ferguson, 2013; Sommerfeldt, 2013; Sommerfeldt & Xu, 2014; Sommerfeldt & Yang, 2017; Veil et al., 2015), public sector organizations (Gelders & Ihlen, 2010), administrative officials and programs (Waymer & Heath, 2016), and—in one of the original examples of issues management in the United States—willingness of the nation's citizens to go to war (Bernays, 1952; Ewen, 1996). The critical infrastructure sector is notably

absent from existing issues management literature. Critical infrastructure organizations in the United States, and those comprising the electric distribution "grid" in particular, afford unique insights for public relations.

The electric grid is a foundation upon which societal expectations are built. It is subject to influences from public and private sectors in the form of suppliers and vendors as well as regulatory and funding agencies. Its services touch virtually every citizen in the United States as well as regions of Canada and Mexico (Cohn, 2017; Hughes, 1983; U.S. Department of Energy, 2020). Linking the virtual and physical worlds and connecting across national and international boundaries, the U.S. grid is in constant communication in a global environment (Mattioli, 2014).

Critical infrastructure utilities straddle the boundary of public and private sector organizations. The electricity generation and distribution industry, in particular, accounts for "five percent of the U.S. economy, but the *first* five percent" (American Public Power Association, 2017), due to the salient fact that virtually all other aspects of contemporary U.S. society (e.g., banking, fuel distribution, water distribution, food distribution) depend upon a reliable supply of power. Of this massive system, the major networked interconnections—commonly referred to simply as "the grid"—comprise the delicate and essential machine upon which American society rests (Cohn, 2017). Because of the foundational role of the grid in the United States, energy distribution utilities answer to publics at all levels of government, all social and economic spectra, and across commercial industries and national boundaries. Suppliers and vendors are

as essential to its services as its services are essential to other critical infrastructures.

Critical infrastructure utilities offer public relations scholars many insights into issues management. Technologies are often perceived as neutral tools of society, but infrastructure embeds social and political power as well as economic forces (Parks & Starosielski, 2015); "binding nuclei" that can shape infrastructure with decidedly partisan ends (Hughes, 1983). Infrastructure is often layers of cutting-edge technologies and relics of the past; contested space and manifestations of past social movements (Farman, 2018). Critical infrastructure evolves through the joint efforts of multiple private sector companies and public agencies. Myriad participants in society have, over decades upon decades, contested the meaning of, need for, and evolution of sprawling networks of technologies that support our society.

Public Relations and Pandemics

Public relations plays an essential function in pandemic response (Aylesworth-Spink, 2017). Viruses are not perceptible to human faculties, and so only gain an identity in the eye of publics through their definition and identification as the cause of disease by medical experts, doctors, health communicators, and media (Aylesworth-Spink, 2017). Communications must convey the challenges presented by the pandemic accurately as well as the attendant needs to address it. Communications that do not accurately present the dangers and necessary steps to address the pandemic—either that exaggerate or

downplay the threat(s)—are likely to lose public confidence and willingness to take necessary steps to stem the pandemic (Muzzatti, 2005).

The COVID-19 pandemic has impacted all sectors of economies throughout the world. The economic impact has been likened to that of World War II and produced an unprecedented peacetime medical crisis (Nicola et al., 2020). School closures affected an estimated 900 million students worldwide, approximately 93% of all students (Nicola et al., 2020). Nearly 50% of the U.S. workforce shifted to some degree of remote operation, and 61% of 1,500 hiring managers surveyed expected the significant increase in remote work to continue on an ongoing basis after the pandemic (Ozimek, 2020). Countries experiencing partial to total "lock down" reported corresponding 18% to 25% decreases in energy consumption and 50% to 75% decreases in traffic (International Energy Agency, 2020). These changes in patterns of energy demand challenge electric distribution utilities, and common tactics for increasing personnel safety such as telecommuting are not applicable to many utility personnel.

The COVID-19 pandemic has presented new challenges for public relations practitioners. Rapidly developing and shifting news cycles have challenged management of publics' expectations (Knowles, 2020). Publics have been overwhelmed by the news cycles and resisted messaging due to confusing messages or messaging fatigue, unsure of what information to trust or believe (Levitt, 2020). Despite these challenges, public relations has played and will continue to play an increasingly important role in connecting organizational C-

suites with publics, increasing internal public relations, and linking organizations in business-to-business messaging and strategy (Strong, 2020).

Purpose of the Dissertation

This study builds upon previous issues management literature by: (1) extending wicked problems literature to how issues managers address compounding wicked problems, and (2) incorporating how critical infrastructure organizations engage in issues management.

Compounding Wicked Problems Afford New Insights

Existing literature that studies wicked problems has established the nature of wicked problems, difficulties organizations face in addressing such problems or defining subsections of a problem to address, and difficulties organizations face communicating those needs and strategies to publics. However, the existing literature does not appear to consider how organizations address simultaneous, compounding wicked problems and how conflicting strategies are weighed, communicated, and enacted. Organizational adaptations to the needs of the COVID-19 pandemic afford an opportunity to see how wicked problems compound and how organizations iterate and weigh actions with publics. Wicked problems defy easy solution (Coombs & Holladay, 2018; Rittel & Webber, 1973; Willis et al., 2018), and the threats attending the COVID-19 pandemic and cybersecurity have already challenged organizations to balance actions that may exacerbate the issues attending either or both wicked problems (Khan et al., 2020; Naidoo, 2020).

Electric distribution utilities are vulnerable to cyber attack, and the impacts of those attacks may extend throughout society and across international borders (Greenberg, 2019). Balancing the health of personnel with maintaining secure operations are compounding issues. Exploring how issues managers at public utilities have succeeded or struggled to balance these wicked problems will enrich the academic literature. This study will address the communication strategies employed by municipal utilities to address the compounding wicked problems of cybersecurity and the COVID-19 pandemic.

Wicked Problems are an Issues Management Challenge

Wicked problems require policy actions to mitigate their effects (Rittel & Webber, 1973), deliberative engagement with multiple publics to draw on diverse expertise (Rittel & Webber, 1973; Roper & Hurst, 2019; Willis, 2016; Willis et al., 2018), and long-term/future-focused planning (Peters, 2017; Rittel & Webber, 1973; Roper & Hurst, 2019; Willis, 2016). These strategic management processes require action in advance of any crisis and extend throughout a strategic planning cycle. By engaging diverse publics in the construction of solutions to wicked problems, public relations can improve relationships with publics and facilitate action and investment by publics "…who might otherwise feel disconnected, disillusioned, or disempowered by government or organizational action," (Roper & Hurst, 2019, p. 7).

Wicked problems share some qualities with crises, including the potential to impact an organization negatively, the definition of the problem and its relevance to the organization being in the hands of publics, and needs to manage

information about and influence interpretations of the event before, during, and after the response (Coombs, 2010). Crises require strategic planning, response, and recovery integrated with issue and risk management (Jaques, 2007), as do wicked problems.

Wicked problems differ from crises in that wicked problems have no clear definition, finite conclusion, or "correct" solution (Peters, 2017), while crises present a defined conflict in society or against the organization that might be controlled (Heath & Palenchar, 2008). Because wicked problems have no definitive formulation or solution (Willis et al., 2018), control by an organization is unlikely if not impossible. Crises may be a subset of a wicked problem, for instance the outbreak of COVID-19 at the White House would be a crisis that precipitated from the wicked problem of the COVID-19 pandemic.

Existing public relations literature addresses cybersecurity from a crisis management perspective (Kim & Lee, 2018; Wang & Park, 2017). Unlike crisis communication, an issues management approach holds the possibility of avoiding future incidents by helping the organization identify ways to evolve over time to improve the effectiveness of its actions (Hade & Meisenbach, 2012). Approaching cybersecurity from an issues management perspective is appropriate due to the interconnections between organizational networks and the Internet; a threat on the Internet is inherently an organizational network security concern (Brooks et al., 2018), and those concerns must be managed to avoid or recover from crises. Because cybersecurity of critical infrastructure involves interaction between utilities and regulatory agencies, among other agencies, determination of what is a

priority to an organization is not entirely to its own discretion, as it might be in a risk management approach, and choosing the means to manage risk and mitigate threat are often debated through potential policy and regulatory action (or actions to avoid them) (Singer & Friedman, 2014).

Electric utilities are important for cybersecurity studies. Utilities and grid facilities have increasingly been the subject of evolving, sophisticated cyber threats (Greenberg, 2019). Larger networks inherently entail greater security issues (Singer & Friedman, 2014), and the U.S. grid is itself a massive network, connecting in some way virtually every person living in the United States (Cohn, 2017).

Critical infrastructure, particularly electric utilities, have been the focus of cybersecurity-specific legislation (Kuehn & Mueller, 2014), providing subject-specific policy to contextualize organizational communication and strategies as well as perceptions of publics. Examination of cybersecurity-related interaction of utilities—themselves a mix of public and for-profit entities (i.e., investor-owned utilities or IOUs)—with private sector vendors, suppliers, and customers as well as public sector regulators and funding agencies mirrors the current conventional wisdom that cybersecurity is an inherently public-private enterprise (Eichensehr, 2017; Giacomello, 2014).

Critical Infrastructure is Under-Represented in Issues Management Literature

Studies of issues management have focused on executive government public affairs or public diplomacy (Dutta-Bergman, 2006; el-Nawawy, 2006; Wu & Yang, 2017), activist and NGO advocacy (Coombs & Holladay, 2012; Jaques,

2006; Sommerfeldt, 2013), and corporate organizations (Grunig, 2009; Smith & Ferguson, 2013). Critical infrastructure organizations such as utilities are notably absent from existing literature. Recent cyber attacks have proven that multiple international actors possess the power to cripple or weaponize electric distribution infrastructure, and that multiple agencies within the United States have been compromised by these same attacks (American Public Power Association, 2019; Greenberg, 2019). Ransomware attacks have proven the vulnerability of public authorities (KETV, 2018), and weaponized malware has been found in grid systems, though not yet activated (Greenberg, 2019).

This study used established techniques to investigate issues management practices by electric utilities, expanding the issues management literature into a previously under-investigated—but inarguably critical—sector of society. Expanding academic investigation of infrastructural organizations responds to the call for increased consideration of social and relational roles of technology in public relations (Kent & Saffer, 2014) and enhances understanding of how power is manifested in societal structures that are often assumed to be neutral by the powerful or dominant members of society (Kim & Dutta, 2009). In addition, this study extends the previous issues management literature addressing cultural construction and leveraging of power among publics, use of technology in communication, and social and relational roles of technology in communication.

By exploring influence among infrastructure utilities; their vendors and suppliers; regulatory and oversight agencies; municipal, state, and federal governments; and publics—including the utilities' customers—this study

improves understanding about how power is "perceived, used and shared among publics," (Vardeman-Winter et al., 2013, p. 298). By examining responses to organizational communication and the nature of cybersecurity preparation and response, this study also extends the literature on how technology is leveraged for communication, coordination, and community-building (Sommerfeldt, 2013; Sommerfeldt et al., 2012). Better understanding of the role of technology and the presence and leveraging of power may also improve ethical decision-making by issue managers and public relations practitioners (Place, 2010).

Wicked problems demand a "…collective, discursive, reflective, iterative, problem-focused, and action-orientated form of stakeholder engagement, which requires power and decision-making to be dispersed among the participants…" (Willis et al., 2018, p. 394). Power and legitimacy are the core of the concerns of issues management (Heath & Palenchar, 2008). Power and agency are inherent forces in the interactions among organizations in the hierarchy of public organizations, from national agencies to local governance and service. Legitimacy—of the organization and its perspective on and proposed solution(s) to an issue—is critical for acceptance of messaging and authority by internal or external publics (Coombs & Holladay, 2018). In studies of wicked problems, resilience is often the key desired outcome, since resolution of the problem is not tenable (Willis, 2016). Resilience is a central concern for utilities.

Preview

This multiple-case study examines how communication and management personnel of public electric utilities in the United States communicate with

publics, including relevant federal agencies, industry associations, and vendors about compounding issues of the COVID-19 pandemic and cybersecurity. The study used three sets of data to produce a view of how issues managers perceive and enact their role and develop strategies to address the compounding wicked problems of cybersecurity and the COVID-19 pandemic, as well as the resulting communications and impact thereof: (1) semi-structured interviews with issues managers at public utilities and a trade association; (2) semi-structured interviews with issues managers at collaborating organizations who aid or oversee their efforts to adapt operations to COVID-19 while maintaining cybersecurity; and (3) publicly available organizational communications from utilities and collaborating organizations that address cybersecurity and shifts in operations to adapt to COVID-19. The use of qualitative methods for studying these infrastructure organizations aligns with existing studies of infrastructure (Parks & Starosielski, 2015).

The data collected comprise a multiple-case study, using the member utilities of one trade association as the core focus with data from joint-action agencies (JAAs) and a cooperative utility in another region as comparator case studies. The aggregation of interviews with the trade association and its member utilities and interviews with utilities outside the trade association improves validity through theoretical replication (Miles, Huberman, & Saldana, 2014; Yin, 2018).

Interviews engaged executive, information technology, and outreach communications personnel at electric utilities that are members of the trade

association as well as other utilities throughout the country, and personnel concerned with utility cybersecurity and integration of new communicative technologies at related federal executive agencies and national advocacy agencies. These interviews discerned participant perceptions of the issues attending the COVID-19 pandemic cybersecurity, how they strategically prioritized those issues, and their strategies and processes to communicate those needs to publics. The interviews also interrogated reception of and reaction to communications from other relevant organizations. Purposive and snowball sampling connected communicators and interlocutors at other organizations—legislative, regulatory, peer utilities, vendors, etc.— to explore the influence and power between the organizations, effectiveness or lack thereof of messaging, and how different organizations identify priorities and prioritize responses.

Review of publicly available organizational communications complemented the interviews as a means of reviewing the manifestation of the asserted strategies. While the interviews explored the effects of communication and message strategy among designers and recipients of messages, the communications review provided insight to the resulting messaging and media chosen. The trade association received messaging content and strategies from national-level organizations and provided materials to member utilities. Studying how each member used and augmented the provided materials illustrates differing strategies as well as resources among the utilities. Data gathered from the interviews with utilities, organizations that influence utilities, and organizational communications triangulates the communicative environment and interpretations

by the various interlocutory organizations. This research extends insight beyond understanding what the public relations practitioners and issue managers intended to do or what they think happened by seeking the aggregation of influences to the final public communications.

Wicked problems challenge issues management. Compounding wicked problems further compound organizational strategy. The COVID-19 pandemic presents many novel challenges as organizations adapt business strategies to protect the health of personnel. These same strategies, however, may compound cybersecurity. Cybersecurity and COVID-19 are critical concerns for public utilities and understanding the utilities' approach to prioritizing and communicating about these simultaneous wicked problems extends the public relations literature on issues management and wicked problems. By exploring the lived experiences of communication and management personnel at utilities, interlocutors in government agencies, and coordinating nonprofit associations, this study expands the issues management literature into a previously under-examined but critical sector of U.S. society. This study also extends the nascent literature on organizational responses to COVID-19 and expands the literature on wicked problems in general and cybersecurity, specifically.

Chapter 2: Literature Review

How do issues managers address compounding wicked problems? Wicked problems defy easy resolution and manifest at the confluence of conflicting social priorities or between social and technological issues (Rittel & Webber, 1973). Wicked problems are the product of complicated and embedded social forces, and as a result they defy easy or complete solutions. In addition, any proposed action to mitigate effects of a wicked problem is often limited to an individual, targeted effect and not the source of the problem or other precipitating effects. Issues managers are challenged by wicked problems and seek to identify, understand, and address social, political, technological, and other influences that may impact their organization's operation. Public relations plays a key role in addressing wicked problems by aligning the needs and expectations of multiple internal and external stakeholders and publics with the means available to mitigate or minimize the impacts of these complex problems.

This study examines how issues managers at public electric utilities communicate with stakeholders and publics to devise practices that balance workplace safety and increasing desire for remote work with maintaining informational security and business operations. Understanding how organizations balance the need to distribute their workforce geographically with maintaining cybersecurity can extend understanding of how issues managers use public relations techniques to address compounding wicked problems. Examining critical infrastructure organizations' approach to cybersecurity expands the

literature in two areas that are under-studied in the public relations and issues management literature: cybersecurity and critical infrastructure organizations.

The following literature review first defines wicked problems within the existing literature and then asserts the role of issues managers and public relations as the functions within an organization responsible for addressing wicked problems. The cited literature establishes cybersecurity and the COVID-19 pandemic as wicked problems, and public relations issues management as the place of cocreation with publics that is essential to effective issues management of wicked problems. From a management perspective, issues management is a strategic planning process, in contrast to the iterative nature of problem solving necessary for wicked problems. Finally, relevant literature affirms that both critical infrastructure and cybersecurity are topics lacking in the current issues management literature and affirms the electric utility as a suitable exemplar of critical infrastructure organizations confronting compounding wicked problems.

"Wicked Problems" Are Strategic Challenges that Defy Definitive Solution

The public relations literature addressing "wicked problems" includes work by a handful of theorists, including Capizzo (2019; Capizzo & Sommerfeldt, 2021), Coombs and Holliday (2012), Roper and Hurst (2019), and Willis (2016; Willis et al., 2018). Wicked problems are social issues for which: (1) there is no clear resolution, (2) stakeholders participate in the definition of the problem and identification of the preferred "solution," which may address symptoms[1] of but

[1] Discussion of wicked problems in the document uses "symptoms," following the example of Kent, et al., (2011) to indicate challenges that precipitate from a wicked problem as either an issue or a crisis. Symptoms are the issues and crises to which issues managers respond. In this study, no issues manager responded directly to the root cause(s) of a wicked problem.

not root causes of a wicked problem, (3) all solutions are attended by consequences, and (4) solutions tend to be "good enough" rather than optimal (Roper & Hurst, 2019, p. 3). Unlike technical problems with identifiable solutions, a wicked problem provides no discrete solution, and devising a plan of action depends upon the framing of the aspect of the problem an organization seeks to address (Rittel & Webber, 1973).

Wicked problems were originally considered in the context of planning public policy, and include issues such as climate change, poverty, crime, health care, and other issues of inequality and social support (Peters, 2017). Because the causes and effects of wicked problems are complex, so too are the solutions inherently incomplete in addressing the cause(s) and the effect(s). Iteration of desired courses of action in response to a wicked problem often demands identifying the most desired outcome—which symptoms of the problem does a course of action seek to address (Kent, et al., 2011)—acknowledging that other factors may not be addressed, and additional compounding effects may precipitate (Rittel & Webber, 1973). The end of a project seeking to address wicked problems is most often defined by the end of the program rather than the resolution of the problem; for instance, due to cessation of funding or termination of the program (Rittel & Webber, 1973).

Addressing wicked problems requires social iteration among a group of publics to parse diverse priorities, obligations, and objectives (Willis, 2016). Social processes interact with technical processes, and it is in the former that complex solutions stymie the apparently simple solutions for the latter (Rittel &

Webber, 1973). In the United States, challenges addressing wicked problems stem from American valuation of pluralistic collaboration and collective construction of social priorities: "in a pluralistic society there is nothing like the undisputable public good…policies that respond to social problems cannot be meaningfully correct or false; and it makes no sense to talk about 'optimal solutions' to social problems," (Rittel & Webber, 1973, p. 155). Societal pluralism complicates the process of identifying and prioritizing actions to mitigate the effects of wicked problems, due to the multiplicity of opinions and priorities among the stakeholders and publics.

Wicked problems manifest "at the juncture where goal-formulation, problem-definition and equity issues meet," (Rittel & Webber, 1973 p. 156). The first two of these three facets are elements of strategic planning, and public relations is essential to aligning organizational strategic planning with societal expectations (Grunig, 2006; Grunig & Grunig, 2000). To ensure that the proposed solution provides an acceptable (if incomplete) result and that attendant effects are also acceptable, public relations' role in generating dialogue with stakeholders and supporting dialogue in a deliberative function is necessary for effective organizational response to a wicked problem (Willis, 2016). Such deliberative engagement of multiple and diverse stakeholders in decision making is distinct from strategies and solutions devised and implemented by experts or people in positions of privilege (Willis et al., 2018), underscoring the necessity of a pluralistic pursuit to addressing wicked problems.

Cybersecurity is a Wicked Problem

Cyber attacks are wicked problems. Cyber attacks are a constantly evolving threat stemming from many different motivations; they shift to exploit different weaknesses as prior vulnerabilities are addressed; and even if an organization perceives itself as having "resolved" the issue, actions by activist publics (e.g., malicious hackers) can redefine the issue by identifying a different type of exploit or desired end to an attack, perpetuating the issue and casting doubt on the legitimacy of the organization's position on the issue and its solution (Coombs & Holladay, 2018). As cybercrime and cyberwar have proliferated, the prior conventional wisdom morphed from there being "…two types of organizations: those who have suffered a cyber attack and those who have not," to "…those that have suffered a cyber attack and those that don't know they have," (May, 2017).

Breaches may be caused by any number of factors, including out-of-date software, malware built into systems and software, user error or compromise, and deliberate malicious action, among many others (Greenberg, 2019; Singer & Friedman, 2014). In addition, the nature of cybersecurity problems as temporarily resolvable but never unequivocally solved is the nature of a wicked problem (Rittel & Webber, 1973). All of these potential causes of a breach are manifestations of related issues and compounding problems (see "Cybersecurity and COVID-19 are Mutually Compounding Wicked Problems" for further discussion of how wicked problems compound).

The forces behind cyber attacks and the strategies and tactics to counter them and increase cybersecurity stem from a "complex cocktail of social, political, psychological and economic factors which generate difficult questions for those seeking to address them," (Willis, 2016, p. 308). Means of addressing cybersecurity likewise align with the characteristics of a wicked problem in that "resolution often depends on a change of mindset and behavior by the stakeholders involved," (Willis, 2016, p. 308). In addition to wicked problems presented by cyber threats, increasing connectivity is attended by demands that organizations be ready to respond to a wider range of publics and/or a broader array of other social media managers who may not accept or may seek to influence organizational issues management discourse (Coombs & Holladay, 2018).

Despite having historically been viewed as a technical challenge, cybersecurity is a human challenge: humans are behind the technology on both sides of the cyber event (Greenberg, 2019; Singer & Friedman, 2014). People and their interactions with information technologies are increasingly realized as being as critical—or even more critical—to cybersecurity than technical solutions (May, 2017). Some degree of social engineering is attributable to more than 80% of breaches (Hadnagy, 2018). The human and technical interaction and interrelation, as well as the scope of cybersecurity spanning public and private sectors and touching all technology users, renders cybersecurity a complex sociopolitical issue with no easy solutions—a "wicked problem," (Roper & Hurst, 2019; Singer & Friedman, 2014).

Recent work discussing cybersecurity underscores the need for skills beyond technical approaches to improve system security, including strategic planning and persuasive communications to increase potential for cultural changes and behavioral adaptations by system users (Hamburg & Grosch, 2018; Muncaster, 2020; Plyler, 2020). The intangible, virtual (as opposed to physical), and technological nature of cyber attacks makes them difficult challenges for many publics to understand and requires social and technical tools to address (de Bruijn & Janssen, 2017). Prior efforts by scientists, technology developers, and policymakers to convey the nature and importance of cybersecurity have largely resulted in lack of public understanding of the criticality and scope of the threat (de Bruijn & Janssen, 2017). Effective framing of the complex and confusing dimensions and interactions within cybersecurity is necessary to broaden and strengthen public apprehension of the threats and necessary actions to stem cyber threats (de Bruijn & Janssen, 2017). Framing of such challenges and recontextualizing publics' existing understanding to meet new and evolving challenges is a core function of issues management public relations (Heath & Palenchar, 2008).

Public relations literature addressing cybersecurity has employed Situational Crisis Communication Theory (Kim & Lee, 2018; Wang & Park, 2017). While this approach provides insight into how an organization responded to a particular breach, it leaves out the overall strategy developed by an organization to address the threat and other issues impelling the need for cybersecurity. Approaching cybersecurity from an issues management of wicked

problems perspective opens both the timeline and scope of material to consider. This expanded scope includes relevant strategies to prevent incidents, improve systems, increase resilience, and monitor threats; protocols to respond to an incident and repair public perception of the organization; and sharing of lessons learned and best practices as well as mutual aid agreements and other resilience measures.

The COVID-19 Pandemic is a Wicked Problem

COVID-19 is a wicked problem (Cohen & Cromwell, 2020; Kerr & Glantz, 2020; Moon, 2020; Sahin et al., 2020). Conflicting priorities of "protecting lives versus preserving livelihoods" present governments, businesses, and other organizations with difficult decisions of what risks to assume in a response strategy (Cohen & Cromwell, 2020, p. 1). Governments have weighed actions that may reduce the spread of the pandemic against expected economic impacts (Sahin et al., 2020). The more effective responses to the pandemic have highlighted the role of public relations to communicate needs, build trust, and align public behaviors with necessary actions (Moon, 2020).

Effective government response to the COVID-19 pandemic has demanded an adaptive, flexible approach with transparent messaging (Moon, 2020; Sahin et al., 2020). South Korea's comparatively effective response to COVID-19 demonstrated the essential need to resolve conflicts between science and policy, and the value of public relations in addressing wicked problems by communicating transparently with publics and using new technologies effectively to keep publics informed (Moon, 2020). Transparent communications from the

government bolstered public trust in government programs and increased participation in mitigation programs while minimizing the impacts of misinformation. Long-term adaptation of the types of behavioral changes necessary to curtail a pandemic must overcome both public complacency and lack of confidence in prescribed measures (Sahin et al., 2020). In other nations, citizens of Canada, Germany, and the Netherlands have an overwhelmingly positive view of their government's response, while public opinion in countries that have struggled with responses like Spain and the United Kingdom is split close to evenly between positive and negative views of government efforts (Gramlich, 2020).

Public opinion of government efforts in the United States is also split close to equally between favorable and unfavorable, reflecting the lack of unified federal response in controlling the virus and conflicting messages from government authorities and fragmented responses by states and within states (Gramlich, 2020). By March 13, 2020, all states had declared a state of emergency, but that was the final time the country demonstrated any strategic alignment regarding the pandemic, and states quickly began to open again (Kaiser Family Foundation, 2020). Response and messaging from the federal government has been politicized and is viewed very differently across partisan divides, though public perception of local health providers is positive (Gramlich, 2020). Fragmented messaging and response tactics further complicate the "wickedness" of the pandemic, as potentially effective strategies may be rendered ineffective by resurgences in less diligent neighboring locales or states, virus variants producing

different threats, and the inability or an unwillingness by leaders to unite citizens with a common perception and understanding of the virus. The issues attending COVID-19 have been politicized, changing the dynamic of what should have been a public health issue. Changing approaches to provision of information from one presidential administration to another compounded public trust in what information exists, the completeness of information available, and the motivations behind what information is available and its attendant messaging (Golbeck, 2018).

Research from recent pandemics has set the stage for research on COVID-19. The 2003–2004 SARS epidemic affirmed that publics reacted more to media narrative than organizational messaging, and that media can amplify or undermine an organization's preferred narrative regarding public health measures (Berry et al., 2007; Lewison, 2008). Media narratives may veer from medically verified data and subsequently incite greater public concern than is proportionate (Muzzatti, 2005). The SARS pandemic also illustrated that, while medical developments likely rendered pandemics less of a health threat than they historically had been, the attending economic impacts have significantly increased (Smith, 2006).

Communicating about the pandemic would be a significant challenge simply based on its scale and reach. However, conflicting messaging from government and health agencies, politicization of the pandemic, and the intangible nature of the virus itself (i.e., "visible" only after its impacts have manifested) have impeded coherent framing of the pandemic and the attendant needs to address it. Since there are few universally accepted core issues in the pandemic,

messaging about necessary steps to adapt operations to the pandemic have had little in the way of common frameworks upon which to build.

Cybersecurity and COVID-19 are Mutually Compounding Wicked Problems

Solutions to wicked problems may compound other wicked problems, which may be further exacerbated by difficulty in assessing the effectiveness of solutions or anticipating precipitating effects, which can generate novel wicked problems (Willis, 2016). That any one problem may be symptoms of other problems is a characteristic of wicked problems (Willis, 2016). Some studies have already examined the compounding effects of the COVID-19 pandemic and other wicked problems, including the digital divide with school-age students (Seymour et al., 2020), chronic disease and low-income regions (Melaku et al., 2020), and food systems security and agribusiness (Heck et al., 2020). Cybersecurity is another wicked problem compounded by the COVID-19 pandemic, and which itself compounds strategies to mitigate the pandemic.

One prominent and nearly immediate impact of the COVID-19 pandemic was a sudden and massive increase in telecommuting (Khan et al., 2020; Naidoo, 2020). The abrupt move to telecommuting brought attendant increases in concerns for information security and opportunities for cyber attack (Khan et al., 2020). Home networks and networked devices afford ample opportunities for compromise, and education of necessary precautions has been lacking (Naidoo, 2020). In addition to technological weaknesses, cybercriminals have exploited human behavior indirectly (e.g., through people's tendency to adhere to routine)

and directly (e.g., through social engineering) to gain information for a cyber attack (Naidoo, 2020).

Increasing frequency of cyber attacks has complicated organizations' (private and public sector alike) ability to fully embrace telecommuting while maintaining information and network security (Khan et al., 2020; Naidoo, 2020). Further adaptation of corporate and industrial workforces to increased remote work demands a combination of effective arguments for the need for remote capacity and the ability to maintain productive and effective work in remote capacities, and education of the steps necessary to maintain informational and operational security in these remote environments. Issue managers play a key role in making these arguments and designing and launching the attendant educational efforts.

The sudden and massive increase in telework is a compounded issue for utilities, in assuring the safety of their own personnel and in maintaining reliable service for customers. Increased telecommuting changed demand patterns by customer publics, requiring adaptation by the utility. Internally, remote work entails additional access to command-and-control systems that may compromise an organization's information security and poses a greater risk than utilities may be willing to take, particularly in the wake of recent cyber intrusions and disruptions by foreign powers (Greenberg, 2019). Minimizing risk to organizational personnel while maintaining operations and efficiency demands careful consideration of how operations may embrace a more distanced workforce without sacrificing productivity, and/or how to maintain critical on-site personnel

while minimizing their risk of infection. For utilities, key publics in addressing these issues include organizational personnel, regulatory agencies who may be concerned about employee safety, and oversight agencies and customer publics whose primary concern is reliable energy supply (American Public Power Association, 2014). Managing cybersecurity and adapting operations to COVID-19 are each distinct wicked problems that demand management of many complex and contradicting issues, and strategies to address either compound the ability to address the other through conflicting needs.

Issues Management and Wicked Problems

The public relations issues management function addresses wicked problems (Coombs & Holladay, 2018; Willis, 2016). Issues management is the "strategic core" of public relations (Botan & Taylor, 2004, p. 654). It entails "the management of organizational and community resources to advance organizational and community interests and rights by striking a mutual balance with [publics]," (Heath & Palenchar, 2008, p. 15). As such, issues management demands communication and collaboration with publics. By explicitly or implicitly collaborating with publics to identify and define issues that impact the organization, public relations issues management relies on a spectrum of relations and means of sustaining relationships with publics.

Public relations practitioners cultivate and manage mutually influential relationships between organizations and publics (Coombs & Holladay, 2012; Edwards, 2016). Dewey (1927) famously defined publics as groups of people united to act in response to a particular cause or issue. The term "publics"

recognizes the plurality of priorities and needs that defy a generic approach to messaging and interactions (Bernays, 1928). Two more recent conceptions better serve this study, reflecting a fluid and iterative nature of publics: "publics are a continuing process of agreeing on an interpretation because whether a group of people understands that it shares an interest at a particular time determines whether a public exists," (Botan & Taylor, 2004, p. 655); "Publics are not mere rational actors…Rather, they are constantly projecting a vision of what the social world looks like that is infinitely contestable, revisable, and negotiable—that is the core activity of publics," (Pfister, 2018, p. 15).

Public Relations Cultivates Relationships

Public relations arguably arose from corporate responses to activist critiques of corporate activities. As activists challenged corporate practices, corporations countered with their own messaging that addressed or defused activist concerns (Coombs & Holladay, 2012). Public relations helps align the interests and aspirations of diverse groups and organizations within a society for the collective benefit (Bernays, 1952) by fostering dialogue that builds shared meaning upon which ideas can be measured and iterated in the construction of a mutually beneficial society (Taylor, 2011). Iteration of messages and meaning among the members of a community increases the "…sense of community through the shared narratives which supply people with knowable and collective ways to act toward organizations and one another," (Heath, 2009, p. 40). While the strategy behind the message is the organization's, the perception of the

message's credibility and acceptance of the message is up to the audience—the meaning of the message is cocreated.

Collaboration with publics to address issues and work in a collective interest is the aspirational heart of public relations issues management (Grunig, 2000). Effective issues management must facilitate participation by different groups and types of discourses in pursuit of a mutually beneficial outcome of a public debate (Wu & Yang, 2017). In managing wicked problems, the complexity of the issue and the broad swath of publics affected demands collaborative relationships and engagement of many publics in identifying and devising the desired solutions.

Issues Management is a Function of Public Relations. A primary public relations function is building relationships with key stakeholders and publics (Grunig, 2009). Stakeholders are people who are impacted by an organization's decisions; publics are those who become aware of these impacts and may seek to influence the organization (Grunig & Grunig, 2000). Issues management includes but also extends beyond previous concepts of organization-public relationship building (Heath & Palenchar, 2008).

Issues management as we now define it has been a concern of public relations practitioners and scholars since the earliest days of the field, as they sought to identify societal challenges, perceptions, and constructs that facilitated or impeded organizational strategy and subsequently influenced public expectations of the society in which they and the organization co-existed (Bernays, 1952; Ferguson, 1984; Heath et al., 2013). The 1970s saw the formal

articulation of issues management as an area of focus for public relations, initially defined within corporate communications as a proactive response to perceived threats from public perceptions and sentiment (Botan & Taylor, 2004; Jaques, 2012; Madden, 2012). By the mid-1980s, evolution in the perception of issues management embraced a strategic approach to policy issues that could include the corporation taking steps to influence public perception, as well as reacting to forces of public opinion (Crable & Vibbert, 1985). Reaction to influence on public opinion gave rise to the concept of issues management as a cocreational endeavor, which dominated through the 1990s (Botan & Taylor, 2004; Grunig, 1992).

Scholars in the late 1990s and early 2000s affirmed issues management as a strategic planning and management process at the core of public relations and centered in relationship building (Botan & Taylor, 2004; Broom et al., 1997; Grunig & Huang, 2000). The concepts of dialogue, cocreation, and degrees of symmetry remained prominent in issues management literature through the present day (Botan, 2018; Grunig, 2009; Heath & Palenchar, 2008; Sommerfeldt & Yang, 2017). By the mid-2000s, a strategic view of issues management included consideration of risk and crisis communication within an iterative cycle of research, planning, and communication (Jaques, 2007). Other scholars delved into ethical dimensions of issues management (Place, 2010) and preconceptions of issue motivators (Madden, 2012).

Public Relations Issues Management and Wicked Problems. Willis (Willis, 2016; Willis et al., 2018), Capizzo (2019), and Coombs and Halladay

(2018) account for the bulk of public relations issues management literature addressing wicked problems. In this case, "issues" refers to controversies or points of debate between and organization and publics: "differences of opinion regarding fact, value, or policy, the resolution of which has consequences for the organization's strategic plan and future success or failure," (Heath & Palenchar, 2008, p. 93). Social and policy issues tend to be inherently "wicked" (Rittel & Webber, 1973). Issues may be motivated by concerns including security, equity, fairness, and community values (Madden, 2019), and are frequently intractable (Capizzo, 2019). Issue management is not "how to manage an issue but how to manage *because* of an issue," (Jaques, 2010, p. 440).

Internal or external publics' perception of the issue may also render them "wicked," as publics question the legitimacy of the organizational action or in other ways perpetuate the issue (Coombs & Holladay, 2018). Addressing a wicked problem requires an organization "harness the intellectual assets of its employees" (Willis, 2016, p. 308). Strategic communication by management to organizational personnel is an internal public relations function (McCown, 2007). Therefore, an organization must consider internal public relations issue management before turning its focus to external publics.

In the contexts of both internal and external public relations, cocreational dialogue with stakeholders is essential for devising a best available solution and ensuring the resilience of the organization (Willis, 2016). Public relations' role in deliberative iteration of solutions is essential when addressing wicked problems, to ensure inclusion by "individual citizens, community groups, and service users,"

as well as management and experts (Willis et al., 2018, p. 383). Wicked problems, therefore, support public relations' role as a management function and societal boundary spanner (Willis, 2016), and exemplifies the co-creative nature of issues by relying upon active engagement of relevant stakeholders (Willis et al., 2018).

Internal public relations is one challenge organizations in this study must overcome. Electric utilities have historically been siloed between operations technology (OT) and information technology (IT) (Kavanaugh, 2019; Zimmerman, 2014). While integration of the two has increased over past years with wider adoption of smart grid technology, microgrids, and other distributed generation and advanced metering, additional integration is necessary to meet contemporary challenges, including cybersecurity (Kavanaugh, 2019). For government agencies, inspectors general from across government identified cybersecurity as one of four overarching concerns in effective response to the COVID-19 pandemic (Pandemic Response Accountability Committee, 2020). This includes ensuring secure information technology resources for telework and countering the spike in fraud and cybercrime that followed the onset of the pandemic in early 2020.

Effective external public relations to address the nexus of COVID-19 and cybersecurity for municipal utilities requires coordination, communication, and collaboration between the utilities and the relevant government agencies (e.g., energy and oversight agencies at state and federal levels of government), national associations (e.g., American Public Power Association, National Rural Electric Cooperative Association), local and national media, technology and software

vendors, and hardware and materials suppliers. Effective framing of the issues encountered and persuasion as to the best strategies for addressing the greatest needs is essential for educating publics and improving adoption of the needed behaviors. Framing intangible threats is a historic problem for both cybersecurity and pandemic viruses (Aylesworth-Spink, 2017; de Bruijn & Janssen, 2017).

Encouraging publics to participate in defining and implementing solutions to address problems may spur emergent creativity, which allows publics to apply existing resources to new and emerging problems (Cohen & Cromwell, 2020). Such problem solving could build on the concept of "humble intelligence," identified as a means by which public relations can engage stakeholders in effective collaboration to address wicked problems (Willis, 2016). Embracing a "…collective, discursive, reflective, iterative, problem focused, and action-orientated form of stakeholder engagement," empowers stakeholders and publics and simultaneously increases the pool of expertise working to address a problem and broadens the organizations network of communications and influence (Willis et al., 2018, p. 394).

Issues Management is a Public Relations Strategic Planning Process

Issues management is a strategic management approach to communication that comprises strategic and long-term planning, media relations and monitoring, relational advocacy, and relationship building (Wu & Yang, 2017). Issues management communications include risk and crisis communication and management, corporate social responsibility, and engagement of publics in cocreative decision making (Heath & Palenchar, 2008, p. 5). Strategic public

relations balances the aspirations of an organization's strategic plan (e.g., mission, vision) with constraints inherent to the operating environment (e.g., conflicting priorities and perceptions by publics) (Grunig & Grunig, 2000). Institutionalization of public relations as a strategic management function can improve an organization's ability to cultivate relationships with publics and ensure ethical organizational operations (Grunig, 2006).

Effective issues management demands strategic planning and action to address the underlying societal causes of an issue, rather than its symptoms (Kent, et al., 2011). Strategic planning seeks to understand what forces may threaten or benefit an organization and to devise a detailed, achievable plan for the organization to respond to these environmental conditions to realize a goal or long-term vision (Allison & Kaye, 2005; Bryson, 2018; Nutt & Backoff, 1992). An organization's strategic planning must account for the priorities and perceptions of the publics, so as to not compound existing issues with consequences that may in turn generate new issues. Such awareness and balance demand effective issues management public relations (Grunig & Grunig, 2000). Public relations practitioners can take a lead role in organizational strategic operations and realize greater potential for boundary spanning by employing issues management as a long-range strategy rather than means for short-term prediction (Kent, et al., 2011).

Issues management includes both strategic and tactical elements, requiring "effective mechanisms for information to be translated into action," (Jaques, 2010, p. 443). A comprehensive public relations issues management program will

include identification of measurable strategic objectives and planning, implementation, and evaluation of communication programs aligned with those objectives (Grunig & Grunig, 2000). Embedding issues management as part of the spectrum of activities that include crisis and risk communication and management provides an organization the necessary tools to identify, prepare for, respond to, and recover from potential problems (Jaques, 2010).

Public Relations Issues Management Addresses Legitimacy and Power

At the core of issues management is a "clash" of legitimacy and power, central themes that permeate the issues management literature (Heath & Palenchar, 2008, p. 10). Addressing wicked problems demands organizational understanding of and influence upon societal expectations, and willingness to deliberate on solutions (Willis et al., 2018). For the past century, scholars and practitioners have debated the roles played by public relations in shaping society and how public opinion and organizational strategic management co-create society. Many scholars cite a positive influence that public relations can have on society: In an ideal, ethical, application, public relations can serve as "…a constructive steward of, as well as benefactor of democracy," (Heath et al., 2013, p. 278).

Issues Management Builds Organizational Legitimacy. Legitimacy is an essential quality in issues management (Heath & Palenchar, 2008; Sommerfeldt & Xu, 2014). Issues are socially constructed and therefore perception of the legitimacy of an issue or position toward that issue is also socially constructed (Madden, 2019). Effective issues management requires

publics perceive an issue as legitimate, the organization as a legitimate authority on the issue, and the organization's approach to the issue as legitimate (Coombs & Holladay, 2018; Smith & Ferguson, 2010). By conveying this tripartite legitimacy, organizations use issues management to influence public opinion—or policymakers' perception of public opinion—regarding social issues or policy decisions to influence social and political perceptions of concern to the organization (Edwards, 2016; Heath & Palenchar, 2008; Jaques, 2006).

Organizations can leverage legitimacy cultivated through issues management relationships (Coombs & Holladay, 2015). When advocating for policy, organizations communicate with audiences to achieve strategic goals as well as to maintain their legitimacy (Heath & Palenchar, 2008). Issue managers, either organizational or activist publics, exert influence over prospective solutions by seeking to impose their definition of the issue: "There is power in definitions and by controlling the definition of the issue, issues managers gain an advantage in the process." (Coombs & Holladay, 2018, p. 83). Publics generally perceive organizations as able to influence the direction of issues (Coombs & Holladay, 2018).

Legitimate advocacy hinges upon classic elements of rhetoric, including the ethics and logic of the speaker, as well as commonly recognized qualities for ethical public relations such as symmetrical communication—the aggregation of these factors enhances an organization's ability to influence society (Edwards, 2018). Advocacy communications between an organization and its publics include power as a relevant influence inherent to both parties within their societal context

(Vardeman-Winter, 2016). An organization's social or political means to address an issue includes the potential for discourse to seek to legitimize or delegitimize parties and for policy or social norms to repress publics (Madden, 2019; Smith & Ferguson, 2013). The success of interrelated strategy and communications in issues management depends upon the legitimacy of the organization, which may bolster or undercut power an organization has cultivated and its means for leveraging that power (Sommerfeldt, 2013).

Issues management is cocreative. Publics ultimately determine whether they perceive the organization's legitimacy and power sufficient to accept the proposed solution(s). However, cocreation may manifest in differing degrees among different manners of publics. Consider the continuum of advocacy to negotiated compromise to accommodation (Weaver, Motion, & Roper, 2006): while some organizational interactions may be highly collaborative, others may employ significant degrees of advocacy to a point approaching propaganda (Welch, 2013). Welch (2013) distinguishes propaganda and education broadly as efforts to limit a perspectives and perceptions versus efforts to expand knowledge through new information. This does not make the communication inherently unethical, however; in highly specialized disciplines, it may be necessary for experts to assert a best course of action, and for the public to accept this opinion.

Public relations practitioners define and delineate organizational and public identities as well as accepted knowledge that influences the attendant relationships between organizations and publics (Weaver, Motion, & Roper, 2006). In these fora, a new definition of public relations emerges: "the strategic

attempt to control the agenda of public discussion and the terms in which the discussion takes place," (Weaver, Motion, & Roper, 2006, p. 17). Public relations practitioners must not only inform and persuade publics of the legitimacy of their position, but counter competing claims that may have entirely different political or social ends.

Foucault's (1980) definition of power in relationships used both hierarchies and clusters of relations (Weaver, Motion, & Roper, 2006), much as we see in the policymaking and oversight structure influencing municipal utilities. "Truth and power, therefore, are inextricably linked and serve to reinforce one another," (Weaver, Motion, & Roper, 2006, p. 19). As with propaganda and persuasion, power is not inherently a negative influence in society. Power holds the potential to be as beneficial as it may be destructive, and to correct for societal misconceptions or poor impulses as much as it may indulge the worst impulses of those in possession of it (Weaver, Motion, & Roper, 2006). A power uniformly held by publics is the ability to accept or reject the legitimacy of messaging based on "…whether or not a discourse resonates with their individual or collective subjectivities and perceptions of reality" (Weaver, Motion, & Roper, 2006, p. 20).

Success of corporate public relations in the 20th century is evident in the conflation of the public benefit with economic and corporate benefits (Weaver, Motion, & Roper, 2006). For instance, perception of indicators such as the stock market instead of the unemployment rate to reflect the strength of the economy. In the 21st century, the post-truth environment leaves the meaning (or existence) of cyber threats, their actors, the coronavirus, and government and societal

responsibilities for anti-viral measures bitterly contested. Public relations plays a central role in defining and iterating the constitution of social and political structures and interactions with a goal of reaching not an ultimate "truth," but a relative truth accepted as a "…means of legitimizing, or normalizing, material processes," (Weaver, Motion, & Roper, 2006, p. 19).

Relationships between organizations and publics are complex, affected by dynamics beyond influences isolated to either individual party (Heath, 2013b). As early as 1928, Bernays identified interlocking economic, social, religious, cultural, racial, and other groups—networks of social alignment and shared priorities; he later affirmed this notion: "The web of communications, sometimes duplicating, crisscrossing, and overlapping, is a condition of fact, not theory" (Bernays, 1952, p. 158). Heath (2013b, p. 427) echoes these interlaced interactions that manifest in society: "…organizations have relationships with one another as well as all of the constellations of stakeholder/stake seeker combinations that make up the relevant fabric (network complexity and political economy) of society." News media can frame an issue differently from an organization's preferred narrative and shift the perception by publics (Berry et al., 2007). Organizations wield power by leveraging the legitimacy cultivated through issues management relationships with publics to define the issues and the nature of the problems to be addressed (Coombs & Holladay, 2015). Focus on the relationship itself rather than the organization or imposed labels upon associated parties is in line with previous public relations scholarship (Ferguson, 1984). Exploring the nature of relational interaction independent of imposed identities

and within the guise of "patterns of linkages" builds within existing public relations theory (Broom et al., 1997).

Investigation of Publics' Perceptions Improves Issues Management Scholarship

Issues are not defined solely by an organization or the public relations issues managers therein. Effective management of issues requires understanding the publics affected by an issue and their perspective of the organizations' relevance to and addressing of the issue (Veil et al., 2015). Even though public relations scholarship espouses these ideals, analyses of practice show a disconnect between theoretical cocreation and actual practice (Erzikova & Bowen, 2019; Kim & Dutta, 2009; Roper & Hurst, 2019). While techniques of public relations may align with theoretical best practices, results may differ from those desired if issues managers fail to account for the ability of other participants in a network to influence meaning and perception of issues (Aylesworth-Spink 2017).

Effective issues management entails four components, all of which demand engagement with publics: "systematic issue identification, proactive actions, issues monitoring, and dialogic issue communication," (Heath & Palenchar, 2008; Wu & Yang, 2017, p. 346). Issue identification includes consideration of the publics' perspectives of the issue and means of resolution, and direct engagement with publics improves the organization's ability to target actions and messages to the most effective strategies (Veil et al., 2015). Proactive issues management to identify nascent issues before they reach crisis status demands direct engagement with publics throughout and following the process to address the issue; issues may appear to be resolved only to recur later at the

detriment of the organization (Veil et al., 2015). Monitoring includes review of media to gauge public opinion and response to organizational actions and communication (Aylesworth-Spink, 2017; Wu & Yang, 2017). Dialogic issue communication entails the "claims and counter claims about the legitimate locus of policy decision making...in issue management discourse," (Smith & Ferguson, 2013). Each of these facets theoretically demands direct engagement with publics to discern their perspectives and priorities, define the issue(s), assert legitimacy of positions and solutions, and collaborate as issues emerge and evolve.

Direct engagement with practitioners and publics highlights the nature of intersections and evolution of the issue, including whether the practitioners espoused "...proactive and interactive issues and risk management...in an objective and strategic manner, as opposed to personal opinion, selfishness, and reactive strategies," (Erzikova & Bowen, 2019, p. 7). Such investigation will render the actual actions public relations practitioners undertook and the results and perceptions of those actions by publics, rather than what practitioners perceive themselves as having done. In the case of municipal utilities, it is all the more important to engage directly with publics to discern the effectiveness or lack thereof in communications: "public authorities need to be aware of how best to communicate with the public so that people can exercise appropriate choices and have confidence that matters are under control," (Lewison, 2008, p. 241). Governmental and intergovernmental authorities may hold even more persuasive power than scientific or mass media outlets (Lewison, 2008).

Issues Management Literature Has Overlooked Infrastructure Studies

Studies of issues management have focused on executive government public affairs or public diplomacy (Dutta-Bergman, 2006; el-Nawawy, 2006; Wu & Yang, 2017), activist and NGO advocacy (Coombs & Holladay, 2012; Jaques, 2006; Sommerfeldt, 2013), corporate organizational communications (Grunig, 2009; Smith & Ferguson, 2013), or refer to organizational issues management generally without delineating a societal sector (Madden, 2019; Place, 2010). Infrastructural organizations such as utilities are notably absent.

Infrastructure is created by the intermingling of social and organizational operations with technical systems over long periods of time (Bowker et al., 2010). Infrastructure can be defined as "*pervasive enabling resources in network form*…both static and dynamic elements, each equally important to ensure a functioning system," (emphasis in original; Bowker et al., 2010, pp. 98–99). Studying infrastructure requires consideration of more than the physical plant of technologies, due to the influence of social and organizational dynamics that led their creation (Bowker et al., 2010). Infrastructures are created when organizations resolve "the tension between local and global" (Star & Ruhleder, 1996, p. 114), reflecting the societies in which they developed (Bowker et al., 2010; Cohn, 2017).

Infrastructure Manifests Social and Political Forces

Critical infrastructure policy is developed through multiple levels of government oversight and inter- and intra-industry collaboration and mutual aid. Actions to protect critical infrastructure must address the identified risks and be

applied to uniformly minimize weaknesses. This renders development of policies and solutions to address wicked problems beyond the purview of individual utilities, and limits or eliminates the prospect of cocreation with customer publics.

Infrastructural organizations and their attendant "sociotechnical systems…are not autonomous," and a researcher must "acknowledge the fact that [sociotechnical] systems are evolving cultural artifacts rather than isolated technologies," (Hughes, 1983, p. 465). Utilities are subject to federal and state regulatory agencies and legislatures, industry oversight groups, and expectations and mutual agreements with peer organizations. In addition, they must balance the needs of customers, abilities of suppliers, limitations in engineering, and overlaps and interdependencies with other, otherwise unrelated infrastructures and utilities. Cooperative utilities face additional pressure as nonprofit organizations and accountability to their customers who are also their owners.

Recent cyber attacks targeting electric distribution utilities in Ukraine and the United States (among other countries), and cascading impacts that paralyzed global shipping and shut down hospitals (among other collateral effects), have illustrated both how essential electric service is to modern American society and the vulnerability of that infrastructure to malicious actors (Greenberg, 2019; Singer & Friedman, 2014). Understanding society demands apprehension of the technologies it employs, as those technologies are extensions of the society itself (Castells, 2000, p. 5). The emphasis on individual freedom, networked relationships, and rapid technological evolution espoused in modern online interaction reflect the sociopolitical climate and ideals of cultural shifts in the

United States (Castells, 2000). Rapidly evolving technologies highlight the need to examine interrelationships between people and technical systems (Bratton, 2015).

Approaching communication from an infrastructural disposition expands the scope of analysis to address the material forms and physical media supporting the distribution of communications (Parks & Starosielski, 2015, p. 5). Infrastructure studies consider physical, technological, and human components in socially influential networks, and the role of society in defining and employing these technologies (Cohn, 2017; Parks & Starosielski, 2015). This focus on materiality bridges studies of communication with technical fields and demands consideration of evolving technologies and devices (Parks & Starosielski, 2015, p. 5). Nonhuman participation in networks can impact the network dynamics as much as human: "Technology interacts with institutions and ideology to shape how we make meaning, how we organize our affairs across economic, political, and personal domains, and how we make culture and identity," (Benkler, Faris, and Roberts, 2018, p. 381). Just as the technology may shape the society in which it is applied as the technology evolves through its application, so too might the society shape the evolution of the technology (Hughes, 1983).

Issues Management Shaped the U.S. Electric Grid

The electric distribution "grid" in the United States manifests issues management. The grid as we know it today is an amalgam of invention, gumption and creativity, economic forces, political and social forces, and geography, among many other physical and cultural, human and nonhuman influences (Hughes,

1983). The grid functions as part of a social network that extends beyond utilities and customers, and includes regulatory agencies, funding agencies, suppliers and vendors, and many others upon whom the operation of the grid depends (Hughes, 2012). Examination of the U.S. electric grid must consider human participants and the ways in which they identify and resolve conflicts and competing priorities as well as the evolution of the physical and technological structures as they are influenced by and subsequently influence society and policies (Cohn, 2017; Hughes, 1983).

Deliberative collaboration with publics, advocacy, expertise, and economics all contributed to the infrastructure we know in 2022, with social and political power as the dominant dynamic: "The issue of control was central to [the evolution of the grid]," (Cohn, 2017, p. 223). Organizations spanning public and private sectors and stakeholders at all levels of society have contested the shape and scope of the grid. The construction of the largest technological system in history was not a singular effort but undertaken by a "fragmented industry" that "negotiated the technical and social terms of operation through the informal alliances of a fraternity of experts," (Cohn, 2017, p. 223).

The grid is a series of four linked interconnections overseen by eight electricity distribution reliability councils (Cohn, 2017). From the late 19th century, these interconnections have balanced both technological and financial priorities as electricity providers strove for reliability as well as profitability. Reliability is an essential issue for electricity distribution: by 1897, public perception of access to electric power had already shifted from a luxury

commodity to a service, such that a company manager noted: “shutting down of a line is something almost criminal,” (Cohn, 2017, p. 26).

Advocacy for interconnection also focused on efficiency and reduction of waste in response to growing conservationist concerns in the U.S. public discourse at the time (Cohn, 2017). This rhetorical emphasis was reflected in the language of industry journals, adding the benefits of preservation of natural resources and reduced fuel consumption, pollution, and waste to the previous focus on costs and required investments (Cohn, 2017). Despite the public appeal of this conservationist messaging, improved generation and distribution *increased* consumption of electricity, bolstering the business and bottom lines of investor-owned utilties and public utilities alike: “Whether owned by investors or local government, power companies were in the business to sell electricity,” (Cohn, 2017, p. 37).

The resulting electric grid is a network of networks: command-and-control and communication networks within utilities; communication and mutual aid networks between utilities; communications to and from vendors and suppliers; communications and other interactions with executive, regulatory, and oversight agencies, including policy and regulatory actions; and communications with customers. Evolution of the grid and challenges in technological deployment frequently resulted from non-technical issues, including “institutional and value conflicts,” (Hughes, 1983, p. 462).

Debate—ethical and not—has shaped the grid since the earliest days of electrification in the United States beginning with “publicity contests” between

Edison and Westinghouse advocating for direct or alternating current, respectively (Cohn, 2017, p. 17). These debates comprise "…one private enterprise's endeavor, through political power and legislation, to outlaw the technical advantage of another," (Hughes, 1983, p. 107). Power and influence are also imposed on the industry, as policy and regulation are prominent concerns for electric infrastructures: 2017 alone saw 288 policy deployments across 39 states and the District of Columbia related to grid modernization, resource planning, infrastructure planning, and technology development and deployment (U.S. Department of Energy, 2018).

By the early 20th century, utility personnel shared knowledge "deliberately and widely" (Cohn, 2017, p. 28). Information sharing and the need for common standards to make interconnections feasible sped the evolution and voluntary adoption of standards that allowed interconnections between distribution networks—voluntary rather than state-mandated standards distinguished the evolution of the U.S. grid from contemporaries in European countries (Cohn, 2017). Aspirations for a national-scale, interconnected energy distribution system were articulated by 1911 (Cohn, 2017). Utilities collaboratively iterated standards necessary to facilitate transcontinental interconnection, perceiving imposed regulations as likely to stifle innovation (Cohn, 2017). Such early collaboration among utility professionals cultivated a strong sense of community among the industry professionals: "The grid only works because autonomous operators voluntarily adopted standards practices and equipment for certain key control activities," (Cohn, 2017, p. 31).

Cooperative Utilities Overcame Obstacles for Rural Members. Rural communities were under-served by investor-owned utilties, and debate began in the 1920s as to the role the government should play in ensuring rural electrification (Hughes, 1983). While electric service was increasingly seen as a necessary service rather than a luxury, the cost of extending distribution to rural farms was high, leading to arguments of whether the farm or the utility should absorb the additional cost (Hughes, 1983). The conflicting priorities of the scientific foundation of engineering, the social policy of politics, and the economic drives of a for-profit industry are reflected in a 1925 address by Charles Penrose: "…engineers [have] the responsibility of informing the public about sound policy in order to save it from the reckless ventures of politicians and other laymen treading on the engineers' ground," (Hughes, 1983, p. 309).

Introduced as an executive order in 1935 and formalized by Congress in 1936, the Rural Electrification Act authorized funds for public sector utilities to expand distribution of electricity to communities not served by existing IOUs. Despite widespread protest from IOUs of federal involvement in development of the nation's generation, transmission, and distribution resources, New Deal projects greatly expanded capacity and ensured interconnection with previously unserved rural communities by providing resources for the development of cooperatives (Cohn, 2017).

Communication Networks Facilitate Grid Operation. Communications networks are essential to reliable and secure operations by utilities, including IT, OT, and internal and external communications (Artz, 2020). Dedicated phone

lines linking generation and transmission facilities date to 1904 (Cohn, 2017). As the modern energy distribution system evolved, electrical engineers and utility personnel cultivated a lexicon that at once allowed efficient reference to equipment and processes and demanded specialized knowledge to apprehend (Cohn, 2017). This specialized lexicon may impede coordination with other sectors and communication with publics (including academic study), because such specialization can produce a high-context culture, which reduces comprehension or impedes participation by those not familiar with the culture (Steele, 2016).

Coordination of internal messaging, actions, and strategies complicates external messaging and coordination with other organizations. The "three legged stool" upon which successful grid operation relies includes asset owners and operators (i.e., the utilities), federal government agencies, and equipment suppliers (Artz, 2020). These interlocking networks of organizations, each of which is a network of communications themselves, requires effective intra-organizational and cross-sector communications to manage wicked problems. Recent issues management challenges have addressed controversies of "smart" grids, which apply distributed technologies to aid in load management, facilitate microgrids, and isolate necessary subsectors with embedded generation and ability to "island" or isolate when necessary (Cohn, 2017).

Research Questions

This study examined how issues managers prioritized and adapted to mutually compounding cybersecurity problems and challenges posed by the COVID-19 pandemic. To do so, this study engaged issues managers across

multiple strata of federal, state, and municipal policymaking and oversight of the operation of the U.S. electric grid, including public utilities, regulatory and oversight agencies, and industry associations. Interviews and textual analyses explored the meaning made of the threats and challenges utilities faced and how their place in the community, their responsibility to publics, and the limitations they faced shaped their response to those threats and challenges. Because legitimacy and power are the primary points of focus for issues management (Heath & Palenchar, 2008), examination of issues management must include how organizations define the issue, perceive and identify power, and frame their positions and strategies as legitimate in the context of those power dynamics.

Defining Issues in Compounding Problems

Wicked problems defy finite solutions, rendering linear approaches to strategic planning insufficient for producing desired outcomes. How do public utilities engage in agile, iterative strategic planning to adapt to shifting demands of wicked problems? How do compounding wicked problems change strategic management approaches? Since issues management is part of an organization's strategic planning process, novel issues management concerns demand evolution in an organization's strategic plan. This may include changes to operations, communications, priority publics, and issues management to influence policy, among others.

Cybersecurity has posed an ongoing technological and social challenge, demanding shifts in cultural practices and individual perceptions, and is an increasing concern for energy utilities (Greenberg, 2019; Singer & Friedman,

2014). Public utilities are particularly susceptible to cyber attack due to multiple interconnections with government agencies, vendors, and customers (American Public Power Association, 2019). As subsidiaries of local government agencies and subject to state and federal regulations and oversight, public utilities contend with numerous constraints not faced by investor-owned utilties (American Public Power Association, 2019). As the threat of cyber attack has increased, the abilities of malicious actors have also evolved through shared materials and state sponsorship (Singer & Friedman, 2014). As this threat evolves, many public utilities resist measures to improve cybersecurity, citing costs to customers, restricted budgets from local and state governments, and lack of investment by federal agencies (American Public Power Association, 2019). In addition, within public utilities, a lack of coordination and cooperation between administrative and operations personnel further bifurcates awareness and understanding.

COVID-19 has posed significant technological and social challenges and demanded increased telecommuting and shifting operational norms in many sectors in society. The challenges posed by COVID-19 in relation to public utilities are twofold: First, the utility must adapt its own operations, and distanced command-and-control functions are often not feasible due to the substantial risk posed by such connections. Second, changes in work patterns across the United States have shifted demand and load cycles, to which utilities must adapt. During the first six months of the COVID-19 pandemic, residential energy consumption in the United States increased by as much as 20%, while industrial consumption dropped by 6% (Elavarasan et al., 2020).

This study hinges on the interaction of two simultaneous and mutually compounding wicked problems. Few studies have undertaken this dynamic, and no issues management studies have done so explicitly. The value in this research is to see whether the multiple wicked problems exacerbate the "wickedness" or whether the inherent "wickedness" is not compoundable since each problem is already intractable. Does each become simply a factor in the other's intractability, or do they produce an interaction that demands previously unexamined issues management demands or tactics?

For public utilities, the demands posed by cybersecurity and the COVID-19 pandemic certainly appear to be mutually compounding: Increasing personnel safety by shifting to telework exacerbates cybersecurity. Already a prominent target for cyber attack, utilities do not have the capacity to shift many processes online and must adapt to the pandemic in ways particular to the needs of its operations. Exploring how the utility defines and legitimizes its position to publics who vary in the degree to which they understand the challenges of operating a utility will improve understanding of how issues managers address simultaneous, compounding wicked technical and social problems. Changes in the establishment of legitimacy and power or changes in the networks of interaction for each wicked problem to the compounded issues presented by the two wicked problems in concert may highlight a unique dynamic worthy of further investigation.

RQ_1: How do issues managers identify and prioritize compounding wicked challenges faced by public utilities in simultaneously addressing cybersecurity and the COVID-19 pandemic?

Legitimizing the Organization's Message with Publics

Legitimacy of the organization's approach to a wicked problem begins with its definition of the part of the problem to address (Heath & Palenchar, 2008; Roper & Hurst, 2019; Sommerfeldt & Xu, 2014). Because definition of a wicked problem is inherently imprecise, the organization must account for the reason it is defining a wicked problem in a particular way and why the aspect(s) of the wicked problem the solution seeks to address are the most advantageous at that time (Chrustie et al., 2010). Definition of the challenges to address in cybersecurity or the COVID-19 pandemic may differ between the organization and its publics, and the optimal means for addressing those challenges may be perceived very differently as well.

In the case of a public utility, the organization must define and legitimize its position to legislative and executive agencies, regulatory and oversight agencies, industry associations, and customers, among other publics. Competing priorities include a desire to maintain information security while minimizing costs to customers (and taxpayers, in the case of public utilities) while ensuring oversight agencies of due diligence. Perceptions of cyber risk, for instance, vary widely among public utilities and public sector agencies and associations, as well as the means by which to address risks or optimal levels of risk to assume. Understanding how different issues managers legitimize their stance to these

problems will afford insight to how issues managers address wicked technical and social problems.

RQ_{2a}: How do issues managers legitimize their definition of challenges, priorities, and strategies to address cybersecurity during COVID-19?

RQ_{2b}: How do issues managers perceive the legitimacy of other organizations' definitions of the compounding challenges, priorities, and strategies to address cybersecurity during COVID-19?

Identifying Power in Issues Management

Power is a central concern of issues management public relations (Sommerfeldt, 2013; Vardeman-Winter, 2016; Willis et al., 2018). Power can manifest in the organization's power over publics, and in publics' power over the organization. The power may be political, economic, or based on numerous other factors. Examining how issues managers prioritize and develop messages tailored to publics improves understanding of the power the organization perceives publics as holding.

Organizations participate in communicative networks, and those networks are tools of power (Heath, 2013a; Sommerfeldt & Kent, 2015). Organizational sovereignty—or lack thereof—may be dictated by the nature of the networks within which they operate. Influences may hold political power, as in governmental or regulatory agencies; social power, as in media and customer publics; or other forms of influence and power like peer agencies and vendors. Issue managers exert influence by imposing their definition of the issue and publics generally perceive organizations as able to influence the direction of

issues. Government agencies hold power including funding, regulatory oversight, standards of service, and personnel health protocols. Power from peer organizations could include best practices or breaches at peer utilities, interconnections and load sharing, and mutual aid agreements. Power from industry organizations can include collaborative agreements and information sharing. The degree of influence and the nature of influence of different publics may differ between issues of cybersecurity and issues of COVID-19 response.

Power manifests in many ways in the communicative networks of public power utilities. Cooperative utilities were first founded to overcome socioeconomic forces that left rural communities underserved by investor-owned utilties. Cooperative utilities are directly influenced by state regulatory agencies, trade associations, and their customers who are also their owners. The utility itself holds power as well, both literally and figuratively. Utilities are responsible for the provision of power to their customers and can restore or deny that power, they seek better ways to serve customers and improve their quality of life, and they control the ways in which their member/owners are able to interact with and influence the utility's operation. This study will improve understanding of how issues managers prioritize publics in light of the power they hold and how power is exerted among these interconnected organizations.

RQ$_{3a:}$: How do issues managers identify power held by other organizations and publics relevant to issues of cybersecurity and adaptations to COVID-19?

RQ$_{3b}$: How do issues managers exert power held by their organization regarding cybersecurity and adaptations to COVID-19?

Summary

This study builds upon previous issues management literature by: (1) extending wicked problems literature to how issues managers address compounding wicked problems, and (2) incorporating how critical infrastructure organizations engage in issues management. Wicked problems literature is extensive and well developed, but to-date appears to have taken wicked problems individually. As each wicked problem presents compound, intractable issues that defy definitive solution, situations with compounding wicked problems may present additional factors requiring consideration by issues managers. Since the solution to any subset of issues within a wicked problem may produce novel wicked problems, does a compounded wicked problem further inhibit effective response and mitigation? How are the problems prioritized when pursuing one solution may exacerbate another problem?

Examination of how organizations define issues regarding cybersecurity and the pandemic, how they perceive interactions among (and attendant imbalances in power between) organizations and publics, how the issues managers legitimize their organizations' perceptions of issues attending wicked problems to different publics, and how concurrent wicked problems present compounding issues improves understanding of the means by which organizations engage in issues management. This study explored the experiences of issues managers, information technology and operations personnel at utilities, and interlocutors in peer organizations as well as relevant commercial and advocacy organizations. Review of organizational media and communications regarding

cybersecurity and COVID-19 accompanied interview content to explore what was said as well as why it was said and what influences produced the communications. Analysis of the data highlights overarching narratives and interrogates the data to answer the RQs.

This study affords insights to academics and practitioners alike. The study of utility personnel perceptions and strategies along with their resulting communications informs understanding of internal logic and inclusion of contrasting perceptions and interpretations of communication from utilities by non-utility personnel explores effectiveness of external communications. This multilayered investigation seeks to improve how practitioners cocreate meaning with publics to “solve problems in their environments,” and improve “the ethical ability to promote good or social harmony,” (Toth, 2002, p. 248).

Chapter 3: Method

Wicked problems pose significant societal and organizational challenges. Multiple simultaneous wicked problems may produce compounding challenges for issues managers. The confluence of technical and social concerns with no finite solutions and conflicting priorities leaves issue managers in intractable quandaries. This project explored the experiences of issue managers seeking to moderate multiple simultaneous and mutually compounding wicked problems. Developing a deeper understanding of the perspective of public utility personnel can improve national efforts to engage public utilities in efforts to improve cybersecurity. By seeking to understand how issues managers create and recreate meaning of both cybersecurity and adaptations to the COVID-19 pandemic through social interactions, this study embraces an ethnomethodological structure (Hesse-Biber, 2017).

This study illustrates how issues managers throughout a range of federal, state, and municipal public-sector agencies and associations defined and communicated organizational strategic messages to manage compounding wicked problems and how cascading influences shaped public communications by utilities. This inquiry explores where cocreation of issues management occurs and where communications are asymmetric. Seeking the issues managers' own perspectives and allowing them to relate their experiences without prior imposition of assumed manners of collaboration or lack thereof seeks to minimize researcher bias. Review of publicly available utility communications provides insight into the priority given to the various issues encountered and afforded a

contrast in the issues utilities prioritized in communicating with publics versus those they discussed communicating about with oversight and industry advocacy organizations.

Design

This study employed multiple case studies in its examination of utility issues management. Case studies explore phenomena in context and in depth, and are improved by employing multiple media (Yin, 2018). The multiple-case study is a methodological variation on the (single) case study design that applies a common method of inquiry to multiple subjects to develop broader conclusions (Yin, 2018). In this project, multiple utilities within a single trade organization provide one multiple-case, and a participant utility that is a member of a different trade association in another state provides a different multiple-case comparator. Use of the multiple-case structure improves generalizability of emergent themes by highlighting those that recur in favor of those appearing in individual cases (Miles et al., 2014).

Infrastructure studies do not lend themselves to generalizability because the built environment, political landscape, community integration, and other factors faced by critical infrastructure utilities are unique to each case (Parks & Starosielski, 2015). Embracing the particularity of each participant's experience opens the possibility for unforeseen insights (Roulston, 2013). Approaching a multiple-case study with a goal of theoretical replication suits examining different outcomes and strategies from analogous scenarios (Yin, 2018).

Public utilities in general and cooperative utilities in particular vary greatly in geography, population, affluence, and proximity to major population centers, among other factors. Utilities with a few thousand meters located in an isolated, mountainous region face different challenges than those serving nearly 200,000 meters in mixed agricultural and exurban regions proximate to metropolitan centers. As such, identifying a single "critical," "revelatory" or "unusual" case from the spectrum of co-op utilities is difficult, and may not provide generalizable insight (Yin, 2018, p. 54). As one of the trade associations in this study mused: "If you've seen one electric co-op, you've seen one electric co-op." Multiple-case sampling improves the confidence in and robustness of the data by illustrating phenomena in multiple corresponding situations (Miles et al., 2014; Yin, 2018).

As a multiple-case study, this study engaged issues managers at public utilities and the organizations with which they interact to examine how issues managers at public utilities interpreted communications from oversight agencies and peers and how they communicated to their member/owner publics about compounding issues of the COVID-19 pandemic and cybersecurity. The core of the study are the member utilities of a multi-state trade association. These 15 member utilities range widely in scales of operation (e.g., from fewer than 15,000 to more than 100,000 customers) and socioeconomic demographics (e.g., densely populated urban areas to affluent suburbs to isolated rural areas). The trade association develops and distributes communications for member co-ops to unify messaging and policy. Differences in communication are seen in how utilities

apply communications from superior organizations and what communications they generate themselves. These differences afford insight to varying influence of state agencies across three states, a regional and national trade association common to all member utilities, and federal agencies common to all electric utilities nationwide.

A utility from a second trade association in a geographically distant part of the country provides a point of comparison as to what might be perceived as unusual or convention from the primary case trade organization. Two joint-action agencies (JAAs) in different regions of the country from the trade associations and their member co-ops provide insight into the experiences of the municipal public utility community, which are also public utilities but divisions of local and regional government as opposed to member-owned cooperatives. In addition, the study engaged with national organizations that influence both the trade associations and their member utilities, the JAAs interviewed, and with other public power utilities nationwide to contextualize the data in this study. The utilities, JAAs, and trade associations are subject to different state agencies and regulations, but all receive communication from the same national-level organizations.

Qualitative methods are appropriate for this study. Case studies ask “how and why” questions (e.g., how do issue managers identify and iterate understanding of wicked problems and why do they develop these strategies?) and focus on contemporary events without seeking to control or manipulate the experiences of the participants. The focus here is on meaning made and

subsequently conveyed by the participants—their personal experience and perceptions (Hesse-Biber, 2017; Tracy, 2013). A qualitative case study is the most appropriate method for "tracing operational processes over time," (Yin, 2018, p. 10), and seeking a holistic understanding of participant experiences and interpretations of phenomena, as well as the systems the influence understanding of these problems and prospective responses by institutions and organizations (Hesse-Biber, 2017; Miles et al., 2014; Yin, 2018).

Data Collection

The goal of this study is to understand "what's going on," and the meaning made by individuals of their culture, history, and place. As such, a qualitative approach—in this case semi-structured interviews and review of publicly available organizational communications—is appropriate (Hesse-Biber, 2017; Tracy, 2013). This research combined data from interviews, public communications, and archival records—all recognized media for case study evidence (Hesse-Biber, 2017). By employing publicly available communications as well as in-depth interviews, the study seeks to reinforce data credibility and transferability (Hesse-Biber, 2017).

The interviews highlight the types of information and the perceptions of that information among agencies from federal to utility level. Organizational communications gathered from websites include press releases, news articles, fact sheets, regional lifestyle magazines, and custom utility inserts developed for those magazines. These communications provide insight to what messages finally reached publics and to which publics they were targeted. Analysis of

organizational communication about the confluence of COVID-19 and cybersecurity triangulates data gathered in interviews.

The researcher recruited participants from influential organizations and from joint-action agencies through purposive and snowball sampling based on the researcher's prior professional contacts. The participants from the trade association and cooperative utilities were recruited from a national directory of cooperative utilities published by the National Rural Electric Cooperative Association. From the prospective candidate pool of more than 800 cooperative utilities nationwide, only a handful agreed to participate. Many refused to participate out of concern for legal liabilities, exposure of utility practices or weaknesses, or due to disinterest in the project. Many more never responded in any way to emails inviting co-op personnel to participate. The final set of participants at the utility level was determined more by who responded than by any preconceived design.

Commitment to participation by the tri-state trade association and two of its utilities provoked focused recruiting of the other member utilities, which produced two more participants. Participation by multiple utilities from the one trade association then suggested those and the other (non-participating) member utilities of that trade association as a central focus for the study. The review of communications provided a point for triangulation and allowed inclusion of data from all 15 utilities. To balance data received, the existing interview data from a utility from a different region was used as a comparator and augmented with both its public communications and those from its associated trade association.

The core 15 and comparator utilities' subordination to a common set of national and federal agencies but different affiliated trade associations and state authorities provided insight into how common data and materials were interpreted by a variety of organizations nationwide, and also potentially illustrated different ways that power and legitimacy are leveraged in issues management. This "descriptive" approach therefore illuminates a social phenomenon that is not sufficiently understood (Hesse-Biber, 2017): issues managers' approach to compounding wicked problems affecting critical infrastructure. Beginning with semi-structured interviews, this inquiry explored the lived experiences of personnel performing many different roles in helping public U.S. electric distribution utilities adapt to the COVID-19 pandemic while maintaining cybersecurity. Organizational media produced by participants' organizations augmented interview data; such media are useful "to corroborate and augment" interview data (Yin, 2018, p. 115). Review of organizational communications produced by the interviewees showed how strategy translated into communication. In doing so, this inquiry sought to understand both what the communicators aspired to convey in communications as well as the results of these efforts.

Semi-Structured Interviews

Data collection began with semi-structured interviews with a theoretical sample of energy policy and information security personnel at agencies that influence public utilities. These agencies included federal executive agencies and the intelligence community. The first interviews also included federal- and

national-level organizations that guide or influence operations at utilities or serve as industry advocacy groups. Interviews then engaged information technology and management personnel at two JAAs that supply power to consortia of public utilities in different parts of the country (i.e., spanning generation and distribution). The final stage of interviews involved executive management and communications personnel at cooperative electric utilities and a multi-state trade organization of which five of the co-op utilities were members.

Semi-structured interviews apply existing understanding of the situation and unique qualities of the participants while allowing room for the participant to draw the conversation in directions that may be of interest but outside the scope of the protocol (Hesse-Biber, 2017; Tracy, 2013). The interviews employed a constructivist approach, building rapport with the participants and exploring their understanding of the wicked problems, attending priorities, and necessary strategies (Roulston, 2010; Yin, 2018). Digressions in the interview provided additional richness and insight not anticipated in the initial protocol design (Roulston, 2014).

Interview Participants. The researcher recruited participants representing issues managers across several levels of policy making for public electricity distribution. The 15 interview participants included information technology personnel, outreach communications personnel, and senior management personnel at electric utilities; a communications manager at the trade association; representatives of federal agencies that influence operations at utilities; and

representatives of national advocacy organizations that improve coordination and collaboration among public utilities.

Participant sampling employed both purposive and snowball sampling (Hesse-Biber, 2017). The theoretical sample began with the researcher's existing contacts within the industry and the members of a multi-state trade association, given their explicit expertise with the subjects of the study (Hesse-Biber, 2017). The researcher's previous work in public power and referral by peers in the community improved rapport with participants (Hesse-Biber, 2017; Tracy, 2013; Yin, 2018).

Recruitment of participants from public utilities centered on one multi-state trade association and its 15 member utilities, drawn from the membership contact list of a national organization for co-op public utilities. By representing all 15 utilities that were members of a single trade association through interview participation and/or review of organizational communications and by augmenting that data with interviews of personnel at influential organizations and utilities outside the trade association as points of comparison, the researcher sought theoretical saturation—the point at which the input from participants produces no new insight—and generalizability, to ensure relevance of data beyond the specific instances of a localized sample. (Hesse-Biber 2017). The participant utilities served communities as small as 7,000 meters and as large as more than 175,000 meters, purported to be the largest service base for a public utility in the United States. Service areas ranged from the densely populated suburbs of a major metropolitan area to isolated mountainous and agricultural regions with three or

fewer residents per square mile. Communications staff at these utilities ranged from several dedicated communications professionals to several total administrative staff, with the CEO serving as communications contact and lead issues manager.

Further recruitment relied on snowball sampling, as participants referred the researcher to contacts with whom they communicate regarding cybersecurity practices and/or adaptation of operations to COVID-19. Represented utilities include three that are not from the trade group (one co-op utility and two JAAs), which provide additional points of comparison for the experiences and perspectives of those within the trade group.

The researcher previously worked with federal agency issues managers, national advocacy group leadership, national information sharing nonprofit group personnel, and JAA personnel on multiple projects addressing mutual aid and cybersecurity in the public utility sector. Beginning with those contacts and asking for a referral, the researcher accessed other representatives of public power utility issues management. The final participant group includes representatives from multiple federal agencies, national information sharing and advocacy organizations, trade organizations, and JAAs (i.e., regional organizations that connect generation utilities with multiple public distribution utilities).

Table 1 lists the identifying label for each interview participant, the nature of their organization, the primary publics of their organization that are relevant to this study, and the length of the interview.

Table 1

Profile of Organizations Interviewed for this Study

Identifier	Operational Scale	Primary Publics (in this study)
Federal executive agency	National	Other national organizations, state associations, trade associations
Federal intelligence organization	National	Other national organizations, state associations, trade associations
Information-sharing organization	National	National organizations, state associations, trade associations, utilities
Advocacy organization 1	National	National organizations, state associations, trade associations, 1,400 utilities and 100 joint-action agencies in 49 states
Advocacy organization 2	National	Other national organizations, state associations, trade associations, utilities in 47 states
Trade association 1	Regional: States 1, 2, 3	National organizations, state government, 15 member utilities serving 2 million people
Cooperative utility 1	State 1	98,000 customer/ owners, multi-state trade association, generation utility, state agencies
Cooperative utility 3	State 3	7,000 customer/ owners, multi-state trade association, generation utility, state agencies
Cooperative utility 4	State 3	175,000 customer/ owners, multi-state trade association, generation utility, state agencies
Cooperative utility 5	State 3	170,000 customer/ owners, multi-state trade association, generation utility, state agencies
Cooperative utility 6	State 3	96,000 customer/ owners, multi-state trade association, generation utility, state agencies
Joint-action agency 1, participant 1	State 4	4 member/owner municipal utilities, 4 municipal governments, state agencies
Joint-action agency 1, participant 2	State 4	4 member/owner municipal utilities, 4 municipal governments, state agencies
Cooperative utility 16	State 4	16,000 customer/ owners, multi-state trade association, generation utility, state agencies
Joint-action agency 2	State 5	Member/owner utilities, municipal governments, state agencies

Interview Protocol. The protocol for this study (Appendix D) reflected the four research questions. Open-ended questions afforded participants space and freedom to resist or refuse answering certain questions and affording the opportunity for diversions in conversation and exploration of related topics. This afforded opportunities for insights beyond those initially expected, enhancing the collaborative dimension of research (Roulston, 2014).

First, the protocol established the role the participant plays in internal communications within their organization and their perceptions of the primary utility publics and influences among them. This established a general view of how the participant viewed the communicative environment of their utility or agency. These questions established perceived publics with whom the organization communicates, those they seek to influence, and those who can influence their organization, and other organizations with which they collaborate. Questions from this section include "What are the most important groups with which [your organization] communicates?" which informs RQ2a and RQ2b by identifying the priority publics as perceived by the participant, independent of the direction of communication, and "What groups does [your organization] seek to persuade or influence?" which informs RQ3a and RQ3b by identifying the groups with which the organization must legitimize its position. This section provided a broad view of communication beyond the specific frame of the wicked problems and a preview of power in the network within which the organization operates.

The second part of the protocol explored how participants define challenges attending cybersecurity as a discrete wicked problem. This examined

what aspects of cybersecurity the utilities and coordinating organizations identify as priorities among the many different issues to address and how they communicate and justify these priorities to publics. This section started with internal communications and public relations, for example, “With what other personnel in [your organization] do you communicate about cybersecurity?” and “What communications do you receive from [your organization] about cybersecurity?” which informs RQ1a. This section also addressed external public relations relationships, and types of influence between the utilities and other organizations. For instance, “What other organization has the most influence over your organization’s cybersecurity strategy—i.e., influence over or dictating policy?” and “How does [cited organization] influence your organization’s policy decisions?” inform RQ2a. Lastly, this section explored how the participant’s organization legitimizes its position regarding cybersecurity with these different publics. Questions such as “How do you communicate about cybersecurity with [cited organization]?” inform RQ3a by exploring how strategies differ for different publics and different types of power held by publics. This also framed the subsequent strategies used to communicate with publics and the publics deemed strategic in those communications.

The third part of the protocol explored how participants define challenges attending COVID-19 as a discrete wicked problem. This section mirrored the first section’s questions about cybersecurity, to provide points of comparison and contrast to perceptions of the wicked problems. Questions such as “What personnel in your utility monitor and address COVID-19?” and “What

communications do you receive from your utility about COVID-19?" explored internal public relations channels and informed RQ1b. This section also prompted discussion of external public relations, identification and prioritization of external publics, and perceptions of power and strategies for communicating with those publics. Questions such as "What organizations have the most influence over your organization's COVID-19 strategy—i.e., influence over or dictating policy?" and the follow-up question "How does [cited organization] influence your utility's policy decisions?" informed RQ2b by highlighting external public relations associations and power conferred in those relationships. Finally, this section explored the strategies utilities employ to legitimize their priorities to address COVID-19 with publics through questions such as "How do you communicate about COVID-19 with [cited organization]?" which informed RQ3b.

The fourth part of the protocol explored how the participants perceive the challenges of cybersecurity and COVID-19 as mutually compounding. Having explored each wicked problem individually gives a view into how answers differ when overlaying concerns of concurrent problems. Questions such as "What has been the most surprising challenge in maintaining cybersecurity during the COVID-19 pandemic?" and "How have you communicated about your utility's work to adapt cybersecurity practices to COVID-19 (e.g., org publications, blog posts, media)?" informed RQ4 by exploring what different strategies, communications, points of legitimacy or publics are required in issues stemming from the compounded situation of cybersecurity during the COVID-19 pandemic.

Interview Procedure. The COVID-19 pandemic precluded in-person interviews, which regrettably lost some nonverbal cues and other communications that telecommunications are unable to convey (Irvine et al., 2015). Asynchronous email interviews have proven effective in qualitative research, but the loss of nonverbal facial cues and vocal tenor reduces the data available for review and so were eschewed (Hesse-Biber, 2017). Interviews by telephone preserve vocal tone and inflection, but still miss facial expression. Technical issues demanded conducting one interview by phone. The remaining interviews used Zoom or Google Meet to preserve some facial cues and some nonverbal communication (Abrams et al., 2015).

All interviews were recorded with a voice recorder, with the participant's permission. Each interview began with a few questions about the participant's background and organization, to build rapport. The researcher used probes and follow-up questions to expand participants' discussion and allow the conversation to build organically through subjects the participant was comfortable with or perceived as particularly important. Allowing this room for the participant to emphasize the subjects they perceived as most important and by directly asking the participants about their perceptions and interpretations of communications received from other organizations, the researcher sought to minimize interpretative bias and improve validity of the resulting analysis (Hesse-Biber, 2017). The interviews ranged in length from 52 minutes to 1 hour 13 minutes, averaging 59 minutes 46 seconds.

Collection of Publicly Available Communications

Following the interviews, the researcher sought public relations communications addressing adaptations to the COVID-19 pandemic or cybersecurity. Because the study sought to understand how the two problems compounded, all communications drawn were from March 2020 through January 2022. The communications analyzed were publicly available and so do not present a threat to organizational operations or information security. Qualitative content analysis of organizational media addressing the adaptation of public utilities to operation during the COVID-19 pandemic while maintaining cybersecurity improves understanding of how the goals and strategies expressed in interviews manifest in publicly facing communications and what other ideologies may have influenced organizational messaging (Hesse-Biber, 2017). This analysis focused on the use of terms, metaphors, and quotes to generate meaning, thereby providing insight to the polysemantic nature of texts (Hesse-Biber, 2017).

Collection of documents began with each organization's website. Websites for all 16 co-op utilities (i.e., the 15 members of the multi-state trade organization and the member of the comparator single-state trade association) and both trade organizations were reviewed for relevant communications. The researcher first explored the site navigation for what materials would be intuitively found (e.g., under "Recent News," "Press Room," or "Community" tabs), and then used available website search tools to identify any additional publicly available materials. Because the COVID-19 pandemic is a primary

framework for this study—as one of the two wicked problems defined and due to the need for its presence to compound the issue of cybersecurity—materials were only collected starting in January 2020. Keywords used in website search included "COVID-19," "coronavirus," "cyber security," "cybersecurity," "cyber threat," and "pandemic." Any materials that addressed these issues directly were collected and coded. Exceptions included online articles where a link to another page triggered the search result (e.g., an "additional articles" list that included a link to COVID-19 information). This search produced 316 documents relevant to this study. The 316 documents were classified according to the nature of the intended audience, using the categories External Member/ Owner-Specific, External Public Relations, Relayed External Public Relations, Request for Information, and Internal Public Relations.

External Member/Owner-Specific conveyed information directed to the utility's member/owners[2], specifically. These were often framed in a familiar or first-person voice, and included affirmations of dedication to owner/members (often in the second-person voice) and discussed utility business of specific relevance to member/owners (e.g., annual meetings and member payouts and benefit programs). Communications in this category included webpages with member/owner specific services and content, news releases directed at member/owners, PDFs of mailer inserts, and PDFs of utility-specific sections developed for trade association lifestyle magazines. Both trade organizations

[2] Co-op utilities are jointly owned by the people whom they serve. As such, utilities in this study used the term "member/owners" in place of customers. Member/owners have input to utility annual meetings that guide co-op operations and policy, and in some cases receive annual payouts from utilities depending on financial state.

examined for this study develop a lifestyle magazine that is distributed to member/owners through all member utilities. The utilities are allotted 7 to 10 pages in each issue to add their own content. The content of the lifestyle magazines from the utility-specific sections was coded to the corresponding utility, but content developed for the magazine by the trade association (i.e., content present in all versions of the magazine) was only attributed to the trade organization's communications, even though it was also distributed by all utilities.

External Public Relations documents conveyed news about the utility's activities suitable for audiences (including their member/owners) addressing topics of interest to publics beyond their service area. Content included in this classification used third-person framing of the utility and its member/owners, discussion of utility attributes that would be known to member/owners (e.g., location and service area), organizational boilerplate, and directions "for more information" to public relations personnel rather than member services. Communications in this category were most often press releases published to a dedicated "press room" or "news" tab on the utility's website. In some cases, material from webpage text on other tabs (e.g., COVID-19 strategies and information or a utility's subsidiary broadband provider) met the criteria.

Relayed External Public Relations identified documents developed by another organization and republished on the utility's website or in other proprietary communications. These were often drawn from national and federal organizations, both oversight and information-sharing organizations. Communications in this category were most often PDFs or news item web pages

with infographics drawn from national or federal organizations. Branding from a different source organization than the communicating organization triggered inclusion in this category. However, communications from a utility that were developed by a trade association are not included in this category, because many of the trade associations' communications are developed expressly for the purpose of reducing the need for utilities to develop their own communications.

Communications developed by trade associations and published by utilities are coded to the trade association and not included in the utility profile, to avoid counting the same communication multiple times. Similarly, communications from member utilities that were republished by the trade organization were identified in the writer credit (i.e., utility personnel or trade association communications staff) and categorized under the trade association as relayed public relations.

Request for Information (RFI) indicates a request for information, used by organizations to solicit proposals from organizations to provide services in upcoming utility endeavors. Only one document encountered fit this category, but it was included in the interest of keeping the survey comprehensive. The RFI includes some indication of utility priorities and strategies, so is a useful subject of review even if not conventional public relations.

Internal Public Relations identified communications products addressing organizational personnel. These communications were uncommon in the study, because the study focused on communications publicly available on the utility website, and internal public relations documents are often distributed through

non-public channels. Emergency planning documents, process protocols, and other operational and human resource materials qualify for this category.

Table 2 lists the identifying label for each organization from which communications were collected, the scale of operation, the primary publics of each organization that are relevant to this study, the number of communications collected and reviewed, and the number of communications for the identified intended audiences.

Table 2

Organizational Website Communications Reviewed (March 2020–January 2022)

Identifier	Scale	Primary Publics (in this study)	Data Analyzed (# of Communications)
Trade Association 1	Regional	National/federal organizations, state government, 15 member utilities serving 2 million people	24 external, 5 member/ owner-specific, and 8 relayed public relations
Cooperative utility 1	State 1	98,000 customer/ owners, multi-state trade association, generation utility, state agencies	1 external and 7 member/ owner-specific public relations
Cooperative utility 2	State 2	55,000 customer/ owners, multi-state trade association, generation utility, state agencies	23 external and 17 member/owner-specific public relations
Cooperative utility 3	State 3	7,000 customer/ owners, multi-state trade association, generation utility, state agencies	1 external, 1 member/ owner-specific, and 1 internal public relations
Cooperative utility 4	State 3	175,000 customer/ owners, multi-state trade association, generation utility, state agencies	8 external and 7 member/ owner-specific public relations
Cooperative utility 5	State 3	170,000 customer/ owners, multi-state trade association, generation utility, state agencies	26 external and 24 member/owner-specific public relations
Cooperative utility 6	State 3	96,000 customer/ owners, multi-state trade association, generation utility, state agencies	1 external, 6 member/ owner-specific, and 1 relayed public relations
Cooperative utility 7	State 3	35,000 customer/ owners, multi-state trade association, generation utility, state agencies	5 external and 15 member/owner-specific public relations

Identifier	Scale	Primary Publics (in this study)	Data Analyzed (# of Communications)
Cooperative utility 8	State 3	13,000 customer/ owners, multi-state trade association, generation utility, state agencies	5 external and 6 member/ owner-specific public relations
Cooperative utility 9	State 3	38,000, customer/ owners, multi-state trade association, generation utility, state agencies	7 external, 7 member/ owner-specific, and 1 relayed public relations
Cooperative utility 10	State 3	11,000 customer/ owners, multi-state trade association, generation utility, state agencies	3 external, 6 member/ owner-specific, and 5 relayed public relations
Cooperative utility 11	State 3	31,000 customer/ owners, multi-state trade association, generation utility, state agencies	1 external and 1 member/ owner-specific public relations
Cooperative utility 12	State 3	15,000 customer/ owners, multi-state trade association, generation utility, state agencies	2 external and 1 member/ owner-specific
Cooperative utility 13	State 3	32,000 customer/ owners, multi-state trade association, generation utility, state agencies	1 external and 6 member/ owner-specific
Cooperative utility 14	State 3	12,000 customer/ owners, multi-state trade association, generation utility, state agencies	3 external, 3 member/ owner-specific, and 2 internal public relations
Cooperative utility 15	State 3	58,000 customer/ owners, multi-state trade association, generation utility, state agencies	7 external, 3 member/ owner-specific, and 1 request for information
Trade Association 2	State 4	National/federal organizations, state government, 22 co-op utilities, 2 generation utilities	10 external, 21 member/ owner-specific, and 4 relayed public relations
Cooperative utility 16	State 4	16,000 customer/ owners, multi-state trade association, generation utility, state agencies	1 external and 10 member/ owner-specific public relations

Data Analysis

Data analysis for the multiple-case study was iterative, analyzing data collected and interpreting meaning to define categories and refine collecting of additional data (Hesse-Biber, 2017). Based on Roulston's "constructivist" approach, data analysis included detailed transcription of participant interviews

(Roulston, 2010). Multiple sources of data (i.e., interviews of utility personnel and government and regulatory personnel as well as documents addressing cybersecurity and COVID-19) improved categorization of data and subsequent validity and credibility of conclusions (Hesse-Biber, 2017). Concurrent and subsequent memoing and data analysis accompanied data collection. Data was compiled in notes, graphic formats, and recordings, to aid coding and analysis (Miles et al., 2014).

Then researcher used NVivo software for coding and analysis. Software designed specifically for qualitative study can improve coding and analysis of relationships between and among codes (Hesse-Biber, 2017). While concerns that imposition of a software system on the art of coding and analysis may lose some of the nuance of coding by hand are valid, the additional assurance of ability to maintain the whole data set and afford insights that the program might note among codes that escape the researcher's awareness outweigh the drawbacks (Hesse-Biber, 2017).

Multi-case studies with large sets of overlapping data benefit from the organization and categorization afforded by computer software (Miles et al., 2014, Yin, 2018). In particular, large sets of data resulting from "verbatim records" and studies "using *grounded theory* strategies" (Yin, 2018, p. 167; emphasis in original) particularly benefit from software in data coding and analysis. Clear definition of research objectives and strategy for data collection with direct review of all and imposition of codes by the researcher eliminates the software's influence on the codes themselves and leaves to the software analysis

of the relationship among the factors observed by the researcher (Hesse-Biber, 2017). The search functions of the software and ability to identify and graphically render relationships among concepts and data both speed data analysis and afford additional granularity and attention to detail (Miles et al., 2014).

Coding

Data compiled in notes, graphic formats, and recordings aided coding and analysis (Miles et al., 2014). Coding of notes and transcripts proceeded from initial note taking through data analysis, beginning with primary-cycle codes to capture emergent themes through secondary-cycle to organize and focus the codes as explanatory or theoretical analyses (Tracy, 2013). Multistage, multiplatform coding and analysis helped derive themes and triangulate insights (Corbin & Strauss, 2008). Coding espoused a grounded theory approach, relying on multiple coding passes, reviewing and re-reviewing data to highlight emergent themes and patterns (Hesse-Biber, 2017). This inductive approach requires an "*open ended* and holistic" perspective (Hesse-Biber, 2017).

Comparing the data coded from interviews against the data drawn from the publicly available communications affirmed or challenged the strategies asserted by participants (Hesse-Biber, 2017). Coding of the communications was based on the research questions that guided development of the protocol as well as coding categories that emerged from the interviews. In this case, types of media, language used, communicators cited and addressed, manifestations of power, assertions of legitimacy, and the virus, among others, were all considered

as part of the meaning and forms of influence communications conveyed to publics (Aylesworth-Spink, 2017).

Both forms of inquiry—interviews with issues managers and publicly available communications—were analyzed using a uniform code set. The code set emerged as data collection progressed, similar to a grounded approach, though some structure to the data was imposed in advance, per the protocols. The coding and analysis process was a multistage and multiplatform process, to derive themes and triangulate insights (Corbin & Strauss, 2008). The final data are presented in a mix of formats to preserve participant voices and enhance apprehension of data, including *in vivo* language (Hesse-Biber, 2017), tables (Miles et al., 2014), and case studies (Yin, 2018).

First, the 15 interview transcripts were reviewed and coded. Questions in the interview protocol provoked five levels of inquiry (Yin, 2018). First, the interview questions were derived directly from the three research questions, to ensure that data collected speak to the desired inquiry. Second, parallel questions between the protocols (i.e., for utility and non-utility participants) and within each protocol for each wicked problem guided a common overarching inquiry among the multiple individual cases. Third, notes and memoing during the process identified emergent themes and suggested refinements to the protocol as data were collected and the project proceeded. Fourth, once collection of data was complete, the entire body of data was reviewed to see what overarching questions emerged from the data. Finally, at the end of the study, global data and emergent

patterns and common narratives were reviewed to indicate potential policy or procedural recommendations.

Descriptive codes, categorical codes (i.e., groups of descriptive codes), and analytical codes improved data analysis and highlighted emergent themes (Hesse-Biber, 2017). Multiple levels of coding drew out overarching themes (Miles et al., 2014), while constant comparison helped to ensure that the meta-themes and analysis remained true to the source data (Corbin & Strauss, 2008). The codes initially reflected the major themes outlined in the protocol: Challenges, Legitimacy, Power, Role, and Threats. Memoing provided ongoing assessment and reassessment of data to refine codes and approaches taken by the researcher (Hesse-Biber, 2017). As review of the transcripts and organizational communications progressed, additional codes suggested by emergent themes were captured. Ensuring consistent coding and capture of all codes in all transcripts required multiple passes. The final set of codes greatly expanded on the initial set.

The content of each of the 316 documents captured from the website review was then coded using the same final set of codes as the interviews. Coding of these communications captured the nature of the source organization, the category of communication, and content within the text relevant to the thematic codes. Coding specific sections of text rather than the documents as a whole allowed both for identification of specific passages reflecting a thematic code and for identification of multiple instances of a code within a document, to capture relative emphasis of content (i.e., extend beyond what is there to what has greater or lesser emphasis among the content there). This also enabled more detailed

analysis of the proportion of communications attributable to a particular code or theme, as NVivo calculated the percentage of a document captured by a particular code. The table in Appendix E presents the final set of codes used to analyze both the interview transcripts and the communications captured from organizational websites.

Interpretation

A grounded approach has no distinct turn between analysis and interpretation; both are part of a continuous process beginning with data collection and ending with the report (Hesse-Biber, 2017). Notes produced during the interview and comments on the transcriptions captured potential additional points of inquiry, emergent themes, and potential narratives, which were compiled into primary codes through the constant comparative method (Jupp, 2006). Ongoing interpretation maintained critical engagement with the data and analysis, improving reliability and validity of resulting analysis.

Reliability and Validity

Results of this study aspired to multiple dimensions of reliability and validity. Internal reliability is present when coding is consistent and accurately captures and interprets data by participants and materials gathered for the study (Hesse-Biber, 2017). Reflexivity during coding may also improve validity (Hesse-Biber, 2017). Consistent methodology and fair and transparent reporting can improve the validity of a case study, limiting researcher biases and other aspects of "experimenter effect," (Yin, 2018, p. 20). This study is built to address the four primary forms of validity in case study design (Yin, 2018, pp. 42–47):

Reliability

Reliability centers on whether a study is repeatable and will produce the same results if repeated (Yin, 2018) or whether the methods are consistently applied over time (Miles et al., 2014). While the nature of qualitative inquiry precludes precise replication, use of the protocol to guide the interviews and a single researcher applying constant-comparative coding improves construct validity. The researcher documented all procedures and maintained the chain of evidence used in analysis. While the interviews themselves might not be exactly replicated by future researchers, thorough and diligent collation of materials and transparent documentation and interpretation of data could provide a degree of reproducibility, in that review of the materials should produce similar if not the same conclusions.

Once the initial draft document was complete, the researcher provided copies to all participants for review. This review invited any corrections to the interview data or other information presented in the study, to verify accurate portrayal of the industry and its challenges from the perspective of issues managers within the industry. This sought to minimize interpretative bias by the researcher and improve validity of the resulting analysis (Hesse-Biber, 2017)

Deliberate collection, cataloging, and analysis of data improved the stability of processes over time and provided a check on quality of analysis. In addition, the use of analysis software aided cataloging, collation, categorization, and analysis of the materials collected. The software also tracked all codes defined and where codes were applied, and afforded some tools for consistent

analysis of application and distribution of codes as related to the categories of material and the sources of data.

Construct validity/confirmability

Construct validity or confirmability ensures that the study is appropriate for the phenomena in question (Miles et al., 2014; Yin, 2018). Wicked problems derive from social forces and in novel manifestations depending on the groups affected. Study of compounding wicked problems should allow consideration of environmental factors and actions of the actors without imposition of presupposed frameworks or roles. This approach provides multiple sources of information and a "chain of evidence." Multiple sources of evidence (i.e., utility interviews, non-utility interviews, and public communications) facilitated the development of convergent narratives, and discussing draft conclusions with participants further improved construct validity (Yin, 2018).

Internal validity

Internal validity concerns causal relationships in a study (Yin, 2018) and/or the degree to which the conclusions present an "authentic," reasonable picture of a phenomenon (Miles et al., 2014). Causality is not the goal of this descriptive multiple-case study, but authenticity and an accurate portrayal of the phenomena are. Engaging a single coding mechanism developed from emergent data across multiple parallel cases improved internal validity. Discussing draft conclusions with participants also improved internal validity by providing a check on investigator bias by the principal researcher.

External validity

External validity entails the degree to which the contents of a case study might generalize to other applications (Miles et al., 2014; Yin, 2018). A multiple-case study format improves external validity by drawing on the experiences of more than a dozen different utilities as well as organizations and agencies that have power over them and/or over whom the utilities have power. By drawing on multiple cases and their interlocking communicative counterparts, this study highlights immediate parallels and contrasts among peer organizations. Considering the unique nature of both infrastructural organizations and wicked problems, the cases themselves may not generalize directly, but provide insights into the role and effectiveness of issues managers and their strategies.

Ensuring Ethical Research and Accuracy of Data Gathered

Ensuring ethical practice is an essential quality of excellent qualitative study (Hesse-Biber, 2017; Tracy, 2013; Yin, 2018). This study used multiple methods to preserve research ethics. Because the study involved human participants, the research design and protocol were reviewed and approved by the Institutional Review Board (IRB) (Hesse-Biber, 2017; Tracy, 2013). Final data, including records, recordings, and files, were thoroughly anonymized to prevent compromise of sensitive (personal or industrial) information (Yin, 2018). All participants received an informed letter of consent, affirming confidentiality of participation, anonymity of data, ability to cease participation at any time, and security of data. The researcher disclosed in advance the purpose of the study and associations of the researcher, along with intended techniques and technologies to

be used during the interview. IRB review, letters of consent, and disclosure of intentions and affiliations are all common techniques to improve ethics of qualitative research (Hesse-Biber, 2017).

Other ethical considerations in qualitative research include deception of participants, misrepresentation of stereotyping of participants, and risk of viewing or engaging in illegal activity (Hesse-Biber, 2017). By allowing the participants to frame their own story and then triangulating data gained from them through accounts from other participants, the researcher minimized imposition of his own perspective. In addition, the group sought for participation in this study are working within a professional, technical environment, and standards of operation therein must minimize the potential for legal quandaries. Anonymization of organizations and participants protects individual participants while affording insight to their actions and interactions. The researcher previously collaborated with some participants in a professional capacity for approximately 10 years, so was already familiar with concerns particular to the industry. While not a fully embedded "insider," (Hesse-Biber, 2017, p. 129), participant familiarity with the researcher and recognition of some understanding by the researcher of concerns attending cybersecurity in the public power sector eased access and helped moderate ethical concerns.

Reflexivity

Recognition of differences between the researcher and participants is a critical dimension of effective qualitative study (Hesse-Biber, 2017). The researcher's own background, beliefs, and feelings may influence interpretation of

data, and the backgrounds and perceptions of both researcher and participant contribute to power dynamics in the conversation that can influence and alter data (Hesse-Biber, 2017). Understanding these dynamics and influences can improve conversational dynamics and depth of data gathered. Overlooking influential dynamics may stymie conversation and participant comfort with the researcher or impose the views of researcher such that they influence participant answers (Yin, 2018). For example, while the researcher's extensive prior work with public utilities and associated public- and private-sector organizations afforded some understanding of the industry lexicon and priorities, which may have improved both interpretation of data and building rapport with participants, the researcher was still fundamentally an outsider to the very tight-knit network of communication in public power. As such, the researcher encountered considerable skepticism regarding the legitimacy of the project, and many prospective participants refused to take part due to the sensitive nature of the subjects.

Summary of Data and Analytic Approach

This study collected data through multiple fora: semi-structured interviews explored the experiences and perspectives of issues managers at utilities and issues managers at organizations that influence utilities, and publicly available communications from those utilities and organizations provided insight to the resulting communications as well as the communications influencing utility responses. These data sources were analyzed in multi-step, multi-tiered coding that interrogated the research questions and drew out patterns and points of foci from the different organizations. Comparisons among the scope of operations

highlighted different communicative priorities, and the priorities drawn from interviews were compared with patterns emerging for the analysis of communication products. Analytic software eased the application of uniform codes across the sets of data, and facilitated queries of instance and frequency of codes, among other points of analysis, in a uniform and repeatable manner. The final data both answer the research questions and highlight unforeseen interactions and priorities that build on historic precedent and warrant additional interrogation. These results are presented in the following chapter.

Chapter 4: Results

This study examined how issues managers prioritized and adapted to mutually compounding wicked problems. To do so, this study engaged issues managers across multiple strata of federal, state, and municipal policymaking and oversight of the operation of the U.S. electric grid, including public utilities, regulatory and oversight agencies, and industry associations. Interviews explored the meaning made by issues managers of the threats and challenges utilities faced in maintaining cybersecurity and responding to the COVID-19 pandemic. Participants also discussed their place in the community, their responsibilities to publics, and the limitations they faced responding to those threats and challenges.

Subsequent textual analyses of public relations communications from co-op utilities from March 2020 to January 2022 illuminated the messaging conveyed to member/owner publics and other publics. Because legitimacy and power are the primary points of focus for issues management (Heath & Palenchar, 2008), this examination of issues management comprised how organizations define the issues, how they legitimize their positions and strategies in response to those issues, and how they perceive and identify power from and with other organizations in response to those issues.

The following sections break discussion into topics according to the research questions and arrange data from interview participants and the review of communications according to themes within each area of inquiry. Analysis of data for each section includes input from national and federal agencies that seek to influence utility behaviors (the “influencer level”). This data is drawn from

interviews. The analysis also incorporates data from organizations that collaborate with utilities (the "collaborator level"), which includes interviews with three participants from two joint-action agencies (JAAs), interviews with and communications by the trade association of which 15 of the utilities are members (TA-1), and communications by the trade association of which the last co-op interviewed is a member, located in a different state and region of the country than the first trade association and its utilities (TA-2). Finally, data from the utilities themselves include interview data and communications data from the first five utilities from TA-1 as well as Co-op-16 from TA-2, and data from the review of communications of the other 10 utilities that are members of TA-1.

Table 3 presents the organizations at the "influencer" level that participated in this study. Influencer organizations collect intelligence and compile best practices and other guidance for utilities and organizations across the public power sector as well as other sectors. Each participant is represented with a pseudonym to protect their anonymity as well as the anonymity of their organization. Table 3 defines the pseudonym that will be used to identify them in the remainder of the document and provides a brief description of the participants position in the organization that affords them expertise in this subject matter. The suffix "-p" indicates data from an interview participant (hence the "p"). Even though all data from influencer organizations are derived from interviews, data from collaborative organizations and utility organizations mix interviews and public relations communications, and so need to distinguish participants from communications. The convention is preserved here for clarity.

Table 3

Influencer Organization Participants, Pseudonyms, and Data

Participant/ Organization	Pseudonym	Data Analyzed
Federal Executive Agency	FEAp	Semi-structured interview with a deputy assistant secretary specializing in critical infrastructure protection
Federal Intelligence Organization	INTELp	Semi-structured interview with an intelligence specialist with extensive experience in critical infrastructure and public power
Nonprofit Information Sharing Organization 1	ISOp	Semi-structured interview with a director of legislative affairs for the energy sector
Nonprofit Advocacy Organization 1	ADV-1p	Semi-structured interview with a senior director of security and resilience for public utilities
Nonprofit Advocacy Sharing Organization 2	ADV-2p	Semi-structured interview with a director of intelligence

Table 4 presents the organizations at the "collaborative" level that participated in this study. Collaborative organizations work with utilities to more efficiently and economically provide services to their areas, including state-sponsored JAAs that unite multiple municipal utilities to access to economies of scale and share costs on infrastructure expenses and other initiatives; and trade associations that provide member co-op utilities with advocacy, communications, and other support to improve member services reduce labor and expenses. Each participant is represented with a pseudonym to protect their anonymity as well as the anonymity of their organization.

Table 4

Collaborative Organization Participants, Pseudonyms, and Data

Participant/ Organization	Pseudonym	Data Analyzed
Joint-Action Agency 1	JAA-1p1	Semi-structured interview with a senior information and information technology security engineer
	JAA-1p2	Semi-structured interview with a senior manager of cyber and information security
Joint-Action Agency 2	JAA-2p	Semi-structured interview with a director of information and operations technology
Trade Association 1	TA-1p	Semi-structured interview with a vice president in charge of public relations and communications
	TA-1	24 external, 5 member/owner-specific, and 8 relayed public relations communications
Trade Association 2	TA-2	10 external, 21 member/owner-specific, and 4 relayed public relations

Table 4 also defines the pseudonym that will be used to identify them in the remainder of the document. The pseudonyms distinguish between content provided in an interview and that derived from the review of communications, where appropriate (i.e., a suffix "-p" indicates data from an interview participant [hence the "p"] while absence of the suffix indicates data from organizational communications). The table also provides a brief description of an interview participant's position in the organization that affords them expertise in this subject matter, or the number and type of communications reviewed.

Table 5 presents the utilities that participated in this study and defines the pseudonym that will identify them. Pseudonyms protect participant anonymity as well as the anonymity of their organization, and each organization is assigned a pseudonym as well. The pseudonyms distinguish between content provided in an

interview and that derived from the review of communications (i.e., a suffix "-p" indicates data from an interview while absence of the suffix indicates data from communications). The table also provides a brief description of an interview participant's position in the organization that affords them expertise in this subject matter, and/or the communications reviewed.

Table 5

Utility Participants, Pseudonyms, and Data

Organization	Pseudonym	Data Analyzed
Cooperative utility 1	Co-op-1p	Semi-structured interview with manager of public relations and community outreach
	Co-op-1	1 external and 7 member/owner-specific public relations communications
Cooperative utility 2	Co-op-2	23 external, 17 member/owner-specific public relations
Cooperative utility 3	Co-op-3p	Semi-structured interview with utility CEO
	Co-op-3	1 external, 1 member/owner-specific, and 1 internal public relations
Cooperative utility 4	Co-op-4p	Semi-structured interview with vice president for public relations
	Co-op-4	8 external, 7 member/owner-specific public relations
Cooperative utility 5	Co-op-5p	Semi-structured interview with communications and public relations manager
	Co-op-5	26 external and 24 member/owner-specific public relations
Cooperative utility 6	Co-op-6p	Semi-structured interview with public relations coordinator
	Co-op-6	1 external, 6 member/owner-specific, and 1 relayed public relations
Cooperative utility 7	Co-op-7	5 external, and 15 member/owner-specific public relations
Cooperative utility 8	Co-op-8	5 external and 6 member/owner-specific public relations

Organization	Pseudonym	Data Analyzed
Cooperative utility 9	Co-op-9	7 external, 7 member/owner-specific, and 1 relayed public relations
Cooperative utility 10	Co-op-10	3 external, 6 member/owner-specific, and 5 relayed public relations
Cooperative utility 11	Co-op-11	1 external and 1 member/owner-specific public relations
Cooperative utility 12	Co-op-12	2 external and 1 member/owner-specific public relations
Cooperative utility 13	Co-op-13	1 external and 6 member/owner-specific public relations
Cooperative utility 14	Co-op-14	3 external, 3 member/owner-specific, and 2 internal public relations
Cooperative utility 15	Co-op-15	7 external and 3 member/owner-specific public relations, 1 request for information
Cooperative utility 16	Co-op-16p	Semi-structured interview with utility general manager
	Co-op-16	1 external and 10 member/owner-specific public relations

Table 6 presents the extent to which COVID-19 and cybersecurity featured in the interview conversations. The table is divided into influencer organizations (top third), collaborative organizations (middle third), and co-op utilities, and includes the emergent theme of broadband Internet needs in co-op service territories. Broadband challenges were not part of the protocol, so discussion percentages noted in Table 6 indicate when a participant brought it up of their own accord. The degree to which co-ops discussed this emergent topic without dedicated questions in the protocol is striking—three participants discussed broadband more than cybersecurity.

Table 6

Portion of Interview, by Subject

Participant	Cybersecurity Challenges	COVID-19 Challenges	Broadband Challenges
FEAp	14%	4%	
INTELp	24%	3%	
ISOp	32%	10%	
ADV-1p	20%	2%	
ADV-2p	30%	7%	
JAA-1p1	16%	6%	
JAA-1p2	27%	3%	
JAA-2p	16%	12%	
TA-1p	3%	23%	6%
Co-op-1p	6%	17%	1%
Co-op-3p	7%	10%	8%
Co-op-4p	1%	32%	7%
Co-op-5p	8%	22%	9%
Co-op-6p	10%	20%	3%
Co-op-16p	9%	11%	

Data from NVivio analysis of interview transcripts, rounded to closest percent

Table 7 categorizes the communications reviewed by topic, including broadband access. Inclusion of broadband in Table 7 illustrates the degree to which utilities communicated with publics about the digital divide: not as frequently as the pandemic, but significantly more than cybersecurity.

Table 7

Co-op Public Relations Communications March 2020–January 2022

Organization	Cybersecurity Communications	COVID-19 Communications	Broadband Communications
TA-1	1	20	22
Co-op-1	1	8	0
Co-op-2	0	17	25
Co-op-3	0	0	2
Co-op-4	1	5	3
Co-op-5	2	27	3
Co-op-6	0	8	1
Co-op-7	0	17	3
Co-op-8	2	4	10
Co-op-9	0	8	7
Co-op-10	2	10	1
Co-op-11	0	2	0
Co-op-12	0	3	1
Co-op-13	1	3	4
Co-op-14	0	4	6
Co-op-15	0	9	1
TA-2	12	20	8
Co-op-16	1	11	0
Total	22	176	99

Data derived from communications captured in NVivo, including all external public relations and member/owner-specific public relations communications.

RQ_1: Defining and Prioritizing Issues in Compounding Wicked Problems

The first research question asked how issues managers identify wicked problems and how they prioritize compounding wicked problems. To answer this

question, the interview protocol explored how issues managers perceived the challenges posed by cybersecurity and the COVID-19 pandemic, and whether these challenges are seen as "wicked." The protocol also specifically asked how issues managers perceived the compounding challenges presented by cybersecurity and the COVID-19 pandemic, and to which challenges they gave priority. An emergent theme of broadband Internet service stems from historical (and now politically ingrained) socio-economic disparities that gave rise to the co-op utilities in the 1930s and are still affecting the residents of the service regions 90 years later.

Issues Managers Agreed Cybersecurity is an Unsolvable, Persistent Problem

Participants described cybersecurity as a persistent and increasingly difficult problem. Because the nature of the threats and means of attack are constantly changing, no single strategy is correct or solution final. Many interviews echoed that vigilance and adaptability are key attributes to guard against persistent and intractable threats. The characterization of cybersecurity from influencer, collaborative, and utility organizations all fit the description of a wicked problem.

Cyber threats, including state-sponsored threat actors, threats from non-state actors (e.g. ransomware), directed email threats (i.e., "spearphishers"), and nondirected email and online threats (e.g., worms and viruses through SPAM email) have significant power to affect utilities. All of these threats rely on internal exploits in personnel behavior, software inadequacy, or a nexus of both. Cyber incidents have the power to interrupt service, disrupt utility

communications, disrupt operational technology (OT) and/or information technology (IT) mechanisms, and expose member/owner personally identifiable information (PII), among others. These all entail potential financial and reputational costs to the utility.

All of these threats are also asymmetric: the utility is often unaware of the specific aggressor until an intrusion attempt is made, and there is no iterative recourse available to the utility. Power wielded includes fear, financial repercussions, loss of reputation and trust, and denial of service in either information or grid technologies. In addition, news of successful breaches of other utilities, even utilities in other sectors such as water distribution, can undermine member/owner trust in utility communications and provision of services and leave them wondering when their utility will be similarly affected.

The interview protocol explored whether utilities and organizations that influence their communications characterize cybersecurity in a way that aligns with the definition of a wicked problem presented in the literature review. This first step informs the analysis of the strategies and actions designed in response. Were utilities to only approach cybersecurity as a crisis, for example, the analysis of responses in a framework of wicked problems may not be appropriate. Influencer and collaborative organizations (definitions on pages 95 and 96) inform utility perspectives on and responses to cyber threats, and help parse strategies to improve and maintain cybersecurity. Accordingly, data analysis first examined their perspectives on utility cybersecurity, to see what messages shaped utilities' perspectives.

Cyber Threats are Unsolvable Problems. Participants characterized cybersecurity threats as evolving and therefore unsolvable. Threat actors are constantly exploring new means of gaining entry into utility systems, and frequently leverage previously identified exploits when organizations fail to update systems. Software systems upon which the industry relies have susceptibilities that have gone undiagnosed for years, and likely still have additional weaknesses that threat actors might exploit as yet unidentified. The determination of threat actors from around the globe, the integration of utility service areas within broader transnational interconnections, and vulnerabilities inherent in complex technical systems all pose challenges in utility cybersecurity.

Participants from influencer organizations viewed utility cybersecurity from national and international perspectives. Their concerns for the effects of a breach are not confined to a service territory but span the country with attendant compounding threats that might cause a cascading failure of multiple service areas. Threats come from both domestic and foreign threat actors and may be motivated by political or personal goals. The scope and scale of these threats and impacts leaves no corner of the grid untouched. Utilities' inherent need for communication networks to manage operations and for command-and-control exposes utilities of all scales of operation to the full array of threats. ADV-2p asserted: "There's no such thing [as a comprehensive solution to cybersecurity]...if you touch the internet, you will have a vulnerability."

Participants from collaborative organizations affirmed that cybersecurity will never be solved because the threats are always evolving. JAA-1p2 echoed

ADV-2p's perspective on threat persistence with the analogy of a squirrel and a birdfeeder[3]: Not only are adversaries able to dedicate more time to intrusion than utilities are to defenses, but defenses are all designed around "...what the squirrel did last time," so you are always chasing the place the adversary was before, and unable to anticipate where they actually are now, strategically. In addition to constant evolution in the strategies for effecting a specific compromise, the means of achieving a compromise—the targets—are likewise evolving: "…like supply chain compromises" (JAA-1p1). A utility has to be right in its defenses 100% of the time, while the adversary only needs to be successful once.

Participants from utilities reflected the perspectives and messaging of both the influencer and collaborative organizations. Common phrases included the perception of cyber threats as always changing and evolving and the threat is ongoing. Co-op-3p described cybersecurity as a challenge that has persisted for "decades," and Co-op-16p framed cybersecurity as a constantly changing challenge where you can't go home and consider the job "done" because "...the next week, something new is out there, a new threat is out there."

Looking to potential future threats, JAA-1p2 is concerned that voice recordings of utility executives could be used in audio deepfakes to manipulate utility personnel. At the extreme future extrapolation of cyber vulnerability is the specter of an adversary developing quantum computing capabilities, which would render conventional security obsolete. JAA-2p has resolved to cultivate a best

[3] In trying to keep a squirrel out of your bird feeder, you spend a few minutes trying to devise a system that the squirrel cannot overcome, but the squirrel dedicates all of its time to overcoming your system.

possible understanding of vulnerabilities and accept that eventual failure is likely inevitable: “We do everything we can do. We do everything that we know to do. And if we fail, we fail. But don’t let it be that you didn’t try to do something.” Ultimately, cybersecurity demands an iterative culture of continuous improvement that understands that no current state is a final achievement of security, and techniques that were effective in prior attacks may be overcome in the future.

Cyber Threats are Persistent Problems. Participants characterized cyber threats as persistent—constant and ongoing rather than discrete crises. The cybersecurity threats utilities face are not hypothetical. Framing current threats in the historic, global context, ISOp traced the evolution of threats from international incidents in 2010, 2015, and 2016. A primary point of emphasis for influencer organizations in their communications to utilities is the reality and gravity of the threat and the critical nature every interconnected utility plays in collective security. These threats are not only verified, but they have already succeeded in compromising the United States’ grid. INTELp asserted that “...there are entire networks within the government that, as we speak, are compromised.”

Participants from collaborative organizations not only agreed with the veracity of the threat but have seen the threat first-hand in their own organization. Even though JAA-1 is part of a relatively small-scale utility market, both JAA-1p1 and JAA-1p2 asserted that a utility of any scale is an attractive target for a state-sponsored attacker. JAA-1p2 related that their IT staff track attempted

intrusions by both nation states and cyber criminals "...every day, and they're working the front door and they're working the back door."

Utilities also echoed the collaborative participants' assertion of the reality and frequency with which utilities can positively identify attempted incursions. Co-op-3p, the smallest scale utility interviewed, described threats from state-sponsored actors at all levels of power provision that occur "...every few seconds and [from] country of origin—North Korea, China, Russia, you name it…It's not once every other day or something to that effect, it's all the time. And eventually, somebody finds a way into the system."

Electricity distribution utilities, including these co-ops, rely on computer systems that continue to become more complex to provide additional data so the utility can increase efficiency to preserve its financial viability. Increasingly complex systems entail new vulnerabilities. Between third-party contractors, multiple detection systems, and content filtering, utilities seek to keep up with shifting threat profiles and means of compromise. Co-op-3p lamented: "It is very difficult to detect if somebody is legitimate or an intruder onto your network."

Cyber Threat Responses Require a Cultural Adaptation that Provides an Incomplete Solution. Participants characterized cybersecurity as a challenge that requires cultural rather than technological adaptation, and the steps taken to guard against cyber threats are incomplete. At the influencer level, ADV-1p, ADV-2p, and ISOp have all adopted the term "cyber hygiene" as a way of conveying both the necessity of acts to keep systems safe and the need to make those acts routine. ADV-2p explained: "Hygiene…it's natural for people. [It's]

why we all wash our hands, [and the] same thing on the internet." This metaphor illustrates the ongoing need for cyber awareness and provokes parallels in behavioral adaptations encouraged to respond to the pandemic.

> If you don't want to be safe about the links, you don't want to be safe about your passwords, if you think it's too complicated to have a complex one, it's the same choice you make when you choose not to wash your hands after you go and work in the yard.

The absence of a definitive solution and the persistent nature of the threat requiring metaphoric "hygiene" fit the characterization of a wicked problem.

Despite a robust training program and buy-in from top executives who also participate in training and vocally encourage other personnel to do likewise, JAA-1p2 lamented ongoing difficulties maintaining cyber vigilance. The utility's training has been successful at ingraining the understanding that people are the critical point of failure to the majority of JAA-1 personnel. Most personnel are also conscientious about consulting with IT managers regarding suspicious emails or contacts. The remaining quarter of personnel are bound to engage in risk behavior, and even personnel who adapt good cyber hygiene practices frequently struggle to transpose techniques between professional and personal devices.

Knowledge alone is not sufficient to impel staff to take the necessary action consistently and across devices. Most of the cybersecurity shortcomings discussed were not malicious, they were just due to inattention. Even affirming that they record multiple attempted incursions daily by known threat actors is insufficient to shift behavior. Co-op-3p related that a staff member had used a particular collaboration software for years and so was familiar with it and,

needing a platform for collaboration and seeing it was not currently available in the utility resources, downloaded it.

This shortcoming is not just at the utility level. INTELp related that the agency suspended mock phishing campaigns that tested the vigilance of personnel during the first months of the pandemic, to not overwhelm the personnel during a time of already traumatic adjustment. However, a few months later testing resumed, and the click rate doubled. Personnel have also resisted incorporating security measures like MFA, which INTELp lamented lagged years behind the true need. Human behavior, rather than technology, has proved to be the consistent weak point.

Exacerbating this challenge is utility access to tools and solutions necessary to optimize security. Utilities often cite lack of funds for necessary protections and want to be reliant on the government for guidance and action. At the same time, the utilities often do not seem to have a clear picture of their own systems and vulnerabilities. INTEL-p asked: "[Does] the enterprise side have physical and logical maps of the control network? Do they know the security products that are being provided by the big control system vendors? All those questions are usually no." The government, though equipped to provide intelligence and guidance in educational programs, often falls back on "canned" presentations. The ideal path, according to INTELp is "...public-private partnerships need to be better. We need to have a better understanding of the needs." In the face of rapidly evolving threats that span geographic and political boundaries, responses must be built on thorough knowledge of systems,

capabilities, and weaknesses, and incorporate accurate, current information and techniques. This is beyond the scale attainable by a single entity; effective education about training for cybersecurity and response demands collaboration across the industry.

Issues Managers Disagreed About Lasting Effects of the COVID-19 Pandemic

Participants from collaborative organizations and utilities characterized the COVID-19 pandemic as a significant force that shifted utility operations, upended their means of interacting with customers, and provoked significant financial challenges. However, perspectives about the expected long-term impacts of the pandemic differed, including what a return to a prior state of "normal" for public health and social behavior might or might not entail; the relative transience or permanence of the shift to telework; and technological challenges faced within service areas. As such, many perspectives on the nature of the persistence of the pandemic itself, specifically, differed from the wicked problems frame and suggested that the pandemic may be viewed as an issue within larger public health and socioeconomic wicked problems.

Utilities expressed particular concern about the difficulty of replacing control room operators and technicians in the event of illness. ADV-1p stated flatly: "COVID-19 was a real threat to our workforce." Co-op executives adopted guidance that supported "sequestering their most critical operators away from their families at great costs, in order to keep them in the control room to keep the lights on." ISO participated in the production of an online guide that shared lessons learned from utilities. The core goal of these efforts, ISOp indicated, was

to “keep the lights on” regardless of additional compounding influences—a common refrain among participants and utility public relations communications. ADV-2p elaborated that utilities reacted by identifying personnel who must do their job in-person, and compartmentalizing teams and shifts to minimize risk of loss: “A lot of people did shift assignments at the substations…you’d work 10 hours and then you’d go and you’d sleep in a different part of [the facility], the trailer outside.” ADV-1p affirmed that practices like these and other adaptations to keep co-op personnel safe were recorded by the organization and shared across the utility sector in the “living document” guide.

The COVID-19 pandemic also impeded acquisition of hardware and materials by utilities. Repair and replacement of existing infrastructure, expansion of fiber optic networks for grid command-and-control or customer last-mile provision, and equipment for increasing telecommuting capabilities were all impacted substantially by supply chain issues attending the pandemic. Some of these issues have affected the day-to-day operation of the utility, while others have further compounded the utilities’ issue management of cybersecurity and/or adaptation to COVID-19 and ability to help customers adapt to COVID-19, compounding the issues across multiple tiers of messaging.

As with cybersecurity, the interview protocol established whether the way utilities and the organizations that influence them characterize the COVID-19 pandemic in a way that aligns with the definition of a wicked problem presented in the literature review. State governments and collaborative organizations informed utility perspectives on and responses to the COVID-19 pandemic, either

mandating actions to be taken or advising how to mitigate some of the threat of the pandemic. Accordingly, data analysis first examined collaborative organizations' and utilities' perspectives on the threat posed by the pandemic

Pandemic Challenges Are Evolving but May Not Persist. Participants agreed that the pandemic significantly impacted daily life and business operations, and that a total return to "business as usual" is unlikely. However, the perceived long-term persistence of daily impacts and the lesser or greater degree of return to "normal" differed significantly among participants. Co-op-1 characterized the pandemic as "part of a new reality that has reshaped daily utility operations and forced millions of other businesses to adapt to a very different world." This different world required wholesale reimagining of interactions and creation of a new plan for action and interaction that is "...always evolving. It's still to this day still evolving."

Some participants agreed with the view that the pandemic has significantly shifted expectations and ways of doing business across all sectors, not just among utilities. TA-1p asserted that the COVID-19 pandemic "...has shaken our understanding of normalcy. Its impact is, and will continue to be, writ large on the world stage." While the pandemic itself may not continue in perpetuity, the challenges it has posed will likely continue in greater and lesser forms. Co-op-5p agreed with this perspective:

> ...there's no going back. We're not just going to suddenly wake up one day and COVID is going to disappear and everything's going to go back to normal because whatever normal is, is going to look completely different and we need to be willing to flow with that.

This participant perceived impacts to ways of doing business and providing services and that have highlighted shortcomings in the old models and forced adaptations and concessions. Whether masks and vaccines remain an ongoing concern, the pandemic promises lasting and evolving impacts on the models for business.

In contrast, utility communications addressing external publics rarely framed the pandemic beyond the present and immediate future timeframes. Communications to member/owners usually cited changes "for this year," but rarely forecasted beyond. These changes often address an annual meeting or other discrete events, which may account for the immediate focus.

A few utilities did address the pandemic in a broader scope, however, and those convey a view of the pandemic as a persistent, perpetuating problem. In its communications with its member/owners, Co-op-7p described the challenges of COVID-19 as "evolving," "ongoing" and with "changing circumstances," indicating it was a continuous challenge rather than a discrete crisis. Similarly, Co-op-8 pointed to the "challenges and opportunities presented by the pandemic," also characterizing COVID-19 as ongoing and dynamic rather than finite.

Adaptation to the Pandemic May Have Changed Telework Expectations. Participants disagreed as to the degree to which adaptations to the pandemic will produce a lasting shift to telework, primarily due to differing organizational cultures. Many participants believed that remote work was likely to remain the norm for non-operations personnel, which could simultaneously ease some and complicate other aspects of personnel acquisition, retention, and

performance. Likewise, while utility operational functions are necessarily in-person, steps taken to protect personnel and member/owners will likely remain even if the severity of this particular pandemic recedes.

Participants agreed that the pandemic had a massive impact on work conventions for utilities but disagreed as to whether the changes would linger. TA-1p identified the sudden shift to remote work as the greatest challenge with the pandemic. Remote work had previously been viewed skeptically by utility executives, due to the degree that onsite work is required for operations. “Now it’s the way we’re all doing business. We’re never going to return to the office in the same way.” Co-op-16p also noted how the pandemic has reshaped the day-to-day operations at the utility. While the utility had ample hardware to adapt to remote administration and related needs during the pandemic, the subsequent shift forced a reckoning with assumptions of how the office side of the utility needed to operate: “…what are our essential tasks that we perform on a daily basis, and what are not? And I think we gained a lot of efficiency going through that.”

Conversely, JAA-1p1 perceived the degree of remote work as fleeting and assumed that remote work would persist past the end of the pandemic at a smaller scale than during the pandemic because of the agency’s preference for in-person work. JAA-1p2 affirmed the perception that the degree of remote work at JAA-1 was unlikely to persist due to the agency’s preference for in-person work. This is not evidence of a wicked problem because it is a matter of work culture.

Many co-op participants directly acknowledged technology as the primary challenge in the move to remote work in response to the pandemic. The utility’s

contact center was the “most significant group” still using desktop computers, according to Co-op-3p. Transitioning those employees to work from home required significant equipment acquisition to answer phones and use the necessary software. Co-op-5p related that, while most employees already had a mobile device to make the transition to remote work (for those able to do so), others still relied on a company desktop in the office. Field employees at both Co-op-3 and Co-op-5 already had remote systems, devices, and apps that streamlined the move to remote work and allowed for uninterrupted system monitoring and maintenance and capital improvements.

Adaptation to COVID-19 May Have Reduced Professional Collaboration. Some participants also discussed non-technical challenges attending the pandemic’s broad move to remote work and online mediated interactions, though others disagreed as to the legitimacy of the impact. Participants also discussed non-technical challenges attending the pandemic’s broad move to remote work and online mediated interactions. JAA-2 cited a persistent challenge in the move to remote work in “the lack of ability to have personal conversations, because we would get together in meetings and hallway discussions…the relationships you would build.” These relationships can be essential in a technical environment facing technical challenges (e.g., cybersecurity). Multiple perspectives and multiple “sets of eyes” on systems can be essential in avoiding a problem or overcoming one. Isolating each worker can effectively place blinders on them, limiting their perception and critical appraisal of systems.

Participants also lamented the impacts of Zoom beyond the workplace and in the broader industry culture. JAA-1p2 asserted that any "new norm" will likely see increased virtual conferences and meetings that significantly reduce travel. While beneficial to utility budgets and potentially increasing attendance figures by reducing travel barriers, virtual conferences lack the "hallway conversations" and impromptu socialization that built the strong relationships upon which public power mutual aid and information sharing networks were founded. Alternately, JAA-1p2 believes that whatever in-person meetings remain will likely "be more coveted and perhaps more effective if there's fewer opportunities."

The Pandemic Generated or Compounded Different Technological Problems. Technology played a large role in utilities' adaptation to the pandemic, but each utility faced challenges reflecting their particular operation, and cited these challenges as significant or negligible, accordingly. In addition to the challenges in outfitting personnel with devices to shift to remote work, utilities faced challenges helping their member/owners adapt to mandated office closures during the pandemic. Co-op-4p noted with pride that the impact of the pandemic on the utility was "completely transparent" to its member/owners—the adaptations the utility made to the pandemic did not impact service restorations, billing, or other member/owner-centric activities. However, the ability of a utility to offer all of its services online following the closure of its office lobby did little to help member/owners that lacked reliable internet. Some utilities had installed kiosks in their office lobbies and encouraged member/owners to use them. Others made greater use of a drive-thru, or extended Wi-Fi service to the utility parking

lot to allow member/owners who lacked reliable internet to connect via the utility's public network.

Beyond the scale of utility services, participants frequently brought up challenges that member/owners faced in the widespread move online during the pandemic. Utilities have been integral to their communities since their founding, and many felt a powerful obligation to do all they could to help their communities as they struggled during the pandemic. Co-op-2 cited positive impacts of the pandemic in its forcing societal refocusing on the needs of "vulnerable populations," and to "pull together as a community." Co-op-5 asserted that the pandemic challenged many assumed practices in education, and schooling will likely feel an extended impact by the shift online, use of masking, and vaccine mandates. Such concern for the member/owners beyond the scope of providing service led to many utilities launching member/owner-focused fund-raising efforts to help with financial challenges during the pandemic.

Issues Managers Agreed that Cybersecurity and the Pandemic Compounded

COVID-19 compounded organizational cybersecurity and efforts to ensure cybersecurity. In response to suggested or mandated actions in response to the COVID-19 pandemic, utilities first struggled to identify what roles could shift to remote without undue comprise to system security, to equip new remote workers with the tools necessary to work remotely while maintaining information security, and to design shift schedules for personnel unable to transition to remote work that ensured their safety and adequate staffing of critical facilities.

Work-from-home mandates impelled a new magnitude of cybersecurity. Personnel working from home required additional hardware and software to be able to complete their work through remote access while not compromising the utility. Remote personnel presented a greater target for threat actors, and working from home isolated personnel from the office environment in which they were trained to practice cyber hygiene. Participants from influencer, collaborative, and utility organizations all asserted that being at home may substantially undermine cyber hygiene practices. Further complicating adaptation of cybersecurity during the pandemic included the spread of misinformation and disinformation that impeded collective apprehension of the nature and scale of threats.

Telework Posed Technological Challenges. Participants described varying levels of impact to organization operations resulting from adaptations to the pandemic. Common themes among many participants included the need to acquire hardware and software to speed the transition online, ensuring secure access to the organizational network from dozens of connections through residential Wi-Fi, overcoming phone logistics, and other technical matters. TA-1p related how adapting security protocols to remote work compounded the processes to ensure secure connections to the organization's network: "…it's almost an all-day ordeal just to get one person to reset a password right now. Most of the time, they end up having to drive into the office and get on the Wi-Fi in the parking lot."

In contrast, JAA-1p1 considered the adaptations required as a matter of scale rather than capability: the move to online work did not demand new

cybersecurity practices, even if it demanded additional hardware and software. JAA-1p2 noted that, while the organization had a VPN prior to the pandemic, the shift to remote work entailed enhanced cybersecurity adaptations including limiting access through the VPN to only allow logins from approved countries through conditional access policies. JAA-2p recognized the security complications that attended "extended borders" with remote work: "the biggest impact for COVID-19 was the spread of the utilities or any staff out to their homes." Adaptation to remote work was less of a technical challenge for JAA-2p: "…we had to bump a little bit of bandwidth. It wasn't that big of a deal for us."

ADV-1p perceived that IT personnel at utilities struggled with mandated shifts to telework in response to COVID-19 because telework was not an established practice and accommodating remote work required enhanced cybersecurity tools and training. Likewise, TA-1p affirmed that the pandemic demanded adaptations of cybersecurity in response to the great increase in connected devices and use of online platforms "…from Zoom on down."

Other challenges were specific to the utility, its resource base, and existing hardware. Co-op-1p appreciated the extensive effort by in-house IT to accommodate the move online and work with personnel: "…all sorts of hoops to jump through to get to our information." Multiple co-ops discussed challenges with establishing or expanding use of their utility's VPN, and that slower speeds at which VPN operates compared to in-office access has proven frustrating for personnel. Co-op-6p'sIT staff first updated software on old laptops in the utility's

possession and then augmented hardware resources with laptops sourced from local technology stores.

Several of the co-op participants discussed how the deployment of multi-factor authentication (MFA) and tokens prior to the pandemic improved their ability to adapt cybersecurity to remote work. Reflecting a common sentiment among utilities, Co-op-3p asserted:

> Our cybersecurity is right at the top of our priorities when it comes to safety in general…Our IT team had already implemented proper [security measures] in advance of the pandemic…and a large number of the workforce was used to having to work with those security measures in place.

Security and access measures in place before the pandemic, such as mobile or physical security tokens and similar safeguards, had acclimated personnel to MFA procedures and other security access protocols and eased the switch to remote work.

Co-op-5p launched an MFA-protected intranet. However, the IT department's increasingly robust standards for passwords generated significant protest from personnel until the requirements were dialed back to a tolerable level. Personnel still complain about MFA but have accepted it as a necessary aspect of information security. This anecdote illustrates a common theme of balancing an optimal cybersecurity posture with one the personnel will tolerate. Pushing tolerance rarely approaches optimal security, so both ideals end up compromised in the final execution.

Telework Responding to the Pandemic Increased the Cyber Attack Surface. Participants agreed about the primary risk posed by the increased

telework: the corresponding increase in targets for threat actors. The sudden shift to telework presented a significant challenge for utilities and a massive target for threat actors. FEAp described the sudden, mass shifts to telework and the corresponding increase in threats that demanded "heightened awareness and extra vigilance" from utilities. INTELp affirmed that threat actors increased activity in response to government mandates limiting in-person work during the early stages of the pandemic. TA-1p also recognized the uptick in malicious activity as threat actors sought to take advantage of the shift to remote work. Fortunately, in-house IT training had prepared staff over prior years, and "all that training and preparation kind of went into action…if we weren't properly trained or if people had no clue, I'm sure [there] would have been some sort of compromise in our system."

ISOp affirmed that the move online offered other nations and criminals "increased attack surface area" to exploit U.S. systems. Many programs and tools are available to utilities to address this attack surface, but those resources are cost-intensive and are not aligned with the limited budgets with which public utilities operate. Fortunately, at the time of the interview, no outages or losses of service had been attributed to cyber attack on the electric grid due to the pandemic (NOTE: ISOp perceived two significant cyber attacks that compromised business software used by utilities during the pandemic as *concurrent with* but not *precipitating from* the pandemic; however, these concurrent attacks highlighted the risks that are omnipresent). True to its role, ISOp's organization focused efforts on devising best practices and educational materials for utilities. "We saw

a 96% increase in the number of cybersecurity shares in 2020 compared to 2019 and that trend continues into 2021."

Telework Responding to the Pandemic May Have Undermined Cyber Vigilance. Participants agreed that increased telework resulted in poorer cyber "hygiene." The decreased interpersonal interaction during the pandemic challenged organizations' ability to monitor and identify cyber threats. Interpersonal interactions suffered from the marked decrease of in-person personnel, and challenges manifested from reduced collaboration between colleagues and the corresponding reduced informal cross checks on processes and systems. INTELp believed that decreased vigilance by personnel new to remote work significantly compounded security, speculating that separation from the office environment dissociated personnel from learned cybersecurity behaviors, which led to a spike in cyber incidents immediately following the initial shifts to remote work. Consequently, INTELp questioned the long-term viability of remote work, particularly for utility personnel: "Can the CISO [Chief Information Security Officer] live in Atlanta and work for Southern Cal Edison?" Co-op-6p also felt that the isolation of work-from-home and attendant dissociation with office practices undermined cyber hygiene.

JAA 2p perceived that a major business software breach during the pandemic stemmed from a lack of in-person collaboration that could normally have caught the security issues—the more people reviewing the operation of a system in real time, the greater the likelihood one will notice abnormal behavior. JAA-1p1 countered that the major business software breach was neither directly

related to the pandemic nor to telework: It happened to occur during the pandemic but responsibility primarily fell on in-person staff working at an organizational facility.

Issues Managers Saw the "Digital Divide" Exacerbated by the Pandemic

The protocol specifically sought to explore the mutually compounding effects of COVID-19 and cybersecurity. However, interviews with the utility representatives highlighted additional issues stemming from socioeconomic disparities that the participants perceived to be of greater impact to the utilities and their member/owners during the pandemic than cybersecurity. Socioeconomic disparities have been core concerns of co-op utilities since the Rural Electrification Act created co-op utilities in the 1930s. TA-2 asserted: "When electric cooperatives brought electricity to rural America, the playing field leveled and small towns experienced a renaissance."

Several interviews highlighted the importance of the "digital divide" in the ability of co-ops to adapt to COVID-19 while maintaining cybersecurity. The "digital divide." The "digital divide" is broadly defined as phenomena that exacerbate existing "cultural, geographic, political, and physical barriers" when people already disadvantaged face "gaps in access to computers and the Internet," (Rains, 2008, p. 284). Both time to connect to the Internet and speed of download have been shown as significant factors in Internet use, perceptions of the Internet as a communication resource, and use of the Internet for health-related information seeking (Rains, 2008). Access to broadband Internet and overcoming "digital divide" is important for rural communities and could fundamentally

change the potential for participation in society and reaction and adaptation to shifting norms of interaction and distribution of information.

The "digital divide long preceded the COVID-19 pandemic, but societal adaptations to the pandemic exacerbated the existing inequality. Some utility personnel lacked broadband Internet at their residence and so were unable to work remotely. The lack of broadband access in co-op service areas also compounded member/owner's ability to pursue remote work and schooling. While not one of the two wicked problems at the center of the plan for this study, the prominence with which co-ops identified the need for broadband access, the compounding influence of the pandemic, and the identified solution addressing a symptom[4] of a problem rather than the core problem itself (i.e., broadband access vs. socioeconomic inequality), the proposed solution provoking additional challenges (e.g., supply chain issues with fiber optic cable, challenges to easements, and new legislation necessary to allow utilities to create subsidiary organizations to provide broadband) suit the character of wicked problems, and the compounding nature with COVID-19 suited the framework of this study.

The Digital Divide is Rooted in the Same Inequality That Produced Co-op Utilities. Co-op utility service areas originally comprised rural regions that had insufficient population density or affluence to interest investor-owned utilities. Many of the regions still remain sparsely populated, including farmland and mountainous regions that make cost-per-mile of line expensive. Conversely,

[4] As established in Footnote 1, Chapter 2, discussion of wicked problems in the document refers to the issues or crises that precipitate from a wicked problem as "symptoms." Symptoms are the issues and crises to which issues managers respond. In this study, no issues manager responded directly to the root cause(s)of a wicked problem.

some service territories have experienced significant growth as population centers have expanded into previously rural regions and exurban developments have supplanted farms. For those utilities, this has brought a significantly wealthier customer base that also expects different levels of service, presenting different challenges in member/owner interactions.

While the co-op service areas were originally defined by the absence of for-profit service, the boundaries of service areas were codified by government agencies long ago, leaving the co-op as the only possible provider (i.e., a for-profit does not have the option of calculating an area as now sufficiently profitable to warrant attention), and so historic socioeconomic disparities have been preserved in politically defined boundaries, even if or when that disparity no longer exists. The co-op utility remains a not-for-profit entity, however, and so it answers to member/owners rather than stakeholders and works with more limited financial resources than investor-owned utilities. Socioeconomic challenges most frequently cited by utilities included financial stability, reliability of service, and broadband access to the Internet.

Broadband Internet Is Necessary for Enfranchisement and Adaptation to Pandemic Mandates. Case study utilities affirmed the essential nature of broadband service by characterizing it as a peer to other utility services. TA-1's communications presented broadband service as the "fourth utility," joining the ranks of electric power, gas, and water as essential services for residential and commercial member/owners. This firmly asserts the shift of broadband from luxury to necessity, and the degree to which populations lacking

broadband access are disempowered and underserved. Broadband access is essential to engage fully in contemporary education programs, economic development opportunities, and cutting-edge telehealth, among others.

Several co-ops called back to their founding under the Rural Electrification Act in communications addressing their nascent broadband efforts. TA-2 cited the keynote speech by Sonny Perdue, Secretary of Agriculture, at the 2018 National Rural Electric Cooperative Association (NRECA) conference:

> Rural broadband is not just a luxury—it's essential…I don't believe that America would ever reach the productivity we have today across our nation without abundant flow of electricity…we cannot make America great again without high speed e-connectivity available to every American.

In a press release, a member of the Board of Directors for Co-op-2 recalls the co-op's founding 80 years before asserting that the need for broadband today was nearly the equal of electric service, affording "life-changing service" to co-op member/owners. In another published statement, the president of Co-op-2 viewed the 2020 launch of a broadband initiative in the co-op's service area as "My biggest accomplishment," expecting the service to bring transformative benefits to the rural service area.

In addition to reflecting on ties to history of providing services to their communities and the growing importance of reliable Internet access, several utilities tied the digital divide directly to socioeconomic inequality. In a communication announcing a multi-utility partnership to broaden deployment of broadband, Co-op-9 quoted an assertion by NRECA that more than 20 million Americans lacked broadband access, most in rural areas. Co-op-9 further

explained the geographic barriers that discouraged broadband providers from reaching rural communities, including topographic challenges in the Appalachian and Rocky Mountain states and frozen ground in the northern Midwest and Alaska. The co-op then affirmed that economic factors played an even larger role, in that the Internet providers did not see a sufficient financial incentive from the small customer base to overcome the geographic barriers.

Pandemic Responses Challenged Multiple Dimensions of the "Digital Divide." The lack of broadband access is not just a technological issue; it is a social service issue. Utilities' commitment to their community impelled them to help their member/owners respond to the pandemic, when online bill pay was only one of the digital needs unfulfilled. Multiple co-op participants and co-op communications discussed local students unable to attend school via remote learning, and local people unable to access healthcare because of their inability to use telemedicine.

Several utilities responded by setting up Internet hot spots in their parking lot, launching a publicly available Wi-Fi for member/owners to use. TA-1 produced a series of stories in 2020 profiling co-ops that set up hotspots in their parking lots for local students, and Co-op-8 announced in a press release that it had logged almost 1,000 unique users on these hotspots.TA-2 cited a report asserting that approximately 54,000 school age children in their state lacked Internet service at the beginning of the pandemic. TA-2 utilities partnered with school districts to bring broadband connection to homes in the service area and afford students a chance to engage in remote learning during the pandemic.

Broadband access is not the only issue related to the lack of broadband in co-op service areas: a lack of digital literacy challenges short- and mid-term solutions meant to help overcome the digital divide. TA-1 affirmed that many people in the communities its co-ops serve still rely on on-person interaction for bill paying and other customer service concerns. Many of the utilities have been foundations of their communities for more than 80 years, and the services they offer are ingrained. Shutting the office may not seem to be a great deal, but for many co-op customers it upended their interactions with a trusted service provider. Prior to the pandemic, Co-op-6 installed a kiosk for customers so that they would not have to wait in line to pay, but it saw little use. Co-op-6p lamented: "The kiosk has been around for probably two or three years already…people really didn't know about it, or maybe they are hesitant to use it." Perhaps member/owners perceived this work-around for the lack of Internet access as less optimal than addressing the inequality itself.

Utilities Had to Accelerate Planned Fiber Optic Networks. Many utilities had previously integrated or had begun to construct proprietary fiber-optic networks to improve grid management and metering and incorporate other "smart" command and control technologies. Co-op-9's communications asserted that the new fiber optic cable would improve grid reliability and safety and open new services such as advanced load control and improved telecommunications. These "middle-mile" fiber optic networks, whether already part of the utility communications network or just beginning to be installed to upgrade the network, left only the "last mile" connections to residences and businesses. Several utilities

in this study saw the opportunity to form partnerships and/or subsidiary companies to provide this last mile service or contracted with broadband providers to do so.

Utilities that undertook these projects frequently touted the benefits of their projects with their member/owners, and their corresponding trade associations relayed the achievements to the member/owners of all their member utilities. Co-op-3p was proud of the serendipitous timing:

> Our first customer was connected in November of 2020—so during the pandemic—and that's when we got a strong push for [broadband]…We didn't have a crystal ball, but having this capability within our area was not only a benefit and a luxury, but now it's becoming essential.

Co-op-8 launched its broadband effort in 2008, though construction did not begin for more than 10 years due to legal hurdles in setting up the subsidiary and other issues. During the intervening time, "the lack of access to high-speed Internet suddenly became an even more critical gap to fill…there is no higher calling [for Co-op-8] right now, short of keeping the lights on." In another communication, the utility affirmed that, along with the state moratorium on electricity disconnection[5], the utility and its broadband subsidiary decided to abide by the FCC pledge to "Keep America Connected" by voluntarily suspending broadband disconnection as well. This underscores the utility's conviction that broadband is an essential service rather than a luxury.

---

[5] Early in the pandemic, 34 states passed moratoria on disconnection from service (the remaining 16 approved voluntary moratoria at utilities' discretion). This posed a significant burden to co-op utilities already stretched by financial complications of the pandemic (e.g., the shift to remote work, lack of supplies for maintenance and construction). Most expired by November, 2021 (National Association of Regulatory Utility Commissioners, 2021).

Utilities frequently argued for the necessity of broadband to its member/owner publics. Co-op-9's communications assert both the necessity of broadband and the inherent logic in its integration, to the point that inclusion in grid infrastructure should be automatic. The co-op almost seems to be rallying its own customers to demand this service—which it already planned to offer—or to demand other co-ops follow suit. TA-2 cited the broadband deployment as a way to "close the digital divide" between more urban populations with access to broadband and rural populations that do not. The article highlights the difference that access to versus lack of broadband has made since March 2020, when "our world turned to virtual solutions for education, telehealth and work-from-home situations." TA-2 lauded the new network as "future-proof" and an equalizing factor in Internet access "for 50 years or more."

Additional socioeconomic equalization foreseen in the expansion of rural broadband includes increased potential for telework that may preserve existing population and bring in new population, countering the historic trend of rural communities losing residents to urban centers for the sake of proximity to work. Co-op-5p sees a long-term equalizing influence of access to broadband, as people increasingly seek to work from home and so their place of residence is less tied to a geographic proximity: "...people won't necessarily flock to urban areas, because they'll have one of the same resources available to them out in the rural communities."

These efforts met many complications: nonprofit utilities were not able to provide for-profit services, utilities needed to negotiate with Internet service

providers and lobby for new legislation to provide the necessary means to deliver broadband to their service areas. Utilities also needed to acquire the necessary hardware to build the fiber network, which was itself compounded by COVID-19 as supply chain shortages led to lead times of a year or more on critical materials. In addition, bringing broadband and Wi-Fi to member/owners brings a substantial risk for utilities in cybersecurity. TA-1p noted that the trade association "regularly puts pieces in the [proprietary lifestyle] magazine…to make sure that members understand that as soon as they're online with the cooperative, they're putting everybody at risk. All it takes is one point of entry, as we now know."

The "Digital Divide" is not a Wicked Problem; It's a Symptom.

Despite the power of broadband connection and the myriad complications the lack of broadband holds in contemporary America (before even factoring in the pandemic), it is not a wicked problem itself. It is a symptom of the wicked problem of socioeconomic inequality. Co-op-5 asserted that the issue of access broadband can be "solved, which it should be [in] anywhere from two to five years." The ability to solve a problem eliminates its consideration as a wicked problem. Chapter 5 explores the difference between wicked problems utilities face and their issue-focused strategies for alleviating symptoms of those problems.

RQ_2: Role of Legitimacy in Compounding Wicked Problems

Research questions 2a and 2b asked how utilities legitimize their definition of a wicked problem and how they perceive legitimacy among other organizations' definitions of and strategies to address wicked problems. Questions

of legitimacy and the ability to define what is or is not legitimate center on three factors: (1) Acceptance by publics that an issue exists the way an organization claims; (2) Acceptance by the publics that an organization has authority and knowledge to address an issue; and (3) Acceptance by publics that an organization's approach to the issue is valid and will address the issue in the manner in which the organization claims (Coombs & Holladay, 2018; Smith & Ferguson, 2010). In this study, participants often linked legitimacy with credibility and trustworthiness, which are distinct ideas in that they emphasize perceptions that a source or authority is to be believed, but do not stipulate that the source or authority may influence the definition of the issue or the action to address it.

Issues Managers Prioritize Vetted Sources in Communication Networks

Utilities are embedded in information-sharing networks and mutual aid networks that simultaneously improve the speed at which they vet information and insulate and isolate them from other potential sources of information. Utilities accept the reduced number of information sources in exchange for allowing quick assumption of authenticity of information. Other utilities, national nonprofit advocacy and information-sharing organizations, and government agencies are among these vetted sources of information. The only distinct mention of loss of legitimacy in influencer actions was INTELp's assertion that agency presentations are sometimes perceived as "canned," and not tailored to the needs of attendees of education sessions.

Utility networks of communication are closely knit, carefully vetted, and extremely skeptical of new interlocutors. Admission to the network affords access to many utilities through mutual aid, information sharing, and other support communications, all of which entail exposing the utilities to critical vulnerabilities. By keeping their peer network small, utilities keep the connections known and the information verifiable. This improves the legitimacy of the sources by affirming their expertise on issues and their methods of determining appropriate actions in response to issues in advance, which speeds reaction to issues by reducing the arguments for legitimacy of the advocating organizations to justifying how their action will address the issue(s). Vetted networks of communication also eases utilities' ability to seek replication of intelligence through multiple sources as the best validation of information and provides utilities with additional confidence in the information they choose to relay to their member/owners.

Collaboration in these networks further enhances trust and cooperation. JAA-2p reflected on the impact of the COVID-19 pandemic on these collaborative relationships, concluding that relationships between information sharing and analysis organizations, joint action agencies, public power, and federal organizations benefited from the challenges presented by the COVID-19 pandemic. Legitimacy cultivated during one collaboration strengthens inter-organizational trust, which will benefit these organizations in future collaborations.

Participants from national and regional organizations as well as utilities all emphasized the weight they place on the legitimacy of their sources of information and intelligence. Many organizations have collaborated in formal and informal arrangements for years if not decades. This collaboration cultivates familiarity that speeds appraisal of legitimacy of an organization's knowledge of and authority over an issue. Verification of two of the three parts of legitimacy enhance willingness to accept the legitimacy of the action proposed in response to an issue.

Federal Agencies Lead Development of Guidance Materials. Federal agencies develop policy and provide oversight to the electric distribution sector. These include the Critical Infrastructure Protection Advisory Council—Energy Sector (CIPAC-ES), founded by the U.S. Department of Homeland Security (DHS) and now overseen by the Cybersecurity and Infrastructure Security Agency (CISA). CIPAC-ES supervises and advises the Electricity Sub-Sector Coordinating Council (ES-SCC), led by the U.S. Department of Energy. ES-SCC includes representatives from a dozen prominent national industry associations and oversight groups, including four specifically mentioned in participant interviews: the American Public Power Association (APPA); Edison Electric Institute (EEI); National Rural Electric Cooperative Association (NRECA); and North American Electric Reliability Corporation (NERC), which regulates larger-scale utilities. Two other frequently referenced organizations include the Electricity Information Sharing and Analysis Center (E-ISAC), for which NERC is the parent organization; and the Multi-State Information Sharing and Analysis

Center (MS-ISAC) for which the national nonprofit Center for Internet Security (CIS) is the parent organization.

FEAp discussed the critical role that executive agencies play as authoritative sources of processes and procedures. Trust, FEAp emphasized, is a central requirement between organizations supplying and receiving threat information. Likewise, executive agency strategies that are designed to help utilities respond to threats and breaches emphasize potential mitigation of the threat rather than cataloging organizations affected by a threat. This emphasis conveys that federal agencies are more concerned with alleviating threats themselves than scrutinizing the organizations that suffered the breach. These tactics enhance legitimacy by emphasizing the agency's authority regarding issues affecting utilities and focusing on understanding problems rather than cataloging breached utilities underscores their interest in developing solutions designed specifically to address the issue.

Established collaborative networks and improved understanding of and engagement with relative government agencies are critical during an energy disruption. FEAp conducts emergency response exercises with utilities and national and regional organizations to build and test collaboration and coordination capabilities. FEAp also collaborates with state, local governments, tribal governments, and territorial governments, which can provide insights to bolster local engagement by a public power utility.

During the COVID-19 pandemic, FEA provided guidance to utilities about management techniques derived from previous pre-planning and exercises

conducted to prepare for pandemics. FEAp reflected: “If you look at the guidance that the sector provided, it was very much built on lessons learned…I think it was a very inclusive process. I don’t think we experienced much pushback at all.” This lack of pushback may indicate the acceptance of the advocated solutions as legitimate. The extensive planning and exercises support the appropriateness of the actions prescribed, and the broad base from which information was drawn and to which it is shared illustrates thorough understanding of the issue and appropriateness of the solutions for the utilities.

National Advocacy Organizations Amplify Federal Messages and Vet Information for Sector Organizations. National advocacy organizations are the key sources of information for utilities and trade associations and crucial links between them and the federal government. These organizations work on behalf of utilities to coordinate information and best practices, including collaborating directly with federal agencies and regional organizations to assemble materials or host webinars or meetings, and coordinating communications between member utilities and federal agencies.

The scale of operation for public utilities rarely reaches one that impels compliance with North American Electric Reliability Corporation’s Critical Infrastructure Protection (NERC CIP) requirements or other federal oversight. As such, advocacy organizations provide a valuable filter for practices that are advisable versus inapplicable. The relationships generated between advocacy organizations and member utilities, as well as the authority of the organizations

from which it draws information, bolsters the legitimacy of the organization to utilities.

ISOp affirmed their organization's dedication to its role as a conduit for information between federal agencies and utilities, citing close contacts at the Department of Energy, Department of Homeland Security, and the gas industry (upon whom a lot of generation capacity depends). ISO collaborates with many influential organizations that collect and communicate intelligence and information to improve utilities' operations. Utilities can also provide information to ISO and be assured of confidentiality, so they can share the results of breaches and not incur regulatory repercussions. This improves the quantity and granularity of information available to the sector.

Trade Associations Enhance Legitimacy of National Organizations. The regional level of influence includes trade organizations that provide broad support to national organizations' member consortia. All the above organizations have some degree of more or less direct influence over public electric utilities nationwide. However, none of these have the authority to dictate actions or policies directly; these organizations guide the utilities and provide best practices and insights into beneficial strategies.

Communications from trade associations to utilities reflect the messaging and strategies of the influencer organizations. TA-1p said that the first talking points came from national-level organizations in March 2020, "very quickly…so that everybody was kind of on the same page talking about what their cooperatives were doing." These talking points addressed safety aspects of

COVID response, such as more diligent cleaning, and other information that would be of interest to co-op customers.

TA-1 incorporated those talking points into their lifestyle magazine and member co-ops distributed the talking points in bill-stuffers, through Facebook question-and-answer sessions, on utility websites, and through customer relations personnel over the phone. The COVID-19 talking points were intended to be "a practical response for the inquiries that we're getting." Many of the questions focused on immediate service needs like whether offices were going to be open, and what to do if line workers had to work in close contact with other people. TA-1's legal department and association attorney received parallel guidance from both national organizations and other sources within the state like the corporation commission (i.e., the regulatory body in a state-level agency). The legal department relayed relevant workplace practices and workplace rules from federal government and the state government to co-ops, to filter relevant regulations for them in advance.

Co-op-4p remembered the talking points assembled by the national organizations and distributed through trade associations: "Both [organizations] provided—I don't want to say canned articles—but articles that could serve as starters…They could be adapted for each local co-op." Asked if the provision of this type of information is important, the participant responded: "We counted on that, and they do that. They did that before the pandemic. They'll do that after the pandemic."

To clarify practices and messaging for its member utilities' member/owners, TA-2 adopted the national organizations' "cyber hygiene" frame in an article in its proprietary lifestyle magazine. The article draws material from an NRECA publication that also uses the "cyber hygiene" frame, advocating steps that utility member/owners can take to improve their "hygiene" and protect themselves and their co-op utility. The single article embraces multiple forms of legitimacy, complementing multiple tiers of authority (national nonprofit and local trade association) with clear imagery and parallels to accepted practices.

Both participants from JAA-1 cited the Center for Internet Security (CIS) as a respected authority that provides foundational information. JAA1-p1 noted the foundational influence CIS had on the utility's planning: "We basically took [our cybersecurity remediation plan] straight from the CIS control list and made it into a project plan, and said, 'We're going to do all of these things.'" CIS is also the parent organization of a prominent information sharing organization upon which utilities rely, and which JAA-1p1 repeatedly cited as an influential and trusted source of intelligence and best practices. JAA-1 relies heavily on national advocacy organizations for best practices, cross-industry collaboration, and diagnostic tools developed by an advocacy organization. The advocacy organizations play particularly influential roles for JAA-1p1: "They're always sending us emails about security things related to COVID and plenty of webinars."

Utilities Are Legitimate Sources for National Organizations. ISOp described a collaboration early in the pandemic to develop COVID resource

guides. These guides were influenced by direct feedback from utilities: “We draw influence in a number of ways. Whether [utility owners] send us emails or texts or comment on portal posts or products, they influence us.” This direct correspondence and collaboration may be with analysts, executives including utility CEOs, and communications staff, providing a broad view of utility needs and perspectives. The interpersonal correspondence is accompanied by other analyses: “We’re collecting metrics, areas of risk they want us to focus on, what projects they want us to focus on, programs.”

Developing Informational Resources Enhances Legitimacy.

Information resources that are developed around a specific subject and/or addressing a specific group based on information from that group helps establish an organization as an authority on both subject matter and solutions for a tailored situation. Utilities look for such resources and benefit from their guidance. ISO curates a directory of pre-approved partners that are vetted “based on their mission, their organization” as well as cybersecurity vendors, equipment vendors, and U.S. and Canadian government agencies. This directory is available to member utilities through a portal, which includes means of sharing information and providing feedback to ISO. ISO relies on feedback to tailor its solutions to the needs of utilities. ISOp was aware from the onset of the pandemic that, while “everyone has different risk tolerances,” utilities favor safety and reliability.

ADV-2p emphasized the organization’s commitment to informing utilities about tools and services available and providing a conduit for communications with federal agencies, national advocacy organizations, and information sharing

organizations. This central role allows ADV-2 to facilitate cybersecurity preparedness exercises for utilities that underscore the potential for any utility, regardless of size or resources, to play a significant role in a breach or other cyber event. ADV-2 also acts as a channel to distribute authoritative information and to guide utility practices: "...information flow of vulnerabilities and security concerns is largely verified before it even touches us." They also distribute their research and publications through higher profile organizations like federal agencies to make the intelligence available to others. These documents are frequently "living" documents, regularly updated as new techniques are developed and lessons learned: "...it was an evergreen guide as we learned what was going on, as we've heard stories of issues, problems, solutions, that guide was updated to reflect this."

Vendors May be Trusted or Questioned. Vendors include hardware developers, software developers, and service providers, such as IT assistance or cybersecurity experts. Utilities view these sources with skepticism because of the known profit motive—there is an impelling force beyond the desire for the good of the utility. New vendors are often vetted through established peers or through national-level advocacy or information-sharing organizations.

Familiarity with sources is critical for JAA-1p2 to afford them any credibility: "I can't tell you how many emails I delete from people saying, 'Hey, we've got the next best wizard thing for keeping your firewall safe or keeping your data safe or whatever.'" JAA-1p2 cited a few vendors that the organization

regularly relied upon for intelligence and affirmed that the utility has directly collaborated with them all.

Utilities may include vendors among their group of accepted sources, particularly if the utility has contracted with the vendor for some duration. However, vendors are motivated by profit and may promote their products over competitor products more suited to the utility. As such, utilities may trust the vendor's authority regarding and characterization of an issue but may question whether the advocated solution is really the best way to solve an issue. The profit motive of the vendor is weighed against any information provided and the utility may confirm that information through a second, vetted source.

A breach to a commonly used business software platform during the pandemic massively undercut confidence even in previously vetted and trusted vendors: "How do we know if a vendor is secure for private data, for PII [personally identifiable information]?" asked JAA-1p2 "The [business software] hack is a huge red flag that people have been warning about for five years. 'This is the most likely way they're going to get in,' and then they did."

Misinformation/Disinformation Undermines All Legitimacy. Because of the cascading nature of utility vulnerability, new sources of information and intelligence of all types are treated warily. Co-ops are skeptical of unknown contacts claiming to provide important information. This wariness was heightened during the onset of the COVID-19, when the scope and magnitude were not yet clear and conflicting narratives muddied public understanding. ADV-1p was

alarmed by “the way in which our society accepted some of that misinformation [and] disinformation because of overall divisiveness elevated during COVID.”

Issues Managers Leverage Relationships in Public Relations Communications

Utility communications to member/owners frequently emphasize the role the utility plays in the community and its dedication to member/owners. These tactics appear to be a way to bolster the credibility of the utility’s message (and decision making). In their dedication to the community in general and member/owners specifically, utilities convey a deep understanding of the needs of member/owner publics and identification with their concerns and the challenges they face. Through these tactics, collectively, the utility establishes its legitimacy to the community through its understanding of the needs of the community (i.e., a legitimate understanding of the problem), the dedication it has to its member owners (i.e., legitimate position to address the problem), and intimate knowledge of the communities in general and the member publics specifically that informs their strategies to address the issues (i.e., the right approach to the problem).

Utilities employ slightly different tactics with internal publics. Internal public relations emphasize safety, reliability, and camaraderie, while still asserting the authority of external organizations that influence utility policy. Safety is a common theme in utility communications across all co-ops in this study, and the emphasis in internal communications is usually expressing concern for personnel as well as for the grid operation. Reliability, in turn, is a point of pride for the utilities and personnel, emphasizing that they serve their communities well and are dependable and accountable. Camaraderie builds the

sense of community and relationships within the co-op and is particularly valuable in the often siloed organization of a utility. These three qualities express the utility's understanding of the perspectives and priorities of its personnel, to establish it as a legitimate party to be communicating on their behalf, and that they understand the situation, to establish its authority to address a problem. These collectively, with the authority of sources of information, convey the dependability of the proposed solution.

Utilities' Role in Community Increased Legitimacy of Their Pandemic Response. Publics' perception of the legitimacy of utility communications is enhanced by the place co-ops hold in their communities. The smaller the co-op, the greater a role it serves in the community, and sub-30,000-meter co-ops are "bulwark institutions" according to TA-1p. "They're the organization that everybody turns to build lights at the baseball field—so they're deeply ingrained in the community." With this "bulwark" status, cultivated over more than 80 years of service to the community, co-ops have accrued significant "credibility or a certain amount of goodwill" that can offset some skepticism when publics question the reasoning behind a policy change or action. TA-1p asserted: "There is a degree of goodwill, a degree of local capital that can be spent down when an unusual situation occurs."

In communications with member/owner publics, TA-2 reinforced its own as well as its co-ops' dedication to their communities. An article discussing responses to the pandemic asserted the theme of concern for the community as "...one of the guiding principles for not-for-profit cooperatives." The article calls

back to the founding of co-ops, highlighting that the communities themselves formed them, and that co-ops have supported their communities through multiple crises. Many co-ops examined in this study used similar language to tie the founding of the co-op by the community to the current dedication of the utility to the community during the COVID-19 pandemic.

Co-op-4p discussed many ways in which the co-op tailors its services and interactions to the needs of their community. For example, the population of the Co-op-4 service area has become increasingly bilingual as exurbs sprang up on former farmland. Co-op-4p reflected: "We have a very large Spanish-speaking customer base, which is why all of our advertisements, our notices on our lobby doors, for example, when changes are made, when we introduced the payment kiosks—everything is bilingual." Also, Co-op-4p was the only participant whose utility refused to close their lobby during the pandemic: "It was a priority for us, and I think it's just a reflection of the number of customers who use our lobby." The decision to keep the lobby open also was an acknowledgement of the significant number of member/owners who pay their bill in cash, which is not feasible online or by mail. These efforts recognize the member/owners in their community, and demonstrate to all member/owners that they are seen and valued by the co-op.

Utilities Convey Familiarity to Member/Owner Publics. Utility communications to member/owner publics frequently employ the second-person voice, as though speaking directly to the reader. Phrases like "your co-op," "your

utility," "your electric service," and "your community" connect directly with member/owner publics and engender a sense of familiarity.

Co-op-1p enjoys interacting with member/owners directly at community events and even chance encounters when identified by the co-op logo on a shirt while at the gas station:

> I like being with people and telling the cooperative story. I'm the one at the events with the table and, "Hey, how's it going? You should be a member…make sure you have all the safety things ready for the storm coming."

Co-ops often highlighted such interaction as differentiators between their service and investor-owned utilities, in addition to co-ops' generally lower rates: "...what differentiated us from the investor-owned is having that personal contact with the membership."

Co-op-6p discussed how the utility tries to reflect member/owner interests in communications. "They don't care who the CEO is or not, they want to know [that] their electricity's going to stay on." Reflecting the interests of the readership increases the chance the communications are received, and demonstrates utility awareness of their audiences and authority to speak to their needs.

Participants frequently cited an aspiration to mold communications around member/owner publics' interests. Both TA-1 and TA-2 develop and publish a lifestyle magazine to be distributed to all member co-ops' member/owners. These magazines include some general news about energy and tips for efficiency as well as a several page insert tailored by each co-op with their own messaging. The rest

of these magazines, however, are indistinguishable from a regional lifestyle magazine. Profiles of prominent community members or organizations, feature articles about local destinations, seasonal recipes, puzzles, and other similar content add sugar to the medicine of the utility communications. These magazines provide member/owners with important information about the operations and policies of their co-op utility and provide many other reasons to open the magazine and read.

Utilities Emphasize Safety and Camaraderie with Internal Publics. Communication with internal publics often relies on invocations of safety and assertions of intra-organizational camaraderie to build perceptions of legitimacy in leadership messaging.

"Safety" is the "number one watchword" for electric utilities, according to TA-1p. The theme of safety has spread from protocols for line workers through facilities and now to technology and cybersecurity. "Safety" as a catch-all term for the driving motive behind utility policies has been ubiquitous to the point where its validity as a core value in the utility is assumed. Citing tactics as necessary for safety conveys and inherent validity.

Internal messaging about cybersecurity and related training from co-op leadership emphasizes it as a legitimate concern. ADV-2 described their organization's cyber training approach as emphasizing the holistic nature of cybersecurity—it extends beyond an "entity" concern and pervades both professional and personal life. Any device that accesses organizational systems can provide a foothold for a breach, and the persistence of threat actors outstrips

the vigilance of targeted personnel: “From the lens of the attacker, you’ve just got to find one way and you can take a thousand tries... If you’re the owner, you’ve got to protect against a thousand-plus different potential ways to try.”

While each utility is a small organization, TA-1 and its member utilities recognize that a threat actor only needs a single point of entry in a network, and any utility could be that point for their regional network or the grid as a whole. Multiple utilities confirmed that their IT staff log attempted incursions on a daily basis. Co-op-16 attributed personnel buy-in to factors that included a dedicated, reputable IT team; consistent training with follow-up to reinforce lessons and emphasize the importance of all utility personnel being diligent; and a couple breaches of unrelated organizations in the immediate area that “brought home” the reality of the threat.

JAA-1p1 considered how the utility’s CEO has constructed a unified theme of safety in messaging and communicated personally and frequently with personnel to build rapport. “Our CEO says in his weekly video updates…that his number one priority is to get us all back to work safely.” In accepting new adaptations to cybersecurity that enhance safety but complicate personnel access, JAA-1p2 noted little pushback from personnel, because cybersecurity is just one facet of the organization’s emphasis on the safety of both people and systems: “...we have a safety culture in general, and so I don’t get a lot of resistance.” In addition, the CEO places a high priority on cybersecurity and participates in monthly training: “We assign monthly training on cybersecurity and [the CEO] never doesn’t do his training…none of the senior team ever skips their training.”

Camaraderie among the co-op personnel is another theme asserted as a means for leadership to convey legitimacy through goodwill. Co-op-1 sought to cultivate a sense of camaraderie and provide some levity to utility personnel during the pandemic, to improve their reception of business changes during the pandemic. Co-op-1p related: "We sent out surveys to employees and we…I think we gave an additional paid day off…just little things to kind of be, 'Hey, these are weird times.'" These gestures were not drawn from any particular guidance or other organization, but the utility understood that many people were feeling confused, scared, and/or bored, and "We all worked together and just kind of put together a plan. And of course, the plan was/is always evolving." The co-op has continued this incentive program through the second year of the pandemic and is still seeking to capture the interest of personnel and emphasize "safety and comfort."

Leadership plays critical roles in legitimizing advocated strategies with internal publics. Co-op-4p described the approach utility leadership took to generating camaraderie with personnel during the pandemic: "Our president…was adamant that all of the executive team [continue to work in-person], so all the vice presidents…the leadership team…we were in every day. We did not work from home." In doing so, the president wanted to let operations and field personnel know that the leadership was not asking them to do anything that the leadership personnel would not do themselves. The co-op addressed different safety precautions like daily cleaning of office spaces and more thorough cleaning. Social distancing and masks in the office were required, and no outside visitors

admitted. The leadership still held meetings by Microsoft Teams or Zoom, to preserve distancing even though the personnel were all in the office. “We wanted them to know, you know, we’re in the office every day. We’re here. If you’ve got a concern or a problem, come see us.” In addition, the co-op released a weekly/biweekly online internal newsletter that conveyed the latest recommendations and guidelines for office or field work safety.

Co-op-16 adapted its office expectations to the needs of personnel. The CEO’s philosophy was: “If you can work remotely, go for it. If you've proven to me that you’re going to get your job done at home and if that’s a more comfortable environment for you…go for it.” The CEO’s trust in personnel has been repaid as the shift to remote work seems to have improved employee satisfaction and morale. “There’s been some silver linings in all this that have been a real blessing.”

Issues Managers Emphasized Community and Authority

Legitimacy is a critical concern for utilities when advocating for either cybersecurity measures or adaptations to COVID-19 because the validity of each issue, the effectiveness of potential means of addressing each issue, and attendant expenses may all be points of contention with both internal and external publics. By invoking community, utility leadership asserts that it understands the struggles of the members and personnel. In citing authoritative sources, utilities convey that information they are relaying to member/owners has been reviewed and confirmed by knowledgeable authorities. The most common themes in co-op

communications to member/owners centered on assurances of financial resources, health, and safety.

Pandemic Communications Emphasize Community Safety. Legitimacy was a critical quality for co-ops to convey to publics during the pandemic. TA-1p asserted that its member utilities had spent decades cultivating relationships with their communities, such that even given the challenges and strains of the pandemic, "I suspect there's probably still a well of goodwill that exists" between member/owner public and the utilities. This goodwill is essential for being seen as legitimate in member/owners' eyes. Co-op-3p reflected: "There was still a high percentage of not only the population, but our demographic here at the cooperative that just didn't believe that [the pandemic] was much of an issue."

Co-ops draw on their "well of goodwill" to convey legitimacy to their external publics when there is skepticism about an issue. TA-1 saw this as a particular need as business models shifted when the COVID-19 pandemic closed businesses and public spaces statewide, despite the co-op services areas being rural communities that were not yet impacted by the pandemic: "In an area of low [viral] transmission, when you're closed or you've altered your business policies because of COVID, yet it's not even a threat to your community, customers probably wonder why you were being extra cautious." In addition to goodwill, such messaging aligns with co-ops' historic pairing of safety with health in communications.

Health and safety together are common themes in utility communications. Both TAs and 11 of the 15 co-ops addressed health, safety, and reliability in a

combined 64 communications. The communications assured the member/owners of the reliability of service, and Co-op-8 captured a common sentiment in its asserting that the utility would "provide continuous and uninterrupted electric, solar and broadband services to our consumers." Other utilities proactively sought to identify challenges the mandates posed to member/owners and provide alternate solutions (e.g., free Wi-Fi in parking lots, additional pay stations, appointments for lobby visits to pay bills in cash). Co-op-1p described utility efforts to convey relatable experiences to member/owners: "We asked employees to take pictures of them in their masks, still doing their job, to kind of be like, 'Hey, we're still here. We're still reliable.'"

Co-op participants also universally expressed appreciation for the support of their communities and concern for the communities' well-being. Co-op-1 communications often framed arguments around community or statewide circumstances, rather than focusing on the utility perspective: "[People in our state] are still becoming ill and we decided to cancel the public portions of the annual meeting to keep our members safe and healthy." The co-op also emphasized its commitment to safety in its practices and of personnel while ensuring service to its community: "The Co-op has done everything it can to protect our employees from the spread of the virus while also providing our 103,000 members with reliable power."

Co-op-10 used its communications to express solidarity with struggles faced by member/owners, citing actions taken by the co-op Board "...in an effort to relieve financial stress on members caused by the COVID-19 crisis." Another

communication sought to bolster the utility's legitimacy by countering misinformation:

> There is a lot of information out there about what's effective at killing the COVID-19 virus and preventing its spread. Unfortunately, a lot of that information is false or misleading. Let's get the facts by taking a close look at three of the most common coronavirus myths.

Continuing the theme of safety, Co-op-9 asserted the need to practice social distancing with work crews and personnel on private property: "For your safety and the safety of employees." The co-op also reinforced the theme of reliability of service, noting that utilities are considered essential businesses dedicated to "keeping the lights on—with some social distancing and changes, of course, to ensure they return home safely after a day of work."

Co-op-16 echoed other utilities' mantras of solidarity with the experiences of member/owners and continuing dedication to safety and reliability. "...the COVID-19 pandemic has forced many of us to work with what we have on hand. Running to the store was not an option and, even if you did sometimes, what you really needed was not available." The understanding of uncertainty, scarcity, and other concerns faced by communities during the pandemic conveys the embeddedness of the utility in the community and its connection to community members. The co-op then assures member/owners that they can continue to rely on the co-op for services: "...when the COVID-19 pandemic hit, your cooperative adapted to the circumstances and stayed mission-focused. Our mission is to safely, responsibly, and reliably meet the electrical energy needs of our member-owners."

Co-op-4p related how the co-op sought to provide member/owners with vetted information to help adjust to the pandemic: “We tried to make that COVID resource center online a one-stop shop. That’s actually what we called it internally, a one-stop resource.” The utility used this resource both to inform member/owners and to assure them of the quality and conscientiousness of services they received: “If they had a problem or if they needed service restored or if they were moving…they could be assured that whoever came to their door or on their property that we would be following the CDC guidelines.”

Co-op-4p developed television spots to reach customers and shifted messaging during the pandemic to reassure member/owners and convey collegiality: “That [advertisement] was the one we did initially in the pandemic, we talked about our reliability. We talked about our commitment. You know, they could count on us.” The co-op developed this messaging to reassure member/owners and remind them of the co-op’s commitment to the community. “People were afraid, and the news was heavy, and rightly so…It was a hard time, and we tried to address that externally with a message of commitment, a message of dedication of our employees.”

TA-1 emphasized to member/owners that steps taken were not permanent and were being reviewed for when changes could be appropriate: “Personnel at your electric co-op are meeting regularly to assess the situation as closures, restrictions and the status of the virus change.” TA-1 also underscored that all actions being taken were vetted and in the interest of safety: “Protocols are in place to make sure that the staff, particularly the critical staff, including line

workers and control room operators, are healthy and following procedures to maintain their health." Finally, TA-1 conveyed the collaborative culture of electric power co-ops, and that multiple organizations were in agreement about the steps taken: "Your co-op is also in contact with the other co-ops around the state and has made plans for assistance in case there is a need." These assurances of vigilance, safety, and reliability directed to publics convey the careful authority of the utilities regarding their strategies.

Utility communications expressing solidarity with communities also looked beyond the community to illustrate common struggles in other communities. An article by TA-2 assures member-owners that issues faced by their co-op are being faced by utilities nationwide, and the pandemic will not impede their co-op's ability to "...continue to deliver electricity reliably and safely, according to a report from the North American Electric Reliability Corporation, the nation's grid watchdog." Appeals legitimizing the actions of the TA-2 co-ops can be seen in the comparisons with other utilities and with the assertion that actions are aligned with a vetted authority.

Utilities Cite Authorities to Bolster Legitimacy. Adaptations to COVID-19 significantly impacted most utilities' interaction with their member/owners and internal publics. Many of the actions taken by utilities in response to COVID-19 were mandated by state authorities. These actions were compulsory and included mandates closing public places of business. Mandated closures of places of business cut particularly deep for co-ops, as they lost more personal interaction with member/owners, a distinguishing feature from investor-owned utilities.

Fortunately, the legitimacy they had cultivated with publics minimized the impact. Co-op-3 experienced “Not a lot of pushback really on closing the lobby. We still haven’t opened our lobby and some of my peers in the state even mentioned that they may never open their lobby.”.

Most steps co-ops took in reaction to the pandemic were imposed by state governments. Resulting communications from utilities underscored their commitment to their community and member/owners, to preserve legitimacy while enacting policies that may have been confusing or frustrating for member/owners. One example from Co-op-15:

> After a thorough discussion of the current facts surrounding the coronavirus, review of information from experts about the pandemic’s likely status this fall and consideration of recommendations from health and government officials, the board voted [affirmatively] to cancel the [scheduled] meeting.

Co-op-5 invoked federal and local health authorities in messaging: “We are following guidance from the CDC and other local health organizations and officials to do our part to help mitigate the spread.” The utility offsets the elimination of one option for member/owners by outlining several alternate means to achieve the end: “...we strongly encourage our members to use remote payment options such as online payments, U.S. Postal mail, credit card payments by phone, or, if in-person payments are required, to use one of the payment kiosks located at each office.”

Co-op-8 was a rare utility to cite its own decision-making coupled with a desire to staunch spread of the coronavirus when closing facilities to the public. In one of its four public relations communications that directly addressed the

pandemic, Co-op-8 used collegiality and camaraderie to identify with members' struggles:

> I have yet to meet a person whose life has not been significantly altered, and certainly this is true at [our co-op] where we had to ensure electric reliability while adjusting to new safety protocols…While the challenges caused by COVID-19 have been daunting, I'm overjoyed to see how everyone is pulling together.

Two other communications affirmed the utility "made the decision to close its lobby until further notice" rather than employing passive voice or citing state restrictions or federal guidance. However, Co-op-8 deferred to government leadership for justification of its decision to not hold an annual meeting in person. Co-op-8 included federal guidance in their explanation for canceling the annual meeting—"to comply with federal and state guidelines"—even though the federal guidelines did not compel action." In doing so, the utility sought to legitimize its decision by deferring to power held by other organizations. Co-op-8 also emphasized to member/owners that the new protocols (which reduced in-person services for customers) were made to both emphasize safety and reflect new federal and state guidance and regulations.

National Organizations Guide Cybersecurity. Cybersecurity activities are founded upon arguments by peer and oversight organizations with vetted legitimacy that seek to counter both known and hypothesized threats. Multiple utilities discussed the legitimacy of influencer organizations' arguments being bolstered by the utility's own ability to identify threat actors attempting to access their system daily. The utilities recognize the reality and gravity of these apparent threats, and that knowledge reinforces influencer organizations' arguments for

actions to counter system compromise, which may have already happened to some degree even if it is not yet verified.

FEAp perceived cybersecurity for critical infrastructure organizations as not a partisan or politically charged issue. This improves reception of the legitimacy of an argument by keeping legitimacy of the communicating authority free from partisan prejudice. The mistrust of some COVID pandemic mandates due to disinformation and misinformation have caused a degree of partisan friction in publics that cybersecurity has not been subject to. This improves willingness to perceive cybersecurity authorities as legitimate communicators, their strategies as legitimate in response to the threat, and producing a desired effect in the way argued. For cybersecurity, not lack of legitimacy or education so much as lack of diligence is the core challenge—including different behaviors between work and personal devices.

External PR About Cybersecurity Cites Authorities. Cybersecurity significantly impacts utilities' internal operations but is little-mentioned in customer-facing communications. Strategies to address cybersecurity most often originate from national-level or federal organizations and are relayed through information-sharing and mutual aid networks. The only direct customer impacts come in the event of a crisis, such as a breach or compromise of customer PII, which utilities avoid discussing in hypothetical terms with member/owners until an actual event demands such communication. As such, cybersecurity for the co-op is a legitimate threat within the organization and its communicative sphere of peers and influencers, but it is only applicable to member/owners if the threat has

manifested in a breach of information sensitive to the member/owners. Utilities expressed awareness that member/owner publics have limited interest in what the co-op has to say, and so co-ops refrain from discussing troubling and internally focused subjects in public communications.

As TA-1 co-ops enhanced and expanded online services during the pandemic, concerns arose that this increased member/owner access could compound cybersecurity vulnerabilities. To address this, TA-1 launched a customer education initiative through the organization's lifestyle magazine to convey to utility member/owners that their ability to access utility systems entails risk for the utility as well, and what precautions to take. TA-1 also "borrows messaging" from in-house training exercises for use in the trade association's lifestyle magazine, including member/owners in the educational loop. In addition, the trade association collaborates directly with IT personnel at member utilities to share information and best practices and monitor education and training efforts.

TA-2 published 12 articles educating utility member/owners about cybersecurity over the two years' communications reviewed. These articles are split between informing member/owners of risks they face and means to address them, and articles offering a "look behind the scenes" at challenges the utilities face and how those are being addressed. The latter category frequently cites national-level authorities in the best practices conveyed, including one article that includes a lengthy interview with a representative from NRECA.

RQ_3: Role of Power in Compounding Wicked Problems

Research questions 3a and 3b asked how issues managers perceive power among other organizations and publics and how issues managers leverage the power of their own organization when addressing wicked problems. Interactions of co-op utilities with publics—including influential, collaborative, and member/owner—entail significant dynamics of power. Such influences compel action by the recipient rather than seeking to persuade the recipient to take action. These include regulations from state authorities, cyber attacks and physical attacks, voted changes and payment or nonpayment by member/owners, and the utility's own ability to provide or withhold services.

Any of these influences may come independent of an argument about the merit of the action required, and all may see compounding effects in the face of wicked problems or complicate the wicked problems themselves. The issues generated by the wicked problems also hold power in that they provoke the actions and reactions among the utilities and their publics. In the case of the coronavirus and cybersecurity, JAA-2p identified the power common to both problems: neither threat discriminates among those whom it affects, and the resulting issues can range in scale from mild to existential.

Issues Managers Identify Power Held by Publics

Issues managers respond differently to influences of power than legitimacy. Participants were quick to clarify which policymaking organizations did and did not have power over their utility, and the ramifications of different magnitudes of power. While the communications emphasizing the legitimacy of

the argument exhibited symmetric influence and information sharing in the relationship between utility and publics, interactions based in power were most often asymmetric. Considerations of power in these relations must address external publics and internal publics, and dynamics unique to each public and type of power.

Issues managers are often not in control of the influences upon a utility that affect the utility's provision of services to member/owners. These influences may complicate relationships with member/owners and other key publics without affording the utility reciprocal input. Such asymmetric interactions pose complex challenges for issues managers. External and internal publics exert power over the organization in different ways, and issues managers respond to or deflect that power through different actions.

External Publics May Supply Resources or Impose Policies. Issues managers most frequently spoke of how they perceived and addressed organizations and other publics outside of the utility that hold power over the utility through authority or in action. External issues management perceives power from outside the organization and communicates with publics outside of the organization. Provision of electrical energy for distribution by the co-op and regulation and oversight from state agencies were the most common examples of power exerted over utilities that the participants discussed. State mandates of actions in response to the COVID-19 pandemic featured prominently in utilities' communications, as the utilities responded to the mandates and informed their publics of changes to operations required by those mandates. This is an

imposition of power rather than a symptom of a wicked problem or related issue because the influence on the utility is the action of another organization in response to the problem or issue and not a facet of the problem or issue itself. In addition, the power may be exercised on the utility for any number of other issues not related to a wicked problem.

From an operational perspective, public co-op utilities connect residences and commercial facilities to the grid. They do not generate the electricity they distribute and often are not part of the transmission network, either. As such, co-op utilities rely on generation and transmission utilities—utilities that generate electricity from fuel and utilities that convey the generated energy from the point of generation to the point of distribution, respectively. These utilities operate at a larger scale than co-op utilities and often span multiple states, which subjects them to different regulations than distribution, falling under the oversight of federal agencies including DOE and EPA. They also supply electricity to multiple distribution utilities, others of which might serve many more customers and thereby produce more revenue than the co-op utilities. In the event of compromise to transmission infrastructure, more heavily populated areas may see more immediate attention than the less-populated regions served by co-ops.

State authorities have direct oversight of public co-op utilities, unlike federal agencies, which usually lack any direct authority. As such, state governments can stipulate actions utilities must take, whether or not the action is deemed relevant or advisable by the utility itself (or sometimes already taken by the utility). The state-mandated moratoria on disconnection from service proved a

significant financial burden to co-op utilities (see footnote p. 112) and deferred but did not eliminate debt for member/owners.

Strategies addressing COVID-19 that were mandated by state-level authorities (e.g., lobby closure, masks in offices and member/owner work sites, suspension of disconnection) were not subject to iteration by utilities. Public relations communications from utilities most frequently cited actions that resulted from power imposed on the utility by state governments on two issues: disconnect moratoria and restrictions to business operations and public areas.

One frequent mandate was a need to quarantine for two weeks following potential exposure to COVID or when traveling between states, which would be impractical for a lineman working throughout a community and responding to mutual aid calls. ADV-2p reflected: “Do you want to wait two weeks before you get your power back? Because you have to wait for the lineman to quarantine.”

Electric utilities and organizations working in the sector were additionally concerned about how such complications with the pandemic could compound responses to cyber incidents: “Let’s say a cyber incident happened. And someone triggered their mutual assistance agreement. Well, that entity who is trying to come to help would have had to quarantine for two weeks.” Relatively few critical utility personnel were able to work in isolation, because lineman, substation personnel, and even many executive and C-suite staff were still going to work. ADV-2 and other participants worked to educate governors and improve the adaptation of COVID mandates to better allow for utility needs.

For example, Co-op-4p perceived some level of symmetry of power dynamics in their interactions with legislative and executive organizations, and some degree of influence over the moratorium and other mandates: “We’ve clearly and regularly voiced our input to those various regulations, the moratorium, proposed bills, workplace requirements.” Rather than viewing these actions as impositions upon the utility, Co-op-4 seemed to assert that the utility benefitted from the governor and legislature taking the lead in some decisions and the balance of the utility having power taken away with also having responsibility for the decision and some ramifications taken away from the utility: “ …for a good part of all that legislative regulatory piece, while we had input, we did rely on our state association to do most of that heavy lifting.”

External Communications Cite Imposed Power. Many utilities cited state mandates and federal guidance regarding public access to facilities and events when announcing closing of offices and canceling annual meetings or moving the meeting online, leaning on the authority of these agencies and citing the power imposed as leaving utility without option to do otherwise. Member/owners were subject to the same mandates and likely saw them enacted at many other businesses besides the utility. As such, member/owner objections to actions required by the mandates may attribute problems the mandates pose to the state and not blame the utility.

Co-op-4’s communications elaborated on the influences the co-op cited from national and state-level organizations. In addition to Centers for Disease Control (CDC) guidelines, the co-op cited the governor’s plan for tiered

reopening of businesses and the guidelines for safe work environments enacted by the state agency responsible for occupational safety. Co-op-8 also included federal guidance in their explanation for canceling the annual meeting—"to comply with federal and state guidelines." Co-op-10 also cited the governor and CDC as influences informing the cancellation of in-person events: "Compliance with the Governor's orders and CDC guidance in response to the COVID-19 crisis will make it impossible to achieve a quorum at the Cooperative's Annual Member Meeting."

Co-op-5's communications also reflected on the substantial impact of the state's disconnect moratorium. The governor's moratorium went into effect along with the declaration of a state of emergency. While the utility had already resolved to suspend disconnections, the governor's moratorium took away control of the duration of the moratorium from the utility, and "...as the pandemic continued, that kept getting extended and definitely became prolonged." The utility had already affirmed its decision to suspend disconnection but conveyed the governor's evolving guidelines as those came out and then promoted programs to relieve financial hardship and provide funds for utility bills.

As the moratorium expired a year later concurrent with the expiration of the state of emergency, utilities shifted communications to the steps the utility would take for return to normal, including pursuing past-due balances. Co-op 5-p thought both the creation of the moratorium and cessation of the moratorium posed challenges to the utility, and collectively were "...the greatest influence [by an outside organization] over [the co-op] during the pandemic." Not only did the

governor's order affect the utility's bill collection and remove the power of disconnection, but it also created significant challenges for member/owners:

> ...because [member/owners] accrued these very, very high past due balances, and we had to come up with the appropriate strategies for payment arrangements and getting members to set up a payment arrangement and or to claim the funds that were available to them.

The moratorium on disconnection affected both utility policy and finances. TA-1p characterized the moratorium as a "business disruption" that created hardship for utilities. Co-op-4p affirmed that the moratorium on disconnections for non-payment "...had a big impact on…us as well." Eventual rescinding of the moratorium after the states of emergency were lifted may have restored some revenue to utilities but may have also impacted public opinions of utilities due to the large bills coming due and disconnection again looming.

Member/Owner Publics Influence Utilities. The co-op utility business model empowers the customers (i.e., member/owners) with influence over utility operations and policy, in addition to customer feedback experienced by other utilities. As such, co-op utilities hold additional responsibilities regarding their member/owner publics, as simultaneously parallel to both stakeholders and customers of investor-owned utilities. Co-op utilities felt challenges integrating the mandated actions from state authorities as they disrupted the manner in which member/owner publics had interacted with them. This dynamic is considered an imposition of power rather than a symptom of a wicked problem or related issue because the influence on the utility exists independent of the presence of the problem or issue—the member/owners always have influence on the utility—and

responses to policy changes in response to wicked problems may reflect the utility's relationship with member/owners as much or more than the shift demanded by the wicked problem or issue.

One of the biggest impacts that member/owners conveyed to co-ops during the pandemic came down to disappointment at the closure of offices. TA-1p observed: "A lot of folks in small towns, you know, still like to go down to the office and pay their bills in person and make sure they get the receipt in person." The other greatest frustration was the inability to leverage suggested tools due to the "digital divide"—lack of access to broadband Internet was a frequent subject of communications to and from customers.

TA-1p perceived overall acceptance of the utility adaptations to new business practices during the pandemic, possibly due to the practices being largely imposed upon them by government guidance and mandates. "I don't think that there's been the level of pushback. At least, I haven't heard it, and I regularly communicate with the local co-op PR people." The acceptance is also attributed to the communications personnel clearly conveying information they have and updating member/owners on what to expect.

The primary key to responding to member/owners, according to Co-op-6p, is to listen to them with genuine interest and respond when and as able. "It's just people wanting to feel like they're being heard and being seen before their elected co-op…we make sure we're still responsive to them." If the co-op was not as diligent in honoring member/owner concerns, Co-op-6p was certain that they "would have gotten quite a bit of pushback from people." The co-op's record of

responsive interaction in both customer service portals online and service technicians on-site, and the seriousness with which they take those interactions, is conveyed to member/owners. “Whether it’s us on the PR side or our member service reps, we field thousands of calls and I think the wait time is very minimal, so we’re proud of that…especially in the last 18 months.”

Internal Publics Hold the Power of Noncompliance. Internal issues management must address power dynamics within the organization. Internal issues management may need to compel personnel to adhere to particular guidelines, sometimes for conduct and other times for safety, among other factors. These regulations may be externally imposed policies or responses to externally imposed forces, and utilities must balance the enactment of these policies with the needs of internal publics or face retaliation ranging from pushback to noncompliance. This dynamic is considered an influence of power rather than a symptom of a wicked problem or related issue because the influence on the utility exists independent of the presence of the problem or issue—utility personnel always have influence on the utility in compliance or noncompliance and execution of refusal to execute duties, among others. Personnel responses to policy changes in response to wicked problems may reflect the utility’s relationship with its personnel as much or more than the shift demanded by the wicked problem or issue.

In responding to COVID-19, external publics such as state governments enacted requirements limiting in-person work for nonessential personnel and requiring use of masks. Deployed crews, OT, IT, administrative, and executive

personnel have different degrees to which they are able to work remotely, in some cases not at all and in some cases entirely. Some utilities received significant pushback from field crews and other personnel who did not perceive the necessity of masking, forcing the utility to cite the power imbued by the state to enforce the regulation or communicate with personnel effectively to defuse the controversy.

Internal publics hold the power of noncompliance—deliberately or inadvertently failing to adhere to policies and practices requested by the organization. Utilities have uniformly launched thorough cybersecurity "hygiene" training programs, required of all personnel, and have had great success in motivating personnel to complete the training and demonstrate understanding of both the risks and the means requested to address those risks. However, ingrained behaviors have proven difficult to change. Utilities have been able to impel a certain degree of rigor in some vulnerable points like passwords and use of VPN when telecommuting. This has not impelled personnel to maintain similar rigor on personal devices, some of which they then use to access organizational systems. Personnel have also reinstalled software removed by IT staff because of known exploits. Knowledge can be imparted and tested for verification of understanding but changing behavior has proven a more difficult task. The autonomy or agency of personnel to continue to engage in poor cyber hygiene puts the entire organization at risk.

Issues Managers Leverage Power Held by Their Organization

Organizations may also have asymmetric influence on publics. Actions by the organization can compel action by or withhold valued materials from a public.

Issue managers can influence prospective solutions to problems by imposing their definition of the issue: “There is power in definitions and by controlling the definition of the issue, issues managers gain an advantage in the process.” (Coombs & Holladay, 2018, p. 83). In these asymmetric actions the utility leverages power it holds to influence external or internal publics.

Utilities Provide or Deny Service to Member/Owner Publics. Utilities hold power to provide or deny services to member/owners and provide or deny information to peer utilities and other industry organizations. Issues management during the pandemic included the suspension of service disconnections in recognition of attendant financial hardship by member/owners. In some cases, utilities identified and enacted this strategy independently and in others the utility was required to do so by state agencies. The moratorium on disconnection eased financial hardships experienced by member/owners, and by recognizing the public hardship may have improved the organization’s image and credibility of the utility and state government.

Last-mile fiber optic installations, begun by utilities prior to the COVID-19 pandemic, served to mitigate many member/owner issues with adaptations to COVID-19. With the expanded need for telecommuting and remote learning for schools, the projects proved prescient. Problems still emerged with customers not yet served by the new services, in their perception of being denied a benefit provided to others.

Utilities Enforce Policies with Internal Publics. Personnel are compelled in varying degrees to comply with practices and standards set by the

utility. While some stipulations may be in response to power exercised upon the organization by external influences (e.g., state regulations), the enforcement of resulting policies is up to the organization if it wishes to avoid intervention from the external influencer. Other stipulations may be developed in response to intelligence, best practices, or other information acquired from other sources to guide organizational practices but without the threat of repercussion for noncompliance. These may inform organizational policies, but the deployment and enforcement of the policies are both at the discretion of the utility.

In response to the COVID-19 pandemic, ADV-2 expressed concern about the prospect of vaccine mandates: “If you require your folks to get a vaccine and they’re not qualified, or not able to get one yet, or medically not able to get one, what position does that put the entity in the personnel?” ADV-2 extrapolated the vaccine mandate as a potential “slippery slope” that may lead to other, similar mandates for the flu vaccines.

Many organizational policies are developed independent of outside influence, and their conception through enforcement are purely at the discretion of the utility. The means of enforcing any of these varies on the perceived repercussions and the management philosophy of the utility, with varying compliance and feedback from affected personnel in response. At the collaboration level, JAA-1p1 noted that access to utility Wi-Fi was limited to utility-issued laptops to reduce access and vulnerabilities. The participant lamented the time it took to help troubleshoot authentication processes for personnel. “But besides that, we also have all these new rules and regulations

about when people are allowed to be at work and not, and it's kind of made project scheduling a huge nightmare."

Internal issues management addresses organizational personnel to align their expectations and actions with stipulated policy and to account for their reactions to imposed policies. Internal publics perform the organization's work and they hold the power to withhold their work, promote dissatisfaction or protest among personnel, and/or seek other employment. Utilities have already been challenged to recruit sufficient personnel during the COVID-19 pandemic, and the prospect of needing to replace trained employees is daunting. Disparate requirements for in-person versus remote work capacity and potential friction with personnel lacking the opportunity to choose led to multiple instances of internal issues management to avoid negative escalation by personnel. Internal issues management of these capacities included executive personnel electing to work in the office even when able to telecommute as a show of solidarity to personnel that did not have the option.

Utilities Leverage Disclosure with External Organizations. Divisions within utilities retain and leverage the power to determine what information issues managers might provide or withhold. Utilities control the amount of information made available to publics about the personnel and structure. Co-op-16 related the painstaking steps taken during the previous years to scrub personnel contact information from their website: "We have made a concerted effort over the past couple of years to remove email addresses and desk phones [numbers] and things

like that from the public domain. [We] point everybody to a generic contact form."

Utilities also control information provided to oversight and information-sharing organizations. Utilities that share breach events with ISO are assured of anonymity, but ISOp perceives that there is still significant reluctance to share information. Hesitance to share information is a significant concern, because concealing a breach may leave a vulnerability unidentified and therefore unaddressed. ISOp commented that utility claims of transparency may differ from actual actions regarding disclosure of organizational information. The national level of coordination of public power practices and resilience planning hinges on broad and transparent information sharing.

Despite guarantees of anonymity or protection from repercussions for sharing information about a breach, the actions desired by utility leadership may differ from actual actions regarding disclosure of their experiences with exploits of organizational vulnerabilities. For instance, utility leadership often push for sharing information with Information Sharing and Analysis Centers (ISACs), which collect experiences from across sectors and compile strategies and best practices. To improve transparency with ISACs, utilities that share information about breaches are guaranteed anonymity, and so need not fear regulatory or other oversight repercussions. However, probing the communicative conduits within the organization often reveals a legal team or compliance department that screens all information before it leaves the utility, so information sharing may be slowed or lack additional context that may be helpful to other organizations. ISOp asserted:

"The operators of the grid do their job, the cybersecurity people do their job, the lawyers do their job, and...it all is interconnected." Concealing knowledge of and access to cases of exploit by aggressors to industry organizations and other utilities decreases the pool of anecdotal evidence from which to develop strategies and may leave some vulnerabilities unidentified and therefore unaddressed.

Issues Managers Responded to Power as Crises and Deferred to Authorities

Challenges the participants cited at the confluence of cybersecurity and COVID-19 primarily centered on expanded telecommuting for personnel and heeding state mandates that reduced in-person services for member/owners. Maintaining secure systems while expanding telecommuting by administrative and IT personnel during the pandemic stretched resources, demanded new equipment and additional cybersecurity vigilance, and accelerated the pace at which utilities had been accommodating remote work and moving customer services online. Heeding state regulations that limited public access to places of business challenged the utility's ability to serve customers whose lack of broadband impeded their ability to move to online service or who needed to enact their transactions in cash. For all of these primary challenges, the tools and techniques had already been developed and some were already being deployed; the challenge in the confluence of the pandemic and cybersecurity was the speed at which the tools needed to deploy and the business models shift.

While concerns for each did compound the other and demand some degree of new planning, the tools and techniques were already in place. Adapting to the pandemic and maintaining cybersecurity demanded vigilance and ingenuity, but

not novel communication tools or techniques. FEAp reflected on the agency's response to the onset of the pandemic in similar language to the description of a wide-scale disaster response from a large-scale weather event or other similar disruption.

> We knew about a week before our office closed, that we were going to have to start holding daily calls with the electricity sector and with the oil and natural gas sector—that's what we do in a typical disruption. While this wasn't a typical disruption, we had the structure in place to be able to have this type of conversation.

Messaging About Mandated Actions Uses Crisis Framing. For TA-1p, the sudden shift to remote work resulting from governmental mandates to adapt to the pandemic created an economic and cultural crisis for utilities. "For our association, and I think for a lot of the member cooperatives, too, remote work was considered a possibility, or maybe even a luxury. Now it's the way we're all doing business." The power exerted on the utilities to shift work strategies has, in turn, shifted work culture and expectations.

Co-op-5p reflected on the compounding problems of cybersecurity and COVID-19 in the frame of individual incidents rather than long-term socio-cultural issues:

> ...where we are most successful is when it comes to proactively preparing for a crisis situation and actually successfully working through a crisis situation. There's a lot of things that we do every year throughout the year to make sure that we're ready if something were to happen like that.

This sense of preparedness and confidence conveys a perception of, if not control over the situation, an ability to respond adequately to the

challenges faced. The aspects of the wicked problems addressed were those the utility was already prepared to address, which improved its confidence and sense that the threat was intelligible, knowable.

Communications from other co-ops in response to remote work mandates reflect a crisis mentality. Co-op-16p thought that, while most if not all electric co-ops have a crisis communications plan in place, co-ops had to improvise "some provisions" to adapt to the unforeseen demands of the pandemic. This crisis response ultimately sought to bolster co-op legitimacy with member/owner publics: "We adopted these plans and have implemented them without losing sight of what means the most to our members: the delivery of safe and reliable electricity."

TA-1p described the scramble to assemble tools and define techniques to accommodate the move online as a crisis response to an identified risk. This crisis, however, has morphed into a long-term strategic issue to be managed.

> The new generation of employees that we are going to seek...have come to expect remote work as implicit in any job they take, but they're not going to be in an office….and if they have to choose between an office atmosphere or a virtual office atmosphere, they're going to choose the virtual office.

First, the sector responded to power leveraged by the state governments. Now, perceived power in a potential workforce is shifting remote work from a short-term adaptation to a long-term expectation for which utilities need to plan. Utilities are adapting to cascading impositions of power.

Utilities Cite Authorities in Asymmetric Public Relations. Public relations communications from utilities often discussed restrictions or regulations

imposed on utility services during the pandemic, changes to utility interactions with member/owners due to those restrictions, or steps the utility was taking to help member/owners during the pandemic. Most utilities communicated with member/owners when new mandates impacted utility services and announced actions taken to comply with federal guidelines and state regulations. Announcements of state-mandated moratoria on disconnections were useful for member/owners, but clearly conveyed that these were not actions taken by utilities. Likewise, cancellation or transition to remote engagement scheduled events reflected imposed restrictions, but often were attended by expressions of regret for not being able to meet. The actions were not the utilities' choice.

Paradoxically, some of the challenges pandemic restrictions have placed on co-ops' interactions with member/owners produced tangential benefits for the way co-ops do business. Undermining the type of customer service that distinguished co-ops, like in-person bill pay, ended up forcing member/owner behavior to a previously desired end. Co-op-6p reflected: "It's probably good to have [the enforced lobby closure] because we're trying to move in that direction [online customer service] anyway, trying to encourage paperless billing, trying to let people know that there's multiple ways to pay your bill." Co-ops affirmed that these services were in place prior to the pandemic but were infrequently used. That they were previously in place aided adaptation to the pandemic, and the pandemic served to shift payment habits without the co-op having to appeal to member/owners or exert power over member/owners.

Chapter 5: Discussion

This study asked: (1) how issues managers identify and prioritize compounding wicked problems, (2) how they identify legitimacy and power in publics as influences on their organization's strategy and messaging, and (3) how they leverage power held by their organization to influence perceptions and belief by publics in response to compounding wicked problems. Participants recognized the mutually compounding dynamics of adapting to COVID-19 and maintaining cybersecurity. Both the coronavirus and threats to cybersecurity are viewed as critical concerns for utilities, both are evolving in ways that impede conventional crisis management or defined strategies, and the impacts of both are expected to persist without finite resolution. Participants affirmed that attempts to adapt operations and business practices to address one problem complicated their ability to take the necessary actions to adapt to the other. Participant experiences and organizational communications affirm some and challenge other theoretical concepts and practical frameworks of issues management in the context of compounding wicked problems.

From a theoretical perspective, this study highlighted nuances in the cocreational nature of issues management and expanded understanding of what can make issues management effective or fall short of anticipated achievements. This study also extended understanding the role of issues management of wicked problems with compounding influences between multiple problems. Finally, the study suggests that the wicked problems label may be overused or applied in a way that limits its usefulness.

First, cocreation includes a range of interactions between an organization and its publics from dialogic to educational to advocacy (i.e., from both sides mutually defining an issue to one side presenting vetted information to the other to one side actively promoting a particular perspective or approach). The most effective issues management in this study was a mix of all three in a collaborative environment. Less effective approaches tried to convey information from a trusted source to a public uninterested in or unaware of the legitimacy of the source or enact policies for which publics did not perceive a need and may have seen the policies as impositions on their behavior and freedom. This highlights the granularity at which cultural differences can manifest in the United States.

National culture has long promoted a concept of individualism over collectivism, priming citizens to resist actions that benefit the group but inconvenience the individual. Paradoxically, reliance on the market to develop and deploy new technologies left rural communities behind for both power 90 years ago and broadband Internet today. These same communities that resisted advocated adaptations to the pandemic for collective good formed cooperative utilities that first brought power and now Internet to their communities.

Collectivism itself may not be the barrier so much as the perception that parties outside the community fail to understand its needs and priorities and thereby have no authority to compel action within the community. Community-scale self-reliance has been essential in the past, and what has brought benefit to the community breeds distrust of voices with whom the community is not

familiar. Additional exploration of intercultural communication and cultural intermediaries in issues management could help improve cocreative relationships.

When addressing wicked problems or compounding wicked problems, the theoretical model of issues management is applicable. Issues managers do not address the wicked problem(s) directly but address its symptoms, as they do with issues. The methods of communication and collaboration are similar, and the lack of a finite end or distinct resolution of the issue or problem is common to both. Both also demand ongoing, iterative strategic management on the part of the organization, of which the issues management communications are a part. Compounding wicked problems entailed no discernible new tools apart from an initial need to prioritize the symptoms challenging the organization.

What then, is the use of the wicked problems framework? If issues managers address symptoms of issues that are divisions of wicked problems that are compounding with other wicked problems, is there a need to have the "wicked problems" label at all? Wicked problems are sociological in nature, and originally entailed concepts like racism and socioeconomic inequality. Cybersecurity and the COVID-19 pandemic have both been examined in other academic literature as wicked problems, but (1) Are they really? and (2) What additional value does that afford? First, neither seems to manifest at the scale of the "original" wicked problems. Cybersecurity could be seen as an issue precipitating from a wicked problem of "crime," and the pandemic can be seen as a public health concern, with the precipitating issues being more aligned with socioeconomic inequality and asymmetric benefits in capitalism than with medicine or healthcare. At some

level, the superimposed labels of wicked problems take on a level of abstraction that are not useful. Issues managers do not manage “crime” or “health” at the most conceptual level, nor will an organization likely be interested in their doing so. At the same time, consideration of forces that generated the symptom or issue with which the organization is grappling may produce additional perspective.

Issues managers identified the problems faced by the organizations according to impacts of the problem on the organization and/or its publics, rather than identifying the deeper sociological causes from which the problems precipitated. This might be seen as a logical focus for the organization, but communications asserting legitimacy of the organization’s response or identifying power leveraged against the organization have the power to identify social and cultural forces beyond the context of the organization’s own activities. Utilities are affected by cultural and political forces beyond the scope of their operations, and so can identify the effects of or power in those forces. A cumulative effect of multiple organizations doing so could highlight the sociopolitical narratives that generate wicked problems but that go unaddressed and often unacknowledged. Issues management communications of compounding wicked problems manages the impacts to the organization or its publics because of resulting issues or crises rather than directly addressing the problem itself. Finally, while issues management communications seek to modify behavior or perceptions of the publics in response to the issue or problem, the current applications of power and legitimacy are inadequate to impel lasting change in publics’ behavior.

From a practical perspective, issues management communications about compounding wicked problems only address publics that are also affected by the compounding issues. An organization does not need to communicate with external publics about needs to adapt to compounding effects of multiple wicked problems if the publics are not impacted by the compounding problems as well. Additionally, the study illustrated that issues management by public utilities in the critical infrastructure sector relies primarily on cocreation with other sector organizations and legitimacy with publics, and rarely leverages power. Even then, power leveraged by a utility is often a reaction to another organization's use of power to influence the utility. Finally, issues management of wicked problems and social issues by critical infrastructure organizations focuses strategic planning on resilience following impacts of the problem or issue rather than prevention. Table 8 presents a summary of the theoretical and practical implications.

Table 8

Contributions to Theory and Practice

Theoretical Implications	Insights	Supporting Evidence
Compounding wicked problems require issues management	● Strategic planning identified issues and began adapting processes before problems compounded. ● Collaboration among all levels of information sharing cultivated legitimacy. ● Legitimate investment in the community helped organizations maintain positive relationships with stakeholders.	● Compounding wicked problems did not require new solutions but exacerbated existing needs. ● Collaboration among utilities and with other organizations improved validation and communications. ● Dedication of utilities to their community aided understanding of the needs of their publics. ● Perceptions of organizations as legitimate members of the community affords additional tolerance of needed adaptations.
Issues managers do not directly address the wicked problem(s)	● Messaging addressed the symptoms of the problems prioritized by the organization and how the response will address them. ● Symptoms comprise issues, issues comprise wicked problems. ● Community-level focus of messaging leaves societal context unaddressed.	● Breaking wicked problems into issues into symptoms provides an actionable level of analysis. ● Messaging characterizes impacts on stakeholders rather than overall threat of a problem or issue. ● Overcoming siloing improves internal issues management. ● Issues are often managed as crises. ● Specifying impacts to publics or barriers in legislation directs focus to the local level rather than systemic.
Education, even when enforced by policy, is not enough to change behavior	● Issues managers persuade using legitimacy and power. ● Social and behavioral norms impeded adoption of actions. ● Collaborative networks succeeded where organizational training and communications struggled. ● Combined legitimacy and power gained short term changes in behavior. ● Opposing views used misinformation and disinformation to discredit legitimate arguments.	● Legitimate argument does not compel behavior change. ● Technological solutions rely on human behavior. ● Vetted networks gain buy-in. ● Publics resist arguments made strictly based on policy or education. ● Valid arguments backed with policy produced reluctant compliance. ● Voices opposing policy may not be bound by the same ethics or commitments to community. ● Messages seeking to undermine policy can focus solely on undermining policy or practice.

Practical Implications	Insights	Supporting Evidence
Study of compounding problems requires problem with common publics	● As segmentation of publics is necessary when studying an issue, study of multiple issues requires alignment of publics to produce insight. ● *Communitas* mutual interest approach is an admirable aspiration but difficult to practice. ● Internal publics provide greatest opportunities for study because their interests and those of the organization are largely unified.	● Publics for the pandemic and cybersecurity did not overlap, so few organizational communications addressed the compounding problems. ● Utility member/owners were common publics for both the pandemic and "digital divide," so many organizational communications address compounding issues. ● Utilities defined mutual benefit in many strategic programs, but co-definition was largely limited to networked sector communication and state government.
Issues management by critical infrastructure seeks cocreation	● Cocreative networks speed verification of intelligence and information. ● Dialogic network communications have greater impact than symmetrical public relations communications. ● Legitimacy is not reliably transferrable. ● Advocacy relied on legitimacy in arguments.	● Utilities provide information to collaborative and influential organizations as well as receive it from them. ● The collective interest of the community—in the information network or in the utility public relations—receives more focus than any individual entity. ● Utility perceptions of the legitimacy of information does not convey to the perceptions of internal or external publics. ● Utilities argued legitimacy of state's power to publics and argued legitimacy of publics' needs to state.

Theoretical Implications

Few public relations theorists have addressed wicked problems (e.g., Capizzo, 2019; Capizzo & Sommerfeldt, 2021; Coombs and Holliday, 2012; Roper and Hurst, 2019; Willis, 2016; Willis et al., 2018). This study extends their work in issues management of wicked problems by establishing that: (1) wicked problems compound and require issues management; (2) issues management of compounding wicked problems does not manage the wicked problems

themselves; and (3) power and legitimacy in issues management strategies are insufficient to produce lasting changes in publics' behavior necessary to address the problems.

Compounding Wicked Problems Require Issues Management

This study asked whether compounding wicked problems produced dynamics unique to the compounded problems, and what issues management techniques organizations employed in response to them. While other fields have considered compounding effects of wicked problems (Heck et al., 2020; Melaku et al., 2020; Seymour et al., 2020), public relations literature has not.

This study affirmed that wicked problems do indeed compound. Complex, intractable, ingrained social problems inevitably collide with other complex, intractable, ingrained problems and produce new dynamics for which issues managers must account. The issues arising from these problems mutually compound as well. As the potential solutions to any symptom of one wicked problem may produce additional complications, so too may solutions to a single symptom compound other symptoms of the wicked problem or symptoms of other wicked problems (Roper & Hurst, 2019). Because embedded societal problems are not likely to be isolated in either origin or effect, future studies of wicked problems should consider compounding effects of other persistent, societal problems that influence organizational adaptation and response.

Organizational responses to these issues and problems required the tools and techniques of issues management. Wicked problems and compounding wicked problems did not require different tools or techniques of communication

but did require additional strategic planning and/or crisis response and consideration of additional publics. Participants repeatedly affirmed that they already had mechanisms for communication in place in their networks of collaboration and means of outreach to member/owners. In addition, adaptation to the pandemic did not change the tools or practices of cybersecurity but compounded those tools in the sudden shift to remote work, the need to accommodate increased VPN traffic, and the need to account for personnel security practices at home. Adaptation to the pandemic also did not require novel solutions to the digital divide, as the utilities were already working to deploy broadband services and some has already installed payment kiosks and Wi-Fi in lobbies, but they required accelerating the deployment of fiber optic networks and extending the range of W-Fi to the parking lots for member/owner access.

As with issues and wicked problems, organizational solutions to compounding wicked problems were incomplete and prone to generating novel problems or meeting intractable publics (Roper & Hurst, 2019). Remote work often required expedited acquisition of new hardware and software. The expanded footprint of remote work provided a broader attack surface for threat actors. Supply chain shortages complicated sourcing of materials for expanding fiber optic networks. Policy and regulation hurdles complicated establishment of subsidiary Internet providers, delaying deployment of new fiber optic cable, and some landowners protested use of existing easements, which also challenged construction of the networks. Participants relied on collaboration and communication with internal and external publics to characterize the challenges,

advocate for solutions to issues within the problems, and assert achievements to build rapport and relationships—the tools of issues managers.

Response to Wicked Problems Apply Issues Management Theories in Collaborations with Publics. Wicked problems literature in public relations has established the need for social iteration of priorities, obligations, and objectives among publics (Willis, 2016) and that such deliberative engagement of diverse stakeholders precludes definition of strategies and solutions by experts in isolation of the input of those publics (Willis et al., 2018). Participants in this study prepared for and responded to compounding wicked problems with a combination of strategic planning, risk and crisis management, organizational reputation management, and collaboration with other organizations and publics to resolve conflicting priorities, all of which are issues management techniques (Grunig & Grunig, 2000; Heath & Palenchar, 2008; Wu & Yang, 2017). The participants engaged in this planning collectively, rather than in isolation, through acts of collaboration among multiple organizations across industries and from multiple tiers of government and oversight and public and private sectors, as well as their member/owner publics.

Responses to cybersecurity engaged other organizations and agencies in nationwide networks of communication and collaboration, and then collaborated with internal publics in education and integration of best practices. Threat intelligence was shared by high-level federal agencies and small co-op utilities who suffered breaches. Nonprofit advocacy and information-sharing groups cultivated sector-spanning networks for communication and collaboration, to

improve collective response planning and decision making and to speed vetting of information and subsequent response. The threats and strategies extended beyond individual utilities and even beyond the electricity distribution section, engaging organizations—publics—in multiple other sectors whose communications and software networks link all affiliated organizations in a common and mutually dependent risk and response network.

Responses to the pandemic engaged member/owners and state and federal agencies in communications responding to policy changes and mandated actions, and frequently communicated with member/owners to ensure continued ability to participate in utility. Mandated adaptations to the pandemic included closing of business offices and shifting of personnel to remote work, when possible. Utilities identified staff capable of performing work remotely and acquired necessary hardware and software to best ensure effective and secure remote access. They corresponded with collaborative and influencer organizations to share information about and best practices in maintaining security while increasing remote work, and integrated strategies suggested by influential organizations as new threats presented themselves. Utilities identified needs among their publics that would be challenged by the changes in business plans, and devised stop-gap solutions like extended Wi-Fi.

Participants characterized the strategies developed to address compounding issues in cybersecurity, the pandemic, and the digital divide as those within the utilities' power to influence. Utilities also understood that previously identified challenges in the digital divide were being exacerbated by

the pandemic mandates, and increased focus on those efforts both to help their communities overcome the digital divide and to better adapt to business practices and new models of education during the pandemic. These efforts to address cybersecurity, the COVID-19 pandemic and the digital divide centered on concerns for organizational and community security, equity, and community values, which are characteristics of social issues (Madden, 2019).

However, many of the issues posed by these three problems are broader than the reach of the utilities' issues management. For example, state requirements for business practices in response to the pandemic challenged utilities' provision of service to member/owners and left some utility personnel and stakeholders upset with or frustrated by measures that seemed out of scale with the impact the pandemic had on their community. Inherent disagreement of the scope or implications of these issues among utilities, influential organizations, and publics is inevitable, as wicked problems are without solution as social and policy issues are also frequently intractable (Capizzo, 2019).

In these conceptions, scale is the primary differentiator between the characteristics of a wicked problem and social issue. Wicked problems comprise multiple social issues, which in turn could precipitate crises (Veil et al., 2015). As the wicked problems compounded, organizations had to react to the publics whose relationship with the utility was impacted by those wicked problems, with particular focus on publics at the nexus of multiple compounding problems.

Collaboration Cultivates Legitimacy. Participants engaged stakeholders in the definition of the problem and identification of the preferred solution.

Influential organizations hosted strategic planning and mutual aid development sessions to improve cybersecurity at utilities. These sessions drew participation from utilities across the public power spectrum and at many scales of operation. Utilities host annual meetings for their membership and engage member/owners through social media and other direct communication. These meetings and online fora provide opportunities for participation by stakeholders in the development of utility policies and programs. Participants from utilities also described frequent interpersonal interaction with member/owners that led to discussion of policies and adaptations to the pandemic.

Issues management of wicked problems demands organizational understanding of and influence upon societal expectations and willingness to deliberate on solutions that balance organizational goals with social definitions of the problems and perceptions of equity (Rittel & Webber, 1973; Willis, 2016; Willis et al., 2018). Rather than conclude the problem existed outside the utility's milieu, these utilities lobbied for changes in policy to allow them to facilitate the provision of the new service. The utilities perceived both inherent inequity in the treatment of the people in their service areas and an obligation to serve those people, such that they were willing to shift the scope of the utility's work.

This process balances cultivation of legitimacy of the organization's approach in co-creation of strategies with publics (Heath & Palenchar, 2008), which improves publics' perception of the legitimacy of the approach (i.e., the likelihood it will address the targeted issue in the way it claims). Collaboration also opened the power of influencing the definition of (and therefore perception

of) the core of the problem(s) to be addressed with all interlocutors (Coombs & Holladay, 2012). Adopting the redefinition of broadband service as the "fourth utility" changed it from a luxury to a necessity, and the FCC admonition to suspend disconnect of Internet service reinforced this portrayal. Collaboration with publics to address issues and work in a collective interest is the aspirational heart of public relations issues management (Grunig, 2000).

Organizations that influence the public utility sector collaborate in a broad but insular information-sharing network. This paradoxical characterization reflects the network's expanse and careful vetting of members. The expanse of the network comprises the public utility sector, participants in nonprofit advocacy agencies, government agencies, and select vendors and private-sector agencies. However, as study participants repeatedly underscored, admission to the network is difficult for any non-utility or government agency, and new interlocutors are viewed with skepticism or dismissed outright. This network breadth and privacy (and corresponding security) fosters discussion and sharing of experiences among peer organizations and influential organizations at state, regional, and national scales in a "…collective, discursive, reflective, iterative, problem focused, and action-orientated" forum (Willis et al., 2018, p. 394). This forum allows all stakeholders in the network to contribute as they are able and to draw from it information that informs their practice. Incorporation of different groups and types of discourses in pursuit of a mutually beneficial outcome of a public debate is an optimal strategy for issues management (Wu & Yang, 2017).

These networks of communication and collaboration foster the development of new tools and best practices as collective understanding of cybersecurity risks and threats evolve. Issues managers collaborate in defining and implementing solutions to address problems and share those with peer organizations and other participants in the collective information sharing network. Such collaboration is an excellent way to foster creative problem solving that applies existing resources to emerging problems (Cohen & Cromwell, 2020) and improves creative approaches to devising solutions and solving problems (Willis, 2016). The collaborative networks of the public utility sector are remarkable for their breadth of participants; dedication to comprehensive collection, analysis, and distribution of information; and degree to which participant utilities rely on them for information and communications support.

Cocreative Relationships with Publics Improve Community Identity. In conventional issues management, public relations practitioners define and delineate organizational and public identities as well as accepted knowledge that influences the attendant relationships between organizations and publics (Weaver, Motion, & Roper, 2006), and cultivate and manage mutually influential relationships between organizations and publics (Coombs & Holladay, 2012; Edwards, 2016). In the case of co-op utilities, the member/owner publics quite literally created the organization itself and maintain direct influence over its operation and policies. This affords the utility unusually deep ties to the community. Utility communications reflect these ties by using second-person or first-person collective voices, coordinating fundraising and community support

efforts for members of the community in need, acknowledging the work of members of the community in actions unrelated to the utility's work (e.g., human interest stories in lifestyle magazines), and identifying unique issues affecting the community (e.g., geographic, socioeconomic, and other issues of "place"). The reflections of participants also illustrated the active engagement organizations sought with members of the community and the utility's "bulwark" status in their communities.

Wicked Problems Are Not Managed With Technologies. Technical solutions can address technical problems, but technical solutions do not address social problems at the core of a wicked problem or ensure adoption of the tool by publics. Even though social processes interact with and may be impacted by technical processes, social problems defy technical solutions (Rittel & Webber, 1973). Application of technical resources must be attended by strategic planning and action for issues management to succeed (Jaques, 2010). Awareness of stakeholders' perceptions and engaging with them to pursue solutions is a key responsibility of issues management (Willis et al., 2018). Changing stakeholders' perceptions of the nature of the issues affecting them and behaviors in a way to address or adapt to those problems is necessary to mitigate symptoms of wicked problems (Willis, 2016).

One common theme echoed by participants was that attempts to apply technical solutions to the symptoms of wicked problems that affected their organizations were insufficient. A software patch does not "solve" an organization's cyber risk any more than development of a vaccine "solves" the

pandemic or stringing fiber optic cable “solves” the digital divide. While these technologies improve response to an issue, human participation in the solution to apply the technologies and engage in other practices related to the issue is necessary for effective response to an issue.

In addition, acquisition of a technology demands additional work to deploy it, which is often accompanied by education and training for publics to understand the rationale behind the technology deployed and its necessity to address the problem. In the case of cybersecurity, upgrading hardware and software had comparatively little impact compared to the behavior of personnel. The most advanced systems are ineffective without cyber “hygiene,” and inattention by a single member of personnel at the smallest utility can put the collective sector at risk. The most significant breach that occurred during the interview period was the exploitation of network management software by a threat actor that gave the threat actor access to approximately 18,000 customers of the software, including 40 companies in the defense industrial sector. The malware that produced this breach was identified by a systems specialist at a client company who noticed one employee showed two cell phones registered on the corporate system.

Likewise, the major threat stemming from the pandemic was not a loss of technological capacity, but of human capacity. Without control room personnel, a utility could not operate. Hence the extreme measures taken by utilities to isolate control room personnel and preserve their health. Machines still require human interaction to function. Vaccines and mask mandates have little impact on the

spread of a virus if people refuse to be vaccinated or resist wearing the mask. For internal publics, executives and issues managers conveyed solidarity with operations and field staff that could not work remotely by voluntarily working in person or by recognizing the efforts of in-person personnel in stakeholder communications. Admonitions to use PPI cite imposition of power by state authorities—it is not a matter of a community issue, but a state issue. Inability to engage with stakeholders in person shifted meetings into new media, so that stakeholders could still have their voice heard and vote counted.

Payment kiosks do not address a lack of internet access if they go unused, and expanded fiber optic networks are not effective if the members of a community are not able to afford devices to connect to the Internet or are not sufficiently Internet-literate to make use of online tools. Providing one technology to overcome a systemic imbalance disregards the imbalance and thereby fails to account for its influence on the proposed solution. The overarching goal of all of participants' issues management of compounding wicked problems was to impel a change in expectations and actions in their publics—"a change of mindset or behavior" (Willis, 2016, p. 30)—be those internal or external.

In these cases, strategic planning at both the organizational and sector level (i.e., through the collaborative network) and communications developed at all levels of collaboration together helped participant organizations inform stakeholders of issues arising from these wicked problems. These communications sought to explain the identified solutions and the rationale behind them, including how the results of the technological solutions would

address aspects of the issues in beneficial ways to overcome challenges in the issues. Finally, and critically, the communications sought to motivate actions in response to those issues aligned with the strategic plan. Motivation to use technological solutions beyond the short-term proved the most significant challenge to participants in this study. In addition, these technologies still address only symptoms of political or social conflict (cybersecurity), public health management and communication (pandemic), and socioeconomic inequality (the digital divide).

Issues Managers Do Not Manage Wicked Problems Directly

Participants in this study characterized cybersecurity, the COVID-19 pandemic, and the digital divide with traits that identify wicked problems: persistent, evolving, rooting in sociopolitical forces and inequality, unable to be comprehensively solved in a conventional sense, and with partial solutions that generate further complications (Roper & Hurst, 2019). However, organizations in this study never identified the root causes of the wicked problems, or even identified that their responses addressed subdivisions of a greater social problem as it affected their organization.

All organizations clearly applied a strategic planning approach to address cybersecurity and the digital divide. Strategic planning is essential for effective issues management (Jaques, 2010; Kent, et al., 2011). Planning efforts, information and best practices sharing, and extensive training for cybersecurity have been ongoing for decades. Given the extensive and persistent threat posed to the industry and the comparatively few crises resulting from a breach, these

planning, collaboration, and threat mitigation efforts have been very successful to-date. Likewise, planning efforts, legislative lobbying, and cross industry collaboration to bring broadband service to rural communities for more than 10 years. These actions are important to acknowledge, because they characterize organizational responses to cybersecurity and the digital divide in the issues management conception of public relations rather than a reactive crisis response framework (Veil et al., 2015).

The pandemic saw a more reactive response, as organizations were challenged to meet shifting regulations and mandates, but communications convey organizations' strategic reactions to the shifting environment and adaptations to the needs. No communications found during the survey focused on repairing an organization's image. As with cybersecurity, if utilities were only to approach the pandemic and its impacts in a crisis management framework, the analysis of responses in a framework of issues management of wicked problems may not be appropriate.

Effective issues management addresses the underlying societal causes of an issue, rather than its symptoms (Kent, et al., 2011). This model of issues management includes "...a broader range of publics and social issues" and allows the issues manager to "...act as organizational counselors rather than mere technicians," realizing greater benefit from their practice while ethically balancing organizational objectives and societal benefits (Kent, et al., 2011, p. 339). However, issues management in current practice does not address the issue itself

but seeks to manage the potential impacts to an organization that an issue might incur (Jaques, 2010).

None of the issues managers interviewed for this study, and none of the communications reviewed from the utilities, addressed these three wicked problems (i.e., cybersecurity, the COVID-19 pandemic, and the "digital divide") as "wicked problems," or addressed the societal scale of their impact. Organizations identify the subdivisions of the problems—the "symptoms" (Kent, et al., 2011)—that directly impact them and their publics, and address those in their actions and communications. Communications about cybersecurity do not address why organizations are attacked, nor do communications about the digital divide identify profit-motivated business models that neglect their communities, nor do communications about the pandemic speak to miscommunication by authorities or misinformation about public health undermining response or even about how public health infrastructure in the United States favors profits over communal health. Wicked problems may provide a framework for academic inquiry, but it is not applied by practitioners. The issues manager is not seeking to control the wicked problem any more than they can control an issue; they seek to moderate or counter the impact the wicked problem or issue will have on the organization (Roper & Hurst, 2019).

In this conception, wicked problems are complex phenomena generated from social conflict and inequality. Wicked problems produce impacts and pose challenges at a community level, which are addressed as issues. These issues may impact many organizations and publics. Particular subdivisions of an issue

specific to a type of organization or public, or even individual organizations can be thought of as symptoms—they indicate a greater issue but are only a single manifestation of that multipart issue. Participants and organizational communications in this study most often addressed symptoms, and rarely spoke to broader issues. Participants concerned with broader issue-level framework were more likely from national-level organizations.

Issues management communications focus on impacts. Internal and external communications about adaptations to the pandemic may inform publics why actions are necessary in light of mandates designed to mitigate the spread of the virus, but they do little to impact societal perceptions of the pandemic itself or to develop solutions for the pandemic. Publics relied on perceptions of their own community to determine the legitimacy of these claims, complicating organizational issues management and governmental responses as well (Coombs & Holladay, 2018). Increased cyber vigilance does not deter cyber aggressors, it just encourages them to shift their approach. Utility efforts to bridge the "digital divide" and bring broadband to their member/owners address one symptom of chronic economic/sociocultural inequality, but they do not address the sources of that inequality. Failing to address the underlying causes of a social issue with strategic planning and instead focusing on the symptoms is incomplete issues management (Kent, et al., 2011).

Further, the communications reviewed for this study often did not even address the cause for a particular action. Issues management of the wicked problems in this study relied on a desire for "safety" or security and generation of

solidarity in the community, which are valid bases for issued management (Madden, 2019), but not the root causes. State mandates and guidance from health agencies were cited as the impelling forces behind organizational policy changes, not the threat of the virus itself. Security of systems and PII were often cited as the teleology in cybersecurity, not threat actors trying to weaponize the grid to threaten the country. The lack of broadband service to a community is the reason to lobby state legislature to form a subsidiary company to provide Internet service, not ingrained socioeconomic disparities that have disadvantaged rural communities for more than a century and inspired the creation of the co-op utility nearly a century ago.

"Wicked problems" are not the focus of issues managers. Framing intangible threats is a historic challenge in both cybersecurity and pandemic response for issues management (Aylesworth-Spink, 2017; de Bruijn & Janssen, 2017). One reason for this may be that issues management addresses the "symptoms" of an issue rather than the issue itself (Kent, et al., 2011). So too, is issues management inherently concerned with the issue-level challenges (i.e., the "symptoms" of a "wicked problem."

Organizations in this study managed issues related to cybersecurity by reviewing software and hardware, bolstering organizational security practices, launching training programs for personnel, collaborating in information sharing networks to devise solutions and best practices, and studying breaches of peer organizations to understand vulnerabilities. These are all issues and risk management activities, or preparation for resilience in the face of a crisis.

Likewise, organizations are subject to state government mandates and policies for adaptations to outbreaks of the COVID-19 pandemic and may also choose to follow guidance from state and national health organizations. Policies they enact may be adhered to or resisted by external and internal publics, and that resistance must then be addressed through issues management. Should personnel within the organization become sick, then a crisis response might be necessary. However, none of these strategies seeks to address the coronavirus directly, or improve public health policy, generally.

In all these cases, issues managers continue to manage in response to issues that are constitutive of wicked problems. As issues managers break issues into symptoms they can address, so do they break wicked problems into issues to better strategize responses. This division of a wicked problem into issues into symptoms can take a complex societal problem and allow an organization to strategize a response that applies its resources and tools in a way meaningful to its operation and its publics. Kent et al., (2011) trace this conception of issues management to Jones and Chase (1979, p. 3): "When challenged by today's activism, business tends to react to overt symptoms, rather than by identifying and analyzing fundamental causes of the trend which has lead [sic] to a critical issue."

Even in compounding wicked problems, issues management public relations may help organizations manage "symptoms" of the compounding wicked problems (Kent, et al., 2011), but it does not manage the problems directly. Closing offices and moving staff to remote work addressed some risks of COVID-19, and also compounded cybersecurity issues and exacerbated the

existing “digital divide” in rural communities, but these actions, responses, and even complications are at an issue level and not the overarching wicked problem. These issues are only symptoms of wicked problems of public health and socioeconomic inequality, and not the problems themselves (Kent, et al., 2011).

By broadening the focus of issues management beyond “thinking beyond quarterly earnings or annual reports” (Kent, et al., 2011, p. 537) and take a more active role in the addressing dynamics underlying society. Issues precipitating from wicked problems affect entire communities, not just publics and not kust organizations. By moving beyond the frame of “we versus them, mine/our versus yours,” issues management can move beyond seeing the community as a means to the organization’s end, and as the mutual end desirable by the organization and its interlocutors (Heath, 2013, p. 430). Fostering “…a higher strategic alignment between agencies and their clients,” improves the ability of both the organization and its publics by allowing identification and cultivation of responses better suited to “…large-scale issues and risks,” (Erzikova & Bowen, 2019, p. 7). Advocacy of this nature extends beyond organizational legitimacy or perceptions of the organization by publics. This model of issues management addresses the issue directly, and the publics’ perceptions of it. By addressing “…social norms assumed by the public, regulations enacted by the government, policies proposed by the public or maintained by the government, and other environmental factors,” (Williams & Sommerfeldt, 2021, p. 238) and in doing so “…improve societal and global processes through an ethical framework of practice,” (Williams & Sommerfeldt, 2021, p. 245).

Cybersecurity is Not Managed as a Wicked Problem. Cybersecurity is conventionally approached as a technical challenge. However, cybersecurity is a human challenge: humans are behind the technology on both sides of the cyber event and their role in cybersecurity is increasingly being recognized (Greenberg, 2019; May, 2017; Singer & Friedman, 2014). Social engineering—manipulating people to engage in behavior that puts their organization at risk—plays a role in more than 80% of breaches (Hadnagy, 2018). Recent work discussing cybersecurity emphasizes this human and technical interaction as well as the need for strategic planning and persuasive communications to increase potential for cultural changes and behavioral adaptations by system users (Hamburg & Grosch, 2018; Muncaster, 2020; Plyler, 2020; Roper & Hurst, 2019).

Issues management should be ideally positioned to serve this role, with the capability to frame complex and confusing dimensions and interactions within cybersecurity to increase public understanding of the threats (de Bruijn & Janssen, 2017) and recontextualize publics' understanding to meet new and evolving challenges (Heath & Palenchar, 2008). To date, public relations literature on cybersecurity has employed Situational Crisis Communication Theory (Kim & Lee, 2018; Wang & Park, 2017). Approaching cybersecurity from an issues management of wicked problems perspective should include strategies to prevent incidents, improve systems, increase resilience, and monitor threats; protocols to respond to an incident and repair public perception of the organization; and sharing of lessons learned and best practices as well as mutual aid agreements and other resilience measures.

Cybersecurity is managed as an internal technical challenge requiring alignment of personnel behavior with organizational policy, or as a crisis when a breach or event impacts external publics. Siloing within organizations often renders cybersecurity the purview of an IT team rather than leadership and issues managers. Organizational siloing can impede internal issues management by fragmenting messaging among divisions and obfuscating authority of communicators.

Participants noted that utility leadership took pride in taking the cybersecurity training just like other personnel, to underscore its legitimacy. Participation by leadership may improve the trust of personnel by breaking organizational silos between management and other divisions (Neill & Bowen, 2021). For example, utilities often have organizational silos between executive and administrative personnel, IT personnel, OT personnel, and field personnel.

While IT personnel may apply legitimacy in their arguments for and policies enforcing cyber hygiene and gain power from leadership to implement MFA and other security measures, the issues managers are not the ones managing the issue. IT teams are not usually responsible for personnel alignment with policies, and they might not be viewed as legitimate enforcers of policy. This might have further complicated the mass move to telework early in the pandemic, which saw a series of boxes checked in outfitting personnel with devices and impelling use of tools like VPNs to protect organizational networks. However, actions to manage cybersecurity and communicate about needs failed to align behavior consistently with needed standards. Threat actors took advantage of the

situation, producing the spike in fraud and cybercrime that followed the onset of the pandemic in early 2020.

The COVID-19 Pandemic is Not Managed as a Wicked Problem. The COVID-19 pandemic remains poorly defined and widely contested in the United States. Response to the pandemic would seem an ideal case for issues management because it demands an adaptive, flexible approach with transparent messaging to communicate needs, build trust, and align public behaviors with necessary actions (Moon, 2020; Sahin et al., 2020). Instead, public opinion of government efforts in the United States is split between favorable and unfavorable, reflecting the lack of unified federal response and conflicting messages from government authorities and fragmented responses by states and within states (Gramlich, 2020).

Research from the 2003–2004 SARS epidemic affirmed that publics reacted more to media narrative than organizational messaging (Berry et al., 2007; Lewison, 2008). In addition, medicine has rendered pandemics less of a health threat than they historically had been while the attending economic impacts have significantly increased (Smith, 2006). This could have guided issues management of the pandemic by government and organizations alike, but conflicting messaging from government and health agencies and politicization of the pandemic impeded coherent framing of the pandemic and the attendant needs to address it. Messaging about necessary steps to adapt operations to the pandemic have had little in the way of common frameworks upon which to build.

Organizations have had to adapt to shifting and irregular state mandates, and weather protest and pushback from customers and personnel who question the legitimacy of the health claims. The forecasted economic impacts have been felt across all sectors of the economy and shaken the supply chain for many industries, complicating provision of services and further frustrating publics on both sides of the partisan divide. Finally, the incoherent response from authorities asserting different narratives about the relative strength of the virus, the relative effectiveness of mitigation strategies, and the acceptable level of impact on the economy have left publics without a common perception of what arguments are legitimate.

Existing issues management literature does not address the impacts of other organizations' issues management efforts. Heath (2013) discusses organizations in a web of relationships, and such communicative networks would certainly involve other organizations. The dynamics of a publics' perception of an organization's legitimacy may also be affected by the issues management of another organization, beyond competitors or even beyond the sector. How government agencies communicated about the pandemic and how software companies addressed or obfuscated discoveries of exploits complicated utilities' communications—and relationships—with their stakeholders.

Participants in this study managed the effects of the pandemic on their organization from a crisis perspective: They sourced hardware to facilitate telework; they heeded mandates to close lobbies and announced that they closed the lobbies because of state mandates; they moved meetings online, to outside

venues, or canceled them, citing alignment with local authorities or federal guidelines; they relayed communications from federal health agencies; they communicated solidarity and empathy; and they raised funds for struggling stakeholders. These actions are not proactive strategic issues management or acknowledgement of an ongoing, complex, intractable "wicked" problem.

The "Digital Divide" Is Not Managed as a Wicked Problem. The "digital divide" refers to the gap in technological access, capability, and expertise that occurs in various socioeconomic and geographic manifestations. The digital divide has been defined and studied as a wicked problem (Seymour et al., 2020). However, communications literature seems to have disregarded the digital divide for more than 10 years, and most articles in communication journals date from 2000 to 2008. Those asserted that the gap in broadband access was already being overcome (Rains 2008). Fourteen years later, communities continue to struggle with access to broadband Internet, dubbed in the intervening years as the "fourth utility."

Increasing use of telecommunications for education, health care, and professional work had rendered broadband Internet essential for full enfranchisement in contemporary American society even before the pandemic. The absence of such service is a great disadvantage for the communities left out, and the only factor that determines whether they are included in the network or left out is predominately the calculated profit potential for an investor-owned Internet service provider. That this is accepted speaks to ingrained social expectations.

Many participant organizations took up the challenge of overcoming this inequality for their communities. Rather than identifying the lack of broadband as an issue to be managed or a portion of a wicked problem to be called out, defined, and addressed, participant organizations elected to lobby their state governments for permission to solve the problem themselves and advocated to their stakeholders about the benefits they would realize from the service to be provided. While this may afford a solution for the community, it does not promote a broader awareness of a societal issue or overarching wicked problem that is disenfranchising fellow citizens.

Dynamics and forces that produced the socioeconomic inequality—capitalist prioritization, antiquated political boundaries—remain unacknowledged and thereby unaddressed. Like with the pandemic, the digital divide was treated as a crisis that affected the community, and thereby required government acknowledgement of a service need and approval of provision of that service by a qualified group. It is reminiscent of government response to storm damage or flooding in that it leverages finite resources to address a finite problem in a finite location. It does not manage the wicked problem from which the issue precipitated, so neither the wicked problem nor the issue is acknowledged, let alone addressed.

Education Alone or with Enforced by Policy Did Not Produce Lasting Changes

Persuading publics to adopt new behaviors in a lasting way poses a significant and ethically charged challenge for issues management. Issues management literature focuses on monitoring issues, identifying issues that could

impact the organization, proactively developing responses before the issues evolve into crises, and engaging in symmetrical (or, ideally, discursive) communication with publics to understand their perspective on an issue and frame the rationale for the organization's strategy (Aylesworth-Spink 2017; Erzikova & Bowen, 2019; Heath & Palenchar, 2008; Smith & Ferguson, 2013; Veil et al., 2015; Wu & Yang, 2017).

Participants in this study, by contrast, focused on behavior modification as the overarching goal of their issues management communications. While the steps outlined in the above issues management literature are all important to the process, many participants intimated that changing publics' behavior is the ultimate goal of their communications regarding cybersecurity or adaptation to the pandemic. These modifications may be either direct (i.e., getting publics to do something or do something different) or indirect (i.e., getting them to perceive the organization's actions as legitimate). Cases in this study showed how participant organizations' exercising of legitimacy and/or power have been inadequate to effect the necessary lasting behavioral changes.

Social/Behavioral Resistance Undermined Legitimacy. For both the COVID-19 pandemic and cybersecurity, participants consistently cited human behavior and resistance to change as the primary barriers to successful issues management seeking to limit the impact of wicked problems. Effective information sharing networks and clear channels of power and influence help in identifying a problem and defining actions that can address some of the attendant issues or moderate its impact. However, participants gauged the ultimate

effectiveness of the resulting strategies in the successful acceptance of the need for those actions by the necessary publics and integration into their behavior.

While technology can address and overcome some of the threats presented in wicked problems, the application of those technologies relies on human behavior. In cybersecurity, people identify exploits, people are usually responsible for identifying intrusions, people create the software threat, and people must be diligent in their cyber hygiene to minimize their risk. In the response to the pandemic, people diagnosed and forecast the spread of the virus, people developed the vaccines, people defined the policy responses and mandates to reduce transmission, and people adhered to or ignored the presence of the vaccines and the mandated responses. Pandemic mitigation suffers from human failure to properly follow recommended and mandated behavior. Weak passwords and unvaccinated populations pose greater risks. Passing cybersecurity training and exercising poor cyber hygiene is no more effective than an N-95 mask below the nose. In both cybersecurity and pandemic mitigation, failure to diligently follow the needed mitigation steps posed greater hurdles than resistance to the veracity of identified challenges.

Legitimacy was Insufficient to Modify Behavior. Legitimacy was the primary currency for participant organizations' communications with publics, whether the communications relayed vetted practices or informed publics about changes due to imposed power from legislation or regulation. Legitimate advocacy relies on rhetorical conventions like ethics and logic of the speaker, as well as symmetrical communication to enhance an organization's ability to

influence society (Edwards, 2018). The information sharing networks in which study participants engaged were built to vet and speed apprehension of legitimacy, and participants affirmed that information coming through an information sharing or mutual aid mechanism was considered verified. This step in the issues management process was very efficient and effective, likely owing to the discursive qualities of the information sharing network and the vetted authority of the sources of information within that network.

Subsequent communications to publics both internal and external asserted the legitimacy of the sources and then directed actions to be taken in response. Issues managers sought to reflect the legitimacy of their sources to publics by asserting the veracity of the information and strategies. However, assertions of legitimacy were insufficient to produce the desired behaviors, particularly when publics questioned the applicability of the actions in relation to their own experiences. Individuals within both external and internal publics objected to mask mandates and social distancing requirements, citing low infection rates in the community. Internal publics continued to engage in poor cyber hygiene despite extensive cybersecurity education, demonstration of the reality and proximity of the threat, and buy-in from senior personnel. External publics had to be reminded of mandates requiring masks or closing lobbies and may have understood the availability of apps to address office closures but lacked Internet access to use them. Internal publics also objected to masks or understood a need to shift to remote work but lacked the tools to do so.

In these cases, the organization established its knowledge of the issues and legitimacy of their sources (state mandates and cyber threat), the reality of the issue (the mandate existed even if you doubted the virus, cyber threats were tracked and breaches occurred at peer institutions), and that the strategies proposed were effective to address the issue (wearing a mask meets the mandate, extensive cyber education linked individual behaviors to increased or decreased security). This legitimacy in argument was insufficient to impel the desired behavior adaptations reliably or without protest.

The ineffectiveness of these legitimate arguments could be attributable to the publics' perceptions of the organization and the legitimacy of its arguments. However, other data show that the communities served by the utilities view them as legitimately concerned about the community and long investment as a member of the community. Likewise, if internal publics view other policies and protocols as necessary for safety and adhere to them, something in the argument is missing rather than something in the relationship. From an issues management standpoint, the organization is not accounting for some other environmental factor, which may be conflicting messaging from other organizations that publics view as legitimate or more powerful, or that conflicting messaging undermines the legitimacy of both organizations' messages. Kent et al. (2011, p. 539) describe a similar problem as a weakness of "short-term, quick-fix" practice rather than focusing "…on long-term issues likely to impact an entire industry or area." Short-term strategies, Kent et al. (2011) assert, are likely to fall into strategies to "manage publics" and are therefore more susceptible to unethical practice. The

collaborative, long-term approach could foster a common understanding among an organization and its publics, including other organizations with apparently conflicting short-term messaging.

Power with Legitimacy May Improve Behavior Modification. External and internal publics both received organizational issues management messages about the pandemic and buy-in from both publics was challenged due to skepticism of the validity of the threat and the applicability of the actions to the service area. However, organizational actions to adapt to the pandemic were frequently impelled by state mandates, and so issues management could cite an authority in making its appeal to the legitimacy of its actions and/or leverage the power of the mandating agency.

Power and legitimacy are linked throughout the issues management literature. Legitimacy can increase power and power can reinforce legitimacy; "truth" and force pairing in an invented echo of Machiavelli (Coombs & Holladay, 2015; Sommerfeldt, 2013; Weaver, Motion, & Roper, 2006). Power is not inherently a negative influence in society and can be used by governmental and intergovernmental authorities to influence perceptions even when the legitimacy of scientific authorities and mass media outlets are questioned (Lewison, 2008).

Participants in the study described both internal and external publics' questioning of the legitimacy of the threat of COVID-19 in their communities. While these publics bristled at, for instance, mask mandates, they did not question the power of the government to make the mandate or the legitimacy of the utility

asking for them to comply with the mandate. Likewise, many participants discussed how internal publics acknowledged the legitimacy of the cyber threat to their organization but were unable or unwilling to align their actions with the "cyber hygiene" necessary when accessing systems. When IT groups within utilities inevitably increased security protocols in response through MFA or more stringent password requirements, the internal publics predictably grumbled about the additional hurdles but did not circumvent the security measures or try to have them rescinded. In one case the IT team agreed to "meet in the middle" with password requirements more rigorous than before though not as rigorous as IT had proposed.

Utility communications addressing actions resulting from the pandemic such as cancellation of an annual members' meeting (i.e., an exercise in power), frequently cited chains of authority and verification that impelled the decision (i.e., an assertion of legitimacy). Any denial of service or change to a utility's interaction with member/owners or behavior by their personnel most often leaned on the orders of an influential organization or substantiated guidance from multiple organizations. The underlying messages "They're making us do this" or "All these people agree we should do this" invoke legitimacy even when the action results from power imposed on the utility.

Utilities felt resistance from personnel and member/owners in these interactions, an instance where resistance to the imposition of state regulations was directly felt by the utility. However, the mask mandate was not imposed by

the utility, the utility was trying to enforce the government-mandated social distancing through its communications.

In cybersecurity, behaviors that put the organization at risk persisted even when personnel understood the scale and veracity of the threat posed (i.e., knew that threat actors regularly attempted to access their utility's systems), regular training and certification cultivated and verified understanding of the behaviors required on the part of all members of personnel, and were subject to organizational requirements for personal access security and software stipulations designed to eliminate known exploits. In these examples, mixes of multiple dynamics of legitimacy with an imposition of power were still insufficient.

What seems to be missing from the case study issues management strategies and those defined as optimal in the literature, is the presence of cocreative or dialogic interaction with publics. Cocreational dialogue is a collaboration between the issues managers and internal or external publics to devise a best available solution that ensures the resilience of the organization (Willis, 2016). The characterization of the internal and external publics by participants as recipients of information or training and the need to change behavior is in contrast to the literature's asserted strategy of active engagement of relevant stakeholders (Willis et al., 2018). The publics may have understood the arguments and/or recognized different organizations' power to enforce policy, but they did not accept the arguments and internalize the messaging. Education about cybersecurity that emphasized "yes, us too," and "everything you do makes a

difference" did not overcome internal publics' inattention to cyber hygiene or previous issues encountered by the utility.

In the case study organizations, issues management entails the four components of issues management promoted in the literature—"systematic issue identification, proactive actions, issues monitoring, and dialogic issue communication," (Heath & Palenchar, 2008; Wu & Yang, 2017, p. 346)—but does not include engagement with publics in all of those activities, as the literature also suggests. Systemic issue identification should consider the publics' perspectives of the issue and means of resolution, which improves the organization's ability to target actions and messages to the most effective strategies (Veil et al., 2015).

Proactive identification of issues before they become crises demands direct engagement with publics throughout and following the process to address the issue. Issues may appear to be resolved only to recur later at the detriment of the organization, as has been seen in cybersecurity training (Veil et al., 2015). Monitoring includes review of media to gauge public opinion and response to organizational actions and communication (Aylesworth-Spink, 2017; Wu & Yang, 2017). Dialogic issue communication entails the "claims and counter claims about the legitimate locus of policy decision making...in issue management discourse," (Smith & Ferguson, 2013). Utilities asserted the presence of threat actors and the danger posed to their systems, specifically, and still saw personnel engage in risky behavior and use software previously flagged as vulnerable. Understanding what conflicting priorities compromise internal publics' hygiene

and how to move from "I understand the legitimacy and the reality of the threat" to "I accept the additional steps I need to take as part of my routine" is necessary for effective issues management and prevention of crises.

Perceptions of Truth Compound Issues Management. Public relations plays a central role in defining and iterating the constitution of social and political structures and interactions with a goal of reaching not an ultimate "truth," but a relative truth accepted as a "…means of legitimizing, or normalizing, material processes," (Weaver, Motion, & Roper, 2006, p. 19). Effective framing of the issues encountered and persuasion identifying the best strategies for addressing the greatest needs is essential for educating publics and improving adoption of the needed behaviors. All of these conflict with the amorphous nature of wicked problems, the oblique angle of issues management to the core issues, publics' resistance to persuasion or power due to conflicting ideas or just inattention, and undermining forces of opposing positions that may use ethical or unethical strategies.

Participants cited misinformation and disinformation as compounding problems in issues management of wicked problems. The issues managed are contested ideas: "differences of opinion regarding fact, value, or policy," (Heath & Palenchar, 2008, p. 93). Issues managers define and iterate these differences of opinion with publics. In ethical issues management, these facets of an issue are dialogically iterated between an organization and publics, taking into account the context of each interlocutor and the relative dynamics of power (Vardeman-Winter et al., 2013).

Misinformation and disinformation are the unethical counterpoints to the tools of ethical issues management. Instead of defining their own organization's approach to an issue and conveying legitimacy to their publics, issues managers may seek to "de-legitimize" opposing views by undermining their credibility, legitimacy, and power (Smith & Ferguson, 2013). Issues management literature acknowledges social or political means to address an issue by delegitimizing policy or social norms to repress perspectives or publics (Madden, 2019; Smith & Ferguson, 2013). Issues management of actions responding to the pandemic was greatly complicated by conflicting media messages drawn from conflicting governmental messages. Some of these messages sought to legitimize a position while others simply argued for the inapplicability of other messages. This left many utility publics unsure of whether the threat was genuine or fabricated, and to what degree it might be relevant to their community even if genuine. This emphasizes the context of Heath's (2013, p. 431) "discursive web of relational text." The myriad dynamics and connections in this web render the legitimacy of a single organization insufficient to ensure acceptance of the message by publics.

Practical Implications

This study extends practical understanding of issues management by establishing that: (1) issues management of compounding problems is only necessary when the compounding overlap in problems affects both the organization and the public addressed; (2) issues management by critical infrastructure aspired to be cocreation and emphasizes legitimacy over power.

Issues Management of Compounding Problems Requires Common Publics

The review of communications of 16 utilities produced only one that directly spoke to the nexus of cybersecurity and the pandemic: Co-op-1 developed an article for member/owners addressing a spike in scams seen in late 2020. While this addresses compounding problems between the problems, they are not compounding for the utility, as the study sought. These compounding problems are faced by the member/owners: "As we head into the holiday season, members are increasingly being targeted by utility scammers—particularly those who are threatening immediate disconnection, knowing many members have past-due accounts due to COVID-19 hardships."

This may be a sampling issue. Utilities communicate with member/owners via multiple media, of which the public relations communications on their websites are only one form. For instance, Co-op-6p mentioned communications on this subject that were not found on the website, and so may have been emails or other direct-to-member/owner messaging that did not turn up in the web review. Even so, such a lack of communications indicates that the member/owner publics and other publics are likely not the primary publics for this topic. The extent of discussion in the interviews and the nature of the challenges discussed indicate this was likely an internal issue or one iterated with collaborative or state government organizations.

Studies of issues management of compounding wicked problems must not only look at whether the problems compound for an organization, but whether they compound *with common publics* for that organization. Issues management

builds relationships with publics that share interests in issues, to improve the organization's ability to communicate and influence those publics (Grunig, 2006; Heath 2013b; Wu & Yang 2017). Conventional dyadic analysis of organization/public regarding issues management is troubled when compounding effects of multiple issues are analyzed. Organizations only address compounding issues with publics when the issues compound for the public(s) addressed as well as the organization. The multitude of publics—organizations and individuals, public and private sector—indicate the constellation of relationships an organization has, and how many may have interests in common issues, albeit widely varying in scope and need (Heath, 2013b, Sommerfeldt & Yang, 2017). If no relevant public faces the same compounding issues, there is no need to strategically communicate about the compounding effects of problems or issues.

Utilities engaged in little issues management of the compounding issues of COVID-19 and cybersecurity because the issues are managed with different publics, so little or no external communications of compounding issues were necessary. Strategic public relations approaches identify qualities, interests, and activities of groups of people external or internal to the organization that may affect or have interests that may be affected by the organization (Grunig & Grunig, 2000; Hallahan et al., 2007). Further, in the *communitas* conceptualization, an organization will collaborate with its community to co-define strategies to address issues based on legitimacy and mutual benefit (Heath, 2013b). The communitas approach seems to be the aspiration for the participants

in this study, though better realized in the networks of mutual aid and information sharing than between the utilities and its member/owner publics.

While both wicked problems compounded utilities' response to the issues of each, they did not communicate with the same publics about these compounding effects because the segmentation of publics identified different stakeholders for each set of issues. Only two utilities directly addressed compounding influences of the COVID-19 pandemic and cybersecurity with its member/owner publics, and those were factors impacting those publics rather than the utilties, like consumer alerts to ongoing scams. However, different authorities influenced utility responses to each issue and the subsequent impact on member/owners for each utility. State governments compelled utility actions in response to the pandemic through mask mandates and closure of offices and publicly accessible spaces. National and regional organizations used legitimacy to persuade utilities about proper cybersecurity measures. As such, there was no need to distribute public relations communications that addressed the compounding effects of COVID-19 adaptations and cybersecurity within the utility, because those concerns did not touch member/owners. Conversely, a significant quantity of communications addressing the compounding effects of the pandemic and the "digital divide" were developed precisely because that nexus directly affected member/owner publics.

In contrast, the issues stemming from the pandemic and lack of access to broadband were managed with common publics: state governments and member/owner publics. As such, utilities communications about the compounding

effects of adaptation to the pandemic and lack of broadband addressed both issues to the same publics and therefore produced many communications with the compounding effects as their focus.

Issues of broadband Internet access compounded by pandemic adaptation saw a great deal of external public relations communication, because utilities had multiple publics for whom those compounding issues were of direct relevance. Utilities communicated with member publics to assure them of continued access to services and utility efforts to bring broadband to the service area. Utilities communicated with state legislatures and regulatory agencies about the needs their service areas faced and to gain approval to form subsidiary companies to provide service. Utilities communicated with other utilities to acquire materials in short supply due to supply chain issues, and with internet service providers.

All of these examples consider communications with external publics. In cases of compounding wicked problems, communications with internal publics would likely address compounding wicked problems to a greater degree, as organizational personnel would be involved in the organizational response to the compounding problems (Coombs & Holladay, 2018; McCown, 2007; Willis, 2016). Review of internal public relations communications was very limited in this study, but participants uniformly agreed that organizations at all levels of strategic planning and response contributed to co-op utilities' plans for addressing compounding issues of cybersecurity and the COVID-19 pandemic. Internal public relations communications may address the compounding problems, and

peer-to-peer communications may as well, but external public relations communications would not have a strategic need to do so.

Issues Management by Critical Infrastructure Seeks Cocreation

This study identified dynamics that extend issues management understanding of the role that cocreation plays in issues management for public utilities. The public power sector has developed a closely-knit web of information and influence that processes intelligence and experiences into best practices and procedures. These conduits of information are symmetrical, and utilities inform collaborative and influential organizations as much as the informative and collaborative organizations do in return.

Responses to threats to critical infrastructure must inherently be swift and decisive, and assurances of the accuracy of information about both the threat, the expertise of the communicator, and the effectiveness of the proposed response—all essential qualities of legitimacy (Coombs & Holladay, 2018; Smith & Ferguson, 2010)—allow individual utility and coordinated sector responses to be as efficient as possible. The layers of legitimacy built into the critical infrastructure networks of communication provide issues managers within utilities with a list of trusted organizations to cite when relaying information to member/owners, reinforcing the organization's expertise on the issue, proposed solution, and context (Coombs & Holladay, 2018; Smith & Ferguson, 2010). This network reflects the theoretical goals of cocreation and mutual interest proposed in the literature, but took decades to cultivate and remains insular to protect against misinformation or intrusion. It serves the necessary purpose for this

specific sector, and similar networks for other critical infrastructure sectors, but this seems difficult to replicate for less invested publics or those with differing influences and priorities, including the members of the utilities' communities.

Interactions with member/owner and internal publics aspire to the same level of mutual influence and aid but remain short of the aspirational mark. Interactions with member/owners do open avenues for symmetrical communication, including annual meetings, social media, and in-person events (limited during the pandemic), but the communications still seem to lean on assertions or legitimacy or (more rarely) exercises of power than cocreational dialogue. Communications with external publics about adaptation to the pandemic primarily reassured stakeholders of reliable service or announced alignment with state mandates or federal guidelines. Communications with internal publics about cybersecurity mixed legitimacy (e.g., experiences, lessons from peer institutions, educational programs undertaken by all personnel) with power (e.g., MFA and password requirements). However, these efforts saw varying degrees of adoption, including resistance and pushback from some external publics and personnel.

Critical Infrastructure Organizations Rely on Legitimacy. The overwhelming theme in discussing issues management with influencer organizations, collaborative organizations, and utilities was the emphasis placed on legitimacy in intelligence, information sharing, and communication. This sector demands assurance that the sources of information are authoritative on the topics of which they spoke, that actions proposed to address issues they identified

are appropriate for those issues, and that the actions will provide the intended solutions and outcomes.

The role these organizations play in the daily functions of society engender a keen sense of responsibility and a drive to ensure that any interruptions in service are minimal. Issues managers rely on legitimacy as a pillar of ethical interlocution, both in messages sent and received, as a transparent base from which to argue for the collective benefit of society, publics, and the organization. Issues managers in this sector rely on vetted intelligence to be able to respond quickly and keep ahead of threats, or to have connections across the industry to coordinate messaging and collaborate on responses. Government, nonprofit agencies, and critical infrastructure have cultivated a carefully curated network of information sources over a span of decades, and they rely implicitly on the accuracy of the information shared within those conduits.

The critical infrastructure sphere of communication and influence takes great care in curating its interlocutors to ensure legitimacy to the greatest degree possible. Interlocutors have collaborated for years or even decades, and mutual aid agreements and information sharing mechanisms cultivate close organizational ties between organizations and even interpersonal relationships between personnel (Heath, 2009, Taylor, 2012; Willis, 2016). This cultivated network increases the efficiency by which critical infrastructure organizations engage in issues management, manage social and behavioral dynamics that challenge the successful management of issues and further increases perceived

legitimacy of member organizations through shared construction of meaning and experiences (Taylor, 2012).

Public utilities participate in social networks that extend beyond peer utilities and customers to include regulatory agencies, funding agencies, suppliers and vendors, and other organizations that contribute to the operation and maintenance of the grid (Hughes, 2012). This network of peers and stakeholders improves problem solving and ensures distribution of lessons learned, to help issues managers identify best available solutions (Willis, 2016). Issues managers engage publics in deliberation and iteration of solutions when confronting wicked problems, to span boundaries across the utility sector and many other sectors (Willis et al., 2018). This network provides issues managers with a spectrum of vetted sources of and outlets for information and intelligence.

Dominance of the communicative networks by nonprofit information sharing and advocacy groups seeks to insulate guidance from profit motives or policy objectives. Distrust of new sources of communication results both from the strength of the network ties and suspicion of the motives of new points of contact. Vetted networks of intelligence, information sharing, and mutual aid improves in issues management (Heath, 2013a; Sommerfeldt & Kent, 2013; Sommerfeldt & Yang, 2017; Yang & Taylor, 2014).

Collective participation in defining and iterating problems helps foster creative problem solving and apply existing resources to new problems (Cohen & Cromwell, 2020). The familiarity bred in this network speeds and aligns response and external communications across utilities nationwide, and affords utilities an

expansive net of mutual aid and best practices from which to draw to improve their own operation and recovery. Effective and efficient communication and coordination among the participants in these networks with input from relevant vendors associated with utilities is essential for successful grid operation (Artz, 2020)

Influencers build trust with utilities and improve interactions among organizations in the sector (Coombs & Holladay, 2012; Edwards, 2016; Willis et al., 2018). Though not a formal category in other analysis of issues management, this study used the terms “influencers” or “influential organizations” to denote participants in the networked communications of the energy distribution sector that compiled intelligence and information and distributed it to utilities and collaborative organizations to improve utility operations and decision making. These organizations are deemed “influential” because they do not hold direct power over participant utilities, which operate at an insufficient scale to warrant federal oversight.

Participants from federal agencies and nonprofit organizations regularly referred to the trust built within the critical infrastructure sector and the extensive degree of collaboration and information sharing essential to its efficient operation . The breadth of geography and depth of socioeconomic strata served by the grid demand far broader awareness than is possible by any single utility. The influencer organizations fostered camaraderie and close relationships among sector organizations that could later serve (and indeed have already served) in

mutual aid and information sharing activities to improve resilience of sector operation (Grunig, 2000; Taylor, 2011; Wu & Yang, 2017).

Collaborator organizations rely on legitimacy both to inform reactions to issues and to advocate for measures to utilities (Heath & Palenchar, 2008; Madden, 2019, Sommerfeldt & Xu, 2014). Joint-action agencies and trade associations frequently act as mediators between federal agencies and utilities, particularly smaller utilities whose resources would be strained by attending strategic planning workshops and other cross-industry colloquia sponsored by influencer organizations. Their combined role of filter and guide serves utilities in their decision making and reduces their already strained workforces. The degree of reliance demands that influencers be confident in the information they relay and the actions for which they advocate. In turn, collaborators also serve as conduits for information from individual utilities back to the influencer organizations, ensuring that the "ground level" perspective is seen by organizations that operate at a level that may hinder the granular view of the impacts of their recommendations.

Critical Infrastructure Conveys Legitimacy to Stakeholders. Utilities depend on legitimacy of their sources of information in developing their strategies and communications and seek to convey legitimacy in communications discussing changes of policy with their member/owners and other publics (Coombs & Holladay, 2018; Smith & Ferguson, 2010; Willis et al., 2018). Whether the messages inform the member/owners of the utility's reaction to legitimacy (e.g., recommended best practices) or power (e.g., mandated actions), utilities tend to

cite their influences in their messages. These messages state that the utility is instituting an action in response to government mandates or made a decision based on information from authoritative organizations and tend to characterize the change in policy as "we're taking action because of this authority." This may justify the actions of the utility or seek to minimize its culpability if member/owners object.

Utilities effectively reversed the direction of legitimacy arguments when addressing broadband. In these cases, the utilities argued for the threat posed to the member/owners by the inability to access services needed to functionally adapt to contemporary societal dynamics, that the provision of fiber-optic broadband was the necessary action to address this need, and that the utility was uniquely positioned to make the construction of the needed infrastructure economical and efficient (Coombs & Holladay, 2018; Smith & Ferguson, 2010). These arguments were made to state legislative and oversight agencies to seek approval for the founding of subsidiary companies to handle the new service and were ultimately effective after years to more than a decade of advocacy.

Public relations advocacy literature considers how organizations act on behalf of publics to support issues in the organization's interest and balance interest of society and organization itself (Coombs & Holladay, 2012; Toledano, 2019). In this case, however, the advocacy was clearly more in the stakeholders' interests than the utilities' interest. The proposed solution for bringing broadband to service areas required utilities establish for-profit subsidiaries—for which they

had to lobby for legislative changes—and added another mode of service to the utilities that are already stretched with provision of electricity.

Reflections for Issues Managers

This study explored the perspectives, practices, and actions by issues managers playing different roles in very specialized organizations. Conclusions from this study afford insight for issues managers far beyond those specialized organizations and may resonate with issues managers throughout other organizations, from executive management to operational personnel. Specifically, issues managers are more than boundary spanners between their organization and publics, they also span boundaries between the publics with whom their organizations are invested and other sources of information. Any effort to address symptoms of wicked problems, including technical challenges like cybersecurity and pandemic healthcare, relies on behavioral adaptation by internal and external publics. Education and training must rely on more than vetted information and policy to provoke lasting behavioral adaptation.

Effective boundary spanning includes more than interactions among divisions of an organization or between that organization and its constituent publics. Issues managers should consider how actions by other organizations impact their publics and be ready to advocate on their behalf or bolster other organizations' messages to their publics. Issues managers at these utilities lobbied state governments on behalf of their publics on numerous occasions, including to gain the ability to provide a needed service their communities lacked (i.e., broadband Internet) and to gain exceptions to state mandates to continue

providing services upon which their publics relied (e.g., keeping a lobby open for cash payments despite pandemic mandates closing similar places of business). These actions demonstrated awareness of and sensitivity to needs in the community beyond those within their utility's conventional business model. Such actions deepen the perceptions of legitimacy in the community, bolster the organization's status in the community, build social capital for future times of crisis, and may help the organization broaden its business. Effective issues managers span boundaries for their publics beyond those between their own organization and those publics.

Internal and external issues management needs to recognize behavioral adaptation as an essential end of many technical challenges. It is easy but overly simplistic to consider a technical challenge as requiring a technical solution, and cybersecurity programs in particular tend to focus heavily on VPNs, firewalls, MFA, etc. However, these are just tools in the toolbox. A screwdriver requires a person using it correctly in order to drive a screw. Both internal and external issues management need to consider what actions are desired on the part of publics and to develop programs that will achieve that desired behavioral change. Identifying information to convey and the means to convey it are only part of the issues management process. As with strategic planning, issues management needs to continue environmental monitoring through deployment and awareness of the effects of a program to make necessary adjustments and revisions until the desired results are achieved.

When educating publics about an issue and/or advocating for changes in behavior to address an issue or a symptom of a wicked problem, legitimate information backed by policy is likely only effective for short term compliance with desired behavior. People tend to believe that dangers do threaten them directly, even if they accept the presence of the threat. Personnel can recognize a cybersecurity threat and understand that any point of vulnerability can compromise the organization and still balk at using MFA. More than two years into the pandemic the use of masks and utility of vaccines are as contested—if not even more contested—than they were a year or two ago. Policies requiring a change of behavior are likely to see resistance unless a change in policy is enforced as a new part of culture (e.g., 20 years after a single attempted shoe bombing of plane, everyone boarding a flight in the United States has to remove their shoes and does so with feewer if any outright protests, in contrast to what has been seen with masks).

Treat issues management communications as intercultural communication. We often think of intercultural issues in obvious, national/ethnic terms, but more subtle instances of cultural boundary spanning influence issues management. Rural communities bristled at having to adopt the same restrictions as more populated areas during the pandemic. The digital divide validated some communities' perception that other areas did not see or value them. Technical personnel may not respect the perceptions of executives or communications personnel, and executives and communications personnel may not appreciate the depth of expertise of technical personnel. Both internal and external issues

management needs to be treated as an intercultural endeavor, resisting any assumptions of understanding of the perceptions or priorities of the public before gaining insight from them directly, and gaining partnership with individuals of prominence in those communities to better cultivate the trust needed to influence behavior. Finally, once gained, this trust must not be abused or disrespected, as the effectiveness of both present and future actions depends on the trust being untarnished.

Directions for Future Research

This study expanded the academic literature on issues management and wicked problems to include critical infrastructure organizations and consider compounding effects of concurrent wicked problems. While the wicked problems themselves are frequently beyond the scope of control of any individual issues manager, the sociocultural root of the issues in this study have produced additional effects that warrant examination.

Utilities most actively sought to manage the issue of broadband Internet access, frequently founding entirely new subsidiaries to bring service to their stakeholders. The communications surrounding these efforts addressed stakeholders, state lawmakers, and other publics, advocating on their stakeholders' behalf for the necessity of this service. Issue management of the "fourth utility" communications addressing enfranchisement and equal access to necessary services affords additional avenues for issues management of wicked problems, and financial limitations of public utilities and the rural communities they serve pose compounding wicked problems.

Issues management communications addressing the "digital divide" and affirming utilities' conviction to bring service to their stakeholders also underscores a strong dedication to community. Co-op utility communications emphasize that the utilities were founded by their communities and they frequently reaffirm their dedication to their communities in their communications.

Issues Management Centering Community and Enfranchisement

The role of the co-op utility in the community and its role in advocating for broadband service were frequent and intertwined themes with participants and in organizational public relations communications. In advocating to and on behalf of stakeholders, utilities repeatedly asserted their embeddedness in and dedication to the community. Utilities launched multiple philanthropic efforts to help communities during the community and spent years setting up subsidiary companies to provide broadband service.

Collaborating with publics to develop collective understanding of societal expectations has long been part of public relations and issues management (Grunig, 2000). Issues management can promote public debate about social expectations and what manner of services can be expected for mutual benefit in society (Taylor, 2011; Willis et al., 2018; Wu & Yang, 2017). This dialogue can also iterate expected benefits versus acceptable costs (Willis, 2016). Further exploration of community-centered communication by issues management without the communicating organization benefiting outright from the outcome can build on the deontological model of issues management (Place, 2010). Future

research into issues management can expand understanding of this approach that emphasizes societal benefit over organizational (Heath, 2006).

Utilities were founded by their communities and are "bulwark institutions" of their communities. They have cultivated significant legitimacy and social capital. One of the major tenets of legitimacy in issues management is perception by publics that the organization understands the issue about which it is advocating, and that the solution will fit the issue and provide a desired solution (Coombs & Holladay, 2018; Smith & Ferguson, 2010). Through long integration in the community, co-op utilities have cultivated significant legitimacy and social capital that provide them an unusual degree of legitimacy.

Cocreational Issues Management and Resilience

Issues management does not manage issues; it manages because of issues (Jaques, 2010). Issues management for critical infrastructure does not seek to solve the wicked problems or issues that challenge its operation, but to cultivate resilience in the face of threats, so that any compromise to network service is as short a duration and as small a scope as possible. Reliability has been a central issue for electricity distribution since public perception of its value transformed service from a luxury to a necessary service (Cohn, 2017). This aversion continues today, and while outages are accepted as inevitable, the duration of the outage is minimized to the degree possible.

As one of the extensions of public relations theory afforded by issues management literature (Heath & Palenchar, 2009), cocreational collaboration with stakeholders helps organizations identify best available strategies and improve

resilience (Willis, 2016). Over the course of several decades, information sharing organizations and collaborative organizations have developed a networked community supporting public power. Utilities participate in this network with organizations of widely varying scope and reach in a collective effort to improve reliability, resilience, efficiency, operation, and transparency of public utilities. Information is collected at all points of this network from international to local and contextualized and shared widely for collective benefits. Information from small rural co-ops is valued along with intelligence from federal agencies. Organizations dedicated to sharing information anonymize input to ensure utilities reporting events do not need to fear repercussion for a breach or outage. The emphasis is on collective lessons for the greater benefit.

These cocreative relationships extend in ways that are multiple and far-reaching, as organizations cultivate other relationships with stakeholders, suppliers and vendors, regulatory and oversight agencies, and peer organizations, among others Heath (2013b). Cocreative relations improve problem solving, distribute lessons learned, and collectively identify strategies and solutions that are the greatest benefit (Willis, 2016). The degree to which all participants expressed confidence in and reliance upon this network illustrated the dedication interlocutors bring to this collective, and the commitment all participants have to the benefit of the sector and its member/owners.

Issues Managers can Improve Resilience by Building Collaborative Networks. In its efforts to bolster grid resilience and speed response, the American Public Power Association has promoted and facilitated a mutual aid

network among member utilities. In the construction of the mutual aid network, utilities met to share needs and discuss best means for information sharing, mobilization, and response to events that overwhelm a service area's utility. The development of the mutual aid tools nurtured relationships among the participants, who represented public utilities of all scales of operation from across the country. The solution lay not in more advanced tools or even more sophisticated sensors and control systems, but in the attention and expertise of the people who keep the grid operational every day.

The role personnel play in technical solutions was a recurring theme among participants, and the degree to which effective solutions hinged more on the diligence of people than the sophistication of technology. Studies of the communication of agency in what are assumed to be technical matters would afford greater insight into these dynamics. In addition, the recurrent theme of the challenge of ensuring lasting adoption of behaviors to support technological solutions—cyber hygiene and mask use, for instance—could inform the weaknesses in the current strategies.

Internal Publics are the Key for Organizational Resilience. No matter the level of sophistication built into a system, natural or human threats to the grid can push it to a point of compromise. At that point, skilled personnel are needed to provide flexible problem solving to overcome the breach. Just as the potential loss of personnel was the major threat utilities faced from the pandemic (i.e., without control room personnel, the utility would not operate), grid reliability and resilience ultimately hinged on the utility's personnel. Prominent cyber attacks

have successfully overcome organizations and infiltrated connected networks and large-scale storms have caused widespread loss of service. Seasoned personnel provided the expertise, insight, and labor to restore infrastructure and recover from these events and strengthen infrastructure and response practices against future threats. Collective, dialectical, critical appraisal of an issue provides the greatest likelihood for resilience where technological solutions or impositions of power or logic fall short.

Limitations

Despite the aspirations of this design to engage broad perspectives and provide a degree of generalizability through data saturation, the design poses undeniable limitations. This study sought to explore the lived experiences of issues managers at co-op electric utilities. The number of variables that shape a utility—including the geography, population, and affluence of the service area, the associated generation and transmission utilities, and the state and local government agencies—challenge any generalization of a particular case study. The study sought to improve generalizability by seeking multiple cases, and the data did converge to a point of saturation, but the particularity of experience of co-op utilities does not preclude there being additional factors left unstudied.

Data Collection

The method of data collection posed limitations. The timing of the study both provoked interesting insights from participants and provided considerable challenges in recruiting participants. The study sought to capture perceptions of participants while they struggled with the problems upon which the study focused.

This provided vivid and fresh recollections, but also repelled many would-be participants because the topic of cybersecurity, in particular, was too sensitive given concurrent breaches. While any utility's public relations communications can be accessed and reviewed, the purpose of the study was to compare what they did to why they did it—the confluence of influences that produced a response or how the communications contrasted with the asserted influences.

The researcher recruited participants from influential organizations and from joint-action agencies through purposive and snowball sampling methods based on the researcher's prior professional contacts. The final set of participants at the utility level was determined more by who responded to email invitations to participate than by any preconceived design. To balance data received, the interview data from the comparator utility from a different region was augmented with both its public communications and those from its trade association.

This model offered the desired data set of information and influence coming into the utility, utility issues makers reflecting on their interpretation of the data and the way in which they desired to convey it to their publics, and then the resulting publicly facing communications. However, this manner of sampling precludes the ability to assert saturation. There may be qualities among the utilities that refused to participate that are not visible based on this sample. One inherent limitation of the case study in general is that, while it provides deep insight to a particular case or cases, generalizability is not achievable due to the specificity of each case. Framing this study as a multiple-case study sought to broaden the perspectives afforded, and achieves that goal in insights far beyond

what a single utility might provide, but the proportion of these participants to the entire sector is far too small to assert saturation or generalizability.

While all interviews were recorded with a voice recorder to improve data coding and analysis by allowing review of the conversation, the recordings did not capture any nonverbal cues, including for the online as well as in-person interviews. Participants requested that the conversations via Zoom, for instance, not be recorded within the platform because of security concerns attending recording via online software and potential for breach of cloud storage. All nonverbal communication had to be captured in notes during the conversation, and there was no means by which to later review and verify those perceptions. Interviews by telephone preserve vocal tone and inflection but miss all nonverbal communication. (Abrams et al., 2015).

Data Analysis and Interpretation

The method of data interpretation posed limitations. As a qualitative study, this inquiry produced deep, continuous data that offered glimpses into the perspectives of utility communicators, executives, and technical staff from across the nation, as well as communicators, strategists, and program managers at prominent national and federal organizations. The depth and nature of that qualitative inquiry also challenged interpretation of the data and held the risk of researcher bias. The choices made in how to divide continuous data and what data are worthy of presentation and emphasis inherently introduces a degree of researcher bias. The interviews produced more than 15 hours of conversation transcribed onto 361 pages, and the semi-structured nature allowed exploration of

topics beyond the protocol. The review of communications spanned thousands of communications over the defined timeframe and required determination of what counted as applicable versus not. The study defined the topics of interest, but not the manner by which the researcher identified what constituted relevance to those topics. Of the many emergent topics, the "digital divide" provided the most relevant point of comparison and enlightened the defined purpose of the study to the greatest degree. This does not mean, however, that another researcher would make the same determination.

The codes used across the interviews and communications products helped to identify common themes among the data, and replication of themes across the interviews and across the communications products (though differing somewhat between the interviews and communication products) allows assertion of analytic generalization. This differs from saturation in that, while data have theoretical applicability to situations beyond those strictly analogous to the case(s), it does not assert that further inquiry is unlikely to produce new data (Yin, 2018). Data from interviews and communications across the cases converged in a way that suggested the conclusions presented here, but the researcher acknowledges that the sample may not have provided a complete view of all possible themes.

Conclusion

The data presented in this study illustrate the clear hierarchical relationship between wicked problems and issues management (i.e., that issues managed are subsets of the greater wicked problem) just as previous literature concluded the crisis and risk management were subdisciplines of issues

management (Heath & Palenchar, 2008). Critical infrastructure utilities are a confluence of political, economic, and social forces (Cohn, 2017; Hughes, 1983). As such, utilities share qualities of social organizations that have been the focus of literature addressing wicked problems (Willis et al., 2018). When confronting wicked problems, social organizations tend to not rely "on rules enforced by legal frameworks or government regulation," and "…instead require the development of a climate of trust and mutual support underpinned by compatible values, norms, and social capital" (Willis et al., 2018, p. 388). This has significant bearing on analysis of messaging by municipal utilities, as they depend upon trust and mutual support and are also subject to legal frameworks and regulation. While the "…underpinning principle of issues management is not to avoid legislation, regulation, or crisis," (Heath & Palenchar, 2008, p. 13), public utilities have explicitly conveyed the attraction of undertaking voluntary, cooperative efforts that might stave off additional federal regulation (American Public Power Association, 2019).

Given the United States' dependence on reliable power—"it's 5% of the U.S. economy, but the first 5%" (American Public Power Association, 2017)—public utilities are critical participants in the operation and stability of American society. Understanding how they make meaning of their roles, including their responsibility for relevant threats, are pressing issues. When studying infrastructure, qualitative methods afford deeper insight than quantitative (Parks and Starosielski, 2015). Inquiry into individual perspectives also demands a qualitative approach (Hesse-Biber, 2017), as does examination of the forces that

impact the operation of a critical infrastructure utility (Parks & Starosielski, 2015).

Public co-op utilities are struggling under the compounding influences of multiple concurrent wicked problems. Cybersecurity poses many internal public relations issues management challenges and cross-sector and cross-industry challenges through networks of communication, networks of influence, and networks of aid and collaboration. The COVID-19 pandemic posed both internal and external public relations issues management challenges and forced utilities to react to mandates and other political influences on their interactions with member/owners and their requirements for personnel. Broadband access poses issues management challenges with member/owner publics and state government and regulatory agencies. The concerns of these issues entail behavioral, cultural, economic, geographic, public health, technological, geographic challenges that utilities address through both messaging and action.

This study reinforces the applicability of public relations theories to public organizations (Liu & Horsely, 2007). By accompanying outcomes of semi-structured interviews with case studies of contrasting utilities and employing review of organizational publications resulting from attempts to address the compounding issues of cybersecurity and the COVID-19 pandemic, this study presents a spectrum of experience and multiple media in a coherent and validated analysis of a pressing phenomenon. The multiple-case study format provides insight into the effects of concurrent wicked problems at multiple peer organizations and their prominent publics.

Rendering the experiences of these issue managers in their own words and seeing how their experiences are reflected or contradicted by publics affords direct insight to the role of issues management in compounding wicked problems. Participants from utilities and prominent publics along with communications materials and media help triangulate the data and provide points of comparison and contrast between the stated objectives, resulting communications, and the subsequent reactions. Final data analysis included review of codes across all data sets to unify data collected and draw out multiple levels of narrative. The final data set improves understanding of the role of issues management in addressing wicked problems and broadens understanding of how social and technological forces combine in the development of wicked problems.

Overarching themes in this study, presented in Table 8, extend previous scholarship in issues and highlight opportunities for future research. This study illustrated that issues management relied heavily on establishing organizational legitimacy with publics when communicating about changes resulting from external influences of either legitimacy or power. Issues management communications often reflected strategic planning in advance of the communications, and communications contextualized to the publics being addressed. Communications about cybersecurity or the digital divide presented distillations of broad and amorphous challenges into contexts specific to the member/owner or internal publics being addressed. Legitimacy leaned on vetted networks of information, best practices, and advocacy for resources suited to the challenge. In answer to power leveraged against the utility, utility issues

management still emphasized legitimacy in the utility's actions due to the power imposed by the outside agency. Communications from the utility to both internal and external publics, some of whom vocally objected to the measures taken in response to the COVID-19 pandemic, leaned on legitimacy of the organization's aligning practices with the mandates. Utilities either cited the imposition of power that left them without choice but to follow the mandates or cited a string of organizations advocating in parallel for the actions taken, to bolster the decision making of the utility itself.

In all forms of utility communication beyond strictly informative announcements, arguments asserting legitimacy overwhelmingly outnumbered citation of utility power. This could inform future studies on how relayed communication from one organization or public to another can shift in dynamics between claims of power and legitimacy. Power imposed on one organization may be used to legitimize a change in policy regarding its publics, or legitimate information may be used to justify imposition of power onto publics.

In examining the role of legitimacy and issue monitoring and development of responses and strategies for issues management, this study illustrated how utilities in critical infrastructure cultivated networks of communication to improve assurance of legitimacy in their sources of information and guidance. Extended close collaboration with peer organizations and national-scale advocacy and information sharing entities assures utilities of the quality of information they receive and speeds the rate at which they receive it. These networks also serve as a buffer against misinformation and disinformation and help utilities parse

confusing and sometimes contradictory accounts of security concerns and best practices. By assuring the quality of their guidance and intelligence, critical infrastructure has avoided many of the debates other facets of society have faced in responding to the COVID-19 pandemic. Future studies can explore whether cocreational networks like these have been developed for other issues management endeavors, and the role that organizational peer communities like these play in the concept of community in issues management research.

The study also explored the roles power plays in the issues management efforts of utilities, by illustrating how utilities were subject to and responded to power imposed upon them by state authorities, and imposed power on internal publics. Responses to the COVID-19 pandemic and business adaptations attending it were largely mandated by state authorities. Particularly in the first months of the pandemic, state agencies limited access to businesses and publicly available commercial spaces. Utilities followed these directives with minimal if any protest at the executive level. Utility participants asserted and utility communications also related multiple instances of utilities lobbying state legislature on behalf of their interests or seeking changes in policy to improve their provision of services. While state power over the utilities still appeared to be largely asymmetric, utilities demonstrated that concerted and extended advocacy with state policymakers could produce valuable changes for the utility. This presents opportunities for future study in which relationships are, at turns, asymmetrical (e.g., COVID mandates) and symmetrical (e.g., lobbying and advocacy for legislative changes).

In addition, this study illustrated that resilience is the overwhelming priority of critical infrastructure utilities when responding to wicked problems, and the indispensable role both supply chain and utility personnel play in organization's resilience. Wicked problems are, by definition, without solution. Even symptoms of those problems–prominent issues arising from them and crises precipitating from them—may be beyond the control of a utility. In the absence of a solution, utilities must focus on organizational resilience to reduce service interruptions. Resilience as a strategy for addressing wicked problems or in issues management, generally, could provide a useful frame for future inquiries.

As cybersecurity and the COVID-19 pandemic profoundly impact our present society, myriad other wicked problems are currently at the forefront of our national conscience. Improved understanding of the mechanisms and influences inherent in these phenomena may improve the functioning of our society and all organizations and people in it. While this study was specific in the targeted participants and subjects explored, the primary themes of this study—legitimacy in arguments for public services and policy; power exerted by government, for-profit and nonprofit organizations, and publics; codification of socioeconomic inequality in built infrastructure; attempts to overcome ingrained inequality and realize equitable benefits from contemporary services—are all resonant in national and international conversations. In addition to their role as a boundary-spanning conduits for communications and relationship building, issues managers have the power to shape society. Greater understanding of how the tools and techniques by which it does so, along with the publics and power that might keep

it in check, improve our understanding of the formation and evolution of the society in which we live.

References

Allison, M., & Kaye, J. (2005). *Strategic planning for nonprofit organizations: A practical guide and workbook.* Wiley.

American Public Power Association. (2014). *Mutual aid playbook.* https://www.publicpower.org/resource/mutual-aid-playbook

American Public Power Association. (2017, August 2). *US electric sector provides 5% of GDP, supports 7 million jobs, study finds*. Community Engagement. https://www.publicpower.org/periodical/article/us-electric-sector-provides-5-gdp-supports-7-million-jobs-study-finds

American Public Power Association. (2019). *Regional municipal utility cybersecurity summit summary report*.

Artz, S. (2020, November 10). *Communications needs for public utilities* [Conference presentation]. EnergySec Town Hall - Stronger Together, Online.

Aylesworth-Spink, S. (2017). The failure of public relations during a pandemic outbreak: Using Actor-Network Theory to highlight the news media as a complex mediator. *Public Relations Journal*, *11*, 1–17.

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press.

Bernays, E. L. (1928). *Propaganda*. Ig Publishing.

Bernays, E. L. (1952). *Public relations*. University of Oklahoma Press.

Berry, T. R., Wharf-Higgins, J., & Naylor, P. J. (2007). SARS wars: An examination of the quantity and construction of health information in the news media. *Health Communication*, *21*, 35–44. https://doi.org/10.1080/10410230701283322

Botan, C. H. (2018). *Strategic communication theory and practice: The cocreational model*. Wiley Blackwell.

Botan, C. H., & Taylor, M. (2004). Public relations: State of the field. *Journal of Communication*, *54*, 645–661. https://doi.org/10.1111/j.1460-2466.2004.tb02649.x

Bowker, G. C., Baker, K., Millerand, F., & Ribes, D. (2010). Toward information infrastructure studies: Ways of knowing in a networked environment. In J. Hunsinger, L. Klastrup, & M. Allen (Eds.), *The international handbook of internet research* (pp. 97–117). Springer.

Bratton, B. H. (2015). *The stack: On software and sovereignty*. MIT Press.

Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity essentials*. John Wiley & Sons Inc.

Broom, G. M., Casey, S., & Ritchey, J. (1997). Toward a concept and theory of organization-public relationships. *Journal of Public Relations Research*, *9*, 83–98. https://doi.org/10.1207/s1532754xjprr0902_01

Bryson, J. M. (2018). *Strategic planning for public and nonprofit organizations: A guide to strengthening and sustaining organizational achievement* (Fifth edition). John Wiley & Sons, Inc.

Capizzo, L. (2019). *Managing intractability: Wrestling with wicked problems and seeing beyond consensus in public relations* (Publication No. 27542930). Doctoral dissertation, University of Maryland, College Park. ProQuest Dissertations Publishing.

Capizzo, L. and Sommerfeldt, E. (2021) Defining the contours of contention: facets of intractability in social issues management, *International Journal of Strategic Communication, 15*, 357–374, https://doi-org.proxy-um.researchport.umd.edu/10.1080/1553118X.2021.1932907

Carey, J. W. (2009). *Communication as culture: Essays on media and society*. Routledge.

Castells, M. (2000). *The rise of the network society*. Blackwell Publishers.

Chrustie, C., Docherty, J. S., Lira, L., Mahuad, J., Gadlin, H., & Honeyman, C. (2010). Negotiating wicked problems: Five stories. In C. Honeyman, J. Coben, & G. De Palo (Eds.), *Venturing beyond the classroom* (pp. 449–480). DRI Press. https://www.academia.edu/download/30190531/25-Chrustie-etal-Five_Stories.pdf

Cohen, A. K., & Cromwell, J. R. (2020). How to respond to the COVID-19 pandemic with more creativity and innovation. *Population Health Management*, pop.2020.0119. https://doi.org/10.1089/pop.2020.0119

Cohn, J. A. (2017). *The grid: Biography of an American technology*. The MIT Press.

Coombs, W. T. (2010). Crisis communication. In R. L. Heath (Ed.), *The SAGE handbook of public relations* (pp. 477–488). SAGE Publications.

Coombs, W. T., & Holladay, S. J. (2012). Privileging an activist vs. a corporate view of public relations history in the U.S. *Public Relations Review*, *38*, 347–353. https://doi.org/10.1016/j.pubrev.2011.11.010

Coombs, W. T., & Holladay, S. J. (2015). Public relations' "relationship identity" in research: Enlightenment or illusion. *Public Relations Review*, *41*, 689–695. https://doi.org/10.1016/j.pubrev.2013.12.008

Coombs, W. T., & Holladay, S. J. (2018). Social issue qua wicked problems: The role of strategic communication in social issues management. *Journal of Communication Management*, *22*, 79–95. https://doi.org/10.1108/JCOM-11-2016-0093

Crable, R. E., & Vibbert, S. L. (1985). Managing issues and influencing public policy. *Public Relations Review*, *11*, 3–16. https://doi.org/10.1016/S0363-8111(82)80114-8

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*, 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Dewey, J. (1927). *The public and its problems: An essay in political inquiry*. Swallow Press.

Dutta-Bergman, M. J. (2006). U.S. public diplomacy in the Middle East: A critical cultural approach. *Journal of Communication Inquiry*, *30*, 102–124. https://doi.org/10.1177/0196859905285286

Edwards, L. (2016). The role of public relations in deliberative systems: Public relations in deliberative systems. *Journal of Communication*, *66*, 60–81. https://doi.org/10.1111/jcom.12199

Edwards, L. (2018). *Understanding public relations: Theory, culture and society*. SAGE Publications.

el-Nawawy, M. (2006). US public diplomacy in the Arab world: The news credibility of Radio Sawa and Television Alhurra in five countries. *Global Media and Communication*, *2*, 183–203. https://doi.org/10.1177/1742766506066228

Elavarasan, R. M., Shafiullah, G., Raju, K., Mudgal, V., Arif, M. T., Jamal, T., Subramanian, S., Sriraja Balaguru, V. S., Reddy, K. S., & Subramaniam, U. (2020). COVID-19: Impact analysis and recommendations for power sector operation. *Applied Energy*, *279*, 115739. https://doi.org/10.1016/j.apenergy.2020.115739

Erzikova, E., & Bowen, S. A. (2019). Missed opportunities to make PR great again: How public relations agencies responded to the Trump presidency. *Public Relations Review*, *45*, 101793. https://doi.org/10.1016/j.pubrev.2019.05.014

Ewen, S. (1996). *PR! A social history of spin*. Basic Books.

Farman, J. (2018). A delayed crossing. In *Delayed Response: The Art of Waiting from the Ancient to the Instant World* (pp. 111–135). Yale University Press. http://www.jstor.org/stable/j.ctv7cjvp9

Ferguson, M. A. (1984, August). *Building theory in public relations: Interorganizational relationships*. Association for Education in Journalism and Mass Communication Annual Convention, Gainesville, FL.

Gelders, D., & Ihlen, Ø. (2010). Government communication about potential policies: Public relations, propaganda or both? *Public Relations Review*, *36*, 59–62. https://doi.org/10.1016/j.pubrev.2009.08.012

Golbeck, J. (2018). Data We Trust—But What Data? *Reference & User Services Quarterly*, 57, 196–199. https://www.jstor.org/stable/90019885

Gramlich, J. (2020, September 21). *Americans give the U.S. low marks for its handling of COVID-19, and so do people in other countries*. Pew Research Center. https://www.pewresearch.org/fact-tank/2020/09/21/americans-give-the-u-s-low-marks-for-its-handling-of-covid-19-and-so-do-people-in-other-countries/

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Doubleday.

Grunig, J. E. (Ed.). (1992). *Excellence in public relations and communication management*. L. Erlbaum Associates.

Grunig, J. E. (2000). Collectivism, collaboration, and societal corporatism as core professional values in public relations. *Journal of Public Relations Research*, *12*, 23–48. https://doi.org/10.1207/S1532754XJPRR1201_3

Grunig, J. E. (2006). Furnishing the edifice: Ongoing research on public relations as a strategic management function. *Journal of Public Relations Research*, *18*, 151–176. https://doi.org/10.1207/s1532754xjprr1802_5

Grunig, J. E. (2009). Paradigms of global public relations in an age of digitalisation. *PRism*, *6*(2), 1–19.

Grunig, J. E., & Grunig, L. A. (2000). Public relations in strategic management and strategic management of public relations: Theory and evidence from the IABC Excellence project. *Journalism Studies*, *1*, 303–321. https://doi.org/10.1080/14616700050028271

Grunig, J. E., & Huang, Y.-H. (2000). From organizational effectiveness to relationship indicators: Antecedents of relationships, public relations strategies, and relationship outcomes. In J. A. Ledingham & S. D. Bruning (Eds.), *Public relations as relationship management: A relational approach to the study and practice of public relations* (pp. 23–53). Routledge.

Hade, M. G., & Meisenbach, R. J. (2012). Higher learning: Rethinking crisis communication in response to racial incidents on campus. In D. Waymer (Ed.), *Culture, social class, and race in public relations: Perspectives and applications* (pp. 131–148). Lexington Books.

Hadnagy, C. (2018). *Social engineering: The science of human hacking*. Wiley.

Hallahan, K., Holtzhausen, D., van Ruler, B., Verčič, D., & Sriramesh, K. (2007). Defining Strategic Communication. *International Journal of Strategic Communication*, *1*(1), 3–35. https://doi.org/10.1080/15531180701285244

Hamburg, I., & Grosch, K. R. (2018). Aligning a cybersecurity strategy with communication management in organizations. In B. Peña-Acuña (Ed.),

Digital Communication Management. InTech. https://doi.org/10.5772/intechopen.75952

Heath, R. L. (2006). Onward into more fog: Thoughts on public relations' research directions. *Journal of Public Relations Research*, *18*, 93–114. https://doi.org/10.1207/s1532754xjprr1802_2

Heath, R. L. (2013a). Network theory. In R. Heath (Ed.), *Encyclopedia of public relations* (Vol. 2, pp. 603–605). SAGE Publications, Inc. https://doi.org/10.4135/9781452276236

Heath, R. L. (2013b). The journey to understand and champion OPR takes many roads, some not yet well traveled. *Public Relations Review*, *39*(5), 426–431. https://doi.org/10.1016/j.pubrev.2013.05.002

Heath, R. L., & Palenchar, M. J. (2008). *Strategic issues management: Organizations and public policy challenges*. Sage Publications.

Heath, R. L., Waymer, D., & Palenchar, M. J. (2013). Is the universe of democracy, rhetoric, and public relations whole cloth or three separate galaxies? *Public Relations Review*, *39*, 271–279. https://doi.org/10.1016/j.pubrev.2013.07.017

Heck, S., Campos, H., Barker, I., Okello, J. J., Baral, A., Boy, E., Brown, L., & Birol, E. (2020). Resilient agri-food systems for nutrition amidst COVID-19: Evidence and lessons from food-based approaches to overcome micronutrient deficiency and rebuild livelihoods after crises. *Food Security*, *12*, 823–830. https://doi.org/10.1007/s12571-020-01067-2

Hesse-Biber, S. N. (2017). *The practice of qualitative research: Engaging students in the research process*. SAGE.

Hughes, T. P. (1983). *Networks of power: Electrification in Western society, 1880-1930*. Johns Hopkins University Press.

Hughes, T. P. (2012). The evolution of large technical systems. In W. E. Bijker, T. P. Hughes, & T. Pinch (Eds.), *The social construction of technological systems: New directions in the sociology and history of technology* (pp. 45–47). MIT Press.

International Energy Agency. (2020). *COVID-19: An unprecedented global health and economic crisis*. IEA. https://www.iea.org/topics/covid-19

Jaques, T. (2006). Activist "rules" and the convergence with issue management. *Journal of Communication Management*, *10*, 407–420. https://doi.org/10.1108/13632540610714836

Jaques, T. (2007). Issue management and crisis management: An integrated, non-linear, relational construct. *Public Relations Review*, *33*, 147–157. https://doi.org/10.1016/j.pubrev.2007.02.001

Jaques, T. (2010). Embedding issue management: From process to policy. In R. L. Heath (Ed.), *The SAGE handbook of public relations* (pp. 435–446). SAGE Publications.

Jaques, T. (2012). Is issue management evolving or progressing towards extinction? *Public Communications Review*, *2*, 35–44.

Jones, B.L., & Chase, W.H. (1979). Managing public policy issues. *Public Relations Review*, 2, 3–23.

Jupp, V. (2006). Constant comparative method. In *The SAGE dictionary of social research methods*. SAGE Publications, Ltd. https://doi.org/10.4135/9780857020116.n28

Kaiser Family Foundation. (2020, October 29). *State data and policy actions to address coronavirus*. KFF. https://www.kff.org/coronavirus-covid-19/issue-brief/state-data-and-policy-actions-to-address-coronavirus/

Kavanaugh, C. (2019, September 11). *How utilities can prepare for the next wave of IT/OT integration*. TRC. https://www.trccompanies.com/insights/how-utilities-prepare-it-ot-integration/

Kent, M. L., & Saffer, A. J. (2014). A Delphi study of the future of new technology research in public relations. *Public Relations Review*, *40*, 568–576. https://doi.org/10.1016/j.pubrev.2014.02.008

Kent, Michael L., Taylor, M., & Veil, S. (2011). Issues management makeover: A facelift for an aging theory. In M. Goralski, H. P. Leblanc III, & M. Adams (Eds.), *Business research yearbook: Balancing profitability and sustainability: Shaping the future of business, 18* (pp. 534–541). International Academy of Business Disciplines.

Kerr, D., & Glantz, N. (2020). Diabetes, like COVID-19, is a wicked problem. *The Lancet Diabetes & Endocrinology*, *8*, 873–874. https://doi.org/10.1016/S2213-8587(20)30312-0

KETV. (2018, September 19). Cyber attack paralyzes Beatrice's network. In *NewsWatch 7*. KETV. https://www.youtube.com/watch?v=3yCgDyf8ncE

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). *Ten deadly cyber security threats amid COVID-19 pandemic* [Preprint]. https://doi.org/10.36227/techrxiv.12278792.v1

Kim, I., & Dutta, M. J. (2009). Studying crisis communication from the subaltern studies framework: Grassroots activism in the wake of hurricane Katrina. *Journal of Public Relations Research*, *21*, 142–164. https://doi.org/10.1080/10627260802557423

Kim, N., & Lee, S. (2018). Cybersecurity breach and crisis response: An analysis of organizations' official statements in the United States and South Korea. *International Journal of Business Communication*, 1– 22. https://doi.org/10.1177/2329488418777037

Knowles, J. (2020, September 18). 3 tough challenges PR pros are facing amid COVID-19 uncertainty. *PR Daily*. https://www.prdaily.com/3-tough-challenges-pr-pros-are-face-amid-covid-19-uncertainty/

Kuehn, A., & Mueller, M. (2014). Einstein on the breach: Surveillance technology, cybersecurity, and organizational change. In G. Giacomello (Ed.), *Security in cyberspace: Targeting nations, infrastructures, individuals* (pp. 127–160). Bloomsbury.

Levitt, E. B. (2020, May 26). The challenges for health care communicators as a new normal emerges from the COVID-19 crisis. *PRsay*. http://prsay.prsa.org/2020/05/26/the-challenges-for-health-care-communicators-as-a-new-normal-emerges-from-the-covid-19-crisis/

Lewison, G. (2008). The reporting of the risks from severe acute respiratory syndrome (SARS) in the news media, 2003–2004. *Health, Risk & Society*, *10*, 241–262. https://doi.org/10.1080/13698570802160962

Madden, K. (2012, May). *Lewinian theory: A guiding force for hostile media effects*. Annual meeting of the International Communication Association, Phoenix, AZ.

Madden, S. (2019). The issue with issues management: Considering the emotional and gendered core of issues. *Public Relations Inquiry*, *8*, 299–317. https://doi.org/10.1177/2046147X19872240

Malone, E. F., & Malone, M. J. (2013). The "wicked problem" of cybersecurity policy: Analysis of United States and Canadian policy response. *Canadian Foreign Policy Journal*, *19*, 158–177. https://doi.org/10.1080/11926422.2013.805152

Mattioli, R. (2014). The state(s) of cybersecurity. In G. Giacomello (Ed.), *Security in cyberspace: Targeting nations, infrastructures, individuals* (pp. 23–38). Bloomsbury.

May, R. (2017, September 28). *Your human firewall: The answer to the cyber security problem*. https://www.youtube.com/watch?v=BpdcVfq2dB8

McCown, N. (2007). The role of public relations with internal activists. *Journal of Public Relations Research*, *19*, 47–68. https://doi.org/10.1080/10627260709336595

Melaku, T., Assefa, D., Bayisa, B., & Legese, N. (2020). Research and intervention priorities for mental health of people living with chronic

disease(s) in the midst of the COVID-19 pandemic in low resource settings: A commentary. *Annals of Medicine and Surgery*, *57*, 268–269. https://doi.org/10.1016/j.amsu.2020.07.051

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook*. SAGE Publications, Inc.

Moon, M. J. (2020). Fighting COVID-19 with agility, transparency, and participation: Wicked policy problems and new governance challenges. *Public Administration Review*, *80*, 651–656. https://doi.org/10.1111/puar.13214

Muncaster, P. (2020, September 23). *Most workers not interested in switching to a cybersecurity role*. Infosecurity Magazine. https://www.infosecurity-magazine.com:443/news/most-not-interested-switching/

Muzzatti, S. L. (2005). Bits of falling sky and global pandemics: Moral panic and Severe Acute Respiratory Syndrome (SARS). *Illness, Crisis & Loss*, *13*, 117–128. https://doi.org/10.1177/105413730501300203

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*, 306–321. https://doi.org/10.1080/0960085X.2020.1771222

National Association of Regulatory Utility Commissioners. (2021, September 9). *Map of disconnection moratoria*. COVID-19 News & Resources. Retrieved March 22, 2022, from https://www.naruc.org/compilation-of-covid-19-news-resources/map-of-disconnection-moratoria/

Nicola, M., Alsafi, Z., Sohrabi, C., Kerwan, A., Al-Jabir, A., Iosifidis, C., Agha, M., & Agha, R. (2020). The socio-economic implications of the coronavirus pandemic (COVID-19): A review. *International Journal of Surgery (London, England)*, *78*, 185–193. https://doi.org/10.1016/j.ijsu.2020.04.018

Nutt, P. C., & Backoff, R. W. (1992). *Strategic management of public and third sector organizations: A handbook for leaders* (1st ed). Jossey-Bass Publishers.

Ozimek, A. (2020). The Future of Remote Work. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3638597

Pandemic Response Accountability Committee. (2020). *Top challenges facing federal agencies: COVID-19 emergency relief and response efforts*. Offices of the Inspector General.

Parks, L., & Starosielski, N. (2015). Introduction. In L. Parks & N. Starosielski (Eds.), *Signal traffic: Critical studies of media infrastructures* (pp. 1–27). University of Illinois Press.

Peters, B. G. (2017). What is so wicked about wicked problems? A conceptual analysis and a research program. *Policy and Society*, *36*, 385–396. https://doi.org/10.1080/14494035.2017.1361633

Pfister, D. S. (2018). Public sphere(s), publics, and counterpublics. In *Oxford research encyclopedia of communication*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228613.013.562

Place, K. R. (2010). A qualitative examination of public relations practitioner ethical decision making and the deontological theory of ethical issues management. *Journal of Mass Media Ethics*, *25*, 226–245. https://doi.org/10.1080/08900523.2010.497405

Plyler, K. (2020, January 22). *Effective communication mitigates risk in a cybersecurity world*. Forbes. https://www.forbes.com/sites/forbesagencycouncil/2020/01/21/effective-communication-mitigates-risk-in-a-cybersecurity-world/

Rains, S. A. (2008). Health at high speed: Broadband internet access, health communication, and the digital divide. *Communication Research*, *35*, 283–297. https://doi.org/10.1177/0093650208315958

Ramsey, P. (2016). The public sphere and PR: Deliberative democracy and agonistic pluralism. In J. L'Etang, D. McKie, N. Snow, & J. Xifra (Eds.), *The Routledge handbook of critical public relations* (pp. 186–199). Routledge.

Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, *4*, 155–169. https://doi.org/10.1007/BF01405730

Roper, J., & Hurst, B. (2019). Public relations, futures planning and political talk for addressing wicked problems. *Public Relations Review*, *45*, 101828. https://doi.org/10.1016/j.pubrev.2019.101828

Roulston, K. (2010). Considering quality in qualitative interviewing. *Qualitative Research*, *10*, 199–228. https://doi.org/10.1177/1468794109356739

Roulston, K. (2014). Interactional problems in research interviews. *Qualitative Research*, *14*, 277–293.

Sahin, O., Salim, H., Suprun, E., Richards, R., MacAskill, S., Heilgeist, S., Rutherford, S., Stewart, R. A., & Beal, C. D. (2020). Developing a preliminary causal loop diagram for understanding the wicked complexity of the COVID-19 pandemic. *Systems*, *8*, 20. https://doi.org/10.3390/systems8020020

Seymour, K., Skatebol, J., & Pook, B. (2020). Compounding education disengagement: COVID-19 lockdown, the digital divide and wrap-around services. *Journal of Children's Services*. https://doi.org/10.1108/JCS-08-2020-0049

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Smith, M. F., & Ferguson, D. P. (2010). Activism 2.0. In R. L. Heath (Ed.), *The SAGE handbook of public relations* (pp. 395–407). SAGE Publications.

Smith, M. F., & Ferguson, D. P. (2013). "Fracking democracy": Issue management and locus of policy decision-making in the Marcellus Shale gas drilling debate. *Public Relations Review*, *39*, 377–386. https://doi.org/10.1016/j.pubrev.2013.08.003

Smith, R. D. (2006). Responding to global infectious disease outbreaks: Lessons from SARS on the role of risk perception, communication and management. *Social Science & Medicine*, *63*, 3113–3123. https://doi.org/10.1016/j.socscimed.2006.08.004

Sommerfeldt, E. J. (2013). The civility of social capital: Public relations in the public sphere, civil society, and democracy. *Public Relations Review*, *39*, 280–289. https://doi.org/10.1016/j.pubrev.2012.12.004

Sommerfeldt, E. J., & Kent, M. L. (2015). Civil society, networks, and relationship management: Beyond the organization–public dyad. *International Journal of Strategic Communication*, *9*, 235–252. https://doi.org/10.1080/1553118X.2015.1025405

Sommerfeldt, E. J., Kent, M. L., & Taylor, M. (2012). Activist practitioner perspectives of website public relations: Why aren't activist websites fulfilling the dialogic promise? *Public Relations Review*, *38*, 303–312. https://doi.org/10.1016/j.pubrev.2012.01.001

Sommerfeldt, E. J., & Xu, S. (2014). Legitimation strategies in radical activist issues management. In R. D. Waters (Ed.), *Public relations in the nonprofit sector: Theory and practice* (pp. 185–202). Routledge.

Sommerfeldt, E. J., & Yang, A. (2017). Relationship networks as strategic issues management: An issue-stage framework of social movement organization network strategies. *Public Relations Review*, *43*, 829–839. https://doi.org/10.1016/j.pubrev.2017.06.012

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research*, *7*, 111–134.

Steele, C. K. (2016). The digital barbershop: Blogs and online oral culture within the African American community. *Social Media + Society*, *2*, 1–10. https://doi.org/10.1177/2056305116683205

Strong, F. (2020, June 27). Public relations and COVID-19: Studies surface challenges, changes and optimism. *Sword and the Script*. https://www.swordandthescript.com/2020/06/public-relations-covid-19/

Taylor, M. (2011). Building social capital through rhetoric and public relations. *Management Communication Quarterly*, *25*, 436–454. https://doi.org/10.1177/0893318911410286

Toledano, M. (2016). Advocating for reconciliation: Public relations, activism, advocacy and dialogue. *Public Relations Inquiry*, *5*, 277–294. https://doi.org/10.1177/2046147X16666595

Toth, E. L. (2002). Postmodernism for modernist public relations: The cash value and application of critical research in public relations. *Public Relations Review, 28*, 243–250. https://doi.org/10.1016/S0363-8111(02)00130-3

Tracy, S. J. (2013). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact*. Wiley-Blackwell.

U.S. Department of Energy. (2018). *Smart grid system report* (p. 93). U.S. Department of Energy.

U.S. Department of Energy. (2020, September 19). *Learn more about interconnections*. Energy.Gov. https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/transmission-planning/recovery-act-0

Vardeman-Winter, J. (2016). “Critical public relations is so critical!” Objections, counter-objections, and practical applications to critical-cultural public relations work. In J. L’Etang & D. McKie (Eds.), *The Routledge handbook of critical public relations* (pp. 186–199). Routledge.

Vardeman-Winter, J., Tindall, N., & Jiang, H. (2013). Intersectionality and publics: How exploring publics’ multiple identities questions basic public relations concepts. *Public Relations Inquiry*, *2*, 279–304. https://doi.org/10.1177/2046147X13491564

Veil, S. R., Reno, J., Freihaut, R., & Oldham, J. (2015). Online activists vs. Kraft foods: A case of social media hijacking. *Public Relations Review*, *41*, 103–108. https://doi.org/10.1016/j.pubrev.2014.11.017

Wang, P., & Park, S.-A. (2017). *Communication in cybersecurity: A public communication model for business data breach incident handling*. *18*, 12.

Waymer, D., & Heath, R. L. (2016). Critical race and public relations: The case for environmental racism and risk bearer agency. In J. L’Etang & D. McKie (Eds.), *The Routledge handbook of critical public relations* (pp. 142–150). Routledge.

Weaver, C. K., Motion, J., & Roper, J. (2006). From propaganda to discourse (and back again): Truth, power, the public interest, and public relations. In J. L’Etang, & M. Pieczka (Eds.), *Public relations: Critical Debates and contemporary practice* (pp. 1–21). Lawrence Erlbaum Associates.

Welch, D. (2013). *Propaganda: Power and Persuasion*. London: I.B. Tauris & Co., Ltd.

Williams, G. T., & Sommerfeldt, E. J. (2021). Social advocacy and public relations: Building communitas in the public sphere. In C. Valentini (Ed.), *Public Relations* (pp. 233–248). De Gruyter. https://doi.org/10.1515/9783110554250

Willis, P. (2016). From humble inquiry to humble intelligence: Confronting wicked problems and augmenting public relations. *Public Relations Review*, *42*, 306–313. https://doi.org/10.1016/j.pubrev.2015.05.007

Willis, P., Tench, R., & Devins, D. (2018). Deliberative engagement and wicked problems: From good intentions to practical action. In K. A. Johnston & M. Taylor (Eds.), *The handbook of communication engagement* (pp. 383–396). Wiley Blackwell.

Wu, D., & Yang, A. (2017). China's public diplomatic networks on the Ebola issue in West Africa: Issues management in a network society. *Public Relations Review*, *43*, 345–357. https://doi.org/10.1016/j.pubrev.2017.02.013

Yang, A., & Taylor, M. (2015). Looking over, looking out, and moving forward: Positioning public relations in theorizing organizational network ecologies: Positioning public relations in theorizing organizational network ecologies. *Communication Theory*, *25*, 91–115. https://doi.org/10.1111/comt.12049

Yin, R. K. (2018). *Case study research and applications: Design and methods* (Sixth edition). SAGE.

Zimmerman, T. (2014, February 2). *Achieving IT-OT integration*. POWERGrid International. https://www.power-grid.com/2014/02/26/achieving-it-ot-integration/

Appendix A: IRB Approval Forms

UNIVERSITY OF MARYLAND
INSTITUTIONAL REVIEW BOARD

1204 Marie Mount Hall
College Park, MD 20742-5125
TEL 301.405.4212
FAX 301.314.1475
irb@umd.edu
www.umresearch.umd.edu/IRB

DATE:	January 12, 2022
TO:	Gareth Williams, MA
FROM:	University of Maryland College Park (UMCP) IRB
PROJECT TITLE:	[1706820-3] Issues Management of Compounding Wicked Problems: Cybersecurity and COVID-19
SUBMISSION TYPE:	Continuing Review/Progress Report
ACTION:	APPROVED
APPROVAL DATE:	January 12, 2022
REVIEW TYPE:	Expedited Review
REVIEW CATEGORY:	Expedited review category #7.

Thank you for your submission of Continuing Review/Progress Report materials for this project. The University of Maryland College Park (UMCP) IRB has APPROVED your submission. This approval is based on an appropriate risk/benefit ratio and a project design wherein the risks have been minimized. All research must be conducted in accordance with this approved submission.

Prior to final approval of this project scientific review was completed by the IRB Member reviewer.

This submission has received Expedited Review based on the applicable federal regulations.

This project has been determined to be a MINIMAL RISK project.

Please remember that informed consent is a process beginning with a description of the project and insurance of participant understanding followed by a signed consent form. Informed consent must continue throughout the project via a dialogue between the researcher and research participant. Unless a consent waiver or alteration has been approved, Federal regulations require that each participant receives a copy of the consent document.

Please note that any revision to previously approved materials must be approved by this committee prior to initiation. Please use the appropriate Amendment forms for this procedure.

All UNANTICIPATED PROBLEMS involving risks to subjects or others (UPIRSOs) and SERIOUS and UNEXPECTED adverse events must be reported promptly to this office. Please use the appropriate reporting forms for this procedure. All FDA and sponsor reporting requirements should also be followed. All NON-COMPLIANCE issues or COMPLAINTS regarding this project must be reported promptly to this office.

Please note that all research records must be retained for a minimum of seven years after the completion of the project.

If you have any questions, please contact the IRB Office at 301-405-4212 or irb@umd.edu. Please include your project title and reference number in all correspondence with this committee.

This letter has been electronically signed in accordance with all applicable regulations, and a copy is retained within University of Maryland College Park (UMCP) IRB's records.

Appendix B: Recruitment Letters

The first letter was used during the initial phase of the project and successfully recruited the "influencer" organizations, the two JAAs, and Co-op 16-p. The forward emphasis on cybersecurity repelled many potential co-op participants, and so the second letter was developed and approved by the IRB, emphasizing the inquiry on the COVID-19 dynamic while still acknowledging interest in cybersecurity and how it complicated utility responses to the pandemic.

Original Letter

COLLEGE OF
ARTS & HUMANITIES
COMMUNICATION

2130 Skinner Building
College Park, Maryland 20742-7635
301.405.8979 TEL 301.314.9471 FAX
www.comm.umd.edu

March 10, 2021

Hello:

I write to ask you to participate in a study of how cybersecurity challenges facing electric utilities have been managed during the COVID-19 pandemic. Cybersecurity and COVID-19 are critical concerns for public utilities, and this study seeks to improve understanding of how management personnel at utilities, government agencies, and industry associations iterate the legitimacy of their arguments among dynamics of political and social power in addressing these issues.

I am asking for no more than one hour of your time for a semi-structured interview to discuss your experience identifying challenges at the nexus of cybersecurity and the COVID-19 pandemic as they impact public utilities and the U.S. electricity distribution infrastructure. To ensure accuracy of data and enable subsequent review and verification, I would like to record each interview. If this presents a concern, we can discuss alternate measures that I can take to preserve the content. I will ensure information security and meet needs and concerns you might have regarding anonymization of data.

I am a doctoral candidate in the Department of Communication at the University of Maryland (https://www.comm.umd.edu/people/graduate-students/williams; https://www.linkedin.com/in/gareth-williams-1838951/). My research and teaching both focus on strategic communication and public relations, and the tools and techniques used by organizations—particularly public sector organizations. In my professional work, I have supported clients at the U.S. Department of Energy, U.S. Department of Homeland Security, and the American Public Power Association and its member associations, among other organizations dedicated to power generation and distribution.

This project has been approved by the University of Maryland Institutional Review Board (https://research.umd.edu/about/contact; ref # 1706820-1) and is conducted under the supervision of Dr. Erich Sommerfeldt, Assistant Professor in the Department of Communication. If you have any questions about this research, you can contact Dr. Sommerfeldt at esommerf@umd.edu.

Thank you for your time and consideration; I welcome any questions that you might have.

Sincerely,

Gareth T. Williams
Doctoral Candidate
Department of Communication
The University of Maryland

A CENTURY OF ACHIEVEMENT
DEPARTMENT OF COMMUNICATION, 1901-2001

Revised Letter

COLLEGE OF
ARTS & HUMANITIES
COMMUNICATION

2130 Skinner Building
College Park, Maryland 20742-7635
301.405.8979 TEL 301.314.9471 FAX
www.comm.umd.edu

July 8, 2021

Hello:

I write to ask you to participate in a study of how electric utilities have communicated with customers and government agencies about shifts in operations and other adaptations to the COVID-19 pandemic (e.g., changes in in-person services, policy changes at state and utility levels, and reducing on-site staff while maintaining cybersecurity). COVID-19 has affected all facets of American society, including public utilities, and this study seeks to improve understanding of how utilities, government agencies, and industry associations justify their perspectives and arguments among peer organizations and with utility customers.

I am asking for no more than one hour of your time for a semi-structured interview to discuss your experience identifying challenges of the COVID-19 pandemic as they impact public utilities and the U.S. electricity distribution infrastructure. To ensure accuracy of data and enable subsequent review and verification, I would like to record each interview. If this is a concern, we can discuss alternate measures that I can take to preserve the content. I will ensure information security and meet needs and concerns you might have regarding anonymization of data.

I am a doctoral candidate in the Department of Communication at the University of Maryland (https://www.comm.umd.edu/people/graduate-students/williams; https://www.linkedin.com/in/gareth-williams-1838951/). My research and teaching both focus on the strategic communication tools and techniques used by public sector organizations. In my professional work, I have supported clients at the U.S. Department of Energy, U.S. Department of Homeland Security, and the American Public Power Association and its member associations, among other organizations dedicated to power generation and distribution.

This project has been approved by the University of Maryland Institutional Review Board (https://research.umd.edu/about/contact; ref # 1706820-1) and is conducted under the supervision of Dr. Erich Sommerfeldt, Assistant Professor in the Department of Communication. If you have any questions about this research, you can contact Dr. Sommerfeldt at esommerf@umd.edu.

Thank you for your time and consideration; I welcome any questions that you might have.

Sincerely,

Gareth T. Williams
Doctoral Candidate
Department of Communication
The University of Maryland

Appendix C: Consent Forms

The first form was used during the initial phase of the project and successfully recruited the "influencer" organizations, the two JAAs, and Co-op 16-p. The second form was developed after multiple utilities declined to participate due to the emphasis on cybersecurity, misunderstanding that the focus of the study rested on communications about the issues and did not seek to identify specific tools and solutions used by the utilities. Both forms were reviewed and approved by the University of Maryland IRB.

Original Form

Institutional Review Board
1204 Marie Mount Hall • 7814 Regents Drive • College Park, MD 20742 • 301-405-4212 • irb@umd.edu

Initials: _____ Date: _____

CONSENT TO PARTICIPATE

Project Title	*Issues Management of Compounding Wicked Problems*
Purpose of the Study	*This research is being conducted by **Gareth Thomas Williams** at the University of Maryland, College Park. We are inviting you to participate in this research project because you are involved in operational and/or information security at a public power utility or work with public power utilities. The purpose of this study is to examine how information and operations security managers communicate about changing needs and priorities during the COVID-19 pandemic.*
Procedures	*The procedures involve an interview lasting approximately 60 minutes. Interviews will be audio-recorded. If you do not agree to be recorded, the Principal Investigator will transcribe the conversation in hand-written notes. Questions may include the following:* • *What aspect of public power distribution does your position address?* • *How do you distinguish technical and social challenges in cybersecurity?* • *In what ways has the COVID-19 pandemic complicated ensuring operational and informational security?* • *In what way do cybersecurity practices impede adapting to COVID-19 best practices for work environments?* • *How has your organization strategically prioritized problems and needs arising from the confluence of cybersecurity and the COVID-19 pandemic?* • *With what other organizations do you communicate and collaborate on responses to COVID-19 and cybersecurity?* • *With what organizations do you have a mutual aid or collaborative relationship? What organizations have a strong influence on your organization's operations? What groups do you seek to persuade of the value of your organization's strategy?* • *What is the most important lesson we need to learn from these incidents?*

Initials: _____ Date: _____

Potential Risks and Discomforts	*Because you may be recorded in the interview, this project may present some risks. These risks would be minimized by ensuring anonymity. To ensure anonymity, recordings will be named in a way that mask your real identity and I will assign you a pseudonym while I am analyzing your data. The identity markers such as your specific organization, department, background, and technical tools and procedures will be removed unless you indicate otherwise. Your identity will remain unknown to other participants. You can decline to answer any specific question or to end your participation at any time without penalty. The consent form will be preserved in hard copy and securely stored in the investigator's home office.*
Potential Benefits	*No direct benefit (i.e., compensation) is provided for your participation. Indirect benefits will come in form of improved understanding of communication and strategic management of public power. The study should provide insights to improve how organizations can improve engagement with stakeholders and coordination with peer institutions.*
Confidentiality	*Any potential loss of confidentiality will be minimized by assigning you with a pseudonym to protect your identity and by removing any identity markers. Data will be securely stored on the Principal Investigator home office computer. Computer, hard drives, and USB drives will be password-protected. Only the Principal Investigator (Gareth Williams) and the Project Advisor (Dr. Erich Sommerfeldt) will have access to the data. Your information may be shared with representatives of the University of Maryland, College Park or governmental authorities if you or someone else is in danger or if we are required to do so by law.*
Compensation	*No compensation is offered participants.*
Right to Withdraw and Questions	*Your participation in this research is completely voluntary. You may choose not to take part at all. If you decide to participate in this research, you may stop participating at any time. If you decide not to participate in this study or if you stop participating at any time, you will not be penalized or lose any benefits to which you otherwise qualify.* *If you decide to stop taking part in the study, if you have questions, concerns, or complaints, or if you need to report an injury related to the research, please contact the investigator:* ***Gareth Thomas Williams*** ***2100 Skinner Hall*** ***University of Maryland*** ***gtw1@umd.edu*** ***443-413-8251***

Initials: _____ Date: _____

Participant Rights	*If you have questions about your rights as a research participant or wish to report a research-related injury, please contact:* University of Maryland College Park Institutional Review Board Office 1204 Marie Mount Hall College Park, Maryland, 20742 E-mail: irb@umd.edu Telephone: 301-405-0678 *This research has been reviewed according to the University of Maryland, College Park IRB procedures for research involving human subjects.*	
Statement of Consent	*Your signature indicates that you are at least 18 years of age; you have read this consent form or have had it read to you; your questions have been answered to your satisfaction and you voluntarily agree to participate in this research study. You will receive a copy of this signed consent form.* *If you agree to participate, please sign your name below.*	
Signature and Date	**NAME OF PARTICIPANT** **[Please Print]**	
	SIGNATURE OF PARTICIPANT	
	DATE	

Revised Form

Initials: _____ Date: _____

Institutional Review Board
1204 Marie Mount Hall • 7814 Regents Drive • College Park, MD 20742 • 301-405-4212 • irb@umd.edu

CONSENT TO PARTICIPATE

Project Title	*Issues Management of Compounding Wicked Problems*
Purpose of the Study	*This research is being conducted by **Gareth Thomas Williams** at the University of Maryland, College Park. We are inviting you to participate in this research project because you are involved in organizational communications at a public power utility or work with public power utilities. The purpose of this study is to examine how communications managers communicate about changing needs and priorities during the COVID-19 pandemic.*
Procedures	*The procedures involve an interview lasting approximately 60 minutes. Interviews will be audio-recorded. If you do not agree to be recorded, the Principal Investigator will transcribe the conversation in hand-written notes. Questions may include the following:* • *What aspect of public power distribution does your position address?* • *In what ways has the COVID-19 pandemic complicated policies, operations, and customer engagement?* • *In what way do utility practices impede adapting to COVID-19 best practices for work environments?* • *With what other organizations do you communicate and collaborate on responses to COVID-19?* • *With what organizations do you have a mutual aid or collaborative relationship? What organizations have a strong influence on your organization's operations? What groups do you seek to persuade of the value of your organization's strategy?* • *What is the most important lesson we need to learn from the past couple years?*
Potential Risks and Discomforts	*Because you may be recorded in the interview, this project may present some risks. These risks will be minimized by ensuring anonymity. To ensure anonymity, recordings will be named in a way that mask your real identity and I will assign you a pseudonym while I am analyzing your data. The identity markers such as your specific organization, department, background, and technical tools and procedures will be removed unless you indicate otherwise. Your identity will remain unknown to other participants. You can decline to answer any specific question or to end your participation at any time without penalty. The consent form will be preserved in hard copy and securely stored in the investigator's home office.*

Initials: _____ *Date:* _____

Potential Benefits	*No direct benefit (i.e., compensation) is provided for your participation. Indirect benefits will come in form of improved understanding of communication and strategic management of public power. The study should provide insights to improve how organizations can improve engagement with stakeholders and coordination with peer institutions.*
Confidentiality	*Any potential loss of confidentiality will be minimized by assigning you with a pseudonym to protect your identity and by removing any identity markers. Data will be securely stored on the Principal Investigator home office computer. Computer, hard drives, and USB drives are password-protected. Only the Principal Investigator (Gareth Williams) and the Project Advisor (Dr. Erich Sommerfeldt) will have access to the data. Your information may only be shared with representatives of the University of Maryland, College Park or governmental authorities if you or someone else is in danger or if we are required to do so by law.*
Compensation	*No compensation is offered participants.*
Right to Withdraw and Questions	*Your participation in this research is completely voluntary. You may choose not to take part at all. If you decide to participate in this research, you may stop participating at any time. If you decide not to participate in this study or if you stop participating at any time, you will not be penalized or lose any benefits to which you otherwise qualify.* *If you decide to stop taking part in the study, if you have questions, concerns, or complaints, or if you need to report an injury related to the research, please contact the investigator:* ***Gareth Thomas Williams*** ***2100 Skinner Hall*** ***University of Maryland*** ***gtw1@umd.edu*** ***443-413-8251***
Participant Rights	*If you have questions about your rights as a research participant or wish to report a research-related injury, please contact:* University of Maryland College Park Institutional Review Board Office 1204 Marie Mount Hall College Park, Maryland, 20742 E-mail: irb@umd.edu Telephone: 301-405-0678 *This research has been reviewed according to the University of Maryland, College Park IRB procedures for research involving human subjects.*

Initials: _____ Date: _____

Statement of Consent	*Your signature indicates that you are at least 18 years of age; you have read this consent form or have had it read to you; your questions have been answered to your satisfaction and you voluntarily agree to participate in this research study. You will receive a copy of this signed consent form.* *If you agree to participate, please sign your name below.*	
Signature and Date	**NAME OF PARTICIPANT** [Please Print]	
	SIGNATURE OF PARTICIPANT	
	DATE	

Appendix D: Interview Protocols

Original Protocol

First, I'd like to ask some questions about how your organization ***defines and communicates about cybersecurity and challenges of the COVID-19 pandemic: (RQ1)***

- How does your organization monitor and address cybersecurity needs for public power?
    - With what peers do you communicate about cybersecurity issues with public power utilities?
    - With what other organizations do you communicate about cybersecurity issues with public power utilities?
- What cybersecurity challenges impact utilities?
    - What is the biggest inhibitor of effective cybersecurity for public utilities?
    - What role has your organization played or what steps has your organization taken to help public utilities address cybersecurity?
- What challenges of COVID-19 impact utilities?
    - What role has your organization played or what steps has your organization taken to help public utilities address COVID-19?
    - What new challenges does COVID-19 pose?
- In what way do cybersecurity practices impede adapting to COVID-19 best practices?
    - What has been the most surprising challenge in maintaining cybersecurity during the COVID-19 pandemic?
    - What is the most important lesson we need to learn from maintaining cybersecurity during COVID-19?

Thank you. Next, I'd like to ask some questions about organizations you communicate with about priorities for public utilities, and ***how each party seeks to influence others (RQ2)****.*

- How does your organization seek to influence utilities' cybersecurity practices? (RQ2a)

    - How do you communicate about cybersecurity with [cited organization]?
    - How does your utility influence cybersecurity activities of [cited organizations]?

- What other organization has the most influence over your organization's definition of cybersecurity strategy—i.e., influence over or dictating policy? (RQ2b)
    - How do you communicate about cybersecurity with [cited organization]?
    - How does [cited organization] influence your utility's policy decisions?
- With what other organizations and publics do you collaborate to identify and address issues of adapting cybersecurity to COVID-19? (RQ2a, RQ2b)
    - How do you communicate about COVID-19 with [those organizations/publics]?
    - What organizations or publics have the most influence over public utility's COVID-19 strategy—i.e., influence over or dictating policy?

Thank you. Finally, I'd like to ask some questions about organizations you communicate with about priorities for public utilities, and ***how each party seeks to legitimize its perspective (RQ3)****.*

- With what other organizations do you communicate new practices or policies to adapt cybersecurity practices to COVID-19? (RQ3a)
    - How do you strategize communications to influence the activities or policies of [cited organizations or publics]?
    - How do you select media for [cited organizations or publics]?
    - How have you communicated about efforts to adapt cybersecurity practices to COVID-19 (e.g., org publications, blog posts, media)?
- What organizations or publics communicate with you about adapting cybersecurity to COVID-19? (RQ3b)
    - What organizations' or publics' communications does your organization perceive as most credible? Why?
    - What organizations' or publics' communications does your organization perceive as less credible? Why?

Thank you for your time. These insights are both helpful and valuable. I may be in touch if I need to clarify a point for a future report, though I again assure you that information gathered here will be used in a strictly anonymized manner.

Revised Protocol

First, I'd like to ask some questions about how your organization ***defines and communicates about challenges of the COVID-19 pandemic:***

- *What challenges have public utilities faced in adapting to COVID-19?*
    - *What new challenges has COVID-19 posed?*
    - *What conflicts have you experienced and how have you overcome them?*
    - *With what other organizations do you communicate about issues with challenging public power utilities?*
    - *What communications have you received in response to adaptations to COVID-19?*
    - *What are the challenges in getting people to appreciate the importance of these threats or to prepare for them?*
- *With what organizations and groups do you collaborate to identify and address issues of adapting services to COVID-19?*
    - *What organizations have the most influence over your utility's COVID-19 strategy—i.e., influence over or dictating policy?*
    - *How do you communicate about COVID-19 with [organizations/customers]?*
- *With what organizations and groups do you usually collaborate to identify and address changes to customer engagement and communication?*
    - *What organizations have the most influence over your utility's communications and/or policies?*
    - *How do you communicate with [organizations/customers]?*

Thank you. Next, I'd like to ask some questions about organizations you communicate with about priorities for public utilities, and ***how each party influences others (RQ2)****.*

- *Who in your organization is responsible for developing communications strategy?*
    - *With whom do they collaborate?*
    - *Who implements the communications strategy?*
- *What other organization has the most influence over your organization's policies—operation, etc.? (RQ2b)*
    - *How do you communicate about COVID-19 with [cited organization]?*
    - *How does [cited organization] influence your utility's policy decisions in adapting to COVID-19 strategy?*
- *How does your organization seek to influence other utilities' practices? (RQ2a)*
    - *How do you communicate \with [cited organization]?*
    - *How does your utility influence activities of [cited organizations]?*
    - *What has been the greatest challenge in helping utility personnel take necessary steps?*
- *What organization(s) seem to have the most influence over responses to issues of adapting cybersecurity to COVID-19? (RQ2a, RQ2b)*
    - *How does [that organization] influence your work?*
    - *How do you communicate with [that organization]?*

Thank you. Finally, I'd like to ask some questions about organizations you communicate with about priorities for public utilities, and ***how each party seeks to legitimize its perspective (RQ3)****.*

- *How do you address an audience skeptical of the need for a policy?*
    - *Have you had to overcome skepticism regarding utility communications or new policies?*
    - *How have you addressed internal/external skepticism about new policies or strategies?*

- *What communications have you received in response to adaptations to COVID-19?*

[Compounding Issues]

- *In what ways have adapting to COVID-19 best practices impeded cybersecurity practices?*
  - *How has your organization communicated with other organizations and utilities about the compounding issues of cybersecurity and COVID-19?*
  - *What communications have you received from other organizations about the challenges of maintaining cybersecurity at public utilities during COVID-19?*
  - *How have these challenges and communications with other organizations shifted your perspective on cybersecurity and/or adaptation to operation during a pandemic? How have you conveyed these changes in perspective to other organizations?*
  - *What has been the most surprising challenge in maintaining cybersecurity during the COVID-19 pandemic?*
- *With what other organizations do you communicate new practices or policies to adapt cybersecurity practices to COVID-19? (RQ3a)*
  - *How do you strategize communications to influence the activities or policies of [cited organizations or publics]?*
  - *How do you select media for [cited organizations or publics]?*
  - *How have you communicated about efforts to adapt cybersecurity practices to COVID-19 (e.g., org publications, blog posts, media)?*
  - *How do you convince audience of the credibility of your arguments?*
- *Which has made a greater impact on your perception of or communications about cybersecurity: adapting to the pandemic, or SolarWinds?*
  - *What do you think accounts for the difference?*
  - *What distinguishes the nature of these two influences?*

Thank you for your time. These insights are both helpful and valuable. I may be in touch if I need to clarify a point for a future report, though I again assure you that information gathered here will be used in a strictly anonymized manner.

Appendix E: Codebook

Codebook Developed During Review of Interview Transcripts

Code Category	Subcategories	Code Category	Subcategories
Advocacy		Persuasion	● External audience ● Internal audience
Challenges	● Broadband access ● Changing demographics ● Communication with members ● Compounding: Broadband/ COVID ● Compounding: Broadband/grid ● Compounding: COVID/ monetary or financial ● Compounding: Cybersecurity/ COVID ● COVID-19 ○ Action predating ○ Action responding to ● Cybersecurity ● Geography ● Monetary or financial ● Political ● Reliability ● Resilience ● Safety ● Supply chain	Power	● Access to information ● Customer agency ● Denial of service ● Monetary ● Political ● Regulation and requirement
		Role	● Collaboration ○ Cross-industry ○ Information sharing ○ Mutual Aid ● Co-op original role ● Customer communication ● Electric Industry (general) ● Information Sources ● Leadership ○ Education ○ Peer groups ○ Subsidiary groups ● Within State
Co-op attributes		Threats	● Cyber ● Physical ● Political ● Reputation
Legitimacy	● Community commitment ● CSR ● Cybersecurity ● Intelligence source ● Safety ● Threat of COVID-19		