2023-03

WILLINGNESS TO PARTNER IN PUBLIC-PRIVATE PARTNERSHIP FOR CYBERSECURITY OF CRITICAL INFRASTRUCTURE

Esquibel, Judy M.

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/71999

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DISSERTATION

WILLINGNESS TO PARTNER IN PUBLIC-PRIVATE PARTNERSHIP FOR CYBERSECURITY OF CRITICAL INFRASTRUCTURE

by

Judy M. Esquibel

March 2023

Dissertation Supervisor: Kathryn J. Aten

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2023	**3. REPORT TYPE AND DATES COVERED** Dissertation

4. TITLE AND SUBTITLE WILLINGNESS TO PARTNER IN PUBLIC-PRIVATE PARTNERSHIP FOR CYBERSECURITY OF CRITICAL INFRASTRUCTURE	**5. FUNDING NUMBERS**
6. AUTHOR(S) Judy M. Esquibel	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Public-private partnerships (PPPs) are crucial for securing critical infrastructure (CI) against cyber-attacks, yet little is known about how public and private organizations develop willingness to partner for CI cybersecurity. This research addressed this gap through a qualitative, multiple-case analysis of four PPPs related to cybersecurity, each involving two organizations and an additional, follow-up PPP. The research developed a process model that challenges the conventional view of willingness as fixed or static and proposes a new perspective that captures the process of constructing willingness. The research highlights the usefulness of activity theory in exploring this concept and presents the process model that describes this new understanding of willingness. Constructing willingness to partner is an activity path commencing with a catalyst that prompts relational partnering activities and generates partnering frames of emulation, insight, and connection, along with emerging commitments. These commitments generate intangible partnering resources including competence, reputation, and social capital, which support the construction of willingness to partner. The activity path comprises three subprocesses: initiating interaction, generating commitment, and legitimizing partnering. This research enhances the literature on PPPs and CI cybersecurity by offering a detailed description of how public and private organizations construct willingness to partner.

14. SUBJECT TERMS public-private partnerships, willingness, cybersecurity, critical infrastructure	**15. NUMBER OF PAGES** 115
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

WILLINGNESS TO PARTNER IN PUBLIC-PRIVATE PARTNERSHIP FOR CYBERSECURITY OF CRITICAL INFRASTRUCTURE

Judy M. Esquibel
Chief Warrant Officer Four, United States Army
BS, Hawai'i Pacific University, 2005
MS, Hawai'i Pacific University, 2010

Submitted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY IN INFORMATION SCIENCES

from the

NAVAL POSTGRADUATE SCHOOL
March 2023

Approved by: Kathryn J. Aten
Departments of
Defense Management,
Information Sciences
Dissertation Supervisor
Dissertation Chair

Don Brutzman
Department of
Information Sciences

Raymond R. Buettner
Department of
Information Sciences

Erik Jansen
Department of
Information Sciences

Paul Lester
Department of
Defense Management

Approved by: Alex Bordetsky
Chair, Department of Information Sciences

Joseph P. Hooper
Vice Provost of Academic Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Public-private partnerships (PPPs) are crucial for securing critical infrastructure (CI) against cyber-attacks, yet little is known about how public and private organizations develop willingness to partner for CI cybersecurity. This research addressed this gap through a qualitative, multiple-case analysis of four PPPs related to cybersecurity, each involving two organizations and an additional, follow-up PPP. The research developed a process model that challenges the conventional view of willingness as fixed or static and proposes a new perspective that captures the process of constructing willingness. The research highlights the usefulness of activity theory in exploring this concept and presents the process model that describes this new understanding of willingness. Constructing willingness to partner is an activity path commencing with a catalyst that prompts relational partnering activities and generates partnering frames of emulation, insight, and connection, along with emerging commitments. These commitments generate intangible partnering resources including competence, reputation, and social capital, which support the construction of willingness to partner. The activity path comprises three subprocesses: initiating interaction, generating commitment, and legitimizing partnering. This research enhances the literature on PPPs and CI cybersecurity by offering a detailed description of how public and private organizations construct willingness to partner.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CCSI	cyber critical services and infrastructure
CEO	chief executive officer
CI	critical infrastructure
CIO	chief information officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	chief information security officer
CMA	Cyber Mutual Assistance
CRISP	Cybersecurity Risk Information Sharing Program
DHS	Department of Homeland Security
DOE	Department of Energy
DOJ	Department of Justice
EEI	Edison Electric Institute
E-ISAC	Electricity Information Sharing and Analysis Center
ESCC	Electricity Subsector Coordinating Council
FBICC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FSSCC	Financial Services Sector Coordinating Council
GCA	Global Cyber Alliance
GHP	Greater Houston Partnership
IR	inter-organizational relationship
ISAC	information sharing and analysis center
ISAO	information sharing and analysis organization
JV2	Jack Voltaic 2.0
LA	Los Angeles
LAPD	Los Angeles Police Department
NCIJTF	National Cyber Investigative Joint Task Force
NERC	North American Electric Reliability Corporation
NYC	New York City

NYC3	NYC Cyber Command
NYPD	New York City Police Department
PNNL	Pacific Northwest National Laboratory
PPP	public–private partnership

ACKNOWLEDGMENTS

I am filled with sincere gratitude for the support I have received throughout my journey to complete my dissertation. My heartfelt thanks go first and foremost to God, whose unwavering love, guidance, and blessings have sustained me. Without His grace and mercy, this achievement would not have been possible. I also extend my deepest appreciation to my family for their unconditional love, support, and encouragement. Their sacrifices, prayers, and unwavering belief in me have been my driving force, and I could not have achieved this without them. I would like to express my gratitude to Dr. Kathryn Aten, my Committee Chair and Supervisor, for her unwavering professionalism and selfless dedication in supporting me throughout my academic journey. Her tireless hours of mentorship and guidance, and the sacrifices she has made to help me achieve my goals, are deeply appreciated. In addition, I would like to convey my appreciation to Dr. Erik Jansen for generously volunteering his time and sharing his wisdom, and to Dr. Ray Buettner, Dr. Don Brutzman, and Dr. Paul Lester for their support and invaluable feedback, which has contributed to my success. I am also deeply grateful to my primary research contacts who provided invaluable assistance throughout my research, including Lieutenant Gustavo A. Rodriguez, a retired member of the NYPD Intelligence Bureau; Dr. Steve McElwee, Chief Information Security Officer at PJM; Mr. Lance LaBreck, Business Continuity Manager at the California Independent System Operator; and Mr. Carlos Recalde, President and CEO of Sheltered Harbor. Their willingness to participate and share their experiences made this study possible, and I am extremely grateful for their generosity. I want to pay tribute to Mr. Umesh Verma, Founder of Cyber Houston, who was a valuable subject matter expert and contributed greatly to this study before his passing. He will be deeply missed, and his contributions will be remembered. A special thank you also goes to the dedicated individuals at the NPS Graduate Writing Center. Without their support, I would not have been able to make it through my academic journey. Finally, I express my deep appreciation to the U.S. Army leadership, LT General Stephen Fogarty, Colonel Andy Hall, and Chief Warrant Officer Five John M. O’Reilly, for their unwavering support throughout this endeavor. Their encouragement and guidance have been invaluable to me.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The increasing frequency and severity of cyber-attacks on critical infrastructure (CI) in 2009–2022, including incidents such as the SolarWinds Orion, Kaseya, Colonial Pipeline, JBS Foods, and Log4Shell attacks, as well as vulnerabilities in the Log4j library, have brought attention to the need for a more comprehensive approach to protecting CI from cyber threats (Phillips, 2021). In April 2022, recognizing the critical effect cyber-attacks can have on the U.S. economy and citizens' well-being, the U.S. Congress called for a reevaluation of the country's approach to the cybersecurity of CI (Strengthening American Cybersecurity Act, 2022). Because both public and private organizations play a role in securing CI from cyber-attack, the cybersecurity of CI requires public–private cooperation (Solansky & Beck, 2021). There remain, however, many barriers to creating public–private partnerships (PPPs) (Caldwell & Wilshusen, 2014). Research on PPPs has focused generally on identifying factors that influence the performance of PPPs after they are created, ignoring the important processes that precede formal partnering. This research fills this gap by exploring how public and private organizations construct a willingness to partner in support of cybersecurity for CI.

Cybersecurity researchers agree that PPPs are vital to the cybersecurity of CI (Busch & Givens, 2012; Solansky & Beck, 2021). The public sector regulates CI; however, the commercial sector owns the vast majority (approximately 85%) of CI assets (Busch & Givens, 2012; Germano, 2014; Michel-Kergan, 2003). The public sector has access to intelligence about threats and the more comprehensive, broader environment while the commercial sector has the authority and responsibility that comes with ownership (Chen, 2020). Thus, ensuring the cybersecurity of CI requires partnering.

Researchers agree that willingness is a prerequisite for partnerships (Du et al., 2012; Solansky & Beck, 2021). For PPPs to succeed, organizations must be willing to partner. Despite this understanding, most research on PPPs assumes there is willingness and focuses on the performance of partnerships after they are established. This dissertation focuses on the processes that precede organizations' partnering in formal PPPs through a qualitative, multiple-case analysis exploring five cybersecurity-related PPPs. The research analyzes archival data and semi-structured interviews with subject-matter experts representing member organizations within the five PPPs. The findings contribute to a better understanding of PPPs by describing the process through which the public and private organizations constructed willingness to partner to address the cybersecurity of CI.

A. CYBER THREATS, CI, AND THE IMPORTANCE OF CYBERSECURITY

Cybersecurity threats exist because of vulnerabilities that offer opportunities for cyber-attacks. There are numerous cybersecurity threats; however, the most severe threats are physical effects that lead to health, safety, and environmental consequences in the real world (Morris & Gao, 2013; Habibzadeh et al., 2019). Cybersecurity attacks can cascade into safety risks that lead to physical harm to the system and its environment.

As new security challenges have emerged, leaders' conceptualization of CI has changed and is becoming more complex (Moteff et al., 2003). Leaders now recognize that CI includes more than transportation systems, such as systems of bridges, railways, and roads (Dunn-Cavelty & Suter, 2009; Yang & Wu, 2013). Leaders' conceptualization of CI initially expanded to include power plants and grids, oil and gas pipelines, and telecommunication facilities (Amin, 2005). More recent conceptualizations have been even broader. Presidential Directive 21 defines CI as follows: "distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations" (White House, 2013, para. 2).

In October 2021, the U.S. House of Representatives Homeland Security Subcommittee introduced the Securing Systemically Important Critical Infrastructure Act. The bill re-emphasizes that infrastructure within cyberspace is critical and recognizes the role of the private sector in ensuring cybersecurity. The bill provides the Cybersecurity and Infrastructure Security Agency with the authority to develop a process to designate the essential parts of CI to be secured by the private sector (Securing Systemically Important Critical Infrastructure Act, 2021).

This shift in conceptualization recognizes increased potential threats. Sophisticated adversaries seeking to harm U.S. CI will most likely target information stored in computer networks and will use networks to monitor and collect data for potential multi-pronged attacks involving cyber elements. Moreover, a cyber event combined with a physical event (e.g., a hurricane or pandemic) could cause a cyber intrusion and corruption where multiple parts of CI are impacted, and physical effects result in a catastrophic outcome. Following Presidential Directive 21 and the Department of Homeland Security (DHS)'s usage, CI is conceptualized here in terms of DHS's 16 identified CI sectors encompassing its interconnected organizational systems and vital assets, including information systems and networks (Cybersecurity & Infrastructure Security Agency, n.d.). This broader conceptualization of CI includes infrastructure that if compromised would critically debilitate national security.

B. PUBLIC–PRIVATE PARTNERSHIPS

PPPs are collaborative inter-organizational relationships between public and private entities that are formally or informally structured; they include strategic alliances, partnerships, associations, coalitions, joint ventures, franchises, research consortia, and networked organizations (Cheng et al., 2021; Solansky & Beck, 2021). The cybersecurity community views the formation of PPPs as an effective way to achieve mutual goals and enable critical security infrastructure (Busch & Givens, 2012). As early as the 1980s, CI projects began incorporating PPPs, which were then viewed as valuable assets for revitalizing economic marketability and aiding in social programs (Jacobson & Choi, 2008). The seriousness of cyber-attacks and their consequences has resulted in an expanded recognition of the value of PPPs, including their role in cybersecurity (Bhatia et al., 2016; Gordon et al., 2015; Kaijankoski, 2015; Solansky & Beck, 2021; White et al., 2019).

PPPs have now become a prominent alternative form of governance that often dominates public management thinking (Christensen & Petersen, 2017). As noted, there is considerable diversity in CI. Each of the 16 sectors identified by DHS has unique task interdependencies and organizational designs. Thus, there is also considerable variation in the goals, membership, and organization of public–private partnerships (Moteff et al., 2003). Given this diversity, many argue that it is difficult to determine and measure the value of PPPs (Blue-Banning et al., 2004; Chen, 2020; Henrick et al., 2017; Kingsley & Waschak, 2005; Mulgan & Albury, 2003; O'Halloran, 2017; Yang & Wu, 2013). Practitioners and researchers, however, have continued to assert that substantial benefits result from collaboration within cybersecurity, and researchers have continued their attempts to define and understand the structure and value of these partnerships.

C. WILLINGNESS TO PARTNER: A GAP IN UNDERSTANDING

Willingness is a prerequisite and an essential element of partnerships (Bazzoli et al., 1997; Bhatia et al., 2016; Bishop & Davis, 2002; Chaserant, 2003; Du et al., 2012; Einbinder et al., 2000; Mohr & Spekman, 1994; Solansky & Beck, 2021). Despite this truth, research on willingness to partner is limited, and explanations of how and why organizations become willing partners remain unclear (Bazzoli et al., 1997; Hare, 2011; Rosas & Camarinha-Matos, 2010).

Research has explored activities related to partners, such as collaboration, participation, cooperation, coordination, communication, engagement, and sharing (Amayah, 2013; Besley et al., 2018; Bhatia et al., 2016; Du et al., 2012; Khoshdel & Bakhshan, 2015; Solansky & Beck, 2021; Yu et al., 2011). Limited studies of organizational collaboration have explored "willingness to share" (Du et al., 2012). However, there is no explicit, consistent definition of willingness to partner in the literature on PPPs, and willingness is generally assumed. Further, when research has investigated willingness, it has focused on a particular point in time or stage within a relationship, such as when a project ends in an outcome (Addae-Boateng et al., 2015; Benitez-Ávila et al., 2019; Kelly, 2012).

Because willingness to partner is a prerequisite of partnering, a complete understanding of organizational partnerships requires research investigating how organizations' willingness to partner emerges over time. The importance of PPPs in securing the cybersecurity of CI further supports the need for additional research and a focus on these partnerships.

D. RESEARCH QUESTION AND RESEARCH DESIGN

This dissertation contributes to the literature on organizational partnerships by exploring how public and private organizations construct willingness to formally partner to enable the cybersecurity of CI. To answer this question, this inductive, multiple-case research analyzed qualitative data using process and case analysis techniques (Langley,1999; Yin, 2010). The research explored five cybersecurity-related PPPs that shared the same goal of enabling the cybersecurity of CI. These PPPs formed in different geographic locations, represented different sectors, and included municipality and sector-led partnerships. The research involved analyzing documents and interviews using three sensemaking strategies for analyzing cases and process data: narrative construction and temporal bracketing, coding, and visual mapping (Langley, 1999; Yin, 2010). The analysis resulted in a midrange process theory that explains how the public and private organizations of the focal PPPs constructed willingness to formally partner to enable CI cybersecurity.

E. CHAPTER ORGANIZATION

The remainder of this dissertation is organized as follows. Chapter II consists of the literature review, which provides a further review of research on PPPs and related research that helped to frame and guide the analysis. Chapter III describes the cases and research methods. Chapter IV presents an initial analysis and preliminary model. This initial analysis served to ground the researcher in the data and guide subsequent analysis. The preliminary model resulted in a slight revision to the research question, to focus on construction, and more clearly defined the early stages of partnering and constructing willingness that became the focus of the final analysis. Chapter V presents and discusses a model that describes how the focal organizations constructed willingness to partner in PPP to enable CI cybersecurity. The final chapter examines the implications and limitations of this dissertation research, makes recommendations for practice, and discusses the contributions this research makes to the existing field of study.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

This chapter provides context for understanding what is known and what needs to be better understood about willingness and PPPs. It discusses how research on inter-organizational relationships has approached studying PPPs. It further discusses the role of PPPs in CI cybersecurity and the importance of partnership formation and partner selection. Willingness is central to this research. This chapter discusses how willingness has been treated in research related to inter-organizational partnerships. This chapter also presents activity theory, resourcing, and framing as theoretical tools used to explore and investigate individual and organizational activities throughout the partnership formation process.

A. PUBLIC–PRIVATE PARTNERSHIPS—A STATE OF KNOWLEDGE

PPPs are a type of inter-organizational relationship (IR). Research on IRs describes their structure, membership, and governance and explores how these factors influence the performance of inter-organizational partnerships. IR research suggests that these factors may influence how and why PPPs form and the outcomes PPPs achieve. Additionally, IR research suggests that context shapes PPPs and the information sharing within them.

1. Inter-organizational Relationships

IRs are social systems that involve two or more organizations working together to form a partnership for a common goal and, thus, create potential value (Phillips et al., 2000). IRs are multiorganizational systems composed of essential activities that shape their structure, membership, and governance, which generate connections and interactions over time (Lowndes & Skelcher, 1998; Mackintosh, 1992; Trist, 1983; Van de Ven, 1976). IRs include strategic alliances and cross-sector partnerships (CSPs), both of which may comprise public and private organizations. The goals and objectives of strategic alliances and CSPs can be long term or short term, formal or informal, and can take many forms, including PPPs (Austin, 2000; Austin & Seitanidi, 2012; D'Alessandro et al., 2014; Todeva & Knoke, 2005; Wang & Rajagopalan, 2015).

The structure of an IR refers to the key actors and the arrangement of the relationships developed over time (McQuaid, 2000). Membership involves partnering with individuals and organizations, making decisions, or sharing resources (Stadtler & Probst, 2012). As partnerships formalize, structural mechanisms such as formal agreements and contracts become established (McQuaid, 2000). Governance refers to how organizations arrange the structure of IRs through the implementation of rules and regulations by those in positions of authority. Governance refers to the structural means organizations arrange to form an IR (Huber et al., 2013; Van de Ven & Walker, 1984; Zaheer & Venkatraman, 1995). IRs include PPPs, strategic alliances, CSPs, joint ventures, coalitions, and networks (Holland, 1984).

Strategic alliances and CSPs can be, but are not always, PPPs. However, these types of IRs bear further discussion because they can affect how PPPs form. Gutierrez et al. (2016) state that "same-sector partnerships" are often strategic alliances (p. 55). Strategic alliances and CSPs share similar characteristics. Both comprise public and private organizations that work together to achieve a common goal (Austin, 2000; Austin & Seitanidi, 2012; Stadtler, 2011). However, there are some critical differences between the two. One difference is the level of cooperation and collaboration. Strategic alliances typically have an existing structure developed among their organizational relationships. Therefore, they involve a high level of cooperation and collaboration, with organizations sharing resources, knowledge, and expertise to achieve a common goal (D'Alessandro et al., 2014; Wang & Rajagopalan, 2015). In contrast, CSPs can have either a low or high level of cooperation and collaboration, which allows the member organizations to work together in a more ad hoc or informal manner (Gutierrez et al., 2016). Another difference is the diversity of industry among member organizations. For example, strategic alliances usually include organizations from a specific sector of industry, e.g., finance or energy, or government that work together to achieve a particular goal (Lavie et al., 2012). CSPs include organizations that represent various industries that bridge different sectors, e.g., the financial sector working with the energy sector (Austin, 2000; Austin & Seitanidi, 2012).

Within IR research, a focal organization—or focal firm—within a partnership often serves as a referent, which offers a perspective for understanding how value is created within a collaborative arrangement (Doz & Hamel, 1999; Gutierrez et al., 2016; Oliver, 1990; Sarkar et al., 2009). A referent organization may not lead an IR's efforts but may play a distinct role in forming the IR. The referent organization becomes the "object of inquiry" (Trist, 1983, p. 269) within the "sphere of interest" (Scott & Thurston, 1997, p. 417) that comprises the system of relations it must maintain within a field. The field encompasses the community of organizations that share the common goal of the IRs, such as providing healthcare (Bazzoli et al., 1997) or, in this dissertation research, cybersecurity. The referent organization is a reference point for partnering with other organizations and sometimes is the leading organization in a particular field, industry, or network; other organizations seek to emulate it (Bazzoli et al., 1997; Sarkar et al., 2009; Trist, 1983). Within PPPs, strategic alliances, or CSPs, one or more partner organizations may be considered referent organizations due to their leadership or dominance in a sector or industry. This organization may serve as a model that encourages other organizations to form similar partnerships (Doz & Hamel, 1999; Gutierrez et al., 2016; Oliver, 1990; Trist, 1983; West & Milio, 2004).

2. PPPs and the Cybersecurity of CI

Research suggests that PPPs can bring value to cybersecurity by allowing organizations to collaborate and share information, knowledge, and resources to enhance efficiency and effectiveness of efforts to ensure cybersecurity. Knowledge exchange in cybersecurity takes various forms and is structured in relationships between organizations working together in collaboration. While researchers agree that information sharing is crucial for cybersecurity, it is difficult to assess the extent or outcomes of information sharing in PPPs. This section reviews key findings of research on PPPs and the cybersecurity of CI and introduces two models of PPPs that emphasize information sharing for the CI of cybersecurity.

a. Knowledge and Information Sharing

Cybersecurity experts agree that information sharing among private and public organizations has benefits, suggesting the potential of PPPs to support cybersecurity. Public and private organizations need to share information and knowledge to provide mutual assistance and improve resilience (Clinton, 2011; Dunn-Cavelty & Suter, 2009; Gordon et al., 2015; He et al., 2018; Healey, 2015; Manley, 2015; Pala & Zhuang, 2019; Sharkov, 2016; White et al., 2019). Organizations that share knowledge are more likely to increase efficiency and effectiveness (Mckenzie & Van Winkelen, 2006; Tishuk, 2012). Cybersecurity-focused PPPs may increase the efficiency of cybersecurity by enabling strategic development that promotes understanding and avoids duplicating efforts and may increase effectiveness by developing joint strategies for information sharing to support resilience (Brown, 2018).

Information is critical for assessing, monitoring, and responding to threats. Cybersecurity information includes reports of incidents, threats, vulnerabilities, and mitigations, as well as situational awareness, best practices, and strategic analyses (Goodwin & Nicholas, 2015). Cybersecurity information enables safety, security, efficiency, and resilience (He et al., 2018; Sharkov, 2016). Recognizing the importance of information sharing, the U.S. government often leads efforts to enable information sharing between the public and private sectors through legislation, such as the Homeland Security Act of 2002 (Gordon et al., 2003) and the Information Sharing Act of 2015, which was established to facilitate the exchange of cyber-threat indicators and defensive measures between the government and the private sector (Cybersecurity Information Sharing Act, 2016).

Information sharing involves cyber-threat intelligence-sharing activities across organizations (Gordon et al., 2015). Recognition and evaluation of information that flows within technology mechanisms (e.g., e-mail, chat, and websites) enhance comprehensive sharing. Several researchers who have studied cyber-attack outcomes agree that these information-sharing methods are valuable tools; they argue, however, that in-person exchanges better facilitate cybersecurity (O'Brien, 2003; Rid & Buchanan, 2015; von Solms & van Niekerk, 2013). One outcome of PPPs is increased personal exchanges, which may facilitate greater information sharing.

Information sharing among private and public organizations does occur. However, organizations remain reluctant to share information related to cybersecurity. Some leaders also remain concerned about the effectiveness of focusing on information sharing as a goal (Johnson, 2016). The challenges of assessing the extent and usefulness of information sharing further drives this skepticism (Fleming & Goldstein, 2012). Additionally, information sharing occurs at different levels of organizations and involves multiple information systems; this complexity can contribute to the challenges of assessing information sharing and concerns about its value (Bhatia et al., 2016). However, economics-based research suggests that information sharing provides value by reducing the uncertainty associated with cybersecurity investments (Gordon et al., 2015; Jasper, 2017).

Information sharing and knowledge exchange between public and private organizations can allow collaborative innovation that results in the transformation of practices and increases organizational longevity and reliance (Mulgan & Albury, 2003). Experts in the cybersecurity domain suggest that knowledge exchange occurs through structured relationships involving organizations working together in collaboration. Examples include internships, apprenticeships, cyber exercises, and incident response (Nyre-Yu et al., 2019), which are supported with formal procedures, best practices, and resources, allowing private-sector employees to be embedded in government cyber organizations or participate in government events. PPPs can provide opportunities for these types of relationships and knowledge exchange. One example, Cyber Mutual Assistance (CMA; ICS Village, 2018), is a voluntary program, inspired by traditional mutual assistance practices (Federal Emergency Management Agency, n.d.), that focuses on sharing cyber-related capabilities (e.g., skilled personnel). The energy sector has been the only industry to adopt CMA.

b. Information Sharing and Analysis Centers and Information Sharing and Analysis Organizations

Over the past 25 years, PPPs in support of cybersecurity have been implemented in two models. The first model is the information sharing and analysis center (ISAC), explicitly designed for sector-specific organizations that operate within a strategic alliance, e.g., the energy sector (Gordon et al., 2015; He et al., 2018). This model was followed by the 2015 creation of the information sharing and analysis organization (ISAO; ISAO Standards Organization, n.d.-a). ISAOs differ from ISACs in allowing more flexibility in arranging a partnership among public and private organizations and establishing best practices (ISAO Standards Organization, n.d.-a; White et al., 2019;). ISACs and ISAOs represent prime examples of PPPs in CI cybersecurity. Despite the focus of some on information sharing, Healey (2015) emphasizes that the most successful PPPs often concentrate on solving problems together to mitigate cyber vulnerabilities and prevent or respond to cyber incidents on CI rather than focusing on sharing information.

In summary, IRs play a crucial role in the collaborative efforts of organizations in achieving a common strategic goal. PPPs, strategic alliances, and CSPs are different types of IRs that can bring value to cybersecurity through information sharing, knowledge exchange, and resource utilization. Despite the importance of information sharing, it is complex, and its value is difficult to assess. Leadership and governance are critical factors in the success of PPPs and collaborations. The two specific PPP models introduced highlight the significance of information sharing for CI cybersecurity. Overall, IRs serve as a platform for organizations to work together toward a secure and efficient cybersecurity system.

B. THE NATURE OF PARTNERSHIP FORMATION

The existing IR literature describes governance modes and four stages of partnership formation and highlights partner selection, whereby organizations begin building relationships, as the most crucial stage. This IR research sheds light on the dynamics of informal and formal governance, which are complementary ways of organizing, coordinating, and collaborating. Relational governance is particularly relevant to this dissertation research, as it focuses on the early stages of partnerships, when formal agreements are rare. The research selected for review here also emphasizes partner selection as critical to successful partnership outcomes and notes the role that expected gains or benefits play in that selection process.

1. Informal and Formal Modes of Governance in IRs

The IR literature refers to two forms of partnership governance and partnership formation dynamics for PPPs: informal and formal (Zaheer & Venkatraman, 1995). Partnership governance dynamics are the actions and processes organizations perform to conduct relational and contractual governance (Hagedoorn et al., 2000). Relational governance refers to informal actions and processes while contractual governance refers to formal actions and processes (Ring & Van de Ven, 1994). Relational governance is based on trust, mutual understanding, and cooperation while formal governance relies on clearly defined rules and legally binding agreements. These two forms of governance apply different methods to manage relationships and resolve conflicts but are complementary approaches to organizing, coordinating, and collaborating (Huber et al., 2013).

Relational governance refers to an ongoing informal arrangement of relationships and interactions between organizations based on trust, mutual understanding, and cooperation, and in the context of partnership formation, relational governance dynamics are also informal (Hagedoorn et al., 2000). In relational governance, organizations rely on informal mechanisms, such as personal relationships, social norms, and shared values, to coordinate their activities and manage conflicts. Most scholars agree that activities during partnership coordination, which involves partner selecting and direction setting, are structured through relational governance dynamics (Benitez-Ávila et al., 2019). Relational governance is based on established trust, shared history, and mutual understanding, and organizations use the relational governance dynamics that arise during partner selecting as criteria to assess possible partners (Zamiri & Camarinha-Matos, 2019).

Contractual governance, by contrast, refers to formal agreements and contracts that organizations use to govern interactions and coordinate their activities. Contractual governance is usually based on legally binding contracts and formal arrangements. Most scholars agree that collaboration activities, which focus on implementation and institutionalization, are structured through contractual governance dynamics (Benitez-Ávila et al., 2019).

In summary, relational governance involves informal dynamics based on trust, mutual understanding, and cooperation. Contractual governance refers to formal agreements, legally binding contracts, and explicit rules (Weber et al., 2020). During partnership formation, the interplay of relational and contractual governance dynamics signals early organizational interests, which in turn signal the transformative potential and the partnership's capacity to reach its goal (Seitanidi & Crane, 2009; Stadtler, 2011).

2. Partner Selecting in IRs

Forming a partnership is generally characterized as consisting of two to five stages or phases. According to Gray (1998), these include partner selection, negotiation or direction setting, implementation, and institutionalization. Researchers studying partnership formation often highlight partner selection as the most critical stage. Partner selection initiates the pre-development stage, when social coordination begins in the partnership formation process. Organizations and individuals informally engage in interacting, identifying, assessing, and choosing potential partners through informal decision-making and problem-solving strategies (Chen et al., 2008; Kumaraswamy et al., 2007; McQuaid, 2000; Ring & Van de Ven, 1994; Seitanidi & Crane, 2009; Stadtler, 2011). During the partner-selecting stage, individuals and organizations begin to assess their resource needs and intentions, and this stage may result in a willingness to form partnerships (Lowndes & Skelcher, 1998). Many researchers agree that organizations seek to identify potential partners to overcome resource limitations and improve efficacy by pooling resources (Lowndes & Skelcher, 1998). For example, an individual or organization may benefit by accessing a potential partner's intangible resources such as skills, expertise, social capital, and reputation. Partners access others' intangible assets through knowledge exchanges that start after partner selection, through coordination and collaboration. However, the potential to accrue these benefits and subsequent benefits, such as improved competence, influences initial partner selection (Lavie et al., 2012).

During the partner-selection stage, organizations identify potential partners by assessing other organizations' expertise and abilities and, hence, their potential to provide new skills and knowledge (Davis & Mentzer, 2008). Selection includes evaluating the different competencies, abilities, and knowledge that other organizations can bring to a potential partnership. Both skills and expertise can be valuable resources that organizations may access through partnerships. Additionally, organizations consider the connections and networks of other potential partners. Organizations seek to tap into the existing social and professional networks of potential partners that will enhance the resources and capabilities of the partnering organization, ultimately leading to improved efficiency and effectiveness (Hagedoorn et al., 2000).

Organizations often select partners to gain a reputational advantage, so they consider the reputations of potential partners during the selection process. Organizations can accrue several benefits from partnering with high-status organizations (Martin de Castro et al., 2004). Partnering with an organization or joining a partnership that has a positive reputation can enhance stakeholders' perceptions of an organization's credibility (Ford et al., 2020). Organizations can enhance their reputations by associating with reputable individuals and organizations. Additionally, an organization's reputation directly impacts potential partners' willingness to engage in partnering; thus, an organization's existing partnerships can influence its chances of pursuing new partners and new opportunities (Brune, 2009). Partnering with high-reputation organizations can also improve the visibility and reach of a partnering organization (Chandler et al., 2013; Roberts et al., 2021).

This effect, however, differs between public and private organizations. For a public organization, reputation greatly influences public perception and trust (Schultz et al., 2019). A positive reputation can attract more support and resources, such as funding, partnerships, and volunteers. A private organization's reputation is primarily determined by its interactions with stakeholders: customers, partners, and investors (Petkova et al., 2008). A positive reputation can help a private organization establish a loyal customer base, attract new business opportunities, and secure investments (Castelo Branco & Lima Rodrigues, 2006). A positive reputation can also help the partnering organization attract and retain top talent (Earle, 2003). Considering potential partners' skills, expertise, social capital, and reputation during the selection process can lead to improved outcomes, enhanced stability, and a longer-lasting partnership for an organization. Several researchers agree it is essential to evaluate these factors for successful partnership results (Belliveau et al., 1996; Chen et al., 2008; van den Hooff & de Ridder, 2004; Osei-Kyei et al., 2017; Wu et al., 2009).

3. Resourcing and Framing

Researchers and leaders of organizations have long recognized that resources play a vital role in organizational performance, and organizational scholars have given central attention to resources (Feldman & Worline, 2011). The literature recognizes the value of both tangible and intangible resources, such as financial assets and reputation, respectively. The study of resources has led to several perspectives (Allee, 2008). The resource-based view of the firm focuses on how resources lead to a sustainable competitive advantage (Barney, 1991, 2001). Dynamic capabilities focus on the effects resulting from capabilities (resources) created through organizational processes (Eisenhardt & Martin, 2000). A more recent perspective views resourcing as an ongoing organizational process (Feldman, 2004; Howard-Grenville & Hoffman, 2003). As discussed previously, research suggests that organizations form partnerships to increase their potential for gaining benefits through tangible and intangible resources that they acquire through partnering. Thus, the literature on resourcing can illuminate our understanding of partnering.

Resourcing occurs internally as well as externally. Brush et al. (2001) suggest internal resourcing occurs among individuals and organizations using organizational resources to change existing resources into something different or more valuable. Feldman's (2004) conception of resourcing stems from social practice theory, which considers how people pursue various interests and discover new opportunities for action as they navigate different practices and settings. This view of resourcing is consistent with perspectives on partnering.

As discussed, a desire to gain resources may encourage organizations to seek partners and opportunities for partnering. As organizations assess and select potential partners, they may either deliberately or unintentionally share knowledge and improve each other's skills, leading to the development of new and more advanced abilities (Ayuso et al., 2006; Otola, 2016). Ultimately, these transformations can increase the potential value of intangible resources and make them more valuable to the organizations that hold them.

Research on framing views frames as resources (Howard-Grenville & Hoffman, 2003). The concept of frames originated in the social sciences and has been used for both descriptive and analytical purposes (Goffman, 1986). Framing refers to the process by which individuals attempt to give meaning to their interpretation of events and conditions. Individuals' interpretations can create new perspectives that are then collectively constructed to create collective frames that serve as resources for future interpretations

(Benford & Snow, 2000; Feldman, 2004). These shared meanings can guide actions (Gutierrez et al., 2010; Howard-Grenville & Hoffman, 2003; Leonardi, 2011). Collective frames can serve as a tool to diagnose situations or problems and mobilize action toward solutions (Entman, 1993; Kubal, 1998; Van Gorp, 2007). For example, consistent with this view, Mackintosh (1992) proposes that frames may serve as negotiation tools in partnerships. This notion suggests that framing and frames may play a role in the formation of PPPs.

C. WILLINGNESS AS AN OBJECT TO STUDY

Within the social science literature, researchers view willingness as an intention or motivation to act. This section first discusses willingness and how it is studied across disciplines. Research has emphasized the importance of willingness as a factor in collaboration and partnering. This research, however, often uses willingness as an independent variable that is static rather than processual. Literature on trust, a similar construct, however, sometimes adopts a processual approach. The second part of this section explores processual research on trust and how it may inform research on willingness to partner. Another limitation of much of the literature on willingness is a focus on the individual level. The third part of this section presents activity theory as a tool that allows a multi-level analysis, which may benefit the study of willingness to partner.

1. The Construct of Willingness and How It Is Studied

The construct of willingness is broadly studied across disciplines of social psychology (Jost, 2012; Pomery et al., 2009; Van Lange et al., 1997), sociology (Liebe et al., 2011; Matear, 2014), and behavioral economics (Almås et al., 2016; Buser, 2016; Sunstein, 2002). Research has sought to understand the factors that influence an individual's motivation to engage in a particular behavior or activity. Willingness is the degree to which an individual is motivated to engage in a particular behavior or activity. According to Pomery et al. (2009), willingness is goal oriented and influenced by several factors, including attitudes, norms, an individual's perceptions, self-efficacy, and past behavior. Partnering is an iterative and complex process (Scott & Thurston, 1997);

partnering organizations must be willing to engage in activities within and beyond the boundaries of an organization.

Researchers use the concept of willingness to understand the factors that drive an organization’s readiness to participate in PPPs. The term *willingness* has many definitions, including motivation, intention, readiness, openness, or eagerness and commitment. Razak et al. (2016) have reviewed the knowledge-sharing literature and found that commitment is a key factor in related behavior. In the context of IR formation, commitment to knowledge sharing can impact the success of information exchange and collaboration. For example, a committed individual or organization will be more likely to actively participate and share valuable information in a partnership. The work of Besley et al. (2018) highlights that enjoyment of the experience and belief in one’s impact drive an individual’s willingness to engage with others. Raban and Rafaeli (2006) have found that an individual’s perception of information ownership affects the willingness to share it. Du et al. (2012) have found that a strong partnership leads to a greater willingness to share information in supply chain relationships. Yu et al. (2011) have shown that effective communication and confidence in individuals can enhance an organization’s reputation and willingness to communicate. A study by Rosas and Camarinha-Matos (2010) assesses an organization’s readiness for collaboration using practical and relationship-based factors. A tool developed in the study considers willingness an important factor in finding suitable partners. By understanding these drivers of willingness, researchers can better understand how organizations establish successful PPPs.

Researchers exploring PPPs often center on organizations’ relational or contractual governance processes such as collaboration, participation, cooperation, coordination, communication, engagement, or sharing, and assume the presence of willingness (Amayah, 2013; Bazzoli et al., 1997; Du et al., 2012; Einbinder et al., 2000; Khoshdel and Bakhshan, 2015; Yu et al., 2011). Researchers studying PPPs have viewed willingness as a static variable and used it to measure and predict PPP outcomes (Bazzoli et al., 1997). For example, Amayah (2013) has used willingness as a measure of motivation and the influence of sharing knowledge among public organizations. Most of the limited research on willingness in partnerships measures willingness at a single point in time. Willingness has not been fully explored as a process.

Many researchers who investigate PPPs focus on the organizational and contractual aspects of governance processes, such as collaboration, participation, cooperation, coordination, communication, engagement, and sharing, and often treat willingness as a static factor (Amayah, 2013; Bazzoli et al., 1997; Du et al., 2012; Einbinder et al., 2000; Khoshdel & Bakhshan, 2015; Yu et al., 2011). Amayah (2013) and Bazzoli et al. (1997) are examples of researchers who have used willingness as a static variable to measure and predict PPP outcomes, with Amayah (2013) specifically using willingness as a measure of motivation and the influence of knowledge sharing among public organizations. However, the limited research on willingness in partnerships has measured this variable only at a single point in time and has yet to fully explore its dynamic nature as a process.

2. A Need for a Process Perspective

Existing research demonstrates the importance of willingness in partnering. To achieve effective PPPs, public and private organizations must be willing to partner (Rosenau, 1999). Research has not, however, fully explored how willingness is constructed over time. Literature on trust, a similar construct, recognizes that trust is built gradually over time. Trust develops through individuals' and organizations' acts of commitment, which occur throughout coordination or collaboration activities as a partnership is forming (Lewicki & Bunker, 1996; Waddock, 1988). Khodyakov's (2007) research highlights studying trust as a process while utilizing the concept of agency to consider the "temporal-relational context of action" (p. 116). This idea of an action context suggests that researchers can gain a multi-level understanding of individuals and organizations during partnership formation by observing their actions and activities. Research on PPPs that support cybersecurity suggests a need for understanding PPPs broadly from the holistic, process perspective. A deeper understanding of willingness to partner from a processual perspective will help fill this gap in knowledge.

3. Activity Theory

Activity theory presents a practical way for researchers to analyze the connections and ties between actors and their actions. The essential elements of activity theory include subjects, objects, tools, rules, communities, and divisions of labor (Engeström, 2014; Kuutti, 1991). Activity theory is a framework for studying human activity, including the interactions between individuals and organizations and the social and cultural context in which they participate (Engeström, 2014). It views activity as a system of actions, decisions, and events that shapes the environment and considers the role of human agency in this process (Engeström, 2014). Activity theory allows a theoretical and methodological perspective that considers the inter-organizational level of analysis (Phillips et al., 2000; Scott & Thurston, 1997).

Activity theory offers unique benefits and capabilities for analysis and is not limited to individual, material, or historical context. It uses activity as the basic unit of analysis, referred to as cultural-historical activity theory (Engeström, 2014; Kuutti, 1991). The components of an activity system include subjects, objects, mediated tools, rules, communities, and divisions of labor that characterize the cultural and social context of human activity. Activity theory incorporates the concept of agency, the ability of individuals or groups to make decisions and shape their environment, but places agency within the context of an activity system. This theory provides a useful lens for exploring dynamics of human activity and relationships between individuals and their surroundings.

D. SUMMARY

In conclusion, this chapter has highlighted the significance of exploring willingness to gain a more complete understanding and PPPs in the context of CI cybersecurity. The concept of willingness plays a crucial role in the analysis of inter-organizational dynamics and is central to this dissertation research. The discussion further underscores the significance of partner selection and formation in PPPs, highlighting the need for a better understanding of these concepts in CI cybersecurity. Finally, the chapter showcases the use of activity theory, resourcing, and framing as useful theoretical tools for investigating individual and organizational activities during the partnership formation process.

III. METHODS

This chapter describes the research design and methods this research used to investigate the process through which private and public organizations construct willingness to partner in support of CI cybersecurity. This inductive, multiple-case research analyzed qualitative data using process and case analysis techniques (Langley,1999; Yin, 2010). Consistent with the inductive approach, the analysis was iterative, and the research design continued to evolve through the data collection and initial analysis. For readability, the research methods are presented more linearly than they occurred.

The research initially focused on eight organizations within four cybersecurity-related PPPs (Langley,1999; Yin, 2010). A fifth PPP was added midway through the data collection process per a recommendation from an interview participant. The research yielded a midrange process theory that describes how the focal partnerships' public and private organizations constructed willingness to formally partner to enable CI cybersecurity.

Lincoln and Guba (1985) have identified and described four strategies for establishing the trustworthiness of qualitative research, credibility, dependability, confirmability, and transferability. Qualitative researchers can ensure trustworthiness through systematic and transparent analysis, rich and varied data sources, and readers' trust or confidence in the interpretation and findings. As is typical of case analysis, this dissertation research relied on varied types of data collected from multiple sources, which allowed comparisons and checks between the sources. The research also drew on multiple analysis techniques, which allowed further comparisons and checks. The research proposal was reviewed and approved by the Naval Postgraduate School's Institutional Review Board. This chapter introduces the PPP cases and selection process, details the data collection process, and presents the data analysis approach.

A. CASE SELECTION

This research initially analyzed eight organizations in five PPPs: New York City Cyber Critical Services and Infrastructure, Cyber Houston, Cyber Mutual Assistance, and the Cybersecurity Risk Information Sharing Program. The research analyzed one public and one private organization in each PPP. A fifth PPP, Sheltered Harbor, was added during the analysis on the recommendation of an interview participant. All five PPPs formed after President Obama's 2013 Executive Order 1363, which aimed to unite public and private organizations to enhance cybersecurity by forming partnerships. When this research was conducted, each of the five PPPs was operating to address cybersecurity in CI. Figure 1 displays the PPPs and the organizations within them.

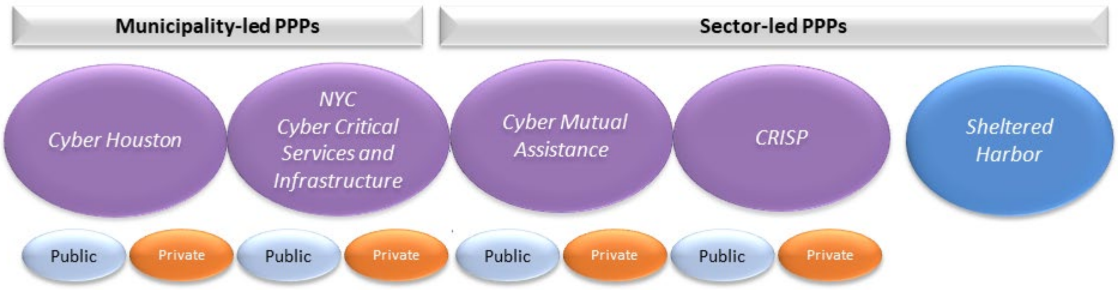


Figure 1. Selected Cases

The selection criteria for the initial four cases included commonalities and variations to allow comparison. The four initially selected PPPs shared the same goal—to enable CI cybersecurity—and were participating in either or both information-sharing and mutual aid activities. The PPPs were formed in different geographic locations, including two large metropolitan areas. The energy sector led two initial PPPs, and municipalities led the other two. The municipality-led PPPs were CSPs. A strategic alliance within the financial sector led to the fifth additional PPP. Thus, the PPPs represented different CI sectors.

1. New York City Cyber Critical Services and Infrastructure

Cyber Critical Services and Infrastructure (CCSI) is a municipality-led PPP in New York City (NYC), the largest city in the United States (Manhattan District Attorney's Office, n.d.). Activities to initiate the partnership began in 2013. The PPP was formally established in 2017 by the four founding organizations: the Manhattan District Attorney's

Office, the New York City Police Department (NYPD), the NYC Cyber Command (NYC3), and the Global Cyber Alliance (GCA). Its goal is to protect NYC's CI from cyber-attacks by developing a collective strategy to increase communication and awareness about cyber risks and to develop partnerships among public and private organizations. The PPP also seeks to rally volunteering experts and develop best practices for city-wide information sharing and mutual aid. Leaders have recognized the ongoing role of NYC CCSI in inspiring the evolution of public and private organizations partnering to enable the cybersecurity of CI (O'Boyle, 2022).

2. Cyber Houston

The Cyber Houston PPP is a municipality-led coalition of business leaders, specialists, and subject-matter experts in the Houston, Texas, region. Activities to initiate the Cyber Houston PPP emerged from the Greater Houston Partnership (GHP) in 2013, and the PPP was formally established in 2015. The GHP was formed in 1989 to develop a community of business leaders and became known as the largest Chamber of Commerce in the Houston region (ISAO Standards Organization, n.d.-a). Umesh Verma—business leader, entrepreneur, and chief executive officer (CEO) of a Houston information technology business—joined the GHP and subsequently founded Cyber Houston. The organization aims to develop a community of public and private business and government cybersecurity leaders to engage public and private organizations in the region's critical cybersecurity issues. Cyber Houston focuses on developing relationships among vendors and sales supply chain networks because that is where Cyber Houston perceives the most significant risk to be. Cyber Houston seeks to educate third-party vendors and help bring more cyber rigor to its organizations. Cyber Houston is an established ISAO.

3. Cyber Mutual Assistance

CMA is a North American energy sector–led framework for partnering across the energy industry. Activities to launch the CMA program began in 2014 through a group of CEOs known as the Electricity Subsector Coordinating Council (ESCC), and the PPP was formally established in 2016. CMA seeks to develop relationships for resource sharing to provide "surge capacity" to support individual companies should a cyber-attack exceed their ability to respond (Fehrman, 2016). CMA is a voluntary program that began with approximately 40 organizations and grew to include hundreds. Today, CMA is considered a model for preparing and responding to cyber-attacks (ESCC, n.d.).

4. Cybersecurity Risk Information Sharing Program

The Cybersecurity Risk Information Sharing Program (CRISP) is an energy sector–led platform to monitor situational awareness in the energy sector. Activities to create CRISP began in 2014 with an initiative between the U.S. government's Department of Energy (DOE) and energy industry participants, including ESCC members. The PPP was formally established in 2016. CRISP enables sharing and analysis among energy sector–related public and private organizations of timely and relevant information to mitigate threats to cybersecurity. Today CRISP serves as a model within the U.S. energy sector for information sharing and CI protection programs (DOE, n.d.).

5. Sheltered Harbor

Sheltered Harbor is a not-for-profit organization. Activities to initiate Sheltered Harbor began in 2014, and the PPP was formally established in 2015. Shelter Harbor's mission is to develop standards for the U.S. financial sector to maintain public confidence during worst-case scenarios such as cyber-attacks. The financial industry is well versed in mutual aid—the voluntary exchange of resources—to prepare and respond to natural disasters (e.g., hurricanes). Sheltered Harbor serves as a model of PPP within the U.S. financial sector, demonstrating how public and private organizations can work together to provide mutual aid and shape data vault standards (Sheltered Harbor, n.d.).

B. DATA SOURCES

This research involved collecting and analyzing three data types: interviews, documents, and videos. Data (interviews, documents, and video) were collected between January and June 2022. Coordination with critical informants began in early 2022 and continued throughout the research.

The researcher conducted 22 interviews with founders and members of PPPs, as shown in Table 1. The interviews lasted between 1 hr and 1.5 hr and were recorded and transcribed for review and analysis. The documents included all online news reports, YouTube videos that mentioned the PPPs or founders, and additional documents suggested by study participants, as shown in Table 1. The data provided a rich picture of the activities that occurred through the formation of each partnership, with interviews and documents providing two different sources of information about the events.

Table 1. Data Sources

Data Source Description	Volume/Amount
Semi-structured interviews Interview transcripts Post-interview notes/summaries Cyber Houston NYC CCSI CMA CRISP Sheltered Harbor	22, totaling 1,030 min (1–1.5 hr each) 98 pages 51 pages Two founders, three members Two founders, four members Two founders, three members Three founders, two members One founder
Online articles	47 (94 pages)
Annual reports	Three (216 pages)
Hearing reports	Two (12 pages)
PowerPoint presentations	One (23 pages)
Online public videos	Seven (420 min)/18 pages of transcripts

C. DATA ANALYSIS APPROACH

The analysis proceeded through two analysis stages, which are described in Chapters IV and V, respectively. Stage 1 analysis resulted in a preliminary, simplified model describing the partnership adoption phases. This preliminary model did not explain the willingness to partner but instead focused on later phases after willingness is built. This preliminary model helped build the researcher's understanding of the phenomena and served as an analytical tool that guided the subsequent Stage 2 analysis and final model building. The researcher drew on the preliminary partnership adoption phase model as a lens through which to initially organize and then build a model explaining the antecedent process through which the organizations became willing to partner.

Consistent with an inductive approach, the researcher began by organizing the data. Then, the researcher analyzed the data using sensemaking strategies for analyzing cases and processing data, including narrative construction and temporal bracketing, coding, and visual mapping (Langley, 1999; Yin, 2010). These strategies are "generic approaches, rather than step-by-step recipes or techniques" (Langley, 1999, p. 694). Finally, the researcher cycled iteratively through the strategies, focusing first on each case and then comparing the cases. Each PPP represented a case with organizations and activities as the focal unit of attention.

1. Organizing

The researcher began the analysis to organize and become deeply familiar with the data. Before designing the study, the researcher socialized the research by conducting exploratory inquiries with subject-matter experts. These initial discussions did not provide data for the analysis but helped to refine the research design and to familiarize the researcher with the context. The researcher took detailed notes and generated research memos after each discussion. Research memos are detailed notes that the researcher takes throughout the data collection and analysis to capture thoughts, as well as examine and reflect on one's engagement and developing ideas (Langley, 1999; Yin, 2010). The memos synthesized the researcher's takeaways from each discussion, her overall understanding of the context, changes in her understanding, and additional questions and focus areas.

Following the research proposal presentation and throughout the data collection, the researcher prepared transcripts and summaries as she collected data. The researcher consistently formatted the pieces of data and organized the transcripts and documents by case and time, eventually inputting all data into ATLAS.ti, a qualitative data analysis software. Following the completion of the interviews, the researcher carefully read the entirety of the data (interview transcripts and documents) and continued to prepare research memos. The memos became more focused on theory building as the analysis progressed.

2. Narrative Construction and Temporal Bracketing

Narrative construction involves writing a detailed account of events (Langley, 1999). The researcher constructed a temporal narrative of the progression of each PPP and prepared a detailed description of each PPP and a timeline of the events that transpired from the earliest initiation activities as described by participants through the formal establishment of each partnership. The narrative described each PPP's structure, governance, and membership and the events, actions, decisions, and actors that emerged in each case.

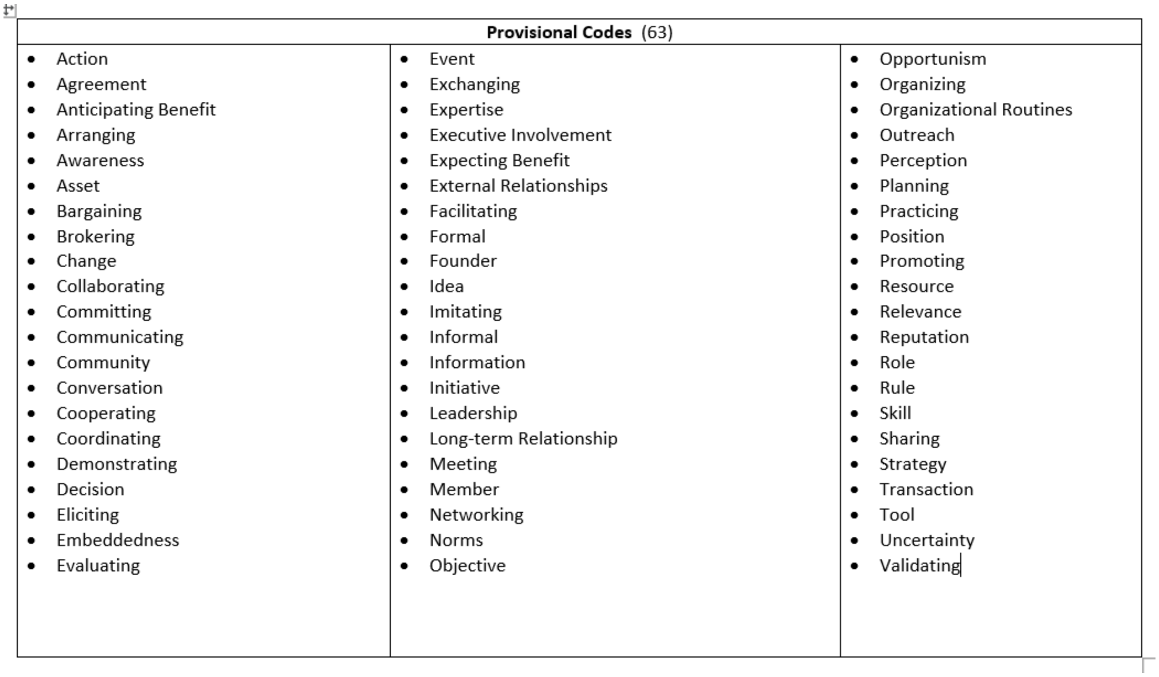
Temporal bracketing is an approach to process analysis that involves breaking a narrative or timeline into segments based on identifiable shifts or changes and then comparing the segments to understand temporal dynamics. The decomposition of data into adjacent sequential periods enables the detailed examination of how actions of one period led to changes in the context, which might influence activity in subsequent periods (Langley, 1999). Temporal bracketing is not meant to provide a predictable, sequential process but is a way of structuring the description of events to allow comparisons across different segments.

The researcher carefully reviewed each narrative and noted fundamental shifts to identify and bracket phases in each timeline. Then, within each case, the researcher compared the activities in the phases. Finally, following the within-case analysis, the researcher compared the phases between the cases.

3. Coding

The researcher coded the data using ATLAS.ti qualitative data analysis software. The researcher followed Langley's (1999) suggestion for using coding in process studies rather than conducting a grounded theory analysis. The purpose of coding was to create further familiarity with data and to identify and group actions, events, and decisions into categories to identify critical activities and outcomes for subsequent conceptualization and model building. Coding ran concurrently with and informed the other strategies. During the first coding round, the researcher coded in vivo, selecting text segments relating to actions, events, and decisions and labeling them using participants' words and phrases. The researcher then read through these segments and grouped them to develop a set of emergent codes, as shown in Table 2.

Table 2. Initial Codes



Provisional Codes (63)

- Action
- Agreement
- Anticipating Benefit
- Arranging
- Awareness
- Asset
- Bargaining
- Brokering
- Change
- Collaborating
- Committing
- Communicating
- Community
- Conversation
- Cooperating
- Coordinating
- Demonstrating
- Decision
- Eliciting
- Embeddedness
- Evaluating
- Event
- Exchanging
- Expertise
- Executive Involvement
- Expecting Benefit
- External Relationships
- Facilitating
- Formal
- Founder
- Idea
- Imitating
- Informal
- Information
- Initiative
- Leadership
- Long-term Relationship
- Meeting
- Member
- Networking
- Norms
- Objective
- Opportunism
- Organizing
- Organizational Routines
- Outreach
- Perception
- Planning
- Practicing
- Position
- Promoting
- Resource
- Relevance
- Reputation
- Role
- Rule
- Skill
- Sharing
- Strategy
- Transaction
- Tool
- Uncertainty
- Validating

Next, the researcher reviewed the data, iterating between the analysis strategies to group the initial coded text segments into 15 action categories. The categories with example quotations are shown in Table 3.

Table 3. Codes and Example Quotations

Actions	Quotations
Partner engaging	"So, we [the founding organizations] conduct a briefing on . . . , in a large conference room, inviting approximately 50 CISOs from public–private organizations."
Boundary spanning	"We built up a very rich, robust distribution list email over the last eight years. However, most importantly, we've gotten out of our offices to meet these people and shake their hands and have coffee to develop rapport within the community. Know these people by their first name and build that trust with these people."
Signaling	"That same month my boss [the] commissioner asked the question, 'What is the answer [to include] for the private sector?'" "So while the NYC Cyber Command Center has a great capability that they developed to monitor endpoints, they still need the ability to know the people."

Actions	Quotations
Anticipating benefit	Bringing the CISOs together “brings the public–private sector together, in concert with the [four] founding agencies, and we started running from there!”
Problem/ solution	Problem: “As a first responder to Ground Zero 21 years ago and being assigned to a cyber taskforce, for the last 9 years of my year career, I can say that we are in cybersecurity where we were on counterterrorism on September 10, 2001.” Solution: The founders “met with NYC organizations to talk with the NYC Cyber professionals about whether we needed something. Do we need a new association? Everybody’s answer was surprising: ‘Yes.’ And I think we all went in saying, ‘Well, there must be something that exists to achieve this goal, but maybe we, our office is not part of it.’ The answer we got back from the cybersecurity community within NYC [was] . . . ‘No, you need to do this, you need to create something!’”
Opportunity	“At that moment, the commissioner looked at me [one of the founders] and asked, ‘Why don’t we have a cyber command?’”
Skills/ knowledge (competence)	“We needed to have some of our best subject-matter experts to figure this out. So, the money was minimal. Representation included the big banks, service providers, and trade associations. Money was a small part of it. The bigger contribution came from the subject-matter experts.”
Role relevance (reputation)	“When it comes to sharing, CISOs are of critical infrastructure, whether it be transportation, power, telecommunications, you know we are talking about all 17 critical infrastructure sectors and to include the agency CISOs for NYC!” “When you start sending them relevant information like that, you, the sender becomes relevant!”
Network (social capital)	The founder said to himself as he looked at the CISOs meeting for the first time and realized, “‘Oh my, they don’t even know each other!’ So, within the first 60 seconds, this meeting is already a success! That was the unofficial start of the NYC-CCSI working group.”
Exchanging	“The 50 CISOs meeting each other was the first time these leaders were exchanging [business] cards, and that to us [founding organizations] was a success!”
Committing	When sharing information, “we send emails out. A CISO [chief information security officer] of a power company gets those and responds with, ‘Thank you for sharing this . . . and thank you for [sharing] the indicators of compromise. We will reform our firewalls immediately.’”
Bonding	“Representatives of 16 organizations came together for a cyber tabletop exercise. This . . . session, convened by the founders . . . , was a unique convention of cybersecurity professionals, and it highlighted the need to increase communication and prepare as a group.”

Actions	Quotations
Executing commitments	A founding member, subject-matter expert assisted the working groups with developing a new plan: “So, I helped them put together a business plan. In two and a half months, we came up with the approach.”
Assessing	As an outcome of the cyber exercises, a founder noted a need to establish partners through local volunteers: “Now we’re making our efforts public, as we look to create a team of teams among NYC’s local cybersecurity experts to share intelligence and provide a coordinated response to cyber-attacks. If you are one of those experts, the NYC CCSI is an unprecedented opportunity to serve and protect new and best practices.”
Imitating commitments	The founding organizations established “a real-time operational center to protect against cybersecurity threats; until last week, the two-year effort known as NYC CCSI was completely virtual.”

The researcher continued reviewing the categorized data, including the interview transcripts, research memos, and narrative descriptions, working to refine the categories to capture critical aspects of the process in the cases fully. The researcher then created a table mapping key actions, activities, and governance categories that emerged. Table 4 shows the final codes and map.

Table 4. Final Codes and Code Map

Actions	Activities	Governance
Partner engaging	Initiating interaction	Coordinating
Boundary spanning		
Signaling	Generating commitment(s)	
Anticipating benefit		
Problem/solution	Ideas (frames)	
Opportunity		
Skills/knowledge (competence)	Resources	
Role relevance (reputation)		
Network (social capital)		
Exchanging	Legitimizing partnership	
Committing		
Bonding	Designing & implementing	Collaborating
Executing commitments		
Assessing	Institutionalizing	
Initiating commitments		

4. Visual Mapping

A visual map displays the data as a graphic representation of the researcher's interpretations and findings throughout the analysis process. Visual mapping is a crucial step in enabling researchers to organize and discover connections and facilitating the conceptualization of insights from the data (Miles & Huberman, 1994).

The researcher relied on visual mapping throughout the analysis process and used it in conjunction with coding and temporal bracketing to identify links between codes (see Table 4) and phases in the progression of partnering. The researcher initially constructed simplified visual timelines for each case (see Figure 2).

An initial Stage 1 analysis drew on the case narratives and simplified timelines to generate a preliminary, simplified model of partnership adoption phases. Next, the researcher iterated through cycles of complicating and simplifying the timeline maps, drawing on the other analysis strategies and the literature. The researcher bracketed and labeled the timeline maps, cycling between the coded data and the literature and comparing within and between the cases. The researcher intentionally complicated the maps by adding labels from the literature and additional observations from the coded data to the timeline maps (see Figure 3). As Langley (1999) notes, "Process data are messy" (p. 691). The researchers sought to capture this messiness by intentially complicating the maps. Figure 3 presents an example of a more complicated map. The researcher then moved to simplify the complexity to generate a more conceptual depiction. She continued through cycles of complicating and simplifying, iterating between the emerging theory, the data, and the literature to develop a midrange theory (presented and explained in Chapter V) that describes how the focal organizations constructed willingness to partner.

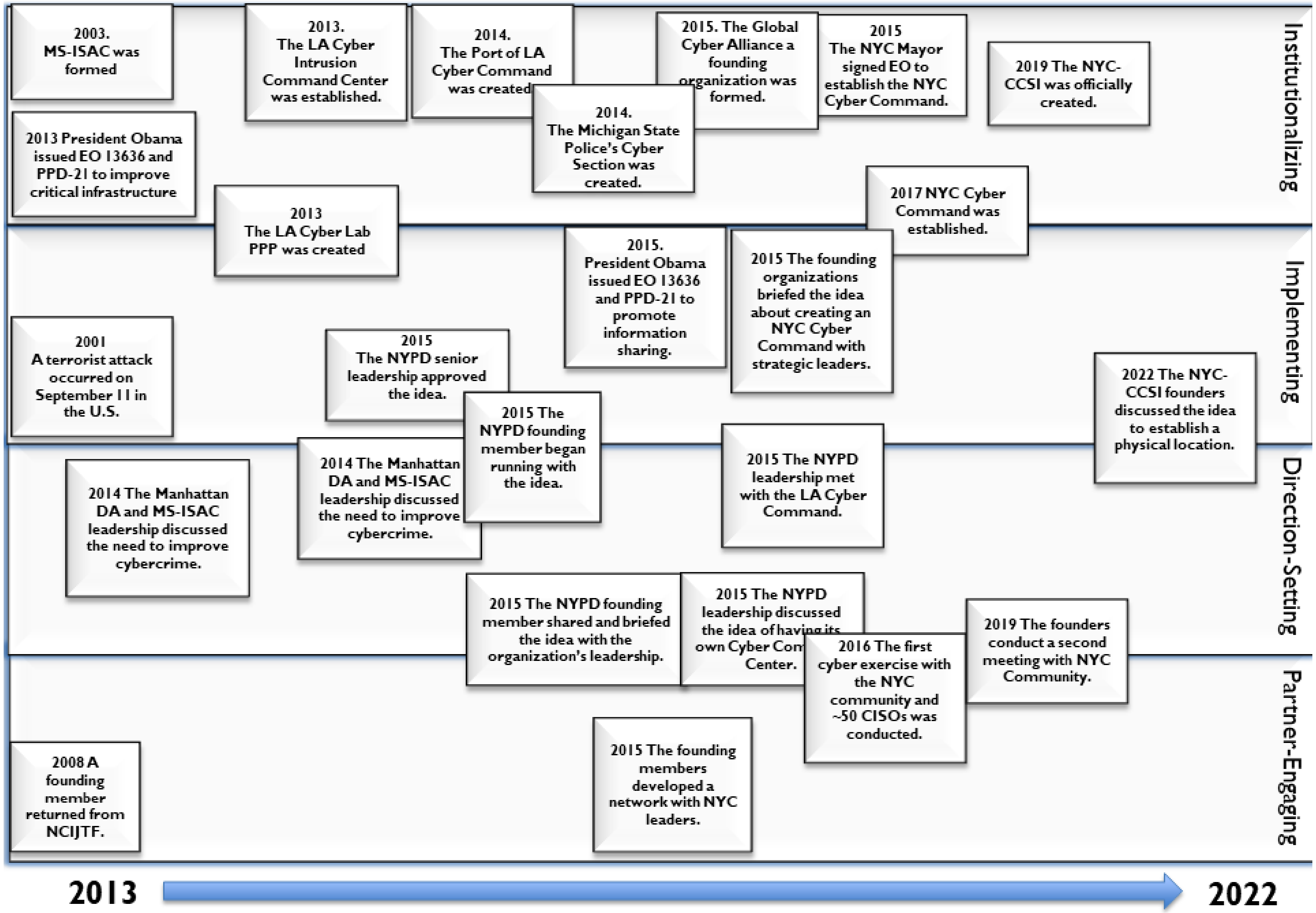

2003. MS-ISAC was formed
2013. The LA Cyber Intrusion Command Center was established.
2014. The Port of LA Cyber Command was created
2015. The Global Cyber Alliance a founding organization was formed.
2015 The NYC Mayor signed EO to establish the NYC Cyber Command.
2019 The NYC-CCSI was officially created.
2014. The Michigan State Police's Cyber Section was created.
2013 President Obama issued EO 13636 and PPD-21 to improve critical infrastructure
2013 The LA Cyber Lab PPP was created
2017 NYC Cyber Command was established.
Institutionalizing
2015. President Obama issued EO 13636 and PPD-21 to promote information sharing.
2015 The founding organizations briefed the idea about creating an NYC Cyber Command with strategic leaders.
2001 A terrorist attack occurred on September 11 in the U.S.
2015 The NYPD senior leadership approved the idea.
2015 The NYPD founding member began running with the idea.
2022 The NYC-CCSI founders discussed the idea to establish a physical location.
Implementing
2014 The Manhattan DA and MS-ISAC leadership discussed the need to improve cybercrime.
2014 The Manhattan DA and MS-ISAC leadership discussed the need to improve cybercrime.
2015 The NYPD leadership met with the LA Cyber Command.
Direction-Setting
2015 The NYPD founding member shared and briefed the idea with the organization's leadership.
2015 The NYPD leadership discussed the idea of having its own Cyber Com Center.
2016 The first cyber exercise with the NYC community and ~50 CISOs was conducted.
2019 The founders conduct a second meeting with NYC Community.
2008 A founding member returned from NCIJTF.
2015 The founding members developed a network with NYC leaders.
Partner-Engaging
2013
2022

Figure 2. Simplified Visual Timeline

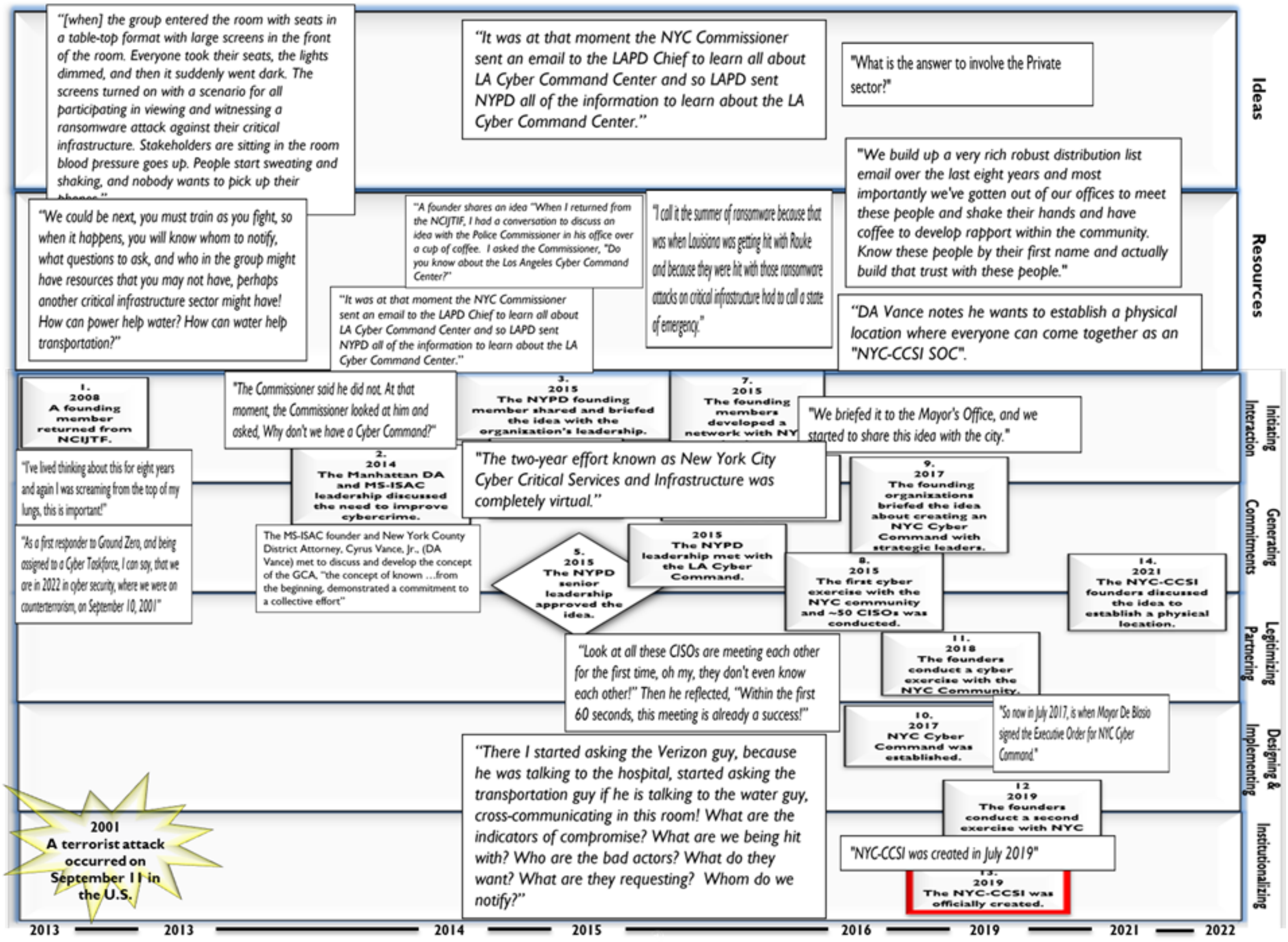

Ideas
Resources
Initiating Interaction
Generating Commitments
Legitimizing Partnering
Designing & Implementing
Institutionalizing
“[when] the group entered the room with seats in a table-top format with large screens in the front of the room. Everyone took their seats, the lights dimmed, and then it suddenly went dark. The screens turned on with a scenario for all participating in viewing and witnessing a ransomware attack against their critical infrastructure. Stakeholders are sitting in the room blood pressure goes up. People start sweating and shaking, and nobody wants to pick up their phones.”
“It was at that moment the NYC Commissioner sent an email to the LAPD Chief to learn all about LA Cyber Command Center and so LAPD sent NYPD all of the information to learn about the LA Cyber Command Center.”
"What is the answer to involve the Private sector?"
"We build up a very rich robust distribution list email over the last eight years and most importantly we've gotten out of our offices to meet these people and shake their hands and have coffee to develop rapport within the community. Know these people by their first name and actually build that trust with these people."
“We could be next, you must train as you fight, so when it happens, you will know whom to notify, what questions to ask, and who in the group might have resources that you may not have, perhaps another critical infrastructure sector might have! How can power help water? How can water help transportation?”
“A founder shares an idea “When I returned from the NCIJTIF, I had a conversation to discuss an idea with the Police Commissioner in his office over a cup of coffee. I asked the Commissioner, "Do you know about the Los Angeles Cyber Command Center?"
“It was at that moment the NYC Commissioner sent an email to the LAPD Chief to learn all about LA Cyber Command Center and so LAPD sent NYPD all of the information to learn about the LA Cyber Command Center.”
"I call it the summer of ransomware because that was when Louisiana was getting hit with Rouke and because they were hit with those ransomware attacks on critical infrastructure had to call a state of emergency."
“DA Vance notes he wants to establish a physical location where everyone can come together as an "NYC-CCSI SOC".
1. 2008 A founding member returned from NCIJTF.
"The Commissioner said he did not. At that moment, the Commissioner looked at him and asked, Why don't we have a Cyber Command?"
3. 2015 The NYPD founding member shared and briefed the idea with the organization's leadership.
7. 2015 The founding members developed a network with NY
"We briefed it to the Mayor's Office, and we started to share this idea with the city."
"I've lived thinking about this for eight years and again I was screaming from the top of my lungs, this is important!"
2. 2014 The Manhattan DA and MS-ISAC leadership discussed the need to improve cybercrime.
"The two-year effort known as New York City Cyber Critical Services and Infrastructure was completely virtual.”
9. 2017 The founding organizations briefed the idea about creating an NYC Cyber Command with strategic leaders.
“As a first responder to Ground Zero, and being assigned to a Cyber Taskforce, I can say, that we are in 2022 in cyber security, where we were on counterterrorism, on September 10, 2001”
The MS-ISAC founder and New York County District Attorney, Cyrus Vance, Jr., (DA Vance) met to discuss and develop the concept of the GCA, “the concept of known …from the beginning, demonstrated a commitment to a collective effort”
5. 2015 The NYPD senior leadership approved the idea.
2015 The NYPD leadership met with the LA Cyber Command.
8. 2015 The first cyber exercise with the NYC community and ~50 CISOs was conducted.
14. 2021 The NYC-CCSI founders discussed the idea to establish a physical location.
“Look at all these CISOs are meeting each other for the first time, oh my, they don't even know each other!” Then he reflected, “Within the first 60 seconds, this meeting is already a success!”
11. 2018 The founders conduct a cyber exercise with the NYC Community.
10. 2017 NYC Cyber Command was established.
"So now in July 2017, is when Mayor De Blasio signed the Executive Order for NYC Cyber Command."
“There I started asking the Verizon guy, because he was talking to the hospital, started asking the transportation guy if he is talking to the water guy, cross-communicating in this room! What are the indicators of compromise? What are we being hit with? Who are the bad actors? What do they want? What are they requesting? Whom do we notify?”
12 2019 The founders conduct a second exercise with NYC
"NYC-CCSI was created in July 2019"
13. 2019 The NYC-CCSI was officially created.
2001 A terrorist attack occurred on September 11 in the U.S.
2013
2013
2014
2015
2016
2019
2021
2022

Figure 3. Complicated Visual Map

THIS PAGE INTENTIONALLY LEFT BLANK

IV. STAGE 1 ANALYSIS: PARTNERSHIP ADOPTION

This chapter presents a description and initial analysis of each case. It concludes with a summary of the results of this initial analysis, a preliminary, simplified model that identifies partnership adoption phases. This preliminary model was an initial step. It does not explain the process through which organizations constructed willingness to partner but helped to build the researcher's understanding of the phenomena. The analysis resulted in a slight reframing of the research question and an analytical tool that guided subsequent analysis and the development of the final model, which is described in Chapter V.

The Stage 1 analysis revealed that following an initial catalyst, founders engaged in activities in five phases before their organizations entered a formal partnership: initiating interaction, generating commitments, legitimizing partnerships, designing, implementing, and institutionalizing, as shown in Figure 4.

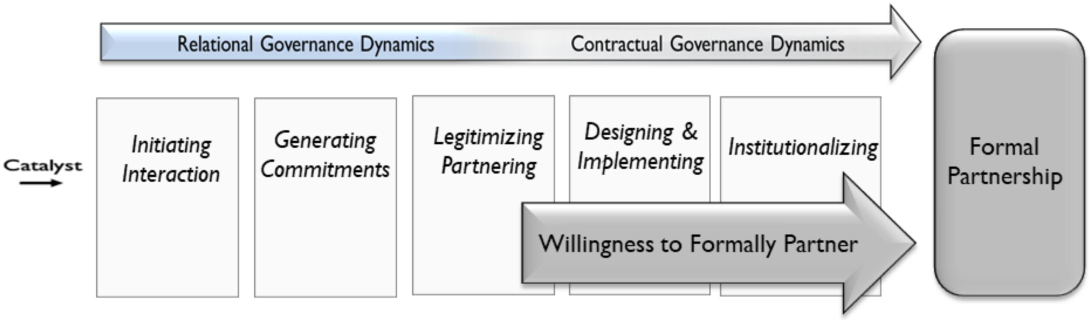


Figure 4. Preliminary Process Model

The following analysis outlines the five phases of activities that occur before formal partnering. The analysis indicates that partnering is constructed through activities over time. The analysis highlights that willingness to partner is continually constructed and reconstructed over time as individuals and organizations perform activities. This initial analysis resulted in a slight reframing of the research question—from the original How do organizations *become* willing to partner? to How do organizations *construct* willingness to partner?

A. NYC CYBER CRITICAL SERVICES INFRASTRUCTURE

CCSI was formally established in 2017 by four founding organizations: the Manhattan District Attorney's Office, the NYPD, NYC3, and the GCA. CCSI seeks to increase communication and awareness about cyber risks and to develop partnerships among public and private organizations. Activities that preceded formal partnering began in 2013.

1. Catalyst

In 2008, one of the early instigators of interaction (henceforth, Founder A) attended a course at the National Cyber Investigative Joint Task Force (NCIJTF) that focused on cybersecurity. During the course, Founder A learned about his peers' experiences and concerns, and two exemplar organizations focused on addressing cybersecurity concerns—the Los Angeles (LA) Cyber Command Center, established in 2013, and the Michigan State Police Cyber Command Center, established in 2014. These organizations showed how involving law enforcement in fighting cybercrime could enable cybersecurity. Founder A had served as a first responder following the devastating September 11, 2001 (9/11), attack on the Twin Towers, and memories of that day remained fresh in 2008 when he attended the course. He recalled the 9/11 attack while attending the training: "I have lived thinking about this for eight years, and again, I was screaming from the top of my lungs, 'This is important!'" Founder A's recollection of the 9/11 attack, combined with his path forward, suggested that the course provided a potential problem–solution set that catalyzed Founder A to identify opportunities for interaction.

2. Initiating Interaction

Later, in 2015, Founder A met casually with colleagues at the NYPD. Two leadership representatives from the NYPD and Founder A shared an idea he had been developing since the NCIJTF course. He recalled, "I had a conversation to discuss an idea with the deputy commissioner in his office over a cup of coffee. I asked the commissioner, 'Do you know about the LA Cyber Command Center?,' and the commissioner then asked, 'Why don't we have a cyber command?'" Founder A recalled, "It was at that moment [after the conversation] the NYC [deputy] commissioner sent an e-mail to the LAPD [Los

Angeles Police Department] chief [asking] to learn all about LA Cyber Command Center." Founder A began advancing the idea of a cooperative partnership, interacting with other NYC stakeholders to share the concept of a cyber command.

3. Generating Commitments

Founder A had gained the NYPD deputy commissioner's agreement that establishing an NYC command center would provide the valuable capability to enable cybersecurity within NYC. However, the NYPD deputy commissioner still wondered how to make it happen. Founder A explained while the idea of an NYC cyber command center was needed, the deputy commissioner still wondered, "What is the answer [that will allow us] to involve the private sector?" In response to the deputy commissioner's questions, leaders of four organizations that became founding members of CCSI drew on their developed network to gather 50 chief information security officers (CISOs). Founder A explained, "We built up a vibrant, robust distribution list. . . . Most importantly, we got out of our offices to meet these people and shake their hands, have coffee to develop rapport within the community. Know these people by their first names and build that trust with them." The meeting developed interest and trust among community members. Founder A noticed that the CISOs started to exchange contact information, making commitments to continue conversations and interactions with each other. Founder A was amazed and whispered to the leaders from the four organizations who had organized the gathering, "Look at all these CISOs meeting with each other for the first time. Oh my, they do not even know each other!" The leaders believed the gathering was a success.

4. Legitimizing Partnering

The initial gathering of involved CISOs became the unofficial start of NYC CCSI. In July 2017, NYC3, one of the four founding organizations, was preparing to be officially established. Before that time, NYC3 had not existed as an organization but had been officially recognized by the mayor of NYC. The founding organizations briefed the concept of the NYC3 to strategic leaders such as the NYPD commissioner, Mayor de Blasio's office, and other key NYC stakeholders. Founder A noted, "We briefed it to the mayor's office, and then we started to share this idea with the city." These conversations were shared across NYC. Soon thereafter, Mayor de Blasio signed the executive order initiating NYC3 (N.Y.C. Exec. Order No. 28, 2017).

5. Designing and Implementing

In November 2017, leaders from the four founding organizations announced the initiation of NYC CCSI as a PPP; however, it remained in development. The early PPP members knew a vital aspect of the PPP would be soliciting members and gaining their commitment to the coalition. In December 2018, NYC CCSI representatives organized a cybersecurity tabletop exercise with 30 cross-sector stakeholders to increase communication, provide awareness, and prepare as a community (Vance & O'Neill, 2019). Founder A described the experience:

> The group entered the room. The seats were arranged in a tabletop format, large screens in front, the lights dimmed, and then it suddenly went dark. Next, the screens turned on with a simulated scenario where participants began to experience a ransomware attack on their critical infrastructure. The participant's blood pressure increased, and nobody wanted to pick up their phones.

Leaders of the four founding organizations were elated and believed the cyber exercise had a profound impact. More significantly, they noticed cross-sector conversations among individuals representing various organizations. For example, a representative from a telecommunications company started talking to the hospital and then asked the transportation representative whether they were communicating with the water sector. Founder A recalled some of the questions exchanged: "What are the indicators of compromise? What are we being hit with? Who are the bad actors? What do they want? What are they requesting? Whom do we notify?"

6. Institutionalizing

During the summer of 2019, numerous ransomware attacks were reported among cities in Texas and Louisiana (Allyn, 2019). Members of the NYC CCSI referred to this season as the summer of ransomware. The events resonated deeply with NYC CCSI members; they leveraged them as learning opportunities to educate their community, thus prompting the NYC CCSI to conduct additional cybersecurity exercises. One participant recalled taking away that it was essential to know whom to connect with before a cyber event: “We could be next, and you must train as you fight, so when it happens, you will know whom to notify, what questions to ask, and what resources another critical infrastructure sector might have!” The NYC CCSI worked for more than two years to develop and formalize the PPP. The PPP eventually publicly announced a physical location for the NYC CCSI in downtown Manhattan (Paul, 2021).

B. CYBER HOUSTON

The Cyber Houston PPP was formally established in 2015. The organization seeks to build a community of public and private business and government cybersecurity leaders to engage in the region’s critical cybersecurity issues. The Cyber Houston PPP emerged from the GHP, an organization formed in 1989 that became the largest Chamber of Commerce in the Houston region (ISAO Standards Organization, n.d.-a). Activities that preceded the formal partnership began in 2014.

1. Catalysts

In 2014, the Enron scandal resulted in the 2002 Sarbanes-Oxley Act, which required business organizations to maintain and report financial records. Thereafter, business leaders were responsible for protecting their data and information technology networks. One early initiator of interaction (henceforth Founder B) recalled the evolving understanding of responsibilities: “In Houston, we saw all this unfold. All these changes transpiring [were] the beginning of cybersecurity because organizations now had to be concerned about two things—decrease the attack surface and reduce the in-network real-time—because it is not a matter of if but when you will be infiltrated.” The Enron scandal helped to create momentum for interaction. Founder B drew on the scandal to highlight a problem and the potential benefits of acting together—to initiate interaction with others.

2. Initiating Interaction

In 2014, Founder B was approached by a colleague, a CEO from an energy company, who wanted to discuss an idea. The CEO wanted to create a cybersecurity task force within the GHP. The purpose of the cybersecurity task force would be to educate senior leaders such as CEOs and board members within the Houston region about cybersecurity-related risks and to help them understand threats. Founder B thought his colleague's idea for the task force was an excellent way to address the cybersecurity concern within Houston.

3. Generating Commitments

Although Founder B thought creating a cybersecurity task force within the GHP was a brilliant way to provide education, Founder B was concerned that it might be difficult to gain support from other organizations. Founder B told his colleague, "I will need your support." Founder B recalled that the CEO responded, "Okay, let us meet again soon to share your thoughts." Then, over a couple of weeks, Founder B worked to develop the idea into a business plan. The next step was to present the plan to the GHP's CEO, and the partnership agreed to the plan. The GHP agreed that the cybersecurity task force would consist of hand-picked regional business leaders serving as subject-matter experts. Founder B recalled that his pre-existing connections to subject-matter experts helped to facilitate the plan's acceptance: "The key to establishing members . . . [was] being connected with business and community leaders within the Greater Houston region." The cybersecurity task force became the first step in the creation of the Cyber Houston partnership.

4. Legitimizing Partnering

During the subsequent year, the cybersecurity task force became a high-performing task force, comprising 70 members. But over the following three years, the demands on subject-matter expertise began to weigh on the GHP. This burden led the GHP's CEO to decide that the cybersecurity task force needed to move outside the organization and become a separate PPP. Founder B agreed to take on the task of developing a separate PPP, setting up initial funding and then connecting with sponsors to create the Cyber Houston PPP. Founder B explained how he engages others: "It is all done as good corporate citizens; we get that business and invest back in it. It is a simple Chamber of Commerce and a trade association model. I am doing it through the lens of civic leadership."

5. Designing and Implementing

As Cyber Houston began development, the founder's first idea was to educate Houston C-suite business leaders about cybersecurity. Founder B recalled the benefits of this approach: "The C-suite could enable communication to educate the whole community." In 2018, Founder B, with a team of other early members, collectively developed a website with cybersecurity tools that could be virtually shared among the community. One of the first tools developed was a framework and questionnaire (i.e., a cyber assessment tool) to help CEOs and the board of directors understand and quantify cybersecurity risk from a reputational risk perspective.

That same year—one year after Houston had experienced Hurricane Harvey—there was an opportunity to educate the community. The opportunity was the Jack Voltaic 2.0 (JV2) cybersecurity exercise (Bell et al., 2019). Founder B learned about the exercise from a member of the Army Cyber Institute at West Point. Founder B saw JV2 as an opportunity to share with the mayor of Houston and his advisors what might happen if a cybersecurity event occurred during a natural disaster like Hurricane Harvey. The mayor agreed to sponsor JV2 and dedicated a City of Houston representative to lead the activity. During the JV2 exercise, participants gathered in a room to discuss a scenario that demonstrated how public and private organizations must work together as a community when a cyber-attack occurs during a physical event like a hurricane. Participants at the event shared ideas and learned from each other.

6. Institutionalizing

In 2019, Founder B initiated the Cyber Houston Summit, which connected C-suite and senior executive leaders responsible for CI. The summit consisted of panel discussions and presentations to provide education on cybersecurity. Founder B recalled the benefits of the forum: "One of the essential things we have [in] our relationship with all the local educational institutions is [that] many are now members of this [Cyber Houston] coalition, which is essential to develop [ing] the future workforce."

Founder B's original ideas for Cyber Houston were accepted in 2016; then, in 2019, Cyber Houston officially became Houston's first ISAO (Cyber Houston, n.d.). Cyber

Houston's transition to operating as an ISAO further legitimized the PPP by demonstrating that it was part of the trusted cybersecurity community of ISAOs. Members felt this initiative allowed them to remain flexible enough to conduct mutual aid and information-sharing activities without formal agreements. For example, as one member explained, if an organization needed mutual assistance, a member could informally reach out to another member: "Someone can step in to help you or point you in the right direction; just being a member of Cyber Houston automatically gives them that member card for those types of resources." With an ISAO standing, Cyber Houston provides members with a more flexible way to share information than is found in ISAC information sharing. As the member explained, "I know it is okay to share with you, and I am willing to trust you because you are part of the Cyber Houston group." Cyber Houston's members formalized the partnership when they officially established the PPP as a DHS-recognized ISAO (Cyber Houston, n.d.).

C. CYBER MUTUAL ASSISTANCE PROGRAM

The CMA PPP was formally established in 2016 to provide "surge capacity" in support of individual companies, should a cyber-attack exceed their ability to respond, by developing relationships for resource sharing (Fehrman, 2016). Activities that preceded formal partnering began in 2014 among a group of CEOs known as the ESCC.

1. Catalysts

By 2015, numerous cyber-attacks, such as those in Ukraine, had drawn leaders' and the public's attention. One early initiator of CMA, William J. Fehrman, shared his perspective on the attack on Ukraine's electric distribution system. He noted that the attack emphasized "how serious any attack against critical infrastructure can be" and that "the Ukraine attack also demonstrated [that] security cannot be limited to protecting and defending systems; it requires a plan for responding and recovering when confronted" (Fehrman, 2016). This attack drew the attention of other leaders to the risks of cyber-attacks and served as a catalyst for interaction.

2. Initiating Interaction

Before the Ukraine cyber-attack, energy industry leaders had gathered to conduct the 2014 GridEx II exercise and discuss the need to develop a unified approach to cybersecurity (North American Electric Reliability Corporation [NERC], 2014). In 2015, energy-sector stakeholders continued discussions and began discussing the idea of using the concept of traditional mutual aid as a coordinated response during a significant cyber event. During a meeting with senior leaders, one of the CEOs of the ESCC suggested, “I think we as an industry need to respond in a supportive manner, and not just [share] for transformers but also [for] cyber-attacks.” The CEO’s idea stemmed from a perspective of traditional mutual aid practices whereby industry organizations share spare transformers. However, other leaders were hesitant about the idea. One of the founding members recalled, “Everyone in the room scratched their head while another said, ‘What are we going to do with that idea? You cannot do that in cybersecurity!’”

When the December 2015 Ukraine cyber-attack occurred, energy-sector leaders came to the conclusion that a similar devastating event could happen in the United States. The Ukraine cyber-attack was an illegal entry into an organization’s computer and supervisory control and data acquisition systems resulting in a series of outages that affected the electrical grid, leaving approximately 250,000 people without power (Electricity Information Sharing and Analysis Center [E-ISAC], n.d.-b; Stoddart, 2022). One early initiator of CMA recalled, “This attack underscored the need to act upon this discussion of the CMA” (Fehrman, 2016). In response to this event, the energy sector formed the E-ISAC and published the joint *Analysis of the Cyber Attack on the Ukrainian Power Grid* (SANS Industrial Control Systems & E-ISAC, 2016).

3. Generating Commitments

The idea to develop mutual aid into CMA eventually led government leadership to initiate communication with private-sector executives. By November 2016, industry-wide discussions emerged from discussions about the 2015 cyber-attack in Ukraine and conversations during the GridEx III exercise.

The GridEx III exercise was an executive tabletop exercise that brought senior industry and government leaders together and provided them with an opportunity to talk through a cyber-attack scenario and assess and improve upon current processes and procedures. Founder D described the senior executive tabletop: “Senior industry meets with senior government officials. Those conversations rely on discussions about how our industry has robust ways beyond traditional mutual assistance to respond if a major cyber incident impacted our ability to serve customers and affect the grid.” These discussions highlighted the need for an organization like CMA.

The ESCC’s leadership created the CMA task force to explore the idea (Fehrman, 2016; ESCC, n.d.). The activities of the task force eventually led to the evolution of the industry’s mutual assistance framework beyond traditional natural disasters. One founding member recalled, “Clearly, there were earlier discussions on cyber threats before that, but those two events [the 2015 Ukraine cyber-attack and 2016 executive tabletop exercise] drove people together to focus on something that needed to be addressed.”

4. Legitimizing Partnering

In 2016, CMA was officially launched as a program. The ESCC appointed the Edison Electric Institute (EEI) as the official program manager to represent and facilitate the design and implementation of CMA on behalf of the entire North American energy industry. The EEI’s role was to ensure that all perspectives from the community were included in the development of CMA. Regarding the organization’s role, one participant recalled one of the founding members sharing, “We want to make sure we have all those models [different ideas and perspectives] represented.” In addition, the EEI was tasked with assembling resources, such as experts in the field, necessary to develop relationships and legal frameworks, which began to legitimize partnering.

5. Designing and Implementing

Two years after the establishment of CMA, in 2018, the EEI began designing and implementing the formal partnership by gathering feedback from the entire community. In addition, EEI representatives facilitated the development of the CMA program by implementing subcommittees, leveraging the 2018 GridEx IV to develop standards and legal agreements and educating the community to provide awareness and build membership.

The EEI implemented subcommittees composed of experts to design and structure the CMA program. The subcommittees were elements within the program with touchpoints throughout the year to bring the program together. For example, during GridEx IV, the subcommittees developed standards and legal agreements. One founding member described how participants worked together to develop the legal agreements: “An organization would volunteer or be selected to play the role of a responder to work through the [CMA scenario] process so other organizations could learn.” As industry participants developed the program, they realized membership became a primary objective. Thus, an essential next step for founding members was to provide awareness and educate the rest of the community about the program. At a minimum, organizations willing to participate as CMA members had to consent to a mutual non-disclosure agreement and designate an individual with the appropriate cyber skills, experience, and authority (ESCC, n.d.).

However, many potential members were either reluctant or slow to join CMA. Founder D recalled another person voicing their concern: “[They said,] ‘We do not want to share our resources. A cyber incident resulting in a utility organization being attacked and impacted by ransomware may not have the resources for rapid restoration.’” Like mutual aid, one aspect of CMA is sharing resources among organizations during emergencies. However, a difference with CMA is that the organization in crisis might need a skilled person (e.g., a computer forensics expert). Initially, this notion concerned potential members, who thought they would be obligated to share valuable experts, but eventually, organizations realized that CMA did not require a commitment to do so.

Some organizations were faster to accept the idea of joining CMA for fear of possible mandates from regulators. One founding member (henceforth Founder D) recalled another member’s explanation of his organization’s interest in CMA: “[He explained], ‘It is because we fear the government, the regulator side, fear of what we are exposing by doing this.’” During this time, founding members of CMA who were senior leaders in their organizations (e.g., CEOs) stepped in to encourage slower-adopting organizations to join. Over time, slower-adopting organizations’ concerns were addressed by developing CMA standards and a legal framework. Founder D recalled, "[We said] let us have a standard set of templates for legal agreements so we can make lateral contracts with each other. We do not have to go to a master-level committee to activate it." These agreements structured the emerging partnership and served as tools that enabled organizations to reach out to fellow member organizations and request help.

6. Institutionalizing

CMA was built on the energy sector's traditional mutual aid practices that had developed over the past century in response to natural disaster events. CMA was formalized in 2018 but continued to evolve to include CSPs with other strategic alliances. Over time, the energy sector's executive leadership sought to involve and learn from outside perspectives. Moreover, ongoing cyber-attack events, such as the May 2021 Colonial Pipeline ransomware attack, reminded the energy industry of the value of cross-sector CMA participation. Thus, the energy sector continued to seek the involvement of more natural gas services. This expansion was reflected in the reports on the continuing tabletop exercises: "Compared with the GridEx V Tabletop . . . the discussion benefitted from the more robust participation of natural gas operators and natural gas trade associations in the United States and Canada, some of whom are part of the natural gas industry's National Mutual Assistance Program" (NERC & E-ISAC, 2022, p. 11).

D. CYBER RISK INFORMATION SHARING PROGRAM

CRISP was formally established in 2016, with the mission of enabling timely information sharing and analysis among energy sector–related public and private organizations to mitigate threats to cybersecurity. The activities that created CRISP began in 2014 with an initiative between the U.S. government's DOE and energy industry participants.

1. Catalysts

In 2012, a cyber-attack against the energy industry was significant enough to cause the DOE to notice and take action. During the 2012 cyber-attack on Saudi Arabia's Aramco oil firm, 30,000 workstations were struck by Shamoon malware (Dehlawi & Abokhodair, 2013). This event demonstrated the potential threat of a cyber-attack to the energy sector. The DOE has a critical role in supporting the energy industry. Following the Aramco attack, the DOE sought to develop a capability to enable information sharing and analysis with private industry organizations to mitigate cybersecurity threats.

2. Initiating Interaction

The Aramco attack catalyzed interest in forming a partnership involving the DOE and the private sector. In 2013, DOE leadership invited the energy industry to participate in a research-related pilot to improve information sharing, which led public-sector leaders to engage with private-sector senior executives. A participant recalled that the DOE had consulted with the ESCC to contact industry leaders, saying, “We are going to conduct a pilot, and we would like you to be part of the pilot.” The pilot involved the energy industry and Pacific Northwest National Laboratory (PNNL) representatives as subject-matter experts in leveraging a newly developed sensor technology to improve information sharing. This capability allowed information technology data to be collected and later analyzed to detect potential cyber threats (E-ISAC, n.d.-a).

3. Generating Commitments

Five private utility organizations were selected and agreed to participate in the newly formed pilot, initially referred to as the Energy Sector Networking Monitoring Program (E-ISAC, n.d.-a). The pilot consisted of the public entities’ providing private organization representatives with access to educational briefings about the capability. The pilot’s concept entailed having the participating private organizations deploy capability sensors on their networks. During the discussions, government and industry representatives developed collective understanding, trust, and appreciation of the pilot.

4. Legitimizing Partnering

The participating private-sector organizations agreed to install government sensors on their network as an experiment to assess the potential mutual benefit of the pilot. This experiment was deemed initially successful. One founder (henceforth Founder E) recalled thinking, “Hey, this has the potential to become the most effective form of public–private partnership!" The pilot bridged the gap between the public and private sectors because they now had an opportunity to share information to help mitigate a potential cyber-threat. Founder E, who participated in the pilot, shared a recollection of how the technology worked and mutually benefited participants:

> The principle is that you take characteristic network data from their network that is not privacy sensitive. It gives enough information to tell who is talking to whom, and you send that to a VPN [virtual private network] to PNNL. Then, they copy that to a classified network where they compare and can say, "We see a nation-state threat on your network." Then, they could create analytical products for us and say here is something we should take care of, but we may need to be able to tell you why, but we can tell you this is something you need to take care of.

The pilot was off to a good start when, suddenly, participants received a notification from the Department of Justice (DOJ) to cease the pilot. Founder E recalled the DOJ's notification message: "You cannot put sensors on private industry networks."

5. Designing and Implementing

The postponement of the pilot was a barrier, but it also presented an opportunity. The DOE and participating utilities worked together to overcome the hurdles that had stopped the pilot. They took several actions. For example, the term "sensors" could not be used; instead, participants adopted the term "information-sharing devices." Another activity involved clarifying that the DOE was not "collecting" information; participants "shared" the data. Last, the program had to display login banners noting the "U.S. government is monitoring," along with legal agreements. The pilot eventually re-emerged and was rebranded as CRISP.

The energy sector dedicated time to educating security leaders and the community about CRISP, which was essential in determining the most appropriate members for the emerging partnership. One challenge the founder faced was developing a suitable governance model. Founder E recalled that the question on everyone's minds was "How do you take a pilot program with five participating organizations and create a self-sustaining, self-funding program?" The larger utilities recognized CRISP as an investment, so they committed money and subsidized smaller utilities. CRISP used a standardized shared-cost model and services agreement (DOE, n.d.). Over time, the approach reduced the cost to participating organizations and improved the overall governance model. NERC and E-ISAC, energy-sector regulators, agreed to manage CRISP with organizations funding their participation (DOE, n.d.). The decision that NERC and E-ISAC would manage the program concerned some industry members, who feared sharing information could lead to mandates and fines. The energy industry addressed this concern by forming a governance committee. The E-ISAC's role was governing the outreach by serving as the primary security communications channel for the electricity subsector (E-ISAC, n.d.-b). PNNL handled all the technology, data sharing, and analytics shared with members within the energy-sector community.

6. Institutionalizing

After CRISP re-emerged, ongoing cyber-attack events, such as the May 2021 Colonial Pipeline ransomware attack, reminded the energy industry of the value of maintaining cross-sector participation in the program. As a result, energy-sector organizations agreed to expand CRISP by including the oil and natural gas sector (DOE, n.d.). Over time, this endeavor enabled the energy sector to launch Cybersecurity for the Operational Technology Environment, a similar program to facilitate information sharing.

E. SHELTERED HARBOR

Sheltered Harbor was formally established in 2015 with a mission of developing standards for the U.S. financial sector to maintain public confidence. The activities that initiated Sheltered Harbor began in 2014.

1. Catalysts

By 2014, numerous cyber-attacks, including the one to Ukraine's power grid, had drawn leaders' and the public's attention to the threat of cyber-attacks and had elevated concerns that the threat of attacks was intensifying. Leaders in the financial sector were considering the potential ramifications of cyber-attacks. The Sony hack resonated with financial-sector leaders, catalyzing their interaction. As noted by a chief information officer (CIO), "The Sony attack was a huge warning!" (Keenan, 2017).

2. Initiating Interaction

Following the Sony hack, a group of senior executives in the financial sector discussed the risk of a similar event in their industry and the possibility of including the Sony hack as a scenario in the Hamilton exercise. The Hamilton exercise series is a two-year joint U.S. government–financial services sector effort to enhance coordination related to cyber incident response (Maurer & Nelson, 2020). The series is intended to help government and sector stakeholders better prepare for and respond to a significant cyber incident in the financial services sector. The exercises explore issues from both "whole of government" and "whole of sector" perspectives. As one leader explained (henceforth Founder F), "A few of us thought, this time, when we run the Hamilton exercise, [what if we] take this [Sony] scenario to the community and ask the question, 'What if this were a bank or a broker? What would happen?'" The small group agreed that these questions were best addressed collectively during the next Hamilton exercise. The senior executives believed presenting a scenario like the Sony hack would connect members such as regulators and others within the community, provide awareness and education, and help to collectively develop a solution to improve security and resilience. Founder F explained, "It is important we have an answer in the direction that is equally important."

3. Generating Commitments

In 2015, the Hamilton exercise was held. As in previous iterations, participants gathered in a room to share ideas and feedback as they walked through the tabletop exercise scenario. This scenario, though, quickly revealed that everyone participating needed to prepare better. One participant recalled the CISO in the room saying, "This cannot happen to us!" The participant recalled, "Nobody in that group could provide a solution. Everyone said, 'We never thought like that!'" Participants concurred that this was not a problem that the financial industry could address through each organization working alone. The solution had to be a concept that key stakeholders were familiar with and trusted; they decided to leverage the concept of mutual aid.

4. Legitimizing Partnering

A significant outcome of the Hamilton exercise was that financial industry members and regulators agreed to put forward the idea of Sheltered Harbor. Nearing the end of 2015, in December, organizations began to commit resources to support the design of Sheltered Harbor. Preliminary resources included funding and participation of subject-matter experts. Founder F noted, “We had significant players in these working groups, and each of these institutions has a relationship with their customers.” The participating organizations perceived the costs as minimal compared to the significant benefit of pooling their most talented experts to develop Sheltered Harbor. As noted by Founder F, “We brought in our best subject-matter experts to figure this out.” Organizational leadership designated subject-matter experts to form three distinct working groups focused on banking, brokerage, and technology. The financial industry and government representatives converged quarterly during the joint meeting of the Financial and Banking Information Infrastructure Committee (FBICC) and the Financial Services Sector Coordinating Council (FSSCC). The industry’s board members were pleased to share with the regulators the news that they had started the working groups.

5. Designing and Implementing

In 2016, the FBI alerted the financial industry that an actor had been attempting to infiltrate its systems for over four months. The financial industry’s board-level leadership was concerned and frustrated. They were frustrated that regulators were taking the lead in solving the industry’s problems. The working groups needed help to make progress. Although many ideas were generated, board members could act on none of them. Board members sought another industry subject-matter expert and business leader to help advance the development of Sheltered Harbor. This individual would eventually lead the design of Sheltered Harbor. Founder F recalled the discussion of the idea with him, saying, “You are the kind [of person] we need who understands technology and the industry.”

Soon thereafter, Founder F had the opportunity to observe and listen to working groups as they presented their ideas. After three meetings, Founder F identified a theme among their collective thoughts: “It was pretty clear . . . what people were thinking [by their actions]: '[We needed] a way to store this data [securely in] some kind of vault.'" Founder F also identified a concern with the working groups' plan. He was concerned about Sheltered Harbor's role in collecting and storing data. He recalled, "As I listened to each of these working groups, particularly the technology working group, communicating how this data was going to be taken in by Sheltered Harbor, [it] was a red flag."

Founder F met with the board members to share what he had learned. He asked them, "Do you realize these workgroups assume Sheltered Harbor will be responsible for collecting all this data?" He recalled that he had warned them, "We could not get enough money to build the infrastructure to make this safe enough, and it would become the biggest target on the planet! We will never be able to protect it!" After discussing this matter, the board members agreed with Founder F and suggested that he work with the working groups to refine the plan.

Over the subsequent six weeks, Founder F assisted the workgroups in developing a new plan, and collectively, after two and a half months, they developed a new approach. Members of the working group formed a standards-setting body to design how the data would be protected and to implement the standards. Founder F noted this approach involved the Federal Deposit Insurance Corporation (FDIC): "Handing it to the FDIC, the industry [was] solving it for themselves and their customer." Industry leaders believed they should solve the problem, especially since they owned the data. Furthermore, Founder F emphasized that since financial institutions own their data, they should have the operational capability: "These institutions have a legal and moral responsibility to control the data." However, the financial industry still needed to establish trusted data vault standards.

During the next series of FBICC–FSSCC quarterly meetings, the group discussed the value of its idea to the public. After a few sessions, it developed an answer to the question "What does it mean to maintain public confidence?" In the summer of 2016, the industry presented its plan to regulators. The regulators viewed the plan favorably and agreed that the industry would own the certification standard and that regulators would develop the seal. The financial industry created Sheltered Harbor's unique restoration platform and data-vaulting standards and agreed to train regulators. Sheltered Harbor's vaulting standards are proprietary, so participants must be financial institutions or service providers.

6. Institutionalizing

In its development stage, Sheltered Harbor consisted of 34 board members. In 2017, during the next FBICC–FSSCC quarterly meeting, the regulators requested that the private sector train and certify its examiners; the financial industry agreed, and the Sheltered Harbor standards were implemented into the examiner handbooks (Recalde & Shook, 2021). As of 2018, financial industry representatives had trained 600 examiners from the FDIC, the Office of the Comptroller of the Currency, and the Treasury Department, to name a few, on Sheltered Harbor's certification standards. In addition, the financial sector viewed Sheltered Harbor as a collective approach to defining data-vaulting standards. Founder F noted, "The Sheltered Harbor brand is synonymous with data vaulting and its connection with resilience. All that was possible because of the public and private partnership!" Sheltered Harbor members also worked with consulting firms and the commercial industry to develop tools to put the data into the required standards (Maurer & Nelson, 2020).

A final step in the formalization of Sheltered Harbor was for the industry to work on developing membership. As institutions joined, they paid a fee based on a scale, so it was affordable. The founders of Sheltered Harbor began educating others in the sector about the PPP. The founders noticed that the formation of Sheltered Harbor had changed how CISOs viewed their role, as more sophisticated organizations had begun to employ chief resilience officers (McTarnaghan et al., 2022). One founder expressed, "This [Sheltered Harbor] all came about because we had the industry working together!" The collective work among founding members and participants enabled the Sheltered Harbor PPP to update the data-vaulting lexicon and standards to improve resilience within the financial industry. In 2019, Sheltered Harbor was formally established, institutionalizing the financial industry's collective approach to providing a reliable layer of security.

F. CONCLUSION

This initial analysis revealed that the founders of PPPs in this research drew on an initial catalyst. Founders engaged with others in initiating interaction, generating commitments, legitimizing partnering, designing and implementing the partnership, and finally institutionalizing the partnership.

In similar research, researchers have treated catalysts as events that resonate in an individual's mind and trigger a desire to connect to an idea (Garud & Karnøe, 2003; Pearce et al., 2022). In these cases, catalysts were salient events across potential partnership communities and generated interactions between at least two individuals. The event resonated with individuals in potential partner organizations, and individuals or groups then recalled and drew on the catalyst to call others to action.

Initiating interaction involves engaging with others to communicate an idea or opportunity (Besley et al., 2018; Penuel et al., 2013). In these cases, following the catalyst, founders initiated interactions by connecting with a catalyzing event while recognizing an opportunity or threat and engaging in coordinated activity with others inside and beyond their organizations.

Generating commitments began with the joint development of an idea. Individuals representing the organizations negotiated relationships for future potential membership and signaled a commitment to continue the interaction. They exchanged information and advocated a collective understanding and appreciation of the catalyst while seeking champions for that understanding. The collective understanding was co-created through brainstorming, generating, and articulating potential courses of action.

Legitimizing partnering helped to jointly advance the comprehension of a problem for which partnering served as a solution. In related research, researchers have suggested that organizations collectively utilize ideas and resources to legitimize actions, such as forming partnerships (Benford & Snow, 2000; Howard-Grenville & Hoffman, 2003). In these cases, representatives from various organizations shared their ideas and resources, enhancing their comprehension of partnership as a solution. They then formed committed relationships to maintain and further develop their collective understanding and connections. The founders' shared ideas and connections became intangible resources they could continuously rely on to legitimize the establishment of partnerships.

Designing and implementing began as the member organizations moved to formal agreements and contractual governance. The organizations collectively developed their shared commitment. They designed procedures and created and grew structures to ensure follow-through on agreements. They acted on agreements that required action, implemented commitments and partnering, and generated a membership apparatus to shape the structure and authorize efforts to implement the partnership.

Institutionalizing activities formalized the partnerships. The organizations structured and regularized ongoing interactions among stakeholders and often replicated elements of the partnership in other contexts. Partners reflected on the PPP's progress and assessed whether to sustain or end it: this assessment persisted after the partnership was formalized and activities continued. Over time, the new activities and practices became established as a new norm or convention.

This analysis has identified and described five phases of activities that precede formal partnering, suggesting that willingness to partner is constructed and reconstructed over time; there is not a single point in time at which willingness emerges. Instead, the social engagement that supports willingness continues throughout the development and into the operation of the partnership. This initial analysis resulted in a slight reframing of the research question and provided an analytical tool that identified the activities in the early phases of the partnering process, which are the focus of the analysis presented in Chapter V.

THIS PAGE INTENTIONALLY LEFT BLANK

V. STAGE 2 ANALYSIS: A CYCLICAL PROCESS OF CONSTRUCTING WILLINGNESS

This chapter describes the cyclical process by which founders and organizations in the focal PPPs constructed a willingness to partner in support of CI cybersecurity. The initial analysis resulted in a simplified model of the partnering phases or stages, which were the focus of subsequent Stage 2 analysis This chapter presents the results of the final stage of analysis and describes the cyclical process through which individuals and organizations in the focal cases constructed willingness to partner.

As shown in Figure 5, which depicts a cyclical model of constructing willingness to partner, the process commences with a catalyst that prompts relational partnering activities and initiates an activity path (illustrated by the winding arrow in the figure). The partnering activities become more formal over time as the founders and organizations construct willingness to partner. Founders and organizations in the PPPs engage in partnering activities with each other and potential partners, generating, and drawing on, partnering frames (shown at the top of the figure) and emerging commitments (shown at the bottom of the figure) to generate further action and the activity path. The frames include emulation, insight, and connection. Emerging commitments generate intangible resources including competence, reputation, and social capital. The activity path comprises three activity subprocesses: initiating interaction, generating commitment, and legitimizing partnering.

The first subprocess is initiating interaction, whereby individuals connect to a catalyst and frame an opportunity. The second subprocess is generating commitment, whereby individuals and groups generate commitments to share, champion, formulate, prototype, and test ideas. The final subprocess is legitimizing partnering, whereby groups and organizations formalize collaborative opportunities to negotiate and secure commitments (see Figure 5).

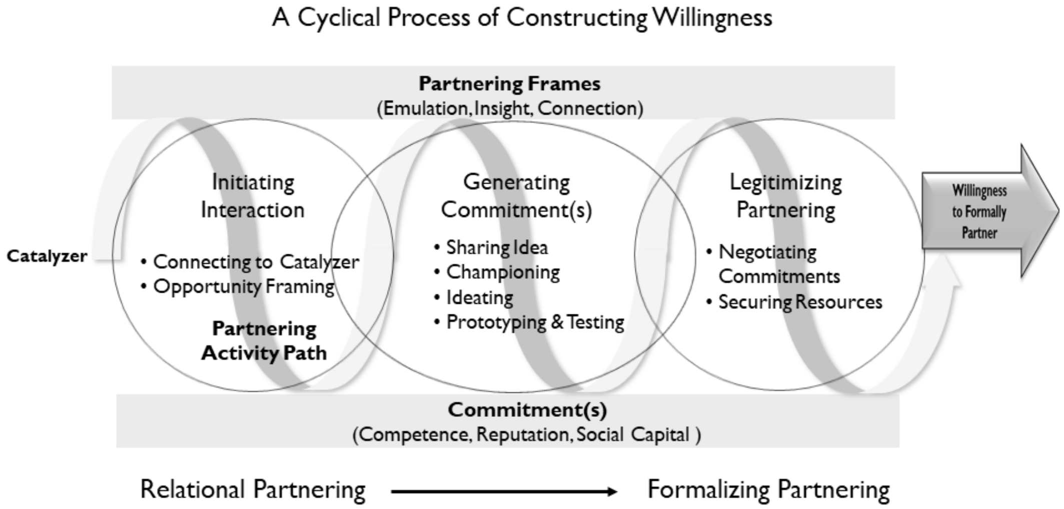


Figure 5. A Cyclical Process of Constructing Willingness

A. CATALYSTS, PARTNERING FRAMES, AND COMMITMENTS

As indicated in Figure 5, the process begins with a catalyzer that drives the initiation of interactions. In each case, the founders described a catalyst event, decision, or action that highlighted threats or opportunities. The founders attributed their desire or collective experience of engaging with others within and outside their organizations to a catalyzing event. For example, in the NYC CCSI case, the 9/11 terrorist attack was a catalyst that prompted a founder to act. In the Cyber Houston case, the Enron scandal prompted Founder B to act. In the CMA case, the Ukraine cyber-attack motivated energy-industry leaders to initiate discussions. Participants drew on partnering frames to initiate activities that generated initial commitments and then drew on commitments as resources for further activities. Frames and commitments are described in the following subsections.

1. Partnering Frames

Participants drew on partnering frames to encourage interaction and suggested ways of thinking, acting, and committing. Individuals and groups generated and drew on three partnering frames—emulation, insight, and connection—to construct willingness. The emulation frame presented interaction as an opportunity to imitate or surpass an existing practice or model or learn from the negative outcomes of others. The insight frame presented interaction as an opportunity to engage in activities to develop insights or knowledge. The connection frame set up interactions as an opportunity to associate with other individuals and organizations to build connections or social networks. The frames coexisted, and participants drew on them at different times to further interactions, as described in the subsequent sections.

a. Emulation

Emulation refers to mimicking or copying the behavior, attitudes, and communication styles of others. The emulation frame presents partnering as an opportunity to learn from and imitate successful partnerships in the domain or to avoid potential threats. It suggests that replicating the approaches and practices of successful partnerships, rather than trying to develop new and innovative approaches, could lead to successful partnering. This frame suggests that partnering individuals and organizations should connect with others in successful partnerships and emulate their actions. Participants in all five cases drew, at some time, on the emulation frame.

For example, in the NYC CCI case, Founder A referred to existing PPP models when he shared his idea with leadership. He recalled asking them, "Do you know about the Los Angeles Cyber Command Center?" He shared a second example, a panel presentation in which the NYPD had learned from the Michigan State Police that it had developed a team of cybersecurity professionals who worked together to establish better relationships between local law enforcement and municipality residents. According to Founder A, municipalities could benefit from having such a team of skilled professionals to address potential cyber threats and incidents, especially given their limited resources. The Michigan State Police started its own Michigan Cyber Command in 2013. Similarly, in the CMA case, Founder C shared that the CEO of the ESCC had suggested using the mutual aid concept to establish a comparable framework for cybersecurity. As related by Founder C, the CEO said, "I think we need a coordinated response [like mutual aid]. We as an industry need to respond in a supportive manner, and not just for transformers but also [for] cyber-attacks!" Last, in the Sheltered Harbor case, Founder F described how financial-sector leaders considered emulating the Sony hack scenario to educate others in the industry to avoid similar events. He explained, “The Hamilton exercises in 2015 took this scenario and asked the question What if this were a bank or a broker? What would happen?” The Sheltered Harbor case shows how the emulation frame was used to improve industry practices by learning from past events and simulations. Financial-sector leaders considered emulating the Sony hack scenario to educate others in the industry and avoid similar events. The emulation frame enabled financial-sector leaders to learn and improve, enhancing their ability to respond to challenges and adapt to changing circumstances, such as the Sony hack.

b. Insight

Insight refers to gaining a deeper understanding of engaged individuals, including their values, motivations, and goals. The insight frame presents partnering as an opportunity to learn from other organizations by gaining access to new ideas, perspectives, and information to which organizations or individuals might not otherwise have exposure. It suggests that organizations focus on the actions and behaviors of others that could, over time, help them acquire the unique knowledge of effective strategies and practices rather than relying solely on original and creative approaches. This frame suggests that partnering individuals and organizations develop intuition while connecting with successful organizations in the same domain to develop solutions. Participants in two cases drew on the insight frame.

For example, in the Sheltered Harbor PPP, the financial industry utilized the Hamilton exercise as a tool to gain valuable insight into the potential impact of cyber-attacks on neighboring organizations. In this instance, exercise participants changed their perspectives from a belief that such attacks could not happen to the realization that the industry lacked effective solutions to the problem. Founder F described the moment when participants perceived their experience: “Someone on the government side said, . . . ‘The [Hamilton exercise] got people thinking, changed the tone of the conversation with the industry.’ Everyone [participating in the room] said, ‘We never thought like that!’” The exercise prompted individuals to consider the potential impact of cyber-attacks on their neighbors, which had not been previously considered. In the CRISP case, the DOE suggested the idea of inviting the private sector to join the pilot program to share a newly developed tool designed to enable information sharing with the private sector. Founder C shared, “Someone in the DOE had this idea: ‘What if we shared this with the private sector? What if we used the same type of technology to put sensors on industry networks? . . . Could that have value?’” This instance indicated a new perspective or approach that might have led to greater collaboration and more effective responses to cyber threats. Participants drew on the insight frame to encourage activities to increase knowledge and understanding of the cyber landscape within a particular industry to make better-informed decisions.

c. Connection

Connection refers to developing mutually beneficial relationships with individuals and organizations. The connection frame presents partnering as an opportunity to establish and maintain successful long-term partnerships. It suggests cultivating mutually beneficial relationships with others that could lead to the development of social networks and successful partnerships. This frame suggests that partnering individuals and organizations associate with other reputable and successful individuals and organizations to develop social capital and establish partnerships.

For example, across all cases, potential partners shared similar interests with a common domain. For example, in the Sheltered Harbor case, the Hamilton exercise participants agreed that addressing certain questions collectively signaled an informal desire to work together to tackle common cybersecurity challenges. In both the Sheltered Harbor case and the CRISP case, senior leaders thought they could unite community members, increase awareness, and jointly find ways to improve security and resilience. Working with the private sector to tackle cybersecurity challenges was a common theme, reflecting a collaborative approach to establishing partnerships to address shared concerns. The connection frame suggests that by partnering, organizations may access valuable resources, both tangible and intangible, such as knowledge and expertise, which they might have otherwise been unable to obtain. The frame suggests that organizations can increase their competitiveness and effectiveness through connections established in partnerships.

The connection frame also suggests that organizations should partner to enhance their visibility and influence within their industry to open doors to new business opportunities.

Individuals and organizations began constructing willingness to partner following a catalyst event, decision, or action. Founders drew on the catalyst to generate partnering frames that presented opportunities and suggested actions and commitments. Over time, the actions created resources, including the initial commitments and frames that individuals continued to build and draw on, to support the construction of further willingness to partner through activities in the three subprocesses, as described later in this chapter.

2. Commitments

Individuals and groups generate commitments that serve as a crucial resource for achieving their goals. These commitments are intangible relational resources that evolve over time. As organizations seek to establish a partnership with other organizations in the initial stage, the organizations have different goals and priorities and may not fully trust each other. However, as they engage in collective activities and start to work collectively toward a common goal, they develop shared commitments. Over time, these commitments deepen and become more formalized. The organizations then establish joint governance structures and create dedicated teams to manage the partnership. In this sense, these commitments provide a framework and serve as resources for individuals and organizations to construct willingness in partnership formation.

Individuals and groups generate and draw on three critical intangibles—the relational partnering resources of competence, reputation, and social capital. Members of the organizations leverage these intangible partnering resources to manage situations and create additional resources through their collective activities at different points in time. All three of these partnering resources offer valuable intangible benefits that in turn drive the development of willingness.

a. Competence

Competence involves both skills and expertise and refers to the ability to effectively apply that knowledge in real-world situations. Competence as a partnering resource presents a benefit in offering to grow a potential partner's skill set, knowledge, and expertise. It suggests that enhancing competence can increase the perception of confidence within organizations. This resource suggests that partners seek individuals or organizations with a high level of skill and expertise to leverage their specialized knowledge, expand the partnership's reach and impact, and effectively achieve common goals. Participants in all five cases drew, at the time, on competence as a partnering resource.

For example, in the CRISP case, Founder C noted that the energy industry recognized the importance of collaborating with the government on the DOE pilot project. Founder C highlighted that the participating public and private organizations demonstrated competence by testing new initiatives through the pilot project, which was crucial in identifying and addressing potential issues and refining their approach before deploying it more widely. Moreover, the electricity industry acknowledged the value of collaborating with the government to learn from highly skilled professionals. As one participant noted, "PNNL has the technology, analytics, and skilled workforce." In the CMA case, Founders C and D recalled how the industry relied on the competence of field experts as resources to develop the needed legal frameworks. The legal framework was created through the collective activities of participating industry experts.

For example, Founder C of the CMA case described how the electricity industry leveraged the knowledge of field experts as resources to develop legal frameworks. Similarly, Founder F of the Sheltered Harbor case described how the financial industry leveraged its competent professionals to establish design teams: "We needed to have some of our best subject-matter experts to figure this [how to design Sheltered Harbor] out. Money was a small part of it, [but] the bigger contribution came from the subject-matter experts." These two examples illustrate how industries use intangible resources such as competence to navigate situations, distinguishing them from those that have not invested in such resources. Thus, the organizations' and their members' competence in creating and leveraging resources can significantly impact their effectiveness in responding to any given situation.

b. Reputation

Reputation refers to the opinions, beliefs, and perceptions that others hold about a person, organization, or entity. Reputation as a partnering resource presents a potential benefit in that a partner organization enhances its own reputation through association with a partner's image or organizational brand. A good reputation can increase organizational credibility and social capital. Partnering organizations that prioritize maintaining a positive reputation are capable of building better relationships with stakeholders to enhance the success of the partnership. Participants in all five cases drew, at the time, on reputation as a partnering resource.

For example, the CEO and chairman of Sheltered Harbor said to Founder F, "You are the kind we need, someone who understands technology, the industry, and can make something happen." Founder F was enlisted to advise and assist the design teams in creating Sheltered Harbor, based on their trust in his reputation for delivering results. This example demonstrates the value of reputation as an intangible resource, which helped foster trust and credibility between Founder F, the design teams, and the financial sector as a whole. It is likely that Founder F's positive reputation, built on his deep understanding of both technology and the industry, played a key role in this process. The case of NYC CCSI highlights the crucial role played by a positive organizational reputation in enabling collaboration and achieving common objectives. In this case, while the reputation of the four founders was certainly important, the positive reputation of the organizations they represented served as a key asset in advancing the NYC CCSI and likely contributed to its eventual success. For example, each of the four founding organizations—the NYPD, Manhattan District Attorney's Office, GCA, and NYC3—was a unique organization with an established reputation and capability.

c. Social Capital

Social capital refers to the benefits obtained through individual relationship connections, social reach, and networks that increase organizational visibility and influence and, thereby, can facilitate cooperation and collaboration. Social capital as a partnering resource offers potential benefit to mobilize resources powerfully and rapidly and encourages trust, cooperation, and a shared understanding. Participants in all five cases drew, at the time, on social capital as a partnering resource.

In the NYC CCSI case, Founder A recalled the unofficial beginning of the working group, saying, "We invited about 50 CISOs from public–private organizations. Then, I noticed the CISOs start sharing contact information with each other." Surprised to realize that these individuals did not know each other before the meeting, Founder A thought to himself, "Oh my, they don't even know each other!" Despite this lack of familiarity, within the first minute of the meeting, the sharing of contact information had already made the event a success. Founder A's example emphasizes the crucial role of social capital as an intangible resource. Specifically, the founders used their social connections to bring together approximately 50 CISOs from public and private sectors and enabled them to meet and exchange contact information. This accomplishment demonstrated the potential impact of social capital in promoting and achieving cross-sector collaboration and building new relationships among diverse groups. The value of social capital in forming the Cyber Houston task force was also demonstrated through the founder's connections. As Founder B noted, "So, with my corporate background, I have a lot of connections within the cybersecurity world with business leaders: CIOs, CISOs, and CEOs." By leveraging their extensive network of contacts, Founder B assembled a team with the necessary expertise and resources to effectively begin addressing the cybersecurity challenges facing the Houston community. This example highlights how social capital can be utilized as an intangible resource to foster collaboration and achieve shared objectives.

Effective PPPs require a diverse range of competencies, including technical expertise, financial management skills, communication and negotiation skills, and the ability to manage complex relationships and stakeholder interests. The development and sharing of these competencies are essential to building the willingness of PPP stakeholders to work collaboratively toward a shared goal. Overall, competence, reputation, and social capital as relational intangible resources are an important factor in constructing willingness in PPPs because they provide stakeholders with the knowledge, skills, and expertise required to effectively contribute to the partnership and work collaboratively toward achieving a shared goal.

B. THE ACTIVITY PATH THROUGH THE SUBPROCESSES

Within the process model, there are three subprocesses: initiating interaction, generating commitment, and legitimizing partnering. Figure 5, which depicts an activity path through each subprocess, illustrates how individuals and organizations seek to engage in partnering activities with others and achieve successful outcomes. The first subprocess, initiating interaction, involves identifying opportunities and connecting with potential partners. The second subprocess, generating commitment, involves building support and momentum around shared ideas and goals. The final subprocess, legitimizing partnering, involves formalizing the partnership and negotiating commitments. By following this activity path, individuals and organizations enhance their ability to succeed in their partnering efforts and achieve their shared goals more effectively.

1. Initiating Interaction

In each case, an individual or group initiated interaction by connecting to a catalyzer and connecting to an opportunity. Individuals and groups engaged in activities, drawing on partnering frames and making initial commitments. These activities, partnering frames, and initial relational commitments served as intangible resources, which supported further activities and, eventually, more formal commitments.

Connecting to the catalyzer involves initiating interaction and collaboration by individuals' drawing attention to a catalyst event and reflecting on its potential impact. For example, in the Cyber Houston case, Founder B referred to the Enron scandal as a catalyst based on his experience in data security. The Enron scandal prompted a greater emphasis on compliance but also highlighted the need for more robust cybersecurity measures. In another example, the CMA case, Founders C and D shared the story of a well-respected CEO with extensive experience in the energy industry. After learning about the impact of the cyber-attack on Ukraine, the CEO recognized the importance of being more proactive in protecting and defending the industry's infrastructure. Thus, individuals or groups acknowledged a connection between their organization or community and the catalyst, reflecting on how the situation could affect them or their organizations and suggesting the catalyst could lead to similar effects on others.

Connecting to opportunity involves individuals and groups finding ways to collaborate. The individuals or groups in the five cases articulated the potential of collaborative activities as opportunities for or means of mitigating threats. For example, from the NYC CCSI case, following the 9/11 terrorist attack, Founder A perceived an opportunity to avert future tragic incidents in NYC. Founder A reached out to his leadership to share his idea to discuss an opportunity. Founder A recalled the meeting with his NYPD leadership over a cup of coffee as an exciting moment. Founder A asked his leadership, "Do you know about the LA Cyber Command Center?" At the time, the NYPD's top brass was unaware of it, but after Founder A explained the idea, he and his leadership imagined the type of capability a cyber command would bring. The conversation sparked the notion of NYC's having a similar ability to ensure critical systems, such as transportation and utilities, remain operational in the face of a cyber-attack. It was an opportunity, echoing the 9/11 terrorist attack, that highlighted the need for action. At that moment, the NYC commissioner sent an e-mail to engage with the chief of the LAPD to learn all about the LA Cyber Command Center. Thus, the LAPD shared with the NYPD information to learn about its Cyber Command Center. Founder A's leadership realized that this opportunity could provide the protection that NYC sought. The leaders saw an opportunity to eradicate this sense of vulnerability by seeking out and engaging with others who shared similar goals to join forces and ultimately form a partnership in preventing such tragedies from happening again.

2. Generating Commitments

Commitments form through a generative process that involves four subprocesses: sharing, championing, ideating, prototyping, and testing. In each case, individuals and organizations engaged in activities, drawing on partnering frames and generating commitments with potential partners both within and outside their organizations. These activities, partnering frames, and relational commitments served as intangible resources, which supported further activities and eventually more formal commitments. The process of generating commitments involved sharing, championing, ideating, prototyping, and testing. In this way, the next step in the process set the stage for the formalization and legitimization of partnerships.

Sharing an idea involves the activities of imparting knowledge between two or more individuals. In the example of the Cyber Houston case, Founder B recalled, “A fellow CEO [who represented a different sector] suggested to me [that] we begin a cybersecurity task force.” This fellow CEO, from a different sector, had suggested starting a cybersecurity task force to educate executive-level leaders in the region on cybersecurity risks and potential threats. This interaction was more than just sharing information; it was an offer to collaborate toward reducing the risk of cyber-attacks in the city and helping CEOs safeguard their organizations from potential harm. Founder B recognized the value of this offer and saw an opportunity for collaborating to achieve the shared goal of increasing cybersecurity awareness in the region.

Championing involves the activities of individuals who advocate a collective understanding and appreciation of the catalyst, opportunity, or threat and strive to gain support from those who comprehend the situation. For instance, in the case of Cyber Houston, when Founder B and a colleague discussed the idea of creating a cyber task force, Founder B expressed his concern: “So, I said that [a cybersecurity task force] was all great, but I am going to need your support!” However, his colleague responded positively and asked for Founder B’s thoughts on the idea. A few weeks later, Founder B felt confident enough to start planning the idea. In this scenario, Founder B was passionate about implementing a new sustainability initiative in the organization. He and his colleague knew that it would require significant changes to current practices and would likely face resistance from some team members. However, Founder B believed in the importance of the sustainability of resources and was committed to making it a priority for the organization. Thus, they began championing the initiative by sharing their vision with colleagues and seeking support from key stakeholders. Over the course of several weeks, Founder B met with other colleagues to discuss the initiative’s potential benefits and solicit their feedback and ideas for implementation. He also connected with external experts and organizations to learn best practices and gather additional support for the initiative. Through ongoing efforts, Founder B built a coalition of supporters for the sustainability initiative and ultimately achieved its successful implementation.

Ideating involves the activities of generating alternatives, co-creating, and articulating potential courses of action by two or more individuals. In the context of the Cyber Houston scenario, Founder B and a fellow colleague's task force idea developed through an exchange of thoughts, leading to the creation of a cybersecurity task force plan within the GHP. Another example presented within the CMA case regarding the ideation process, according to the recollections of Founders C and D, involved a collective effort among various organizations within the industry to identify the industry's needs and develop a program to address them. They particularly emphasized the importance of designing the "necessary legal frameworks" to support the program and leveraging the industry's strengths and resources.

Ideating involves the activities of co-creating and articulating potential activities or courses of action by two or more individuals. In the context of the Cyber Houston scenario, Founder B and a colleague engaged in ideation and exchanged thoughts that led to the development of a cybersecurity task force plan within the GHP. Similarly, Founders C and D described how organizations within the electricity industry worked collectively to identify their needs and design the "necessary legal frameworks" to structure the CMA program. The process leveraged the industry's strengths and resources. These examples also highlight the importance of ideation in developing innovative solutions to complex problems through collective efforts.

Prototyping and testing involve the collective activities of two or more individuals to explore and assess a potential idea. Founder B and a colleague worked to create the business plan over several weeks and sought feedback to refine and improve it—akin to iterating and refining a physical prototype. They then presented the plan to the CEO, who recognized its potential and endorsed it, leading to the formation of a cybersecurity task force that could address cybersecurity challenges in the Houston region. In another example, the Sheltered Harbor case, industry representatives presented a restoration plan to regulators, which later served as the prototype for the resilience plan. The plan was tested during the Hamilton exercise, which involved the participation of regulators, and the restoration plan received unanimous support from all regulators, who considered it the perfect solution. According to Founder F, the execution of the Hamilton exercise resulted in a “resounding success,” with every regulator unanimously agreeing that the restoration plan was precisely what the industry required.

In summary, the cases highlighted the crucial role of generating commitments in building willingness toward forming a partnership. This process involves collectively sharing knowledge with potential partners to create a shared understanding of the opportunity or threat. Through activities such as sharing, championing, ideating, prototyping, and testing, individuals and organizations can work effectively together toward a common goal. Establishing commitments forms the basis of support.

3. Legitimizing Partnering

Each case involved organizations’ legitimizing their partnership by negotiating commitments and securing resources. Members of these organizations engaged in activities and drew on partnering frames to establish their commitments. Legitimizing partnering refers to the activities in which organizations actively work within a subprocess to validate and formalize collaborative opportunities by demonstrating the acceptability of partnering. Legitimizing commitment involves reinforcing the credibility and validity of an organization’s promises.

Negotiating commitments involves the joint activities of organizations to establish and reinforce the validity and credibility of their promises to one another. In all five cases, public and private organizations progressed toward establishing standardized practices. For example, joint exercises, such as GridEx and Hamilton, were used as tools to negotiate commitments collectively. These activities and exercises helped organizations develop standardized practices and routines that facilitated the construction of commitments. In the Sheltered Harbor case, the financial industry established certification standards to prove its legitimacy. In the Cyber Houston case, the founder and committee members worked across multiple organizations in the Houston region to provide awareness and education about cybersecurity threats to senior executives. This effort ultimately led to the creation of a yearly summit for Cyber Houston, which standardized a way to communicate the outcomes and value of the partnership to members and potential members. Within this subprocess, organizations negotiate commitments and secure resources. Thus, these organizations have worked to establish standardized practices and communication methods to improve their effectiveness and legitimacy. Within this subprocess, organizations negotiate commitments and secure resources.

Securing resources involves the collective activities taken by organizations to obtain and allocate the necessary assets, capabilities, and other resources to support their collaborative efforts. As Founder F pointed out, "Banks want to be able to put a seal up like the FDIC." Going on to describe how the PPP established standards, he said that in addition to having an official seal, "we [Sheltered Harbor] also helped to define what a secure data vault look [ed] like. All that was possible because of the public and private partnership." The development of the Sheltered Harbor seal and inclusion in the FDIC's examiner handbook is an example of the commitment of participating public- and private-sector stakeholders in securing the necessary resources through coordination and collaboration. This collective effort not only exemplified the legitimacy and credibility that could be achieved through effective public–private partnerships but also helped to enhance the resiliency of the financial sector in the face of cyber threats. For example, within the CMA case, Founder D said,

> We are sustaining a community now and continue to reach out to new [CMA] members. It used to be just electricity, but we've opened it up. We've recognized that natural gas is part of our supply chain, and especially in our footprint, much of our fleet has switched over to natural gas. We recognize even though we don't interconnect with them and do things with them on a daily basis, a cyber-attack on them could impact us and all of the utilities.

This example describes how the electricity sector evolved over time to establish commitments by securing resources beyond its own strategic alliance and reaching out to new members to expand the CMA PPP. Founder C's example highlights the interconnectivity and interdependence between different utility stakeholders in the supply chain and the potential impact of a cyber-attack. It underscores the importance of recognizing the broader impact of one's actions and investments on the environment, and how securing resources can help build partnerships and mitigate risks.

C. SUMMARY

In conclusion, this chapter described the cyclical process through which the individuals and organizations in the focal cases constructed a willingness to partner in PPPs for cybersecurity in CI. The process described in this chapter comprises three subprocesses: initiating interaction, generating commitment, and legitimizing partnering. Each subprocess involves activities and draws on partnering frames and commitments. The partnering activity path generates intangible relational resources and partnering frames and commitments, which also become resources available to support increasingly formal commitments.

VI. DISCUSSION AND CONCLUSION

This study makes three key contributions to the literature on PPPs. First, it challenges the prevailing perspective in the literature on PPPs—that willingness is fixed or static—and it argues for a new definition to better capture the processes by which organizations become willing to partner. Second, it highlights the usefulness of activity theory as a means of exploring this newly defined concept of willingness. Third, the study presents a processual model that describes this new understanding of willingness. This chapter discusses the implications of these findings for both existing and future research in this area. It also considers the limitations of this research and provides recommendations for future studies.

A. RECONCEPTUALIZING WILLINGNESS: CHALLENGING THE PREVAILING PERSPECTIVE

In this research, the concept of willingness was explored at the organizational and inter-organizational levels of analysis and defined as dynamic commitments constructed over time. For humans to establish agency and for organizations to establish partnerships, they take actions that are demonstrations of willingness. Willingness is not a fixed state but rather a continuous process that requires ongoing efforts to build and strengthen partnerships. The dynamic construction of willingness to partner is influenced by evolving partnership commitments, partnering frames, and intangible, relational resources. This process occurs in broader social, organizational, and inter-organizational contexts. Partnering here means commitments between organizations to shared objectives or formalized inter-organizational commitments that are legitimized and institutionalized.

Most of the existing research on willingness focuses on fixed or static perspectives at the individual or organizational levels of analysis. This study has emphasized the importance of dynamic influences that shape willingness at the inter-organizational level. This research focuses on the interactions and negotiations within and between organizations that relate to developing formal partnerships. It includes the broader social and organizational cultural norms that impact these interactions. This study emphasizes that willingness is not a one-time event but rather a continuous process that builds over time. This observation implies that will must be ongoing and continuously constructed, even after formal partnering, for PPPs to be successful. Recognizing the constructed and ongoing nature of willingness can help organizations position themselves to form and sustain successful partnerships. Ultimately, this research highlights the interconnectedness and complexity of the process of constructing willingness and underscores the importance of ongoing efforts to maintain and strengthen partnerships over time.

B. EXPLORING THE CONCEPT OF WILLINGNESS THROUGH ACTIVITY THEORY

Activity theory was a useful framework for comprehending the complex relationships among actors, tools, and environments in partnership development. The use of activity theory revealed three activity subprocesses: initiating interaction, generating commitment, and legitimizing partnering. Activity theory suggests that constructing willingness to partner begins with initiating interactions, which marks the beginning of partnership formation. Once partners interact, they engage in generating commitments by negotiating and coordinating to establish a shared vision, tasks, and goals. The analysis in this dissertation has highlighted activities for legitimizing commitments. It suggests that these commitments are essential to formalizing collaboration as a social activity system that enables partners to develop and work toward shared objectives.

In exploring the concept of willingness through activity theory, three key points emerged. First, activity theory enables the analysis of willingness at multiple levels of analysis, including individual, group, organizational, and inter-organizational levels. This observation provides a more comprehensive understanding of the factors that influence partnership formation and development. Second, while activity theory is a robust framework, it may overlook micro-level interactions and the emotional factors that motivate an individual’s willingness to partner. Finally, despite its limitations, activity theory offers a valuable lens for exploring the complexities of willingness and informs the design of more effective tools and environments to support successful partnerships. In conclusion, activity theory provides a valuable framework for understanding the complex relationships among actors, tools, and environments in partnership development. By using this framework, researchers may gain a more nuanced understanding of the processes underlying partnership formation and development.

C. PRESENTING A MODEL THAT DESCRIBES THIS NEW UNDERSTANDING OF WILLINGNESS

This research contributes a conceptual model for exploring willingness as a dynamic and evolving process (see Figure 5 in Chapter V). The cyclical process involves a catalyst, partnering activities, and the development of emerging partnering frames, intangible resources, and commitments that lead to more formal partnerships over time. This contribution to the literature on PPPs offers a more comprehensive and dynamic model of how partnerships form over time. The model leads to an emphasis on the importance of ongoing efforts because willingness is framed as a continuous process. The findings highlight the importance of shared frames, intangible resources, commitments, and activities for promoting successful partnerships.

Overall, the model sheds light on the relational dynamics that enable successful partnerships. The conceptual framework needs to be extended to other partnerships in the CI cybersecurity field to see whether it maintains some fidelity in describing and understanding those relationships. It also may be useful to highlight the critical role of founders as leaders in facilitating the willingness construction process. It may provide insights for practitioners and policymakers involved in PPPs. Overall, it may serve to create a perspective that highlights the need for organizations to be flexible in constructing partnerships and responsive to the changing needs and expectations of their partners.

D. DISCUSSION AND IMPLICATIONS

This section discusses key takeaways that can inform partnering strategies and leadership practices as well as possible implications and applications of constructing willingness. Two key implications for practice are discussed in the following paragraphs. First, leaders should actively focus on practices that facilitate willingness construction. Second, they should recognize the importance of intangible resources in partnership development and strive to develop and deploy these resources. The analysis of the participants' experiences in this research suggests that by adopting these practices and strategies, organizations can construct and maintain willingness to partner. This observation will help build strong, lasting partnerships to support the cybersecurity of CI and meet the challenges of an ever-changing landscape.

First, leadership activities that foster the construction of willingness to partner can be an asset for organizations seeking to achieve CI cybersecurity. These activities involve practices such as adopting specific strategies and actions that promote shared frames, commitments, and collaborative interactions. By prioritizing such practices, leaders can play a crucial role in shaping their organization's culture and success in partnering. Facilitating willingness construction can help create a shared understanding of the role of partnering in the organization's vision and objectives, which are essential for achieving successful partnering (Jacobson & Choi, 2008). These practices can lead to increased employee engagement in collaborative activities and productive and innovative partnering. The participants' experiences suggest organizations that prioritize the construction of willingness to partner can create a culture of trust and mutual respect for collaboration between and within organizations. This, in turn, can enhance employee motivation and commitment, leading to better partnering and outcomes for the organization. By adopting leadership practices that facilitate the continued construction of willingness to partner, organizations can benefit from partnering and build a foundation for success within their organizations.

Second, organizations should recognize the importance of intangible resources in partnership development. While resources such as physical assets are critical to the success of any organization, intangible, relational resources such as competence, reputation, and social capital can also play a crucial role in building strong partnerships. Intangible resources enhance an organization's credibility with potential partners. For example, an organization with a reputation for innovation and thought leadership in a particular industry may be more attractive to potential partners hoping to tap into that expertise. Similarly, organizations with strong networks and relationships with key stakeholders may be better positioned to forge partnerships that can drive growth and innovation. By recognizing the importance of intangible resources in partnership development, organizations can leverage these assets to create strategic partnerships that are mutually beneficial, support the cybersecurity of CI, and contribute to the long-term success of PPPs and the organizations participating in them.

In addition, this research suggests important implications for the military's non-lethal targeting strategies—defense leaders should consider the critical role of intangible resources in modern warfare. Traditionally, military targeting has focused on physical targets such as weapons, vehicles, and buildings. However, in situations where the adversary possesses significant intangible resources like social networks, ideology, and propaganda capabilities, this traditional approach may not be effective. To develop effective non-lethal targeting strategies, the U.S. military must consider an adversary's intangible, relational resources. While this concept may not be directly relevant to traditional defense tactics, it is essential for modern warfare. Adversaries today may have intangible resources that are just as potent as physical assets and cannot be destroyed through physical means alone. By considering intangible resources, military leaders can develop more effective non-lethal targeting strategies that address the adversary's capabilities holistically. This approach can help reduce the overall impact of the adversary's intangible resources and lead to a more successful outcome for military operations. Therefore, it is important to include intangible resources when developing the military's non-lethal targeting strategies.

E. LIMITATIONS AND FUTURE RESEARCH

This research was bounded by three key limitations. First, the analysis was based on a limited number of case studies, which might not have been representative of all PPPs. These organizations belonged to distinct sectors and did not represent all organizations and sectors that engage in PPPs. Second, while the study has proposed a process model describing the construction of willingness to partner in PPPs, the model has not been tested; it describes the process experienced by the individuals and organizations that participated in the research, but the explanations and implications it suggests likely require further refinement. Third, the research design asked participants to recall past events. The participants made sense of past events, given the outcomes and experiences that followed, telling their stories in a generally linear fashion, which might have made causal attributions that otherwise could not be supported. Thus, the construction of willingness might be less linear than portrayed in the model and important influences and relationships of lesser importance. Future research should address these limitations.

Future research should expand investigations to encompass additional types of PPPs, strategic alliances, and CSPs, while also delving into the process of willingness construction in a variety of contexts. Real-time studies on willingness formation should also be conducted. In addition, future studies should consider how characteristics such as organizational goals and values, availability of skilled personnel and technical expertise, and organizational flexibility and adaptability influence the construction of willingness. Finally, future research should identify and investigate leadership practices that may foster the establishment and maintenance of willingness to collaborate, as well as the impact of leadership practices on PPP longevity and performance and organizational performance in PPPs. Research should identify and examine strategies and measures that leaders can adopt to encourage and maintain willingness over time. This dissertation research emphasizes the necessity for a more nuanced and dynamic comprehension of willingness formation and suggests future research directions while recommending specific steps that leaders can take to support the construction of willingness to partner in PPPs.

F. CONCLUSION

In conclusion, this study makes contributions to the literature on PPPs, challenging prevailing perspectives by proposing a more processual definition of willingness to partner that better captures the dynamic processes by which organizations socially construct a willingness to partner. This research demonstrates the usefulness of social activity theory in exploring this newly defined concept of willingness. Additionally, this research presents a model that describes this new understanding, providing a framework for future research in this area. While this research is not without limitations, its findings may provide insights for both researchers and practitioners interested in understanding how organizations can develop and sustain willingness to engage in PPPs. Overall, this study advances a new understanding of willingness as a dynamic, inter-organizational process.

LIST OF REFERENCES

Addae-Boateng, S., Wen, X., & Brew, Y. (2015). Contractual governance, relational governance, and firm performance: The Case of Chinese and Ghanaian and family firms. *American Journal of Industrial and Business Management*, *5*, 288–310. https://doi.org/10.4236/ajibm.2015.55031

Allee, V. (2008). Value network analysis and value conversion of tangible and intangible assets. *Journal of Intellectual Capital*, *9*(1), 5–24. https://doi.org/10.1108/14691930810845777

Allyn, B. (2019, August 20). *22 Texas towns hit with ransomware attack in "new front" of cyberassault*. NPR. https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault

Almås, I., Cappelen, A. W., Salvanes, K. G., Sørensen, E. Ø., & Tungodden, B. (2016). Willingness to compete: Family matters. *Management Science*, *62*(8), 2149–2162. http://dx.doi.org/10.1287/mnsc.2015.2244

Amayah, A. T. (2013). Determinants of knowledge sharing in a public sector organization. *Journal of Knowledge Management*, *17*(3), 454–471. https://doi.org/10.1108/JKM-11-2012-0369

Amin, M. (2005). Energy infrastructure defense systems. *Proceedings of the IEEE*, *93*(5), 861–875. https://doi.org/10.1109/JPROC.2005.847257

Austin, J. E. (2000). Strategic collaboration between nonprofits and business. *Nonprofit and Voluntary Sector Quarterly*, *29*(1), 69–97. https://doi.org/10.1177/089976400773746346

Austin, J. E., & Seitanidi, M. M. (2012). Collaborative value creation: A review of partnering between nonprofits and businesses: Part I. *Nonprofit and Voluntary Sector Quarterly*, *41*, 726–758. https://doi.org/10.1177/0899764012450777

Ayuso, S., Rodríguez, A. M., & Ricart, J. E. (2006). *Using stakeholder dialogue as a source for new ideas: A dynamic capability underlying sustainable innovation*. (Working Paper no. 633). Universidad de Navarra, Center for Business in Society. https://media.iese.edu/research/pdfs/DI-0633-E.pdf

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Barney, J. B. (2001). Is the resource-based "view" a useful perspective for strategic management research? Yes. *Academy of Management Review*, *26*(1), 41–56. https://doi.org/10.2307/259393

Bazzoli, G. J., Stein, R., Alexander, J. A., Conrad, D. A., Sofaer, S., & Shortell, S. M. (1997). Public–private collaboration in health and human service delivery: Evidence from community partnerships. *The Milbank Quarterly*, *75*(4): 533–561. https://doi.org/10.1111/1468-0009.00068

Bell, P., Bennett, D., Butler, R., Esquibel, J., Gordon-Tennant, C., Hall, A. . . . Pfeifer, J. (2019). *Jack Voltaic: Critical infrastructure and public–private partnerships*. Army Cyber Institute at West Point. https://digitalcommons.usmalibrary.org/cgi/viewcontent.cgi?article=1045&context=aci_rp

Belliveau, M. A., O'Reilly, C. A., III, & Wade, J. B. (1996). Social capital at the top: Effects of social similarity and status on CEO compensation. *Academy of Management Journal*, *39*(6), 1568–1593. https://doi.org/10.2307/257069

Benford, R. D., & Snow, D. A. (2000). Framing processes and social movements: An overview and assessment. *Annual Review of Sociology*, *26*, 611–639. https://doi.org/10.1146/annurev.soc.26.1.611

Benitez-Ávila, C., Hartman, A., & Dewulf, G. (2019). Contractual and relational governance as positioned-practices in ongoing public–private partnership projects. *Project Management Journal*, *50*(6), 716–733. https://doi.org/10.1177/8756972819848224

Besley, J. C., Dudo, A., Yuan, S., Lawrence, F. (2018). Understanding scientists' willingness to engage. *Science Communication*, *40*(5), 559–590. https://doi.org/10.1177/1075547018786561

Bhatia, J., Breaux, T. D., Friedberg, L., Hibshi, H., & Smullen, D. (2016). Privacy risk in cybersecurity data sharing. *ACM Workshop on Information Sharing and Collaborative Security*. https://doi.org/10.1145/2994539.2994541

Bishop, P., & Davis, G. (2002). Mapping public participation in policy choices. *Australian Journal of Public Administration*, *61*(1), 14–29. https://doi.org/10.1111/1467-8500.00255

Blue-Banning, M., Summers, J. A., Frankland, H. C., Nelson, L. L., & Beegle, G. (2004). Dimensions of family and professional partnerships: Constructive guidelines for collaboration. *Exceptional Children*, *70*(2). https://doi.org/10.1177/001440290407000203

Brown, M. (2018). *Cyber imperative: Preserve and strengthen public-private partnerships*. National Security Institute, George Mason University. https://nationalsecurity.gmu.edu/2018/10/nsi-policy-paper-cyber-imperative-preserve-and-strengthen-public-private-partnerships/

Brune, A. (2009). Meaningful distinctions within a concept: Relational, collective, and generalized social capital. *Social Science Research 38*(2), 251–265. https://doi.org/10.1016/j.ssresearch.2009.01.005

Brush, C. G., Greene, P. G., Hart, M. M., & Haller, H. S. (2001). From initial idea to unique advantage: The entrepreneurial challenge of constructing a resource base. *Academy of Management Perspectives*, *15*(1), 64–78. https://doi.org/10.5465/AME.2001.4251394

Busch, N. E., & Givens, A. D. (2012). Public–private partnerships in homeland security: Opportunities and challenges. *Homeland Security Affairs*, *8*, Article 18.

Buser, T. (2016). The impact of losing in a competition on the willingness to seek further challenges. *Management Science*, *62*(12), 3439–3449. https://doi.org/10.1287/mnsc.2015.2321

Caldwell, S. L., & Wilshusen, G. C. (2014). *Critical infrastructure protection: Observations on key factors in DHS's implementation of its partnership approach* (GAO-14-464T). Government Accountability Office.

Castelo Branco, M., & Lima Rodrigues, L. (2006). Corporate social responsibility and resource-based perspectives. *Journal of Business Ethics*, *69*(2), 111–132. https://doi.org/10.1007/s10551-006-9071-z

Chandler, D., Haunschild, P. R., Rhee, M., & Beckman, C. M. (2013). The effects of firm reputation and status on inter-organizational network structure. *Strategic Organization*, *11*(3), 217–244. https://doi.org/10.1177/1476127013478693

Chaserant, C. (2003). Cooperation, contracts and social networks: From a bounded to a procedural rationality approach. *Journal of Management & Governance 7*, 163–186. https://doi.org/10.1023/A:1023620127268

Chen, J. Q. (2020). A framework of partnership. *The Cyber Defense Review*, *5*(1), 15–26. https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%20FULL_WEB_1.pdf

Chen, S.-H., Lee, H.-T., & Wu, Y.-F. (2008). Applying ANP approach to the partner selection for strategic alliance. *Management Decision*, *46*(3), 449–465. https://doi.org/10.1108/00251740810863889

Cheng, M., Liu, G., Xu, Y., Chi, M. (2021). Enhancing trust between PPP partners: The role of contractual functions and information transparency. *SAGE Open*, *11*(3). https://doi.org/10.1177/21582440211038245

Christensen, K. K. & Petersen, K. L. (2017). Public–private partnerships on cyber security: A practice of loyalty, *International Affairs*, *93*(6), 1435–1452. https://doi.org/10.1093/ia/iix189

Clinton, L. (2011). A relationship on the rocks: Industry–government partnership for cyber defense. *Journal of Strategic Security*, *4*(2), 97–112. http://dx.doi.org/10.5038/1944-0472.4.2.6

Cyber Houston. (n.d.). *Home page*. Retrieved March 4, 2023, from https://www.cyberhouston.org/

Cybersecurity Information Sharing Act of 2015: Final guidance documents–Notice of availability, 81 F.R. 39061 (2016). https://www.federalregister.gov/documents/2016/06/15/2016-13742/cybersecurity-information-sharing-act-of-2015-final-guidance-documents-notice-of-availability

Cybersecurity & Infrastructure Security Agency. (n.d.). *Home page*. Retrieved March 4, 2023, from https://www.cisa.gov/

D'Alessandro, L., Bailey, S. J., & Giorgino, M. (2014). PPPs as strategic alliances: From technocratic to multidimensional risk governance. *Managerial Finance*, *40*(11), 1095–1111. https://doi.org/10.1108/MF-07-2013-0165

Davis, D. F., & Mentzer, J. T. (2008). Relational resources in interorganizational exchange: The effects of trade equity and brand equity. *Journal of Retailing* *84*(4), 435–448. https://doi.org/10.1016/j.jretai.2008.08.002

Dehlawi, Z., & Abokhodair, N. (2013). Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. *IEEE International Conference on Intelligence and Security Informatics*, 73–75. https://doi.org/10.1109/ISI.2013.6578789.

Department of Energy. (n.d.). *Home page*. Retrieved March 4, 2023, from https://www.energy.gov/

Doz, Y., & Hamel, G. (1999). *Alliance advantage: The art of creating value through partnering*. Harvard Business School Press.

Du, T. C., Lai, V. S., Cheung, W., & Cui, X. (2012). Willingness to share information in a supply chain: A partnership-data-process perspective. *Information & Management*, *49*(2), 89–98. https://doi.org/10.1016/j.im.2011.10.003

Dunn-Cavelty, M., & Suter, M. (2009). Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179–187. https://doi.org/10.1016/j.ijcip.2009.08.006

Earle, H. A. (2003). Building a workplace of choice: Using the work environment to attract and retain top talent. *Journal of Facilities Management*, *2*(3), 244–257. https://doi.org/10.1108/14725960410808230

Einbinder, S. D., Robertson, P. J., Garcia, A., Vuckovic, G., & Patti, R. J. (2000). Interorganizational collaboration in social service organizations: A study of the prerequisites to success. *Journal of Children and Poverty*, *6*(2), 119–140. https://doi.org/10.1080/713675966

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, *21*(10–11), 1105–1121. https://doi.org/10.1002/1097-0266(200010/11)21:10/11<1105::AID-SMJ133>3.0.CO;2-E

Electricity Information Sharing and Analysis Center. (n.d.-a). *Cybersecurity Risk Information Sharing Program (CRISP)*. https://www.eisac.com/s/crisp

Electricity Information Sharing and Analysis Center. (n.d.-b). *Home page*. Retrieved March 4, 2023, from https://www.eisac.com/s/

Electricity Subsector Coordinating Council. (n.d.). *Home page*. Retrieved March 4, 2023, from https://www.electricitysubsector.org/

Engeström, Y. (2014). *Learning by expanding: An activity-theoretical approach to developmental research* (2nd ed.). Cambridge University Press.

Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, *43*(4), 51–58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x

Federal Emergency Management Agency. (n.d.). *Home page*. Retrieved March 4, 2023, from https://www.fema.gov/

Fehrman, W. J. (2016). Mutual assistance in the cyber age. *Electric Perspectives*.

Feldman, M. S. (2004). Resources in emerging structures and processes of change. *Organization Science*, *15*(3), 295–309. https://socialecology.uci.edu/sites/socialecology.uci.edu/files/users/feldmanm/Feldman_2004.pdf

Feldman, M. S., & Worline, M. C. (2011). Resources, resourcing, and ampliative cycles in organizations. In G. M. Spreitzer & K. S. Cameron (Eds.), *The Oxford handbook of positive organizational scholarship* (pp. 630–641). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199734610.013.0047

Fleming, M. H., & Goldstein, E. (2012). *Metrics for measuring the efficacy of critical-infrastructure-centric cybersecurity information sharing efforts*. Homeland Security Studies and Analysis Institute. http://dx.doi.org/10.2139/ssrn.2201033

Ford, J. K., Riley, S. J., Lauricella, T. K., & Van Fossen, J. A. (2020). Factors affecting trust among natural resources stakeholders, partners, and strategic alliance members: A meta-analytic investigation. *Frontiers in Communication*, *5*, Article 9. https://doi.org/10.3389/fcomm.2020.00009

Garud, R., & Karnøe, P. (2003). Bricolage versus breakthrough: Distributed and embedded agency in technology entrepreneurship. *Research Policy*, *32*(2), 277–300. https://doi.org/10.1016/S0048-7333(02)00100-2

Germano, J. H. (2014). *Cybersecurity partnerships—A new era of public–private collaborations*. NYU School of Law, Center on Law and Security. https://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf

Goffman, E. (1986). *Frame analysis: An essay on the organization of experience*. Northeastern University Press.

Goodwin, C., & Nicholas, J. P. (2015). *A framework for cybersecurity information sharing and risk reduction*. Microsoft. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVoNh

Gordon, L. A., Loeb, M. P., & Lusyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, *22*, 461–485. http://dx.doi.org/10.1016/j.jaccpubpol.2003.09.001

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Gray, B. (1998). Collaboration: The constructive management of differences. In G. R. Hickman (Ed.), *Leading organizations: Perspectives for a new era* (pp. 467–480). SAGE Publications. (Reprinted from *Collaboration: Finding common ground for multiparty problems*, pp. 1–25, by B. Gray, 1989, Jossey-Bass)

Gutierrez, B., Howard-Grenville, J., & Scully, M. A. (2010). The faithful rise up: Split identification and an unlikely change effort. *Academy of Management Journal*, *53*(4), 673–699. https://www.jstor.org/stable/20788787

Gutierrez, R., Marquez, P., Refico, E., & Reficco, E. (2016). Configuration and development of alliance portfolios: A comparison of same-sector and cross-sector partnerships. *Journal of Business Ethics*, *123*, 55–69. https://doi.org/10.1007/s10551-015-2729-7

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, *50*, Article 101660. https://doi.org/10.1016/j.scs.2019.101660

Hagedoorn, J., Link, A. N., & Vonortas, N. S. (2000). Research partnerships. *Research Policy*, *29*, 567–586. http://dx.doi.org/10.1016/S0048-7333(99)00090-6

Hare, F. B. (2011). *The interdependent nature of national cyber security: Motivating private action for a public good* [Doctoral dissertation, George Mason University]. Mason Archival Repository Service. https://hdl.handle.net/1920/6312

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. *Risk Analysis*, *38*(2), 215–225. https://doi.org/10.1111/risa.12878

Healey, J. (2015). *Breaking the cyber-sharing logjam*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2015/02/AC_BreakingCyber-SharingLogjam_WEB.pdf

Henrick, E. C., Cobb, P., Penuel, W. R., Jackson, K., & Clark, T. (2017). *Assessing research-practice partnerships: Five dimensions of effectiveness*. William T. Grant Foundation.

Holland, R. C. (1984). The new era of public–private partnership. In P. R. Porter & D. C. Sweet (Eds.), *Rebuilding America's cities: Roads to recovery* (pp. 209–211). Rutgers University, Center for Urban Policy Research.

Howard-Grenville, J. A., & Hoffman, A. J. (2003). The importance of cultural framing to the success of social initiatives in business. *Academy of Management Executives*, *17*(2), 70–84. https://www.jstor.org/stable/4165957

Huber, T. L., Fischer, T. A., Dibbern, J., & Hirschheim, R. (2013). A process model of complementarity and substitution of contractual and relational governance in IS outsourcing. *Journal of Management Information Systems*, *30*(3), 81–114. https://doi.org/10.7892/boris.44307

ICS Village. (2018, September 26). *Cyber Mutual Assistance—A new model for electric companies preparing and responding to cyber security emergencies*. https://www.icsvillage.com/talks/cyber-mutual-assistance-a-new-model-for-electric-companies-preparing-and-responding-to-cyber-security-emergencies

ISAO Standards Organization. (n.d.-a). *Cyber Houston*. Retrieved March 3, 2023, from https://www.isao.org/group/cyber-houston-2/

ISAO Standards Organization. (n.d.-b). *Home page*. Retrieved March 2, 2023, from https://www.isao.org/

Jacobson, C., & Choi, S. O. (2008). Success factors: Public works and public–private partnerships. *International Journal of Public Sector Management*, *21*(6), 637–657. https://doi.org/10.1108/09513550810896514

Jasper, S. E. (2017). U.S. cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence*, *30*(1), 53–65. https://doi.org/10.1080/08850607.2016.1230701

Johnson, A. L. (2016). Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation, *North Carolina Banking Institute Journal*, *20*(1). https://scholarship.law.unc.edu/ncbi/vol20/iss1/15

Jost, J. T., Chaikalis-Petritsis, V., Abrams, D., Sidanius, J., Van Der Toorn, J., & Bratt, C. (2012). Why men (and women) do and don't rebel: Effects of system justification on willingness to protest. *Personality and Social Psychology Bulletin*, *38*(2), 197–208. https://doi.org/10.1177/0146167211422544

Kaijankoski, Eric A. (2015). *Cybersecurity information sharing between public private sector agencies* [Master's thesis, Naval Postgraduate School]. Defense Technical Information Center. https://apps.dtic.mil/sti/citations/ADA620766

Keenan, C. (2017, March 27). *How "Sheltered Harbor" provides safety from the cyber storm*. ABA Banking Journal. https://bankingjournal.aba.com/2017/03/how-sheltered-harbor-provides-safety-from-the-cyber-storm/

Kelly, C. (2012). Measuring the performance of partnerships: Why, what, how, when? *Geography Compass*, *6*(3), 149–162. https://doi.org/10.1111/j.1749-8198.2012.00476.x

Khodyakov, D. (2007). Trust as a process: A three-dimensional approach. *Sociology*, *41*(1), 115–132. https://doi.org/10.1177/0038038507072285

Khoshdel, M. K., & Bakhshan, Y. (2015). Measuring willingness to participate and the factors affecting citizen participation (case study on citizens in the 20th Municipal District of Tehran). *Mediterranean Journal of Social Sciences*, *6*(3), 155–162. https://doi.org/10.36941/mjss

Kingsley, G., & Waschak, M. R. (2005, September 16). *Finding value and meaning in the concept of partnership* [Paper presentation]. 2005 MSP Evaluation Summit, Minneapolis, MN, United States.

Kubal, T. J. (1998). The presentation of political self: Cultural resonance and the construction of collective action frames. *Sociological Quarterly*, *39*(4), 539–554. https://doi.org/10.1111/j.1533-8525.1998.tb00517.x

Kumaraswamy, M. M., Ling, F. Y.-Y., Anvuur, A. M., & Rahman, M. M. (2007). Targeting relationally integrated teams for sustainable PPPS. *Engineering, Construction and Architectural Management*, *14*(6), 581–596. https://doi.org/10.1108/09699980710829030

Kuutti, K. (1991). The concept of activity as a basic unit of analysis for CSCW research. In L. Bannon, M., Robinson, & K. Schmidt, K. (Eds.), *Proceedings of the Second European Conference on Computer-Supported Cooperative Work ECSCW '91*, 249–264. https://doi.org/10.1007/978-94-011-3506-1_19

Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management Review*, *24*(4), 691–710. https://doi.org/10.2307/259349

Lavie, D., Haunschild, P. R., & Khanna, P. (2012). Organizational differences, relational mechanisms, and alliance performance. *Strategic Management Journal*, *33*(13), 1453–1479. https://doi.org/10.1002/smj.1987

Leonardi, P. M. (2011). When flexible routines meet flexible technologies: Affordance, constraint, and the imbrication of human and material agencies. *MIS Quarterly*, *35*(1), 147–167. https://doi.org/10.2307/23043493

Lewicki, R. J., & Bunker, B. B. (1996). Developing and maintaining trust in work relationships. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 114–139). SAGE Publications. http://dx.doi.org/10.4135/9781452243610.n7

Liebe, U., Preisendörfer, P., & Meyerhoff, J. (2011). To pay or not to pay: Competing theories to explain individuals' willingness to pay for public environmental goods. *Environment and Behavior*, *43*(1), 106–130. https://doi.org/10.1177/0013916509346229

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. SAGE Publications.

Lowndes, V., & Skelcher, C. (1998). The dynamics of multi-organizational partnership: An analysis of changing modes of governance. *Public Administration*, *76*(2), 313–333. https://doi.org/10.1111/1467-9299.00103

Mackintosh, M. (1992). Partnership: Issues of policy and negotiation. *Local Economy*, *7*(3), 210–224. https://doi.org/10.1080/02690949208726149

Manhattan District Attorney's Office. (n.d.). *The NYC Cyber Critical Services and Infrastructure (CCSI) Project*. Retrieved March 2, 2023, from https://www.manhattanda.org/ccsi/

Manley, M. (2015). Cyberspace's dynamic duo: Forging a cybersecurity public–private partnership. *Journal of Strategic Security*, *8*(3), 85–98. 10.5038/1944-0472.8.3S.1478

Martin de Castro, G., Saez, P. L., Navas Lopez, J. E. (2004). The role of corporate reputation in developing relational capital. *Journal of Intellectual Capital*, *5*, 575–585. https://doi.org/10.1108/14691930410567022

Matear, M. A. (2014). The role and nature of willingness to sacrifice in marketing relationships [Doctoral thesis, Queen's University]. https://qspace.library.queensu.ca/bitstream/handle/1974/8695/Matear_Maggie_201404_PhD.pdf?sequence=1

Maurer, T., & Nelson, A. (2020). *International strategy to better protect the financial system against cyber threats*. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Maurer_Nelson_FinCyber_final1.pdf

Mckenzie, J., & Van Winkelen, C. (2006). Creating successful partnerships: The importance of sharing knowledge. *Journal of General Management*, *31*(4), 45–61. https://doi.org/10.1177/030630700603100404

McQuaid, R. W. (2000). The theory of partnership: Why have partnerships? In S. P. Osborne (Ed.), *Public–private partnerships for public services: An international perspective* (pp. 9–35). Routledge.

McTarnaghan, S., Morales-Burnett, J., Marx, R., Levy, D., Burnstein, E., Williams, J. L., Oliver, W., & Salerno, C. (2022). *Urban resilience: From global vision to local practice*. Urban Institute. https://www.urban.org/sites/default/files/2022-09/Urban%20Resilience%20-%20From%20Global%20Vision%20to%20Local%20Practice_1.pdf

Michel-Kergan, E. (2003). New challenges in critical infrastructures: A U.S. perspective. *Journal of Contingencies and Crisis Management*, *11*(3).

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis*. SAGE Publications.

Mohr, J., & Spekman, R. (1994). Characteristics of partnership success: Partnership attributes, communication behavior and conflict resolution techniques. *Strategic Management Journal*, *15*(2), 135–152. https://doi.org/10.1002/smj.4250150205

Morris, T. H., & Gao, W. (2013). Industrial control system cyber attacks. *Proceedings of the First International Symposium for ICS & SCADA Cyber Security Research 2013*, 22–29. https://doi.org/10.14236/ewic/ICSCSR2013.3

Moteff, J., Copeland, C., & Fischer, J. (2003). *Critical infrastructures: What makes an infrastructure critical?* (CRS Report No. RL31556). Congressional Research Service.

Mulgan, G., & Albury, D. (2003). *Innovation in the public sector*. Cabinet Office Strategy Unit. http://www.sba.oakland.edu/faculty/mathieson/mis524/resources/readings/innovation/innovation_in_the_public_sector.pdf

North American Electric Reliability Corporation. (2014). *Grid security exercise (GridEx II): After-action report*. https://www.nerc.com/pa/CI/ESISAC/GridEx/GridEx%20II%20Public%20Report.pdf

North American Electric Reliability Corporation & Electricity Information Sharing and Analysis Center. (2022). *GridEx VI: Lessons learned report*. https://www.nerc.com/pa/CI/ESISAC/GridEx/GridEx%20VI%20Public%20Report.pdf

N.Y.C. Exec. Order No. 28. (2017). https://www.nyc.gov/assets/home/downloads/pdf/executive-orders/2017/eo_28.pdf

Nyre-Yu, M., Gutzwiller, R. S., & Caldwell, B. S. (2019). Observing cyber security incident response: Qualitative themes from field research. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 437–441. https://doi.org/10.1177/1071181319631016

O'Boyle, M. (2022, April 7). *Protecting New York's critical infrastructure*. Capalino. https://www.capalino.com/protecting-new-yorks-critical-infrastructure/

O'Brien, K. (2003). Information age, terrorism, and warfare. *Small Wars and Insurgencies*, *14*(1), 183–206. https://doi.org/10.1080/09592310412331300636

O'Halloran, J. (2017). *Challenges of public–private partnerships in cyber security* [Capstone project, Utica College]. ProQuest.

Oliver, C. (1990). Determinants of interorganizational relationships: Integration and future decisions. *Academy of Management Review*, *15*(2), 241–265. https://doi.org/10.2307/258156

Osei-Kyei, R., Chan, A. P., Javed, A. A., & Ameyaw, E. E. (2017). Critical success criteria for public-private partnership projects: international experts' opinion. *International Journal of Strategic Property Management*, *21*(1), 87–100. https://doi.org/10.3846/1648715X.2016.1246388

Otola, I. (2016). Importance of relational resources in the corporate management. In M. Nowicka-Skowron, C. B. Illes, & J. Torzes (Eds.), *Contemporary issues of enterprise management in Poland and Hungary* (pp. 131–138). Szent Istvan University Publishing.

Pala, A., & Zhuang, J. (2019). Information sharing in cybersecurity: A review. *Decision Analysis*, *16*(3), 172–196. https://doi.org/10.1287/deca.2018.0387

Paul, D. (2021, July 8). New York City opens Cyberattack Defense Center. *The Wall Street Journal*. https://www.wsj.com/articles/new-york-city-opens-cyberattack-defense-center-11625778530

Pearce, B. J., Deutsch, L., Fry, P., Marafatto, F. F., & Lieu, J. (2022). Going beyond the AHA! moment: Insight discovery for transdisciplinary research and learning. *Humanities & Social Sciences Communications*, *9*, Article 123. https://doi.org/10.1057/s41599-022-01129-0

Penuel, W. R., Coburn, C. E., & Gallagher, D. J. Negotiating problems of practice in research–practice design partnerships. *Teachers College Board: The Voice of Scholarship in Education*, *115*(14), 237–255. https://doi.org/10.1177/016146811311501404

Petkova, A. P., Rindova, V. P., & Gupta, A. K. (2008). How can new ventures build reputation? An exploratory study. *Corporate Reputation Review*, *11*(4), 320–334. https://doi.org/10.1057/crr.2008.27

Phillips, N., Lawrence, T. B., & Hardy, C. (2000). Inter-organizational collaboration and the dynamics of institutional fields. *Journal of Management Studies*, *37*(1). https://doi.org/10.1111/1467-6486.00171

Phillips, S. (2021, July 8). *Kaseya ransomware attack—Uncovering threats in the hidden supply chain* [Webcast]. BrightTALK. https://www.brighttalk.com/webcast/18735/498392?utm_source=interos&utm_medium=brighttalk&utm_campaign=498392?&utm_source=linkedin&utm_medium=social_organic

Pomery, E. A., Gibbons, F. X., Reis-Bergan, M., & Gerrard, M. (2009). From the willingness to intention: Experience moderates the shift from reactive to reasoned behavior. *Personality & Social Psychology Bulletin*, *35*(7), 894–908. https://doi.org/10.1177/0146167209335166

Raban, D. R., & Rafaeli, S. (2006). Investigating ownership and the willingness to share information online. *Computers in Human Behavior*, *23*, 2367–2383.

Razak, N. A., Pangil, F., Zin, M. L. M., Yunus, N. A. M., & Asnawi, N. H. (2016). Theories of knowledge sharing behavior in business strategy. *Procedia Economics and Finance*, *37*, 545–553, https://doi.org/10.1016/S2212-5671(16)30163-0

Recalde, C., & Shook, J. (2021). *A sheltered harbor in a cyber storm*. Sheltered Harbor & Dell Technologies. https://www.delltechnologies.com/asset/en-au/products/data-protection/industry-market/sheltered-harbor-white-paper.pdf

Rid, T., & Buchanan, B. (2015). Attributing cyber-attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Ring, P. S., & Van de Ven, A. H. (1994). Developmental processes of cooperative inter-organizational relationships. *Academy of Management Review*, *19*(1), 90–118. https://doi.org/10.2307/258836

Roberts, G., Raihani, N., Bshary, R., Manrique, H. M., Farina, A., Samu, F., & Barclay, P. (2021). The benefits of being seen to help others: Indirect reciprocity and reputation-based partner choice. *Philosophical Transactions of the Royal Society B*, *376*(1838), Article 20200290. https://doi.org/10.1098/rstb.2020.0290

Rosas, J., & Camarinha-Matos, L. M. (2010). Assessment of the willingness to collaborate in enterprise networks. *Emerging Trends in Technological Innovation: First IFIP WG 5.5/SOCOLNET Doctoral Conference on Computing, Electrical and Industrial Systems*, 14–23. https://doi.org.10.1007/978-3-642-11628-5_2

Rosenau, P. V. (1999). The strengths and weaknesses of public–private policy partnerships. *American Behavioral Scientist*, *43*(1), 10–34. https://doi.org.10. 1177/00027649921955137

SANS Industrial Control Systems & Electricity Information Sharing and Analysis Center. (2016). *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

Sarkar, M. B., Aulakh, P. S., & Madhok, A. (2009). Process capabilities and value generation in alliance portfolios. *Organization Science*, *20*(3), 583–600. https://doi.org/10.1287/orsc.1080.0390

Schultz, C., Einwiller, S., Seiffert-Brockmann, J., & Weitzl, W. (2019). When reputation influences trust in nonprofit organizations. The role of value attachment as moderator. *Corporate Reputation Review*, *22*, 159–170. https://doi.org/10.1057/s41299-019-00067-z

Scott, M. S., & Thurston, W. E. (1997). A framework for the development of community health agency partnerships. *Canadian Journal of Public Health*, *88*, 416–420.

Securing Systemically Important Critical Infrastructure Act, H.R. 5491, 117th Cong. (2021). https://www.congress.gov/bill/117th-congress/house-bill/5491/text?s=1&r=36

Seitanidi, M. M., & Crane, A. (2009). Implementing CSR through partnerships: Understanding the selection, design and institutionalization of nonprofit-business partnerships. *Journal of Business Ethics*, *85*(Suppl 2), 413–429. https:/doi.org/10.1007/s10551-008-9743-y

Sharkov, G. (2016). From cybersecurity to collaborative resiliency. *SafeConfig '16: Proceedings of the October ACM Workshop on Automated Decision Making for Active Cyber Defense*, 3–9. http://dx.doi.org/10.1145/2994475.2994484

Sheltered Harbor. (n.d.). *Home page*. Retrieved March 2, 2023, from https://www.shelteredharbor.org/

Siqueira Ambrozini, L. C., & Martinelli, D. P. (2017). Formal and relational contracts between organizations: Proposal of a model for analysis of the transactional and governance structures characteristics of comparative cases. *Revista de Administração* [Management Journal], *52*, 374–391. https://www.redalyc.org/pdf/2234/223453319004.pdf.

Solansky, S. T. and Beck, T. (2021). Interorganizational information sharing: Collaboration during cybersecurity threats. *Public Administrative Quarterly*, *45*(1), 105–122. https://doi.org/10.37808/paq.45.1.5

Stadtler, L. (2011). Aligning a company's economic and social interests in cross-sector partnerships. *Journal of Corporate Citizenship*, *44*, 85–106. https://doi.org/10.9774/GLEAF.4700.2011.wi.00007

Stadtler, L., & Probst, G. (2012). How broker organizations can facilitate public–private partnerships for development. *European Management Journal*, *30*(1), 32–46.

Stoddart, K. (2022). Gaining access: Attack and defense methods and legacy systems. In *Cyberwarfare: Threats to critical infrastructure*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-97299-8_4

Strengthening American Cybersecurity Act of 2022. S. 3600, 117th Cong. (2022). https://www.congress.gov/bill/117th-congress/senate-bill/3600/summary/00

Sunstein, C. R. (2002). What's available—Social influences and behavioral economics empirical legal realism: A new social scientific assessment of law and human behavior. *Northwestern University Law Review*, *97*(3), 1295–1314. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=12522&context=journal_articles&httpsredir=1&referer=

Tishuk, B. (2012). Effectively managing partnership evolution: A case study from Chicago. *Journal of Business Continuity & Emergency Planning*, *6*(2), 111–121.

Todeva, E., & Knoke, D. (2005). Strategic alliances & models of collaboration. *Management Decision*, *43*(1), 123–148. https://doi.org/10.1108/00251740510572533

Trist, E. (1983). Referent organizations and the development of inter-organizational domains. *Human Relations*, *36*(3), 269–284. https://doi.org/10.1177/001872678303600304

Vance, Cy, Jr., & O'Neill, J. P. (2019, April 1). New York launches a cybercrime brigade. *The Wall Street Journal*. https://www.wsj.com/articles/new-york-launches-a-cybercrime-brigade-11554160104

van den Hooff, B., & de Ridder, J. A. Knowledge sharing in context: The influence of organizational commitment, communication climate and CMC use on knowledge sharing. *Journal of Knowledge Management*, *8*(6), 117–130. https://doi.org/10.1108/13673270410567675

Van de Ven, A. H. (1976). On the nature, formation, and maintenance of relations among organizations. *Academy of Management Review*, *1*(4), 24–36. https://doi.org/10.5465/AMR.1976.4396447

Van de Ven, A. H., & Walker, G. (1984). The dynamics of inter-organizational coordination. *Administrative Science Quarterly 29*(4), 598–621. https://doi.org/10.2307/2392941

Van Gorp, B. (2007). The constructionist approach to framing: Bringing culture back in. *Journal of Communication*, *57*(1), 60–78. https://doi.org/10.1111/j.0021-9916.2007.00329.x

Van Lange, P. A., Rusbult, C. E., Drigotas, S. M., Arriaga, X. B., Witcher, B. S., & Cox, C. L. (1997). Willingness to sacrifice in close relationships. *Journal of Personality and Social Psychology*, *72*(6), 1373–1395. https://doi.org/10.1037//0022-3514.72.6.1373

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Waddock, S. A. (1988). Building successful social partnerships. *MIT Sloan Management Review*, *29*(4), 17–23.

Wang, Y., & Rajagopalan, N. (2015). Alliance capabilities: Review and research agenda. *Journal of Management*, *41*(1), 236–260. https://doi.org/10.1177/0149206314557157

Weber, W. G., Unterrainer, C., & Höge, T. (2020). Psychological research on organisational democracy: A meta-analysis of individual, organisational, and societal outcomes. *Applied Psychology*, *69*(3), 1009–1071. https://doi.org/10.1111/apps.12205

West, V., & Milio, N. (2004). Organizational and environmental factors affecting the utilization of telemedicine in rural home healthcare. *Home Health Care Services Quarterly*, *23*(4), 9–67. https://doi.org/10.1300/J027v23n04_04

White, G., Harrison, K., & Sjelin, N. (2019). The need for information sharing and analysis organizations to combat attacks on states and communities. *Proceedings of the 52nd Hawaii International Conference on Systems Sciences*, 2852–2860. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/ca1b6784-fcfb-47af-89de-474cf376b5fe/content

White House. (2013, February 12). *Critical infrastructure security and resilience* (PPD-21). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Wu, W. Y., Shih, H. A., & Chan, H. C. (2009). The analytic network process for partner selection criteria in strategic alliances. *Expert Systems with Applications*, *36*(3), 4646–4653. https://doi.org/10.1016/j.eswa.2008.06.049

Yang, T.-M., & Wu, W.-J. (2013). What to share and why to share? A case study of cross-boundary information sharing in Taiwan e-Government. *Journal of Library and Information Studies*, *11*(1), 25–53. https://doi.org/10.6182/jlis.2013.11(1).025

Yin, R. K. (2010). *Qualitative research from start to finish*. Guilford Publications.

Yu, H., Li, H., & Gou, X. (2011). The personality-based variables and their correlations underlying willingness to communicate. *Asian Social Science*, *7*(3). https://doi.org/10.5539/ASS.V7N3P253

Zaheer, A., & Venkatraman, N. (1995). Relational governance as an inter-organizational strategy: An empirical test of the role of trust in economic exchange. *Strategic Management Journal*, *16*(5), 373–392. https://www.jstor.org/stable/2486708

Zamiri, M., & Camarinha-Matos, L. M. (2019). Mass collaboration and learning: Opportunities, challenges, and influential factors. *Applied Sciences*, *9*(13), Article 2620. https://doi.org/10.3390/app9132620

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California