

A DYNAMIC CYBER-BASED VIEW OF THE FIRM

A Dissertation Proposal
Submitted to the
Temple University Graduate School

In Partial Fulfillment
of the Requirements for the Degree
Executive Doctor Of Business Administration

by
Tamara B. Schwartz
Temple University, Fox School of Business
May 2019

Review Committee Members:

David Schuff, Advisory Chair, Department of MIS, Fox School of Business
Susan Mudambi, Dept of Marketing & Supply Chain Mgmt, Fox School of Business
Matt Wray, Department of Sociology, Temple University
Steve Balsam, External Member, Department of Accounting, Fox School of Business

©
Copyright
2019

by

Tamara B. Schwartz
All Rights Reserved

ABSTRACT

Technology, perceived by many organizations to be a tool, has evolved from a set of tools, to a location in which many companies have located their key terrain through digitization. That location is cyberspace, an inherently compromised, hostile environment, marked by rapid change and intense competition. It is analogous to a dark alley lined with dumpsters and shadowy doorways with numerous people seeking to challenge organizational objectives. Despite the prevalence of digitization, which has transformed the organization from an anthropological manifestation to a cyborg construction, there does not currently exist a strategic view of the firm which explores the integration of the organization and cyberspace. This paper conceptualizes the Cyber-Based View of the Firm, a dynamic view designed to capture the complex interactions between people, technology, and data that enable cyberattack. A meta-analysis of current theory frames the research gap into which the Cyber-Based View fits. This meta-analysis, in conjunction with an exploratory case study of the Stuxnet attack, identified the need for physical mediation of the cognitive – informational interaction. Finally, the Cyber-Based View was used as a forensic tool to conduct a qualitative multi-case study. Using a failure autopsy approach, eight events were developed into case studies by examining, coding, and recombining the narratives within the qualitative data. A pattern matching technique was used to compare the empirical patterns of the case studies with the proposed patterns of the research construct, providing strong evidence of model validity.

TABLE OF CONTENTS

	Page
ABSTRACT	iii
LIST OF TABLES	vii
LIST OF FIGURES	ix
 CHAPTER	
1. INTRODUCTION	1
The Changing Landscape	1
Research Motivation	2
Dissertation Structure	4
2. CONCEPTUALIZING A DYNAMIC CYBER-BASED VIEW OF THE FIRM	7
Overview	7
How Do We Define Cyberspace?	8
Literature Review	15
General Themes in Cybersecurity Literature	15
Moore's Law & Sociomateriality	19
Resilience	22
The Resource Based Perspective	26
Salience	30
Game Theory	33
Cybersecurity Investment Decisions – Further Applications of Salience and Game Theory	35
Other Theory	36
Conceptual Model	39
The Cognitive Dimension and Theory	39
The Physical Dimension and Theory	40
The Informational Dimension and Theory	40
Cognitive, Physical, and Informational Bilateral Interactions and Theory	40
Conclusion	41
3. SHAPING THE RESEARCH GAP FOR THE CBV	43
Overview	43
Research Design	43
Validation of Methodology	43
Meta-Analysis of Existing Theory	44
Discussion of Results	47
The Bilateral Physical – Informational Interaction Test	48
The Bilateral Cognitive – Informational Interaction Test	49
The Bilateral Cognitive – Physical Interaction Test	49
The Multilateral Physical – Informational – Cognitive Interaction Test	50
Case Study Analysis of the Stuxnet Attack	52
Conclusion	55

4. APPLYING THE DYNAMIC CYBER-BASED VIEW OF THE FIRM.....	58
Overview.....	58
Literature Review.....	58
Corporate Information Warfare and Cyberattack.....	58
Definitions.....	61
The Cyberattack Phenomenon.....	64
Research Construct.....	65
Mechanics of the CBV.....	65
The Cognitive Dimension.....	66
The Physical Dimension.....	67
The Informational Dimension.....	68
Research Design.....	73
Part 1: Choosing Case Studies for Investigation.....	74
Part 2: Case Study Development and Analysis.....	84
Case Study Analyses.....	90
Analysis of the 2010 Stuxnet Attack.....	90
Analysis of the 2015 and 2016 Ukrainian Blackouts.....	95
Analysis of the 2016 Internet of Things Botnet	101
Analysis of the 2016 - Present Twitterbots	108
Analysis of the 1999 Melissa Virus	113
Analysis of the 2005-2012 Hack of American Business.....	118
Analysis of the 2017 (Not)Petya Ransomware	123
Analysis of the 2010 Manning Disclosure to WikiLeaks	130
Analysis of the 2015 Ashley Madison Hack	138
Results	143
Cognitive Dimension.....	143
Physical Dimension	145
Cognitive – Physical Interaction	147
Informational Dimension	150
Cognitive – Informational Interaction	152
Informational – Physical Interaction	154
Cognitive – Physical – Informational Interaction	156
Summary	159
5. CONCLUSIONS, IMPLICATIONS & FUTURE RESEARCH.....	161
Information Warfare in the Twenty-First Century	161
Deriving, Testing, and Applying the Dynamic Cyber-Based View of the Firm...163	163
The Significance of the Cognitive Dimension: Adaptive Cyber Capability	164
The Convergence of Corporate and Global Information Warfare	171
Contributions to Theory	172
A Novel Definition of Cyberspace	172
Defining the Literature Gap Filled by the Cyber-Based View	173
Generalizability of the Cyber-Based View	174
New Evolutionary Pattern of Cyberthreat Revealed by the	
Cyber-Based View	176
Corporations and Nation States Become Competitive Rivals.....	177

Contributions to Practice	178
Characterizing Cyerattack	178
A Tool to Examine Tradeoffs to Achieve Competitive Advantage	178
Organizations Need to Engage in Continuous Learning Related to Cyberspace	181
Think Like a Hacker – The Knowledge is Accessible	183
Without Boundaries, Understanding Hybrid Warfare is Critical	184
Study Limitations and Future Research	186
REFERENCES	188

APPENDICES

	Page
A. TEST CASE STUDY: STUXNET.....	226
B. REVIEW OF LITERATURE IN FIVE THEORETICAL CATEGORIES RELATING TO THE CBV.....	241
C. A SURVEY OF CYBERATTACKS.....	356
D. IRB APPROVAL.....	360
E. SURVEY RESULTS	363
F. RESULTS TABLES: EMPIRICAL PATTERNS	370

LIST OF TABLES

TABLE	Page
1. Shaping the Cyber Based View of the Firm with Theory.....	16
2. Classification of Twenty Theories.....	45
3. Summary of Findings.....	47
4. Rank Ordered Case Studies Classified by Type of Cyberattack and Type of Attacker.....	82
5. Rank Ordered Case Studies Classified by Industry and Employed Technology Tools	83
6. Codebook for Analysis of Documents.....	86
7. Model Elements & Interactions.....	88
8. Examples of the Cognitive Dimension from Nine Case Studies	144
9. Examples of the Physical Dimension from Nine Case Studies	146
10. Examples of the Cognitive – Physical Interaction from Nine Case Studies.....	148
11. Examples of the Informational Dimension from Nine Case Studies	150
12. Examples of the Cognitive – Informational Interaction from Nine Case Studies	153
13. Examples of the Informational – Physical Interaction from Nine Case Studies.....	155
14. Examples of the Multilateral Cognitive – Physical – Informational Interaction from Nine Case Studies	158
15. Adaptive Cyber Capability in the Hacker Community of Practice.....	167
16. Takeaways for Top Management.....	184
17. Three Cyberattacks Every CEO/CIO/CISO Should Know About	185
 A1. Analysis of the Stuxnet Case Study in the Context of the CBV.....	232
A2. Stuxnet Case Study: Testing Existing Theory & the CBV.....	235
A3. Steps in the Data Collection and Analysis Process.....	237
A4. Data Analyzed for Case Studies.....	237
 B1. Four Tests of Category 1: Technology Growth Theories.....	252
B2. Four Tests of Category 2: Decision Making Theories.....	265
B3. Four Tests of Category 3: Informational & Physical Assets Theories.....	286
B4. Four Tests of Category 4: Online Behavior Theories.....	301
B5. Four Tests of Category 5: Organizational Theories.....	315
B6. Summary of Findings	316
 E1. Ranked Results of Cyberattack Survey	363
F1. Empirical Patterns from Nine Case Studies: Cognitive Dimension	371
F2. Empirical Patterns from Nine Case Studies: Physical Dimension	375
F3. Empirical Patterns from Nine Case Studies: Cognitive – Physical Interaction.....	379
F4. Empirical Patterns from Nine Case Studies: Informational Dimension	384
F5. Empirical Patterns from Nine Case Studies: Cognitive – Informational Interaction	389
F6. Empirical Patterns from Nine Case Studies: Informational – Physical Interaction	394

F7. Empirical Patterns from Nine Case Studies: Cognitive – Physical – Informational Interaction	399
---	-----

LIST OF FIGURES

FIGURE	Page
1. Research Process Flow Chart.....	5
2. Feedback Loop Between the Physical and Informational Dimensions of Cyberspace.....	10
3. The Informational Dimension Joins the Cognitive and Physical Dimensions of Cyberspace.....	11
4. Feedback Across All Three Dimensions.....	13
5. Cyber-Based View of the Firm.....	15
6. A Cyber Based View of Jones (2014) Sociomaterial Observations of Critical Care.....	22
7. Shaping the Cyber Based View of the Firm with Theory.....	39
8. Theory Testing Framework.....	46
9. Summary of Findings.....	52
10. Cyber-Based View Research Construct.....	73
11. Output from Research Randomizer	77
12. Example of Dropbox Filing System for Melissa Virus	85
13. Example of Coding Approach for Melissa Virus Item 5-9	87
14. Pattern Matching Process, Adapted from Almutairi et al., 2014	89
A1. CBV of the Stuxnet Attack.....	236
B1. Summary of Findings	328

CHAPTER 1

INTRODUCTION

The Changing Landscape

A soldier loses his arm on the battlefield and receives a neural prosthetic linking the prosthetic limb to the soldier's nervous system. The brain controlled interface captures his brain transmissions and translates these to command signals (Schwartz et al., 2006) enabling him to stroke the face of his newborn child. *The Six-Million Dollar Man* (Bennett, 1973) is no longer science fiction.

A colleague receives a prompt from her Apple watch that it's time for her afternoon run. She changes into her gym clothes and hits the streets, leaving in her wake a stream of digital dust (Cecez-Kecmanovic et al., 2014).

The automobile industry uses finite element analysis (FEA) tools in combination with CAD drawings to simulate automobile crashes using three-dimensional visualization of how the body of a specific vehicle responds when it crashes into a stationary object, allowing them to track how energy moves through the vehicle's body moment by moment, and enabling a design to be crash tested before it is ever built in the physical world (Leonardi & Barley, 2010).

We have become enmeshed with our technology to such an extent that it shapes our language – if we want to learn something about a particular topic, we *google* it; our habits – it is the rare person who does not experience a panic response to a lost smart phone; and our lived experience – work is no longer a place we must go because technology allows us to work from anywhere. “We are the Borg. Resistance is futile.” (Hornstein & Frakes,

1996). While we have not lost our humanity or our individuality to the collective just yet, the cyborg concept as a human – machine hybrid, is a useful metaphor (Cecez-Kecmanovic et al., 2014) to begin thinking through our immersion in Cyberspace, and by extension, the immersion of the firm in Cyberspace.

Digitization of the firm through process automation, business intelligence systems, robotics, the Internet of Things, and the advent of portable, wearable technology has led us down a path where we are becoming our data through the digital representation of our actions (Cecez-Kecmanovic et al. 2014), which are captured through our devices, social media accounts and other digital interactions. This strengthens the relationship between the posture of the firm and its information technology. This phenomenon has enabled firms to do things that would never have been possible, such as decreasing production costs through automation (Borreau et al., 2012) and fostering innovation in remarkable ways (Leonardi & Barley, 2008), but it has also allowed nation states (Haggard & Lindsay, 2015), organized crime (Choo, 2011), hacktivists (Serracino-Inglott, 2013) and other rivals (Cavusoglu et al., 2008) entrée into the innermost workings of the firm.

Research Motivation

Hacking began in the 1960s with the phone phreaking movement, with teenagers using a whistle offered as a prize in a Cap'n Crunch cereal box, to trick telephone networks (Hatfield, 2018). This resulted in the perception of the hacker community as a nuisance – a perception that has persisted well into the 2000s. But the speed of technological change has expanded the cyber domain within the firm, offering up a huge pool of potential cyber victims (Choo, 2011). This accelerating change has also given rise

to cyberthreat in the larger landscape, evolving cyberthreat from a mere nuisance to full blown information operations.

In 2014, Cyber Risk moved into the top 10 global business risks for the first time (Hartwick & Wilkinson, 2014), but documented cyberattacks have been ongoing for over a decade, rising over 400% from 2005-2014 (Hartwick & Wilkinson, 2014). As new capabilities evolve to combat identity theft, black market business models are changing from data theft to ransomware to hacking as a service (Archer, 2014). Events such as the 2015 hack of Sony Pictures (Haggard & Lindsay, 2015), the 2016 hack of the Democratic National Committee (Mihailidis & Viotty, 2017), and the summer 2017 WannaCry and Petya global ransomware attacks that affected over one-half million computers in nearly 150 countries (Solon et al. 2017) illustrate the escalating threat.

Cyberthreats are expanding because organizational activities are driven by knowledge and the contextual enterprise that generates that knowledge (Dastikop, 2005). The FBI estimated the cost of corporate espionage to be as high as \$100 billion per year as of 2007 (Bressler & Bressler, 2015).

Cyber knows no boundaries, and technology allows threats to masquerade as authorized personnel. A hostile environment is characterized by rapid technological change and intense competition (Caltone et al. 1997). Cyber is the epitome of a highly compromised and hostile environment – there is no such thing as cybersecurity. In order to succeed, firms must first concede that they are operating in an insecure, hostile environment, not a fortress (Schwartz & Schuff, 2018).

Unfortunately, a study conducted by Lallie, Debattista, and Bal (2018) found that 91% of CEOs have such limited understanding of cyberspace that they struggle to

interpret cybersecurity reports and lack the knowledge necessary to drive corrective action, resulting in the perspective that cybersecurity is “perpetually inaccessible” (p. 1110). Because of an inability to measure the intangible effects of cyberattack, the impacts of corporate information warfare and cyberattack are underestimated, and many organizations are reluctant to make the necessary capital investments (Al-Ahmad, 2013). However, with emerging trends showing that Wall Street investors are shifting millions into the cybersecurity sector, adapting to the challenges of cybersecurity will increase the long term sustainability and strategic position of those firms willing to address the emerging threats (Manworren et al., 2016).

An adaptive cyber strategy integrates automation, defense, strategic communications, and enhanced decision making with the full spectrum of a firm’s operations, with the understanding that cyberthreat is both opportunistic and strategic, not an unpredictable act of nature. Knowing how cyberattack unfolds within the firm’s virtual landscape is crucial to the development of such a corporate adaptive cyber strategy (Schwartz & Schuff, 2018). However, at present, there is no theoretical lens through which to understand the structure of the firm’s virtual assemblage, limiting a firm’s dynamic adaptation to mutable threats, digital revenue models, influencing campaigns, and evolving opportunities (Schwartz & Schuff, 2018).

Dissertation Structure

This dissertation is structured in three essays which follow the process depicted in the research process flow chart (Figure 1). The first essay derives a “Cyber-Based View” of the firm to explore the dynamic interactions of cyberspace through a review of the current cybersecurity, information systems, and decision theory literature. The second

essay employs a qualitative meta-analysis of cyber-related literature to examine and test current academic theory to shape the theoretical gap to be filled by the Cyber-Based View framework which examines the dynamic interactions taking place. A case study of the Stuxnet cyberattack is used to illustrate this theoretical gap. The final essay refines the investigative utility of the Cyber-Based View to capture the dynamic interactions of cyberspace by using this theoretical lens to analyze eight case studies of successful cyberattacks using a *failure autopsy* approach. Beginning with the preliminary results from the Stuxnet case study a Cyber-Based View analysis of each case study was developed to examine the interactions taking place within the firm as enablers to cyberattack to see what insights would emerge.

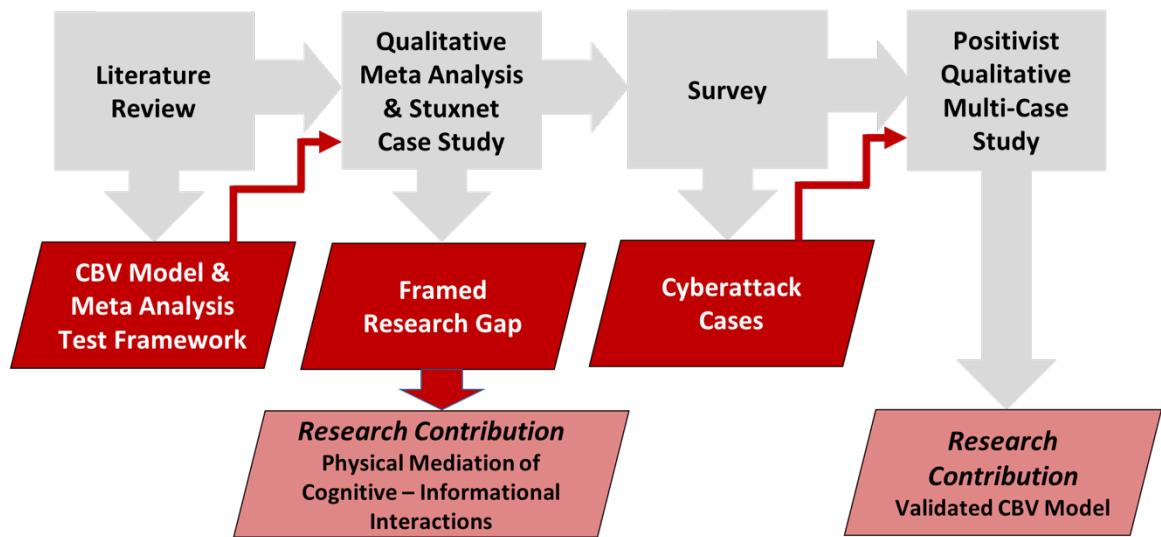


Figure 1: Research Process Flow Chart

The Cyber-Based View is not intended to be a tool solely for cybersecurity, which is a tactical, computer science approach. Instead, the Cyber-Based View is intended to be a theoretical lens exploring the dynamic interactions that are created with digitalization,

enhanced decision making, and process automation. In order to make informed decisions about the trade-offs between capabilities and vulnerabilities that are created with digital and technological solutions, firms must first be able to visualize themselves from a dynamic, cyber-based perspective. By deriving, testing, and applying the Cyber-Based View of the Firm, this paper seeks to answer the following research questions:

1. *How do people, machines, and data interact during a cyberattack?*
2. *How can capturing those interactions enable a firm to build strategic adaptive cyber capabilities?*

CHAPTER 2

CONCEPTUALIZING A CYBER-BASED VIEW OF THE FIRM

Overview

As Ramirez and Chourcri (2016) discovered, “one common ailment of all cybersecurity determined from the literature review is that it is a poorly defined and new academic field, subject to multiple and diverse definitions” (p. 22). In fact, the development of a taxonomy and common language to be used in cybersecurity research is a frequent subject within the computer science discipline (Howard & Longstaff, 1998; Kim, 2010; Ramirez & Chourcri, 2016). The discussion ranges from how to classify computer security incidents (Howard & Longstaff, 1998), and types of hacks (Kim, 2010), to how cyber should be used as a modifier: as in “cyber threat,” “cyber-threat,” or “Cyberthreat” (Ramirez & Chourcri, 2016).

Although there is evidence of multiple, simultaneous interactions taking place amongst people, data, and technology in the cyber domain, current literature does not take a macro-view of these interactions. The absence of both a clear definition and a comprehensive perspective of these interactions dictated the integration of current literature in order to derive a lens designed to examine the research questions. Merging the Information Science, Information Security, Knowledge Management, Social Engineering, and Sociomateriality literature captured a macro-view of the various interactions taking place, offering a new definition of cyberspace and a conceptual framework through which to examine the phenomenon of cyberattack.

How Do We Define Cyberspace?

A common theme in the cybersecurity literature is that cyberspace is both complex and enormous. Human nature is to avoid complexity (Carlo et al., 2012; Smart & Vertinsky, 1984), and this has led researchers to explore cybersecurity as either a computer science security problem (Christin et al., 2010; Howard & Longstaff, 1998; Jing, 2014; Bulgurcu et al, 2010), a tool (Leonardi, 2007; Gaskin et al., 2014; Hirsch-Kreinsen, 2016), or a means to engage in criminal activity (Cavusoglu et al., 2008; Brown, 2015; Choo, 2011). But a macro view of the literature revealed many common themes with Information Warfare (Joint Pub 3-13), including continuity of operations, strategic rivals, decision-making, public policy, and national security.

Cybersecurity applies a physical interpretation to cyberspace, using a Realpolitik lens, which assesses world power based on strong defenses, geography, hierarchy, hard boundaries, and the power of nation states (Arquilla & Rondfeldt, 1999). The information science and information security literature differentiate between information and the systems that deliver information (Chen et al., 2015; McGinn, 1994; Pemberton, 1993). This suggests that cyberspace has both a physical dimension comprised of devices and networks which deliver information, and an informational dimension comprised of something more abstract. Chen et al. (2015) uses the NIST SP 800-60 standard for classifying information assets into four categories:

1. *Data assets*: including databases, data documents, system documents, instruction manuals, educational and training materials, operational or supporting programs, enterprise operation plans, emergency plans, and printed matters.

2. *Software assets*: including application software, system software, development tools, software packages and open source software.
3. *Physical assets*: including computing equipment (i.e. laptops or smartphones), communication equipment (i.e. routers or network switches), storage media, other equipment (i.e. uninterruptible power supplies) and peripherals (i.e., printers, scanners and computer-controlled devices).
4. *Service assets*: including networks and public infrastructure

Pemberton (1993) differentiates information from the devices on which media is stored, which fits into the separated asset classes as defined above, and McGinn (1994) describes the content of a book as being separate from the tome on the shelf.

Cybersecurity literature, which interprets cyberspace as the physical assets that build the networks (service assets) and devices which provide access to information through the networks (Joint Pub 3-12) leads us to the first dimension of cyberspace: *the physical dimension*. Thus *the physical dimension can be defined as the tangible connections between the material world and the virtual world, including devices and networks that provide access to information, including computing equipment, robots, communication equipment, storage media, networks, peripherals (i.e. IoT devices), etc.*

One of the important factors of the physical dimension of cyberspace is that it interacts with information through the transmission, storage, retrieval, and creation of data (McGinn, 1994; Pemberton, 1993). This suggests that cyberspace has an informational dimension comprised of data and information rules (software), and allows the integration of *data assets such as databases, documentation, educational and training materials, planning materials, etc. and software assets, such as business applications,*

decision support software, and process automation into an informational dimension.

Further, the relationship between information and the devices through which information is delivered suggests that there is a feedback loop.

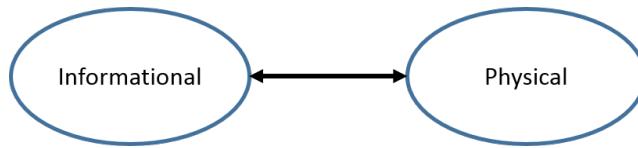


Figure 2. Feedback Loop Between the Physical and Informational Dimensions of Cyberspace

The differentiation of information from the devices and networks that deliver information has begun to lead to the concept of Cyber Defense where organizations identify their critical data and software driven capabilities and prioritize the potential targets (Saydjari, 2004). While cybersecurity is a tactical strategy designed to defend the physical, cyber defense is an operational strategy which integrates the physical and the informational into a larger defensive strategy. This kind of approach is also necessary but insufficient, as it functions at an operational level rather than at the strategic level an adaptive cyber strategy requires.

Adaptive cyber requires an understanding of “Noopolitik,” which “emphasizes the shaping and sharing of ideas, values, norms, laws, and ethics of soft power” (Arquilla & Ronfeldt, 1999), (Arquilla & Ronfeldt, 1999, p. 46). WikiLeaks is an example of the weaponized information of Noopolitik (Xifra & McKie, 2012). Thought communities transcend geography and reside in an intangible place called the “*noosphere*,” described as “an envelope of thought that encompasses the earth” (derived from “*nous*,” the Greek

word for mind) (Teilhard de Chardin, 1959, p. 92) a phenomenon further enabled by the growth of technology.

This concept of noosphere introduces a third element to cyberspace, that of the human mind. Knowledge management literature explores the feedback loop between the human mind and information (Cooper, 2010; Thellefsen et al., 2013; Yuexiao, 1988). Data or datum is a value, which has little meaning to the recipient of that data until it is given context, which becomes knowledge when it is structured and organized as a result of cognitive process (Cooper, 2010).

Thellefsen et al. (2013) explores the feedback loop between information and the human mind, exploring cognition as a mediator between emotion and information where knowledge informs understanding and interpretation of information. Yuexiao (1988) goes a step further and describes information as a uniquely human phenomenon that is an abstract concept “on the same rank with ‘matter’ or ‘energy’” (p. 480). What becomes important is the interaction and interrelation between human thinking and its objects (Yuexiao, 1988). This suggests another bidirectional relationship in cyberspace between the informational dimension and a *cognitive dimension*, where the cognitive dimension is defined as that of the human mind and behaviors such as creativity, decision making, and the growth of knowledge.



Figure 3. The Informational Dimension Joins the Cognitive and Physical Dimensions of Cyberspace

When people speak about the cyber domain, the most tangible definition is the networked infrastructure which creates the internet and telecommunications – the physical dimension, but the most intangible definition begins to describe cyberspace as the “noosphere” (Teilhard de Chardin, 2011) – the integration of information and cognition. Because technology is the primary means of transmitting information amongst people, a comprehensive understanding of cyberspace includes all three elements – people (cognitive), data (informational), and technology (physical).

These three dimensions lead back to the Department of Defense Joint Publication 3-13, Information Operations, which defines an information environment with informational, cognitive, and physical elements where all three elements are interacting simultaneously. Closely tied to the concepts of information warfare contained in Joint Publication 3-13 is the Social Engineering construct. The social engineering literature explores the human as the weakest element of an information ecosystem that needs to be defended (Mouton et al., 2012; Mouton et al., 2014; Mouton et al., 2016; Tetri & Vuorinen, 2013; Flores & Ekstedt, 2016). A social engineer is defined as “a skilled human manipulator, preying on human vulnerabilities using various psychological triggers that could foil human judgment” (Mouton et al., 2012, p. 41).

“Technology on its own is not a sufficient safeguard against information theft; staff members are often the weak link in an information security system” because they are susceptible to manipulation (Mouton et al., 2016, p. 187). Flores and Ekstedt (2016) discuss specific social engineering techniques such as phishing or malicious websites and the failure of technical methods to stop humans from clicking on links that result in the download of malware. The techniques are enabled by the sociomateriality phenomenon.

The concept of sociomateriality draws attention to the way digital technologies have become fundamentally entrenched into the fabric of human activity, making people, process, and technology “inseparable and mutually reshaping” (Gaskin et al., 2014, p. 850). That mutual reshaping is explored by Fuchs et al. (2009) who explain “our concept of the moral system of society is based on a notion of social self-organization as dynamic process, in which human actors communicate in such a way that they produce and reproduce social structures...” (p. 454). The concept of human actors engaged in dynamic change of social structures suggests that the physical dimension also includes *tangible outcomes* as connections between the virtual world and the material world.

Tetri and Vuorinen (2013) look at information ecosystems as an actor network (Latour, 2005) where devices and humans are all elements of the network with social entry points, which could be a human being, or could be something physical, such as a stolen computer or discarded information in a waste receptacle. In other words, because of sociomateriality, there is not just a relationship between people and information, but also between the human and the physical elements of cyberspace, which changes the Figure 2 model from a linear relationship to a feedback loop amongst all three dimensions.

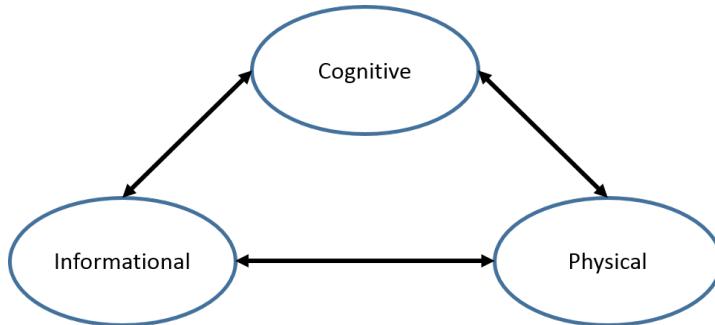


Figure 4. Feedback Loop Amongst Cognitive, Physical, & Informational Dimensions

By making the problem of defining cyberspace bigger and integrating the Information Science, Information Security, Knowledge Management, Social Engineering, and Sociomateriality literature, we can arrive at the following definition: ***Cyberspace is comprised of three, interdependent physical, informational, and cognitive dimensions which continuously interact between systems, individuals, and organizations both within and beyond the firm.*** The interdependent dimensions can be further defined as follows:

- The *Physical Dimension* is the tangible connections between the material world and the virtual world, including both *objects*, such as devices and the networks that connect them, and *outcomes* that result from humans engaged in the dynamic change of social structures. It is a diffused network connected across national, economic, geographical, social, and firm boundaries.
- The *Informational Dimension* is where critical data is created and captured, contextualized, and shared across the firm. It is a vast ecosystem of information, information rules (software), and knowledge resources where data and media of all kinds are processed, stored, distributed, and managed.
- The *Cognitive Dimension* encompasses the human mind. It includes a firm's individuals and groups responsible for information processing, perception, judgement, creativity, decision making, and knowledge growth. It also includes stakeholders and rivals. Factors influencing these elements include individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies (Joint Pub 3-13).

The *Cyber-Based View of the Firm* (Figure 4), provides a graphic illustration of this definition of cyberspace, which can be used to examine the interdependence of individuals, organizations, and systems within the firm. It is intended to leverage existing firm resources for the purpose of building a dynamic, adaptive cyber capability, of which cybersecurity is only a very small piece.

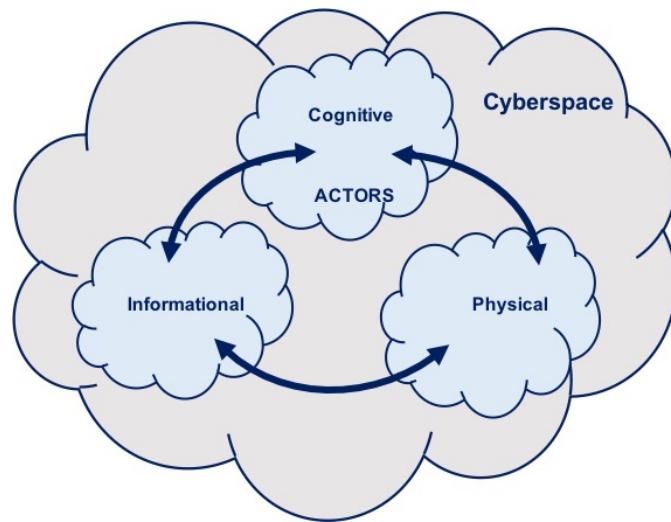


Figure 5. Cyber-Based View of the Firm

Literature Review

General Themes in Cybersecurity Literature

Going beyond the struggle for a basic taxonomy to discuss cybersecurity, exploration of cybersecurity literature reveals a great deal of interest from the systems engineering, information systems, computer science and economics disciplines in critical infrastructure both from a public policy perspective (Gal-Or & Ghose, 2005; Smith et al., 2010; Clinton, 2011) and a resilience or business continuity perspective (Ambs et al., 2000; Cerullo & Cerullo, 2006; Henry & Ramirez-Marquez, 2016; Ortiz-de-Mandojana & Bansal, 2016; Sahebjamnia et al., 2015; Riolli & Savicki, 2003). This particular

interest in critical infrastructure arises because of the extraordinary escalation in cybercrime which Brown (2015) attributes to the “rapid advancements in the functionality of information communication technologies” (p. 56) that are “increasingly interconnected through networked infrastructures” (p. 76) that span geographical boundaries.

Cybercrime and hacker behavior (Karatzogianni & Gak, 2015; Haggard & Lindsay, 2015; Kim et al., 2010; Choo, 2011; Brown, 2015; Cavusoglu et al., 2008) are emerging subjects within the computer science, criminal justice, economics and legal literature due to “the ease with which cybercrime crosses national borders, and the stark challenges for first responders, investigating authorities, forensic interrogators, prosecuting agencies, and administrators of criminal justice” (Brown, 2015, p. 56). Kim et al. (2010) discusses the dark side of the internet which he suggests we will never be able to eliminate, but at best control “to a tolerable level, just has been the case for the offline world” (p. 676). While Cavusoglu et al. (2008), Brown (2015), and Choo (2011) use various theories to understand hackers as strategic rivals. Table 1 offers a high level capture of theory used to shape the Cyber-Based View.

Table 1. Shaping the Cyber-Based View of the Firm with Theory

Theory	Research Discipline	Cyber Topic	High Level Summary	References
Information	<ul style="list-style-type: none"> • Library Science • Information Science 	<ul style="list-style-type: none"> • Defining information 	Differentiates between information, an abstract concept tied to cognition, and the methods and devices through which information is delivered	Pemberton, 1993 Yuxiao, 1988 McGinn, 1994
Information Security	<ul style="list-style-type: none"> • Computer Science • MIS 	<ul style="list-style-type: none"> • Securing information assets 	Identifies information assets (RBV), which they classify into 4 separate categories: physical assets, network assets, data assets, and software assets	Chen et al., 2015 Posey et al., 2013

Knowledge Management	<ul style="list-style-type: none"> • Health Informatics • MIS • Information Science 	<ul style="list-style-type: none"> • Identifying information assets • Understanding critical data 	A feedback loop between human cognition and data to bring context to the data and create meaning, resulting in the growth of knowledge and wisdom	Cooper, 2010 Thellefsen et al., 2013
Social Engineering	<ul style="list-style-type: none"> • Computer Science • Information Technology 	<ul style="list-style-type: none"> • Hacking the human • Social Engineering threat model 	Explores the use of social behavior to influence people to take specific actions that result in access to physical and informational assets. They discuss cognitive measures of social engineering as being evidenced through action	Mouton et al., 2012 Mouton et al., 2014 Mouton et al., 2016 Flores & Ekstedt, 2016 Tetri & Vuorinen, 2013
Sociomateriality	<ul style="list-style-type: none"> • Information Systems • Computer Science • Systems Engineering 	<ul style="list-style-type: none"> • Internet of Things • Dialectics of IT • Digitization • “Cyborg” 	With the internet of things, wearable/portable technology, social media, process automation, and big data, technology and individuals are no longer separate entities. They behave as an integrated, interdependent unit.	Carlo et al., 2012 Gaskin et al., 2014 Cecez-Kecmanovic et al., 2014 Jones, 2014 Leonardi & Barley, 2007 Orlikowski, 2007, 2010 Orlikowski & Scott, 2008
Moore's Law	<ul style="list-style-type: none"> • Computer Science 	<ul style="list-style-type: none"> • Rapid Change 	Explains the rate of technological change	Moore, 1965 Shalf & Leland, 2015 Strawn & Strawn, 2015
Resilience	<ul style="list-style-type: none"> • Systems Engineering • Strategy • Economics • Psychology 	<ul style="list-style-type: none"> • Critical Infrastructure • Proactive Planning • Business Continuity 	Because of automation, information systems are enmeshed with the operation of critical infrastructure and business operations. In order to ensure continuity of operations, information systems and firms must be able to recover quickly after sudden loss of failure	Ambs et al., 2000 Cerullo & Cerullo, 2006 Devendandham & Ramirez-Marquez, 2016 Ortiz-de-Mandojana & Bansal, 2016 Sahebjamnia et al., 2015 Rioli & Savicki, 2003
Resource Based Perspective/ Resource Based View (RBP/RBV)	<ul style="list-style-type: none"> • Information Systems • Economics • Strategy 	<ul style="list-style-type: none"> • Proactive Corporate Social Responsibility • Voluntary Disclosure of Info Security Breaches 	Investing in socially responsible corporate behavior can lead to the development of intangible resources. Proactive approaches to Environmental issues, though costly in the short term, leads to reputational resources, cost savings, and other long term benefits.	Aragon-Correa & Sharma, 2003 Hovav & D'Arcy, 2003 Gordon et al., 2010 Bronco & Rodrigues, 2006 Lockett et al., 2006 Surroca et al., 2010

			Disclosure of both proactive environmental programs and proactive cybersecurity measures suggests a positive effect on reputation	
Salience	<ul style="list-style-type: none"> • Economics • Psychology • Marketing • Strategy 	<ul style="list-style-type: none"> • Security Investment Decisions • Stakeholders 	The salience of alternatives in decision making determines the level of risk-taking or risk aversion, but salience is not based on probability, rather perception of rewards/costs and greater salience is placed on reward. Greater complexity leads to lesser salience with regard to risk.	Bordalo et al., 2012 Herzenstein et al., 2007 Mitchell et al., 1997 Kahneman & Tversky, 1979 Tversky & Kahneman, 1981 Taylor & Thompson, 1982 Bordalo, Gennaioli & Shleifer, 2010
Game Theory	<ul style="list-style-type: none"> • Information Systems • Economics 	<ul style="list-style-type: none"> • Hacker Strategy • Cybercrime • Cyber Policy 	Both hackers and rival firms are strategic actors, and a firm's cybersecurity decisions need to take the strategic nature of rivals (both firms and hackers) into account.	Cavusoglu et al., 2008 Gal-Or & Ghose, 2005
Taxonomy/Classification	<ul style="list-style-type: none"> • Computer Science 	<ul style="list-style-type: none"> • Common language for cyberattack 	Cyberspace, cyberthreats, types of cyberattack and other language used to conduct research in cyber have yet to be defined, so multiple taxonomy papers have been published to propose common language	Howard & Longstaff, 1998 Kim et al., 2010 Ramirez & Chourcri, 2016
Agency Theory	<ul style="list-style-type: none"> • Forensic Science • Information Systems • Organizational Behavior • Public Policy 	<ul style="list-style-type: none"> • Cybercrime • Cyber Public Policy 	Firms, people within firms, and hackers are all agents who make choices related to cybercrime and cyber defense based on the financial incentives and consequences related to cyberattack	Brown, 2015 Smith et al., 2010
Power/Resistance	<ul style="list-style-type: none"> • Organizational Behavior • Public Policy 	<ul style="list-style-type: none"> • Cyber Public Policy 	Individuals within organizations respond to information security policy based on perceptions of power	Smith et al., 2010
Organizational Theory	<ul style="list-style-type: none"> • Strategy 	<ul style="list-style-type: none"> • Organizational adoption of CSR issues 	How firms choose to champion issues of corporate social responsibility such as environmentalism	Bansal, 2003
Social Exchange Theory	<ul style="list-style-type: none"> • Public Policy 	<ul style="list-style-type: none"> • Cyber Public Policy 	How regulatory public policy fails due to a lack of	Clinton, 2011

			perceived benefit to a public – private partnership	
Routine Activity Theory	• Computer Science	• Cybercrime • Cyberthreat • Hacker Strategy	How Routine Activity Theory can be applied to inform and enhance cybercrime prevention strategies	Choo, 2011
Weberian Theory	• Sociology	• Hacker social groups	Discussion of hackers' perceptions of privacy	Steinmetz & Gerber, 2015
Totalitarianism/ Quasi-totalitarianism	• Philosophy • Sociology	• Surveillance • Hacker behavior	Discussion of hackers, hacktivism, government surveillance, and privacy	Steinmetz & Gerber, 2015 Karatozogian & Gak, 2015
Vigilantism	• Technology & Policy	• Hacktivism	Discussion of internet activism and Anonymous as vigilantes	Serracino-Inglott, 2013
Bourdieu's Field Theory	• Media & Culture	• Hacker behavior	How hacker communities contest social capital	Nycyk, 2016
Anonymity	• Forensic Science • Computer Science • Technology & Policy	• Hacker behavior	How anonymity plays a role in hacker behavior and the challenges with attribution of attacks	Haggard & Lindsay, 2015 Brown, 2015 Choo, 2011 Serracino-Inglott, 2013

Moore's Law & Sociomateriality

Conceiving of cyberspace as a domain of interdependent dimensions as depicted in Figure 1 illustrates a number of phenomena at work with respect to the cyber construct. The first phenomenon at work is the growth of cyberspace, which expands the size and scope of both the Physical Dimension and the Informational Dimension. The seedlings that led to the growth of cyberspace were first observed by Gordon Moore in 1965, who observed that the number of components on an integrated circuit had approximately doubled annually since 1959. Though Moore predicted this phenomenon would last only a decade, in 2015, the IEEE celebrated the 50th anniversary of his observation. Known as Moore's law, it has continued to apply to the semiconductor industry for over 50 years (Shalf & Leland, 2015). In fact, the speed of technology growth is so fast, that digital

technologies have become embedded in the fabric of organizations as the capabilities and functionalities of technology emerge (Gaskin et al., 2014).

Cyberspace, which is created by the integration of the cognitive, physical, and informational dimensions, is constantly growing, a phenomenon that can be explained by Sociomateriality theory, which seeks to understand the interdependence of the social—cognitive dimension—with the material—physical and informational dimensions (Orlikowski, 2007, 2010; Leonardi & Barley, 2008; Orlikowski & Scott, 2008; Carlo et al., 2012; Gaskin et al., 2014; Cecez-Kecmanovic et al., 2014; Jones, 2014).

The concept of sociomateriality draws attention to the entrenchment of digital technologies with human activity (Gaskin et al., 2014). Cyberspace, defined with physical, informational and cognitive dimensions, illuminates this immersive relationship.

Information technologies can take existing data and transform it into new kinds of information, enabling people to accomplish things that were impossible in the past (Leonardi & Barley, 2008). “Instead of assuming that entities, people, and technologies have inherently determinate boundaries and properties” (Cecez-Kecmanovic et al., 2014, p. 811), sociomateriality proposes that there are relational effects (Cecez-Kecmanovic et al., 2014). These relational effects can be captured with the Cyber-Based View through the confluence of *the physical dimension* – where the infrastructure and networks (Joint Pub 3-13) enable movement of the digital, *the informational dimension* – where the data is stored, processed, and disseminated (Joint Pub 3-13), and *the cognitive dimension* – where the information moves into the mind of the human. Essentially, cyberspace, with its three dimensions, is a product of the sociomateriality phenomenon.

Gaskin (2014) tells us that “humans and nonhumans are ontologically inseparable in practice,” (p. 851) with organizations comprised of sociotechnical systems consisting of human and technological elements which are nested like Russian Matryoshka dolls (Gaskin, 2014).

“The social world is in a continuous state of becoming” (Carlo et al., 2012, p. 1084). Prior to the year 2000, technological change happened much more slowly, and the impact of new technologies took years or even decades to emerge (Berman & Marshall, 2014), but the exponential speed of information technologies as explained by Moore’s Law (Moore, 1965; Strawn & Strawn, 2015) has caused technological change to occur in a very compressed time span (Berman & Marshall, 2014). It is this exponential, technological growth rate (Strawn & Strawn, 2015), leading to the rapid digitization of the organization, which expands the scale of cyberspace within the firm with “increasingly complex materiality of everyday information systems-mediated work practices” (Cecez-Kecmanovic et al., 2014, p. 810). But rapidly changing environments present organizations with increasing complexity (Carlo et al., 2012). For example, in a sociomateriality study of Critical Care, Jones (2014) found:

“For most staff, the performance of their work was also inseparable from technology. While this was most evident with respect to the devices, such as syringe drivers and drips, used to administer medication or to sustain vital functions, such as hemofiltration or ventilation, the operation and maintenance of which took up a considerable amount of nurses’ time, it was also the case for patient records, whether on paper or computer-based. This reflected not just the time taken in entering or validating data, but the dependence of many work activities on the evidence provided by the record, whether directly, (for example, where the record indicated the timing and dosage of medication to be administered) or indirectly (for example, where the trend in a vital function might prompt a particular intervention, such as adjustment of the ventilation rate. The data held in the record was a key element in the medical staff’s understanding of the patient’s condition on which they based their actions.” (p. 910)

Jones (2014) goes on to explain that regardless of whether the records were digital or paper, that it became “difficult, if not impossible to carry out their work if the record was

unavailable," (p. 910) and that this dependence was even more notable when the patient records were digital (Jones 2014). The Cyber-Based View of this example is shown in Figure 5.

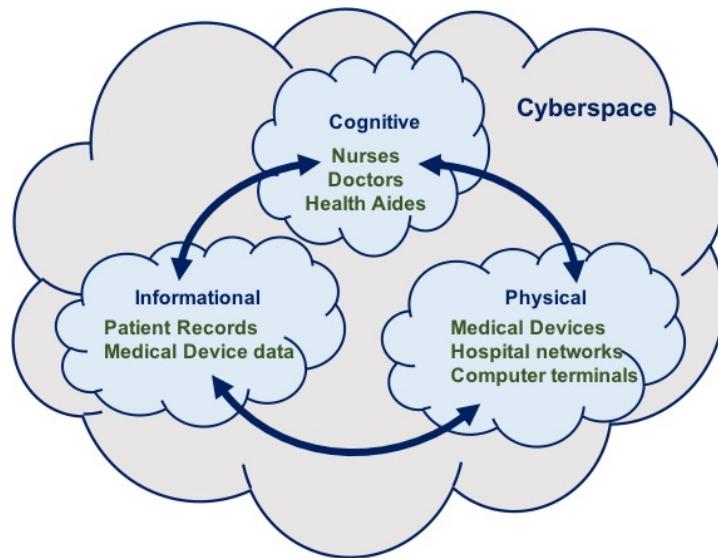


Figure 6. A Cyber-Based View of Jones (2014) Sociomaterial Observations of Critical Care

Cecez-Kecmanovic, et al. (2014) explain that materiality is present in every social phenomenon. They go so far as to suggest that with the advent of wearable technology such as the Fit Bit or Jawbone, human activity is becoming more and more digitized (Cecez-Kecmanovic et al., 2014), making the concept of the cyborg, a human – machine hybrid, applicable to everyday life (Cecez-Kecmanovic et al., 2014). Indeed, as organizations become more cyborg, the Cyber-Based View becomes an essential lens through which to examine firm strategy.

Resilience

Resilience is defined in the systems engineering and psychology literature as the ability of individuals, groups, organizations, and systems (Riolli & Savicki, 2003) as a whole to recover from an event that disrupts expected patterns (Riolli & Savicki, 2003;

Henry & Ramirez-Marquez, 2016; Dinh et al., 2011) and get operations back on track (Dinh et al., 2011). Ortiz-de-Mandojana and Bansal (2016) define resiliency as “an interdisciplinary concept that describes the dynamic development of complex adaptive systems that interact across temporal and spatial scales” (p. 1617). This concept of resilience lends itself to a Cyber-Based View with its physical, informational and cognitive dimensions.

The United States Government has numerous organizations dedicated to making public policy as it relates to cybersecurity and the resilience of critical infrastructure, examples include divisions within the Department of Homeland Security (DHS, 2016), the Department of Defense (USSTRATCOM, 2015), the Department of Energy (DoE, 2016), the Department of State (U.S. DoS, 2014), and the National Institute of Standards & Technology (NIST, 2016). There are also various Public – Private Partnerships to increase cybersecurity situational awareness in the private sector, with Information Sharing & Analysis Centers dedicated to each of twenty-one critical infrastructure sectors (National Council of ISACS, 2016). Critical infrastructure in the United States and other developed countries is particularly vulnerable to cyberattack because the critical infrastructure systems depend on the Internet for information exchange (Zobel & Khansa, 2012; Snedicker et al., 2007). But as Choo (2011) points out, “an open nation cannot shut down its cyber systems for fear of threats. Instead it must build the national resilience needed to maintain an open, yet secure cyberspace.”

Of particular concern are the ripple effects of a cyberattack (Zobel & Khansa, 2012). Because “networks of all types are increasingly vital to numerous aspects of daily life” (Snedicker et al., 2007, p. 954), cascading failures are of primary concern. While a

short term electricity outage is inconvenient, a prolonged loss of power can bring life to a standstill (Henry & Ramirez-Marquez, 2016). The hack that shut down the Ukrainian power grid in Kiev in December 2016 lasted only an hour (Ng 1, 2017), but it was a warning. The same malware that caused the outage was used in an experiment by engineers to hack into the Los Angeles traffic signal systems and create city wide traffic jams (Ng 1, 2017). It is only a matter of time before attacks like these lead to more significant impacts on critical infrastructure.

For example, the sociomateriality phenomenon has led to the introduction of sensor technology into the electric power infrastructure. *The Smart Grid* will add millions of electronic devices via open communication networks throughout critical power facilities, the majority of which are privately owned (Wang & Lu, 2013). This optimization of the electric power infrastructure comes at a cost. By introducing millions of digital entry points into the power grid, the underlying foundation of all critical infrastructure networks becomes accessible to anyone with an internet connection (Wang & Lu, 2013). This, in turn, will affect the resilience of the electrical grid and all those critical infrastructures and operations that it supports (Henry & Ramirez-Marquez, 2016).

It is this complex entanglement of the material into the tapestry of the firm that places cyber resilience at the heart of firm operations. Business continuity hinges on a firm's preparation for disruptive events, and demands anticipatory planning with respect to internal and external resources so that it can effectively cope with disasters (Sahebjamnia et al., 2015). Hackers understand that "technology is a highly effective force multiplier that can be leveraged to facilitate access to a global constituency of victims" (Brown, 2015, p. 100); however, without viewing the firm through a Cyber-

Based View, firm resilience may be overestimated. Attacks on computer systems are increasing at an exponential rate. It is no longer a question of if, but when and how often a firm will be attacked (Dinh et al., 2011; Brown, 2015; Choo, 2011). Consequently, information technology security is no longer a luxury (Cavusoglu et al., 2008).

Despite the fact that cyberthreats include both internal and external business continuity risks (Cerullo & Cerullo, 2006), the majority of resilience literature focuses on acts of nature (Cavusoglu et al., 2008). Cerullo and Cerullo (2006) found that a 2002 survey identified that business continuity professionals “were most concerned with accidental failures first, and natural disasters second” (p. 72). Intentional, externally caused disasters, such as cyberattack, were ranked third (Cerullo & Cerullo, 2006).

In fact, cyberattack is not a product of nature or accidental failure. It is a deliberate human action designed to sabotage operations (Dinh et al., 2011), and in order to determine how to sabotage a firm’s operations, hackers will use a Cyber-Based View-like approach to decide where a firm is least resilient in order to coerce firms to alter their business plans (Haggard & Lindsay, 2015).

Zobel and Khansa (2012) define the resilience of a cyber infrastructure system as its ability to quickly and cost effectively resume close-to-normal operations following a cyberattack. They also offer a second definition: the ability of a system to endure disruption, experience change, and still preserve the same basic identity, structure, functionality, and feedback (Zobel & Khansa, 2012). Snedicker, et al. (2007) express concern that as networks grow and expand (i.e. the growth of cyberspace), there is a decrease in the redundancy and connectivity of many network structures, a critical element of resilience (Snedicker et al., 2007). But it is important to differentiate between

resilience and risk management (Ortiz-de-Mandojana & Bansal, 2016) because “risk management assumes that hazards are identifiable, whereas resilience prepares organizations for the unexpected” (Ortiz-de-Mandojana & Bansal, 2016, p. 1619).

The Resource Based Perspective

This differentiation between resilience and risk management becomes critical to a Resource Based View, which suggests that proactive planning in order to build resilience can lead to the development of intangible resources. For example, a qualitative study of AT&T’s restoration capacity, conducted by Ambs in 2000, found that building in excess capacity to ensure reliability and restoration in instances of outages, created additional capability that can be used to generate revenue. Unfortunately, building resilience is often evaluated in the context of short-term profitability, leading “firms that follow a short-term approach often [to] forgo investments in such practices” (Ortiz-de-Mandojana & Bansal, 2016, p. 1620).

Resilience creates adaptable, perceptive resources that help firms survive and respond to a changing environment (Ortiz-de-Mandojana & Bansal, 2016), but a lack of proactive planning can impact reputation or market share (Sahebjamnia et al., 2015). Proactive companies develop trust and credibility with a variety of stakeholder groups that cannot be easily imitated by competitors (Sharma & Vrendenburg, 1998).

Evidence of this perception is born out in a study by Hovav and D’Arcy (2003), who explored the effect of announcements regarding Denial-of-Service attacks on the market value of firms. Their findings suggest that “there is some indication that [Denial-of-Service attacks] do have an impact on companies that rely on the Web for their business” (Hovav & D’Arcy, 2003, p. 108).

This idea is further supported in a 2010 study by Gordon, Loeb, and Sohail which investigated the impact of voluntary disclosure of proactive security investments. They used a coding approach to determine types of security breaches, and then analyzed the impact the disclosure had on the firm using stock price and earnings per share, concluding that their findings provided “strong evidence that voluntarily disclosing items concerning information security is associated positively with the market value of a firm” (Gordon et al., 2010, p.567).

This relationship between market value and firm disclosures regarding information security closely parallels similar programmatic disclosures related to environmental and Corporate Social Responsibility programs. A 2003 study conducted by Aragón-Correa and Sharma using a resource based view to examine corporate environmental strategy found a proactive environmental strategy to be a dynamic capability that can generate a competitive advantage in a hostile business environment where competitors lack the same capability.

A similar observation was made by Gal-Or and Ghose (2005) with respect to proactive information security investments. They found that increased security technology investments shift demand outward and raise the firm’s price reaction function (Gal-Or & Ghose, 2005). They also identified spillover effects within the industry regarding information sharing related to cybersecurity (Gal-Or & Ghose, 2005). This too, mirrors the impact of proactive environmental programs within industries (Ortiz-de-Mandojana & Bansal, 2016; Bronco & Rodrigues, 2006; Sharma & Vrendenburg, 1998).

In much of the United States Government policy regarding resilience and cybersecurity, the most important policy concept is recognizing that privacy is a

fundamental element of preserving cyber resiliency rather than a trade-off between privacy and security (Hiller & Russell, 2017). Currently the privacy risk model requires an organization to:

1. Audit its data actions,
2. Assess the likelihood of individual privacy harm,
3. Determine the impact that harm would have on the organization (Hiller & Russell, 2017)

Note that this impact is analyzed from the organizational perspective, rather than the private citizen (Hiller & Russell, 2017). This is also very similar to the way a firm's environmental impacts were perceived in the latter part of the twentieth century (Htun, 1990). But as public perceptions have changed, it has become evident that socially responsible firms are able to generate intangible capabilities such as innovation and reputation (Surroca et al., 2010).

Corporate strategies for managing the interface between the firm and cyberspace can be classified along a continuum that ranges from reactive to proactive, not unlike corporate environmental programs (Aragon-Correa & Sharma, 2003). Information technology investments are often assessed with respect to profitability – increased revenue/decreased cost, productivity – reduced defect rate, or consumer value – ease of use or personalized services (Cavusoglu et al., 2008), but ROI is not easily applied to security investments. Intangible losses, such as a loss of reputation or competitive advantage, are not included because they are not directly measurable (Hovav & D'Arcy, 2003). The physical and information dimensions of cyberspace (the material elements) are viewed as distinctly separate from the cognitive dimension of cyberspace (social), but

sociomateriality proposes that technology and organizations are inextricably entangled (Jones, 2014). The use of a Cyber-Based View of the Firm could enable the integration of cyber defense issues with core strategic issues because it changes the perception of cyberspace from one of geographic and physical boundaries created and defended by things, to one that embraces the interdependent nature of the human mind, the information the mind consumes, and the means through which information and machines are used to generate competitive advantage. This integration of corporate performance, cyber defense, and corporate social responsibility recognizes the interconnectedness of cyberspace, economic prosperity, and social equity (Gao and Bansal, 2013).

The exponential technology growth rate has expedited the rate of change in organizations (Strawn & Strawn, 2015), increasing uncertainty. Coping with uncertainty in hostile environments has long been considered a central problem for firms (Aragon-Correa & Sharma, 2003), but a proactive adaptive cyber strategy can build up internal capabilities and knowledge-based assets (Sharma & Vrendenburg, 1998). Intangible resources and capabilities are expensive and difficult to create because they are complex, contextual and ambiguous, which is why they create a competitive advantage (Bronco & Rodrigues, 2006). Gal-Or and Ghose (2005) found that firms engaging in proactive information security behaviors experienced both a direct effect which increased demand, and a strategic effect, which alleviated price competition.

Cyberspace is contested terrain, as are resources and capabilities (Bronco & Rodrigues, 2006). Hackers understand this highly contested terrain, because, as a Cyber-Based View of the firm demonstrates, many of these resources and capabilities are supported in cyberspace. When a firm is confronted with strategic hackers, not only does

the firm's security investment strategy determine system vulnerability, but also the hacker's effort (Cavusoglu et al., 2008).

Organizations are confronted with numerous issues while being limited by managerial and resource constraints (Bansal, 2003), and cybersecurity measures are often not easily measured. How do you quantify the value of the absence of disruption – particularly with a short-term investment approach? However, a study by Ortiz-de-Mandojana and Bansal (2016) showed that “despite resilience not being directly measurable...the practices that lead to resilience resulted in lower financial volatility, higher long-term growth, and a higher survival rate over 15 years of data” (p. 1628). Which suggests that the decision making approaches used to evaluate cybersecurity and resilience investments may be flawed.

Salience

As with most intangibles, it is difficult to attach a financial value to resilience. Further, without a comprehensive understanding of the extent of our enmeshment with cyberspace, analyzing the risks and rewards of cyber investments becomes very challenging. The effect of salience on digitization and cybersecurity choices is unclear, but given the intangible nature of resilience, and the more tangible, quantifiable nature of process automation, it is very likely that salience plays a significant role in how cyber investment decisions are made, both from an automation perspective and from a security/defense perspective. Essentially when faced with decisions that involve risk, the decision makers place greater weight on the upside of a high risk choice when it is salient, thus behaving as a risk seeker (Bordalo et al., 2012).

Salience, as described by Taylor & Thompson (1982), “refers to the phenomenon that when one’s attention is differentially directed to one portion of the environment rather than to others, the information contained in that portion will receive disproportionate weighting in subsequent judgements” (p. 175). The salient payoffs are the outcomes of choice that draw a decision maker’s attention and lead to either risk-seeking or risk-aversion (Bordalo et al., 2012). More generally, salience offers theory surrounding context-dependent choice (Bordalo et al., 2012).

Kahneman and Tversky (1979) observed that people have limited “ability to comprehend and evaluate extreme probabilities” (p. 283). This suggests that while a Cyber-Based View of the firm indicates the considerable interdependence of people, process, information, and technology, our ability to comprehend the potential impact of a successful cyberattack may be limited due the fact that we have little firsthand experience with loss of critical infrastructure as a result of cyberattack. However, the 2008 Russian use of cyberwarfare against Georgia indicates the integration of cyberattack with kinetic attack on the electric power infrastructure by shutting down internet resources at generator rental facilities (Kozlowski, 2014). While the actual tangible costs of this cyberattack were small (Kozlowski, 2014), the rate of technological growth creates more attack vectors, increasing firms’ vulnerabilities (Brown, 2015).

Cavusoglu, Raghunathan, and Yue (2008) found that “an examination of current business practices in IT security management reveals that managers generally view security investment as any other IT investment” (p. 282). A study by Bordalo, Gennaioli, and Shleifer (2010), suggests that decision makers do not take all available information into account, and instead, overemphasize the information that draws their

attention. Though cyberattack has potential to do significant harm, to date, the tangible financial costs have been relatively insignificant from a firm perspective (Kozlowski, 2014). But in 2014, Cyber Risk moved into the top 10 global business risks for the first time, rising over 400% from 2005-2014 (Hartwick & Wilkinson, 2014).

The 2010 Stuxnet attack at the Natanz nuclear facility in Iran, which sabotaged the uranium enrichment facility to such an extent that it set back their program by several years (Zetter, 2014), is a prime example of the significant costs of a cyberattack, however unlikely such an attack may be perceived. Unlike conventional weapons, cyberweapons can be repurposed and reused, so that even the originator of a cyberweapon can have it turned back upon them (Weinberger, 2011), however low the probability might be.

Bordalo, et al. (2012), learned that low probabilities are relatively more distorted than high ones, which supports Kahneman and Tversky's (1979) observation about limited human ability to comprehend extremes. In other words, the perception of a Cyber 9/11 as a black swan event versus a likely possibility, despite the expansion of the internet of things is attributed very little salience, and a risk seeking preference for a significant loss that is probable – cyberattack – over a smaller loss that is certain – the cost of cybersecurity investment (Kahneman & Tversky, 1979). Salience also explains the growth of automation, as the benefits of automation are afforded greater salience than the creation of new vulnerabilities. Tversky and Kahneman (1981) continued to explore the phenomenon of salience, concluding that insurance is more attractive when it eliminates risk versus merely reducing risk. Because of Moore's law, technology is in a constant state of change (Moore, 1965; Strawn & Strawn, 2015; Shalf & Leland), thus cybersecurity investments can only reduce risk, not eliminate it.

Further, as Hiller and Russell (2017) point out that where privacy concerns are at stake, cyberattack impact is measured from the firm perspective, which suggests that stakeholder salience can illuminate to whom and to what managers attention is paid (Mitchell et al., 1997). This reinforces the concept of cyber defense as a Corporate Social Responsibility, without which the salience of involuntary stakeholders placed at risk within a firm's cognitive, physical, and informational dimensions, is less likely to be taken into account (Mitchell et al., 1997; Lockett et al., 2006).

The Cyber-Based View of the firm can offer greater context to cybersecurity investment decisions, as decisions are shaped by the context and salience of payoffs and costs (Bordalo et al., 2012). And, as discussed earlier, the Cyber-Based View can complement the RBP/RBV, which incorporates intangibles such as resilience, into the understanding of payoffs. Finally, the cognitive dimension of cyberspace integrates the very act of decision making, and thus salience, into the Cyber-Based View of the Firm.

Game Theory

But a firm's decision makers are not the only actors functioning in the cognitive domain. Hackers, rival firms and other firm stakeholders are also active in the cognitive domain, which brings in the last significant piece of the Cyber-Based View of the Firm: *Game Theory* and the strategic nature of rivals and adversaries.

While the majority of analysis of the Sony Pictures hack explored the technical dimensions of the attack and the implications regarding North Korea's cyber capabilities, Haggard and Lindsay (2015) explored the attack with respect to motivation and future asymmetric conflict. They found that "there is plenty of evidence that authoritarian

governments use cyber tools to silence critics and dissidents abroad” (Haggard & Lindsay, 2015).

“To win over the masses, the totalitarian agent deploys mechanisms of inculcation. Propaganda is central to the construction of political imaginary of the public. [It] is not aimed at what individuals do, but rather at what individuals think and feel” (Karatzogianni & Gak, 2015). Propaganda is an attack targeting the cognitive dimension of cyberspace. The Sony hack is a prominent example of a cyberattack targeting the cognitive dimension in order to influence a firm’s business plans (Haggard & Lindsay, 2015, p. 6). Another example of a significant hack on the cognitive domain is the 2013 hack of the AP twitter feed by Syrian hackers claiming President Barak Obama has been injured in an explosion at the White House, which led to a 143.5-point drop in the Dow Jones Industrial Average and a loss of more than \$136 billion U.S. Dollars in the Standard and Poor’s 500 Index (Prigg, 2015). Mihailidis and Viotty (2017) explored the use of misinformation in the 2016 United States Presidential Election.

The common link among these three examples is that information was weaponized. In each instance, the attack began on the computers and networks of the physical dimension in order to break into the informational dimension where data was either created, stored or disseminated, and ultimately striking the primary target – the cognitive dimension. In other words, the actors perpetrating these cyberspace attacks were extremely strategic in nature.

Cavusoglu, Raghunathan, and Yue (2008) explain that decision theory explores situations where “nature is the only opponent, but this is inadequate to address decisions about security investments” (p. 283). The above discussion of salience theory suggests

that managers perceive the rewards of digitization as more salient than the risks, but traditional decision models are limited when applied to analyze IT security problems because they “do not allow a firm’s security investment to influence the behavior of hackers” (Cavusoglu et al., 2008, p. 283).

Instead, Cavusoglu, Raghunathan and Yue (2008) proposed that “we need to model threats and vulnerabilities, which are determined by the strategic interactions between organizations and hackers. Game theory is appropriate to model such strategic interactions” (p. 285). When applying a game theory model, they discovered evidence of a first mover advantage for firms who act strategically and make their move prior to hackers (Cavusoglu et al., 2008).

Interestingly, Gal-Or and Ghose (2005) also found evidence of first mover advantage when applying a game theory model to security investment decisions. However, they found evidence of first mover advantage with respect to rival firms (Gal-Or & Ghose, 2005). They also found spillover effects that influenced security investment decisions within the industry, and that “these incentives become stronger with increases in firm size and the degree of competition” (Gal-Or & Ghose, 2005, p. 200).

Cybersecurity Investment Decisions – Further Application of Salience & Game Theory

Both resiliency (disruption or continuity of operations) and the RBP/RBV (tangibles and intangibles) inform decision making – the cognitive dimension – with respect to cybersecurity and digitization investments. But Salience Theory proposes how decision makers weight potential rewards and risks. Salience theory takes into account both confirmation bias and desirability bias (Tappin et al., 2017) and the manner in which “one’s attention is differentially directed to one portion of the environment rather than to

others [such that] the information contained in that portion will receive disproportionate weighting in subsequent judgements” (Taylor & Thompson, 1982, p. 175). Understanding the salience of both digitization (rewards) and cyber vulnerability (risks) in the context of the Cyber-Based View can provide insight into cyber investment decisions.

Game Theory also offers insights related to both cybersecurity investment decisions and hacker behavior. Fielder et al. (2016) used game theory to understand how organizations balance network defense with respect to the cost in implementing a particular defense and the impact defense has on the business, while Gal-Or and Ghose (2005) suggest game theory as a means to explore how a firm’s cybersecurity investment affects rival firms within the same industry.

Cybersecurity investment as it relates to disruption of operations and resilience is often explored in the context of a natural phenomenon (Ortiz de Mandojana & Bansal, 2016), but Cavusoglu et al. (2008) suggest that hackers do not behave in the manner of a natural occurrence, but instead behave as strategic actors: “Hackers attack systems that are vulnerable and those that do not have appropriate controls...Security investment increases the hacker’s costs, and when the hacker’s cost becomes larger than its benefit, the hacker may be forced not to attack the firm in the first place” (p. 285).

Integrating the above proposed theories helps to shape the Cyber-Based View of the Firm (Figure 2) for strategic exploration; these theories are outlined in Table 1 below.

Other Theory

Public Policy literature employs a number of theories to think through how to create cybersecurity policy. Social Exchange Theory has been explored to understand why

regulatory policy does not work (Clinton, 2011), while Agency Theory and Power Theory are applied to explain why people may or may not adhere to information security policies (Smith et al., 2010).

The study of cyberattack also uses a number of different theories, all of which reinforce the concept of hackers as strategic actors (Cavusoglu et al., 2008). Choo (2011) explored cybercriminology using Routine Activity Theory. He observed that “in the context of cybercrime, an assumption is that cybercriminals are:

1. criminally and/or financially motivated
2. seek out opportunities provided by cyberspace such as anonymity and no geographical limitations,
3. acquire the necessary resources for cybercrime by (*inter alia*) using delinquent/rogue IT professionals, and
4. target weakly protected systems/networks and exploiting situations where law enforcement agencies are hampered by jurisdictional, legislative and evidentiary issues, particularly in cross-border cybercriminal cases” (Choo, 2011, pp. 725-726).

Hacker motivation is a common line of inquiry. Steinmetz and Gerber (2015) explored the hacker ethic from a Weberian perspective, specifically seeking to understand hacker perspectives on privacy and surveillance. Privacy and surveillance introduce totalitarianism and quasitotalitarianism into the hacker literature (Steinmetz & Gerber, 2015; Karatzogianni & Gak, 2015). Vigilantism is another theory explored in conjunction with *hacktivists* (Serracino-Inglott, 2013). While two other studies explore hacker culture

as it relates to ethics of hacker communities (Jordan & Taylor, 1998) and apply Bourdieu's Field Theory to understand social capital (Nycyk, 2016).

Anonymity is identified as another factor in cybercrime and hacker sociology (Serracino-Inglott, 2013; Kim et al., 2010; Choo, 2011) and how it creates challenges with respect to attribution (Haggard & Lindsay, 2015; Brown, 2015; Choo, 2011).

“Cyber-personas may relate fairly directly to an actual person or entity, incorporating some biographical or corporate data, email and IP address(es), web pages, phone numbers etc. However, one individual may have multiple cyber-persona, which may vary in the degree to which they are factually accurate, and a single cyber persona can have multiple users” (Joint Pub 3-12, p. I-3). This ability for one hacker to present as many actors in multiple locations at one time, or the converse, many hackers in multiple locations to present as a single actor in one place is highly strategic and plays a significant role in anonymity and attribution challenges.

While these many studies apply different theories to explain hacker behaviors, the common thread is that hackers behave as highly strategic actors, who examine their target organizations from a Cyber-Based View to achieve a specific objective, whether that objective is to coerce a business decision such as the Sony Pictures hack (Haggard & Lindsay, 2015), shut down critical infrastructure (Ng 1, 2017), manipulate financial markets (Prigg, 2015), influence elections (Mihailidis & Viotty, 2017); or to simply monetize firms’ data through a ransomware attack (Scott & Spaniel, 2016).

The integration of the above theory can be applied to the Cyber-Based View as shown in Figure 6, below.

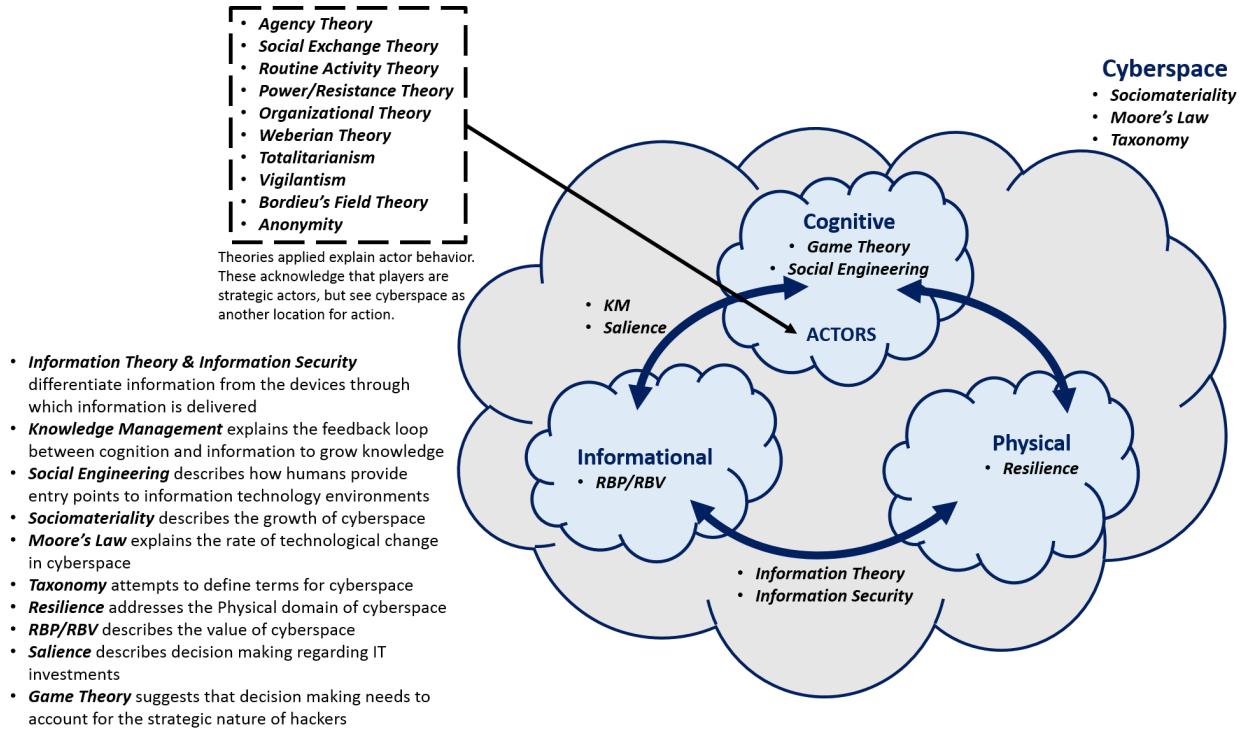


Figure 7. Shaping the Cyber-Based View of the Firm with Theory

Conceptual Model

The Cognitive Dimension and Theory

The cognitive dimension, comprised of minds of employees, customers, rivals, hackers, and other stakeholders can be explained through myriad theory looking to explain human behavior, including: Agency Theory (Brown, 2015; Smith et al., 2010), Social Exchange Theory (Clinton, 2011), Routine Activity Theory(Choo, 2011), Power/Resistance Theory (Smith et al., 2010), Totalitarianism (Steinmetz & Gerber, 2015; Karatzogianni & Gak, 2015), Vigilantism (Serracino-Inglott, 2013), Anonymity (Haggard & Lindsay, 2015; Brown, 2015; Choo, 2011; Serracino-Inglott, 2013), Bourdieu's Field Theory (Nycyk, 2016), and a Weberian Perspective (Steinmetz & Gerber, 2015). Game theory in particular, explores cyber defense in the

context of strategic actors, including the firm, firm rivals, and hackers (Cavusoglu et al., 2008; Gal-Or & Ghose, 2005).

The Physical Dimension and Theory

Because of the sociomaterial phenomenon, Moore's Law, and the convergence of Operational Technology and Information Technology in the firm, the Physical Dimension, which includes tangible devices, wired and wireless networks, sensors, and industrial control systems, is growing very rapidly. This phenomenon introduces Resilience theory to the Cyber-Based View (Cerullo & Cerullo, 2006; Devendandham & Ramirez-Marquez, 2016; Ortiz-de-Mandojana & Bansal, 2016; Sahebjamnia et al., 2015; Rioli & Savicki, 2003) through the literature studying critical infrastructure and continuity of operations (Ambs et al., 2000; Cerullo & Cerullo, 2006; Devendandham & Ramirez-Marquez, 2016; Ortiz-de-Mandojana & Bansal, 2016; Sahebjamnia et al., 2015, Rioli & Savicki, 2003).

The Informational Dimension and Theory

The Informational Dimension, comprised of software, data, media, and explicit knowledge assets integrates elements of sociomateriality, which considers the monumental growth of data generation due to automation and wearable technology (Cecez-Kecmanovic et al., 2014), among other things.

Cognitive, Physical, and Informational Bilateral Interactions and Theory

Cyberspace, which is created by the integration of the cognitive, physical, and informational dimensions, is constantly growing, a phenomenon that can be explained by Moore's law, which describes rapid technology growth, by Sociomateriality theory, which seeks to understand the interdependence of the social, or cognitive dimension, with

the material, the physical and informational dimensions (Orlikowski, 2007, 2010; Leonardi & Barley, 2008; Orlikowski & Scott, 2008; Carlo et al., 2012; Gaskin et al., 2014; Cecez-Kecmanovic et al., 2014; Jones, 2014).

Decision making, which involves the integration of the cognitive with the informational, introduces both game theory and salience. Salience explains why the human mind of the cognitive domain places greater or lesser value – salience – on specific pieces of information (Kahneman & Tversky, 1979; Tversky & Kahneman, 1981; Bordalo et al., 2012), which are introduced into cyberspace through the informational dimension.

Building resources and capabilities, an occurrence explored through the application of the RBP/RBV (Aragon-Correa & Sharma, 2003; Hovav & D'Arcy, 2003; Gordon, et al., 2010; Bronco & Rodrigues, 2006; Lockett et al., 2006; Surroca et al., 2010), can explain the potential for a proactive, adaptive cyber capability to grow new resources and capabilities, and it sits within the feedback loop of the three dimensions.

Finally, there are many within the computer science, systems engineering, and information technology communities who seek to develop language to discuss, study, and understand this complex environment, which explains why theoretical Taxonomy for cybersecurity (Howard & Longstaff, 1998; Kim et al., 2010; Ramirez & Chourcri, 2016) is a common theme in the literature.

Conclusion

Despite the fact that there are existing tools to explore the nature of the firm in the context of institutions, resources and capabilities, there is currently no tool through which to explore the firm as it exists in cyberspace. Thus, in order to examine the research

questions, it became necessary to derive a framework through which the phenomenon of cyberattack could be studied.

By integrating the Information Science, Information Security, Knowledge Management, Social Engineering, and Sociomateriality literature, the following definition was derived: *Cyberspace is comprised of three, interdependent physical, informational, and cognitive dimensions which continuously interact between systems, individuals, and organizations both within and beyond the firm* (Schwartz & Schuff, 2018). The Cyber-Based View framework in Figure 1 was further enhanced through the examination of additional theory, including Moore's Law, resilience, the resource-based perspective, salience, and game theory to provide additional rigor.

CHAPTER 3

IDENTIFYING THE RESEARCH GAP FOR THE CYBER-BASED VIEW

Overview

Chapter 2 derived a definition for cyberspace and the accompanying Cyber-Based View framework. This allows for the next step, which is to position the Cyber-Based View within the existing base of knowledge by framing the gap to be filled.

Beginning with a literature review of each of twenty-one theories, multiple studies within a particular avenue of theoretical literature were examined to determine how a specific theory was being applied to cyberspace phenomena. In order to ensure thoroughness, this theoretical examination was an intentionally broad meta-analysis, extending well beyond the cybersecurity literature to assess how cyberspace is being explored theoretically in communities beyond computer science and information systems, including, but not limited to: sociology, organizational management, security, psychology, and behavioral psychology. The purpose of examining cyberspace phenomena versus cybersecurity was to determine whether or not a true theoretical gap exists, or whether that gap was limited to a particular context.

Research Design

Validation of Methodology

The pilot study began with a case study of the Stuxnet cyberattack to refine a *failure autopsy* and theory testing approach. The case was built using a narrative analysis of journal articles, media interviews, public records, and discussion forums from within the hacker and cyber-security communities. The narrative analysis explored the following questions:

1. Does the event include effects in the physical, informational, and cognitive dimensions?
2. Were the effects in different dimensions interacting?
3. What interactions were taking place amongst the dimensions?

The details of the Stuxnet event were mapped to the three dimensions of the Cyber-Based View, to illustrate the various dimensional effects and the interactions taking place. The many interactions in the case study were then analyzed using the twenty-one theories discussed in the literature review to gain an initial understanding of which interactions and elements of the cyberattack can be explained by existing theory.

Given the broad nature of the theories, applying each of 21 theories individually in a case-by-case analysis of cyberattacks would become redundant given the relationships that were discovered. The relationships among the theories suggested that they should be categorized for further study. This categorization also allows for additional theories to be explored at a later time by creating categories to which new theories can be added, allowing generalization of the theory testing method. The outcomes of the Stuxnet case study are captured in Appendix A.

Meta-Analysis of Existing Theory

Twenty-one different theories were explored in Chapter 2 as part of the literature review and used to derive and shape the Cyber-Based View. This number was reduced to twenty theories by consolidating Weberian theory with organizational structure theories. Using the academic literature, these theories have been classified into the five categories and summarized in Table 2.

Table 2. Classification of Twenty Theories

Category	Description
<i>Category 1: Technological Growth Theories</i> <ul style="list-style-type: none"> • Sociomateriality • Moore's Law • Cyber Taxonomy 	Technological growth theories seek to explain the growth of cyberspace with respect to technological change, technology immersion, and language.
<i>Category 2: Decision Making Theories</i> <ul style="list-style-type: none"> • Salience • Game Theory • Totalitarianism/Quasitotalitarianism 	Decision Making theories explore the relationship between human beings and information with respect to how information is cognitively processed and how data is turned into information and knowledge for decision making.
<i>Category 3: Information & Physical Asset Theories</i> <ul style="list-style-type: none"> • Knowledge Management • Information Theory • Information Security • Resilience • RBV 	Information & physical asset theories characterize information and/or machines as firm resources and explore the defense and resilience of assets as it relates to firm performance.
<i>Category 4: Online Behavior Theories</i> <ul style="list-style-type: none"> • Routine Activity Theory • Anonymity • Vigilantism • Bourdieu's Field Theory • Social Engineering 	Online behavior theories investigate how online communities are formed, how people relate to one another online, how hackers gain access to secure environments, and what motivates human behavior in cyberspace.
<i>Category 5: Organizational Theories</i> <ul style="list-style-type: none"> • Organization Theory • Agency Theory • Social Exchange • Power/Resistance 	Organizational theories explore the interaction of cyberspace and organizational structures, culture, and behavior as it relates to the impact of technology on existing organizations, and the emergence of organizations within cyberspace, including themes of agency, power, and social exchange.

As cyberattack continues to experience exponential growth rates, the list of applicable theory will likely expand; however, it should be possible to place new theories within one of the categories, develop a new category of theory, and apply this theory testing approach to emerging ideas.

Employing a method derived from Farrell's (2013) Five Tests for a Theory of the Crime Drop, this study sets up four tests that a theory must pass to be deemed worthy of further investigation as it relates to the dynamics of cyberspace within the firm. These

tests are proposed as essential to establish 1) which cyberspace interactions can be explained by existing theory, and 2) to frame the gap filled by the Cyber-Based View.

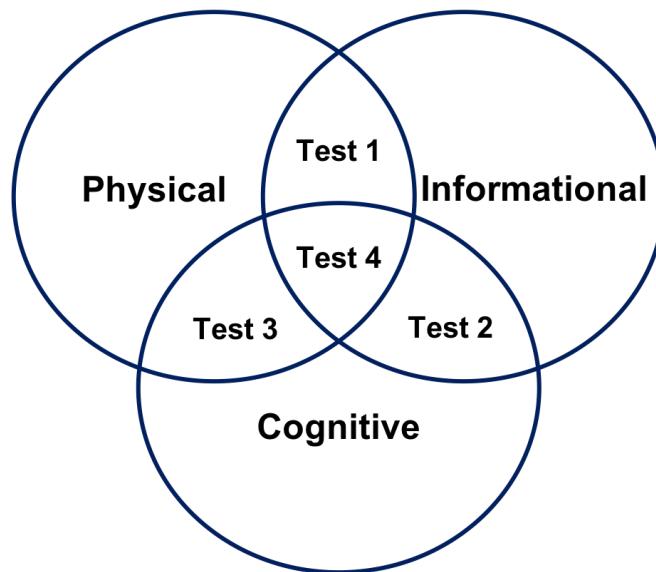


Figure 8. Theory Testing Framework

The four tests (Figure 8) are:

1. The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

2. The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision making and human action?

3. The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

4. The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

When the hypotheses within the theoretical studies were examining the interactions taking place between the specific dimensions identified in the test, the theory would pass the applied test. When hypotheses assumed a specific interaction exists, but was examining another phenomenon, the theory would fail the test.

Discussion of Results

The four tests of each individual theory and a detailed summary of the results are captured in Appendix B. The findings are summarized in Table 3, and visually represented in Figure 9. A theory either fails or passes each test, with a failure indicated as a cross ('X') and a pass as a checkmark (✓).

Table 3. Summary of Findings

Theory	Test 1 P – I	Test 2 I – C	Test 3 P – C	Test 4 P – I – C
Category 1: Technology Growth				
Sociomateriality (Critical Realism)	X	✓	✓	X
Sociomateriality (Agential Realism)	X	X	X	X
Moore's Law	✓	X	X	X
Taxonomies	✓	X	X	X
Category 2: Decision Making				

Totalitarianism/Quasitotalitarianism	X	✓	X	X
Game Theory	X	✓	X	X
Salience	X	✓	X	X
Category 3: Information & Physical Assets				
Knowledge Management & Knowledge Based View (KBV)	✓	✓	✓	X
Resource Based View (RBV)	X	X	✓	X
Information Security	✓	✓	✓	X
Information Theory	✓	✓	X	X
Resilience	✓	✓	✓	X
Category 4: Online Behavior				
Anonymity	✓	✓	X	X
Bourdieu's Field Theory	X	✓	✓	X
Routine Activity Theory	X	✓	X	X
Vigilantism	X	✓	X	X
Social Engineering	X	✓	✓	X
Category 5: Organization Theory				
Organizational Structures	X	✓	✓	X
Agency Theory	X	✓	X	X
Power/Resistance	X	✓	✓	X
Social Exchange Theory	X	✓	X	X

The bilateral physical – informational interaction test

To pass this test, a theory had to demonstrate that the object of study was the interactions taking place between elements of the physical and informational dimensions of cyberspace. For example, Burmester et al. (2012) describes cyber-physical systems as entities in the physical environment that are monitored and controlled by integrating them into a distributed computing environment. Only Anonymity technologies, which explored machine-to-machine information exchanges for identity management, and Category 3 theories, which includes Knowledge Management, the Knowledge-Based View (KBV), the Resource Based View (RBV), Informational Security, Information Theory, and Resilience passed this test. This provided evidence that only the computer science and information systems communities are exploring the physical – informational interaction.

The bilateral cognitive – informational interaction test

The criterion to pass this test requires that the theory being tested demonstrates that the object of study was the interactions taking place between elements of the cognitive and informational dimensions of cyberspace. Theorists have been exploring this bilateral interaction for decades, and probably longer, although this study did not examine literature prior to 1960. Almost every theory examined for the purposes of this study explored the bilateral interaction between the cognitive and informational dimensions. For example, totalitarianism explores the use of propaganda (Fitzgerald & Brantly, 2017), while game theory models how firms share knowledge (Wu et al., 2015; Ezhei & Ladani, 2017; Gal-Or & Ghose, 2005; Gladstein & Reilly, 1985; Gordon et al., 2015) or how rival hackers share information (Hausken, 2017) in order to make better decisions, as well as how strategic rivals leverage information in competition with one another.

The way humans use information is a well-researched phenomenon, and every theory except the Resource-Based View and the agential realist perspective of sociomateriality passed this test.

The bilateral cognitive – physical interaction test

In order to pass this test, the theory being tested must demonstrate that the focus of the study was the interactions taking place between elements of the cognitive and physical dimensions of cyberspace. Of the twenty-one theories examined in this study, only nine theories passed this test, and only three of these nine theories, all of which fell into Category 3, passed the first two tests: Knowledge Management, Information Security, and Resilience.

Appropriate access between an object of security, or physical device, and an agent or stakeholder, both humans, is defined in the Information Security Literature, while the Knowledge Management literature suggests that knowledge management systems are only valuable when employees use them (Wang et al., 2013). The resilience literature examines cyber-physical & human systems, such as the integration of technology and people through such things as neural prosthetics and computer – brain interfaces (Netto & Spurgeon, 2017; Vanderhaegen, 2017; Herrington & Aldrich, 2013). Each of these lines of inquiry satisfy this test for a bilateral interaction between the cognitive and physical dimensions of cyberspace. Thus, three theories passed all the bilateral interaction tests: Knowledge Management, Information Security, and Resilience.

The multilateral physical – informational – cognitive interaction test

Although the Knowledge Management, Information Security, and Resilience literature explore all three dimensions of cyberspace, the avenues of investigation are only bilateral in nature. One can infer that the multilateral physical – informational – cognitive interaction exists, but none of these theories is designed to explore this multidimensional interactive phenomenon. Individual studies within each stream of literature will focus on one set of interactions, for example, the preponderance of the Knowledge Management literature falls into one of two disciplines, strategy and organizational theory, both of which focus on the cognitive – informational interaction.

Organizational theorists gravitate toward the investigation of intraorganizational knowledge sharing (Argote & Fahrenkopf, 2016; Chen et al., 2010; Hsu & Sabherwal, 2012; Lewis et al., 2007; McIver et al., 2013; Oldroyd & Morris, 2012; Sanchez & Mahoney, 1996; Sears & Hoekker, 2014; Sung & Choi, 2012; van Ginkel & van

Knippenberg, 2008), while the strategists explore leveraging knowledge as it relates to resources and capabilities (Turner & Makhija, 2006; Howard et al., 2013; Forbes, 2007; Hult, 2003), innovation (Alexy et al., 2013; Chatterji & Fabrizio, 2012; Ranganathan & Rosenkopf, 2014), and strategic interorganizational alliances (Alexy et al., 2013; Chatterji & Fabrizio, 2012; Ranganathan & Rosenkopf, 2014; Alnuaimi & George 2016; Howard et al., 2013; Schillebeeckx et al., 2016). There is a third stream of knowledge management literature – knowledge management systems – which focuses on the use of information technology to provide a platform for “knowledge articulation, codification, and communication” (Wang et al., 2013). Although all three bilateral interactions are investigated, the investigations are conducted with respect to only one of these bilateral interactions. Thus, knowledge management theory failed this fourth and final test.

The Information Security literature follows a similar pattern, dividing along three avenues. The first, technical information security, investigates the physical – informational interaction (Burmester et al., 2012; Cavusoglu et al., 2009; Chen et al., 2015; Johnston & Warkentin, 2010). The second, behavioral information security, investigates the cognitive – physical interaction or the cognitive – informational interaction ((Belanger et al., 2017; Bulgurcu et al., 2010; Crossler et al., 2013; Cuganesan et al., 2017; Lee et al, 2016; McCormac et al., 2017; Posey et al., 2013; Safa & Von Solms, 2016; Safa et al., 2016; Siponen et al., 2014). Last, information security economics, investigates the cognitive – informational interaction (Angst et al., 2017; Chen et al., 2011; Dor & Elovici, 2016; Gordon et al., 2002; Hovav & D’Arcy, 2003; Huang & Behara, 2013; Love et al., 2011; Mayadunne & Park, 2016). There is no

existing stream of research with the Information Security literature where all three interactions are examined simultaneously, and it too fails the multilateral interaction test.

Only the Resilience literature directly referenced the multidimensionality of cyberspace. DiMase et al. (2015) identify a future need for a framework that integrates an “approach across physical, information, cognitive and social domains to ensure resilience” (p. 291). In the absence of such an integrated framework, they proposed the use of a multi-scale systems engineering framework that addressed only the physical – informational bilateral interaction. In fact, this particular study suggests that there is a specific need for the Cyber-Based View framework to address the complexity of cyber-physical & human systems. Although the resilience literature identifies a need for the Cyber-Based View framework, the resilience theory investigations themselves do not pass this fourth and final test.

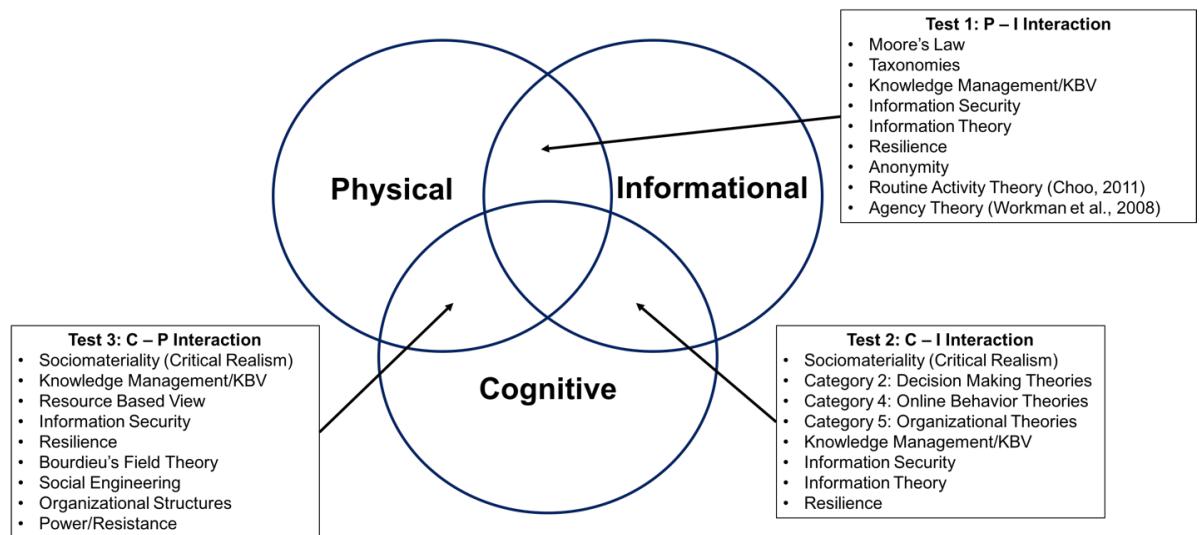


Figure 9. Summary of Findings

Case Study Analysis of the Stuxnet Attack

To demonstrate the utility of the Cyber-Based View as a lens for understanding cyberattacks, the framework was applied to the Stuxnet attack. Using journal and

academic articles, media interviews, and public records, a narrative analysis of the Stuxnet Attack was used to develop a qualitative case study (Jorgensen et al. 2002). In conjunction with the narrative analysis, content used to develop the case studies was coded to look for the interactive dynamics of cyberspace. Multiple forms of media allowed triangulation of the data by combining elements from different discourses to capture the dynamic nature of intertextuality as it relates to the understanding of cyberattack.

According to an NPR broadcast (2016), the Stuxnet Attack is recognized as “the first time to our knowledge that digital code was able to create physical destruction in the real world” (Shapiro, 2016), with many experts comparing it to the atom bomb dropped on Hiroshima and Nagasaki (Shapiro, 2016). The attack, which damaged over a thousand centrifuges at the Natanz Uranium Enrichment Facility (Lindsay, 2013; Nakashima et al., 2012), has been attributed to the United States and Israel (Shapiro, 2016; Sanger, 2012; Rosenbaum, 2012; Paganini, 2016), although neither country has ever confirmed these suspicions (Rogers, 2015). At work in the Stuxnet attack was a choreographed dance leveraging the ecosystem of cyberspace, with elements at work in all three dimensions of the Cyber-Based View – physical, informational, and cognitive.

Information Theory specifically differentiates between information and the devices on which it is presented, which can explain elements of the Natanz infrastructure environment such as the Siemens PLCs and the Siemens SIMATIC Step 7 software (Zetter, 2014) (P – I interaction). *Information Security* also addresses this relationship by defining security methods, such as the “air-gap” to secure the physical devices using

physical security measures, and to secure the software that runs the devices with approaches such as malware detection.

Information Theory and *Knowledge Management* can explain the iterative development of the Stuxnet cyberweapon which involved a feedback loop to turn information into knowledge (I – C interaction), enabling the hackers who developed the weapon to design – build – test the malware to create specific capabilities (Zetter, 2014).

Social Engineering explains how humans can be exploited as social entry points such as the use of USB drives to cross the “air-gap” at Natanz (P – C interaction), or the use of “phishing” emails to entice a person to click on a link that downloaded the malware at Iranian engineering firms with industrial control systems expertise (Zetter, 2014) (I – C interaction). *Salience* can explain the complacency of the engineers who did not perceive any risk to their “air-gapped” systems (I – C interaction), and thus did not monitor their behavior related to the use of USB drives, an organization-wide behavior that could be explored by applying *Organizational Theory*. *Social Engineering* is predicated on humans engaging with and being immersed in technology, a phenomenon that is explained by *Sociomateriality*, but neither *Social Engineering* nor *Sociomateriality* offer a view of the cyber ecosystem in the Natanz facility.

Resilience Theory explores the ability of the individual domains to recover from failure, such as the recovery of the Natanz uranium enrichment process by replacing the failed centrifuges, but it does not explore the relationships that led to the failure. The *Resource Based View* looks at the cognitive (the engineers), physical assets (centrifuges), and informational assets (Siemens SIMATIC Step 7 software) within the organization, but it does not explain the interactions amongst these elements, it merely explores how

those resources relate to firm performance. *Game Theory* can explain the rivalry between the United States, Israel, and Iran, but that rivalry is contained within the cognitive dimension. Despite speculations that the United States and Israel were responsible for the attack (Shapiro, 2016), full attribution is not possible, a factor that can be explored using *Anonymity* theory.

The Stuxnet attack was successful because it orchestrated the interactions between the humans (cognitive), the devices (physical), and the data and software (informational) with iterative behaviors, including the “man-in-the-middle” approach that fed malicious commands to the physical devices, while feeding false information to the engineers to influence their decision making (Zetter, 2014). The software also masked its behavior by causing the physical devices to fail over time in order to keep the engineers confused regarding the cause of the failures (Lindsay, 2013). These interactions involved feedback amongst all three of the physical, informational, and cognitive dimensions in an iterative and simultaneous dance. Though several of these theories can explain interactions between two of the dimensions, only the Cyber-Based View captures both the bilateral interactions and the multidimensional interactions.

Conclusion

Little theory exists at the firm level to examine the nature of the firm as it looks in cyberspace. This comprehensive literature review and meta-analysis of research examining cyberspace phenomena provides evidence of a significant theoretical gap. Although the cognitive – informational interaction is well researched in a wide range of disciplines, including but not limited to psychology, social psychology, sociology, behavioral psychology, information systems, and strategy, the examination of how modes

for delivering information affects this cognitive – informational link is limited to the computer science and information systems disciplines in the form of cybersecurity research.

Current cybersecurity literature is largely limited to the computer science domain, and much of that research is predicated on the notion that there can be security in the cyber domain. The reality is that there is no such thing as security in a hostile environment. While information security technologies are necessary, they are wholly insufficient as a strategy for virtual operations in an inherently compromised and highly contested environment rife with competing discourses (Jorgensen, 2016). The competition to control both the data and the narrative is evident in the literature that examines the cognitive – informational interaction. Unfortunately, the exploration of how tools are used to manipulate and control the informational dimension is presently limited to computer science, which can only offer a technical solution to an inherently human challenge. This study contributes to the existing literature by shaping that gap.

Further, this examination of existing theory being applied to multiple phenomena occurring in cyberspace reveals the absence of available theory to explain the multilateral interactions taking place amongst the physical – informational – cognitive dimensions. Although sociomateriality theory explores the changing nature of the firm as it becomes "cyborg," (Cecez-Kecmanovic et al. 2014), it addresses technological expansion only as it relates to human processes. It does not explore the increasing vulnerabilities this creates within the firm. For example, sociomateriality can explain how the expansion of the Internet of Things led a North American casino to automate the maintenance of a fish tank using wireless sensors connected to computers that regulated the food, temperature

and water cleanliness in the tank (Schiffer, 2017). The Resource-Based View can explain how using the sensors and other IT resources led to the creation of a new capability – fish tank maintenance. What neither sociomateriality nor the RBV can do is clarify the vulnerabilities that connecting the fish tank to the Internet of Things created, which allowed hackers to tap into the casino's secure network and send over 10GB of data to a device in Finland (Schiffer, 2017).

The Cyber-Based View derived in Chapter 2 fills this academic void, providing a new theoretical capability to complement the institutional-based, resource-based, and knowledge-based views of the firm common to strategy literature.

CHAPTER 4

APPLYING THE CYBER-BASED VIEW OF THE FIRM: A CASE STUDY APPROACH TO DYNAMIC INTERACTIONS DURING A CYBERATTACK

Overview

The meta-analysis employed in Chapter 3 illustrated that current theory fails to explain the interactions between people, data, and devices that enables the cyberattack phenomenon. While the meta-analysis study demonstrated that examining only one bilateral interaction at a time is insufficient to explain the dynamics at play during a cyberattack, the study did not explain why capturing all three bilateral interactions and the multilateral interaction aids our understanding of the phenomenon.

The qualitative case study of the 2010 Stuxnet attack provided evidence that the Cyber-Based View offers a viable framework through which to explore these interactions as they relate to a specific instance of cyberattack. This essay further develops the Cyber-Based View theory by exploring how capturing these multiple, simultaneous interactions leads to new understandings related to the cyberattack phenomenon. It then assesses the generalizability of the Cyber-Based View by using it to examine multiple cases of cyberattack to see what common insights emerge across several events.

Literature Review

Corporate Information Warfare and Cyberattack

“Information is the most valuable commodity in the world. It’s more valuable than money, for with it one can make money. It’s more valuable than power, for with it one can achieve power. It’s more valuable than goods, for with it, one can build, acquire, and improve goods. In any business, in any industry, in any part of the world, the right information is absolutely priceless.” (Bruce, 2004, p.11)

Given the power of information to contribute to corporate success and the accessibility to information enabled by cyberspace, it comes as no surprise that the world has entered an age of constant information warfare resulting from the rivalries of nation states, corporations, terrorists, criminals, and private citizens. Information superiority is defined in Department of Defense *Joint Publication 3-13, Information Operations*, as “the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same” (p. GL-3). Information warfare is the active rivalry to attain information superiority, and can be classified into three categories, including *personal information warfare* (e.g. cyberbullying, cyberstalking, or identity theft); *corporate information warfare*, which involves corporate rivalry; and *global information warfare*, which involves nation states and global economic forces (Al-Ahmad, 2013).

Corporate information warfare has existed for a long time including events as far back as the AC/DC current wars between Thomas Edison and George Westinghouse in the 1880s - 1890s (McNichol, 2006) and the incidence of French Intelligence placing listening devices on the Concorde 100 years later (Leyden, 2015). The FBI estimated the cost of corporate espionage to be as high as \$100 billion per year as of 2007 (Bressler & Bressler, 2015). What has changed the landscape of corporate information warfare is the available tools and methods that cyberspace enables (Al-Ahmad, 2013). Cyberthreats are expanding because organizational activities are driven by knowledge and the contextual enterprise that generates that knowledge (Dastikop, 2005).

In the past, adding technology to a firm’s capability portfolio ordinarily added value, but the hyper connectivity of the information economy has transformed technology

from adding value, to adding both value and vulnerability simultaneously, sometimes adding significant vulnerability.

In today's modern information systems, machines, data and software take an increasingly active role, forming sophisticated relationships with one another as well as the human resources with which they interact (Tsvetkova et al., 2017). The complexity of these "human-technological intertwinements" (Linn & Luppincini, 2011, p. 75) is a hallmark of the firm in the information economy, enabling the collection, analysis, and storage of petabytes of customer data and other data assets which provide significant economic benefit, but it has also facilitated access for criminals, nation states, and hacktivists to access corporate information resources (Roberds & Schreft, 2008).

According to a 2016 study by Manworren et al., "The New York Times, published more than 700 articles about data breaches in 2014, compared with 125 in 2013" (p. 261). Customers expect businesses to protect their privacy by ensuring the security of their data from both internal and external threat, but not unlike the businesses with whom they share their personal data, most customers fail to understand the constant risk of data theft (Manworren et al., 2016).

The march toward total digital integration of human life continues (Manworren et al., 2016), and hackers understand this convergence of humans, data, and devices, which allows them to exploit the vulnerabilities that are created through processes built upon the interactions between them (Myauo, 2016). To underestimate cyberthreat because of a conventional, terrestrial understanding of resources and capabilities (Linn & Luppincini, 2011) is to ignore the harsh reality of the hostile cyberspace environment, and yet Manworren et al. (2016) found a Verizon 2015 study indicating that the lion's share of

exploited vulnerabilities were often compromised more than a year after being identified, with “companies making themselves vulnerable through inactivity” (p. 263).

This inactivity can be explained by a study conducted by Lallie, Debattista, and Bal (2018) which found that 91% of CEOs struggle to interpret cybersecurity reports and lack the necessary knowledge to drive corrective action. Oftentimes, the strategic objective of a cyberattack is to disrupt core processes or degrade cyber-physical systems in order to affect decision making and operations (Nguyen, 2013). These intangible effects of cyberattack are extremely difficult to quantify, and thus are often underestimated, with the end result being organizational reluctance to make the necessary capital investments (Al-Ahmad, 2013).

The expansion of cyberattacks increases the need for both computer experts *and operations experts who lack computer expertise* to develop improved tactics, techniques, and procedures. It is critical that everyone, regardless of their programming expertise, understand cyberattack dynamics, the impact of an attack, the methods used to facilitate an attack, and the system vulnerabilities (Manworren et al., 2016) created through digitalization. Knowing how cyberattack unfolds within the firm’s virtual landscape is crucial to the development of corporate strategy (Schwartz et al., 2018). But what constitutes a cyberattack, and how is it related to corporate information warfare?

Definitions

One of the challenges confronting researchers and practitioners alike is the lack of agreement regarding how to define cyberattack (Edwards et al., 2017). Corporate information warfare includes a range of “cyber-incidents,” which Balzacq and Cavelty (2016) conceptualize as “deliberate disruptions of routine and everyday cyber-security

practices, designed to protect networks, computers, programs and data from attack, damage, or unauthorized access” (p. 180).

The most common definitions of cyberattack or computer network attack spring from the Department of Defense Joint Publication 3-12, Cyberspace Operations, which includes the denial or manipulation of information resources. This leads to the following elements being included in cyberattack definitions: *degradation* of information resource quality, *disruption* of access to information resources, *destruction* of information resources, or the *manipulation/alteration* of information to influence decision making (Nguyen, 2013; Brecher, 2012; Joint Pub 3-12).

Archer (2014) describes three types of cyberattacks, which can be derived from this concept of “cyber-incidents” and the denial of access to, or manipulation of, information resources: “cyber exploitation or crime, disruptive activities, and destructive activities” (p. 610).

Cyber exploitation is oriented around data breaches that are the result of network penetration by hackers, resulting in unauthorized access to personal data that has been collected by an organization (Roberds & Schreft, 2008). Cyber exploitation attacks include:

- *Cybercrime*. Technology is used “to commit a crime against a person [e.g. identity theft, stalking], information asset [e.g. defacing a corporate website], intellectual asset, or physical component of society [e.g. medical device, ATM, or automobile]” (Neal & Ilsever, 2016, p. 16-17).

- *Cyber espionage.* Technology is used to gain system access illegally in order to destroy or steal data such as intellectual property, customer data, or other knowledge assets (Linn & Lupicci, 2011).

Disruptive cyber activity curtails access to key information resources by attacking data used for decision making and service delivery rather than cyber-physical systems (Archer, 2014). The WannaCry ransomware attack that shut down the British Healthcare System in May 2017 by denying access to patient health records (Mayor, 2018) is an example of disruptive cyber activity.

Destructive cyber activity uses information and communications technologies to destroy physical devices (Archer, 2014). The most well-known example of destructive cyber activity is the 2010 Stuxnet attack which led to the destruction of centrifuges at Natanz, the uranium enrichment facility in Iran (Zetter, 2014).

Finlay (2018) explores the definition of cyberattack in the context of *violent agency* as the deciding factor to determine whether a cyber-incident should be categorized as an attack. In this context, an attack is understood in terms of violent consequences, including double intent and destructive harming. Double intent includes deliberate destruction using means specifically chosen to cause maximum damage while simultaneously thwarting the target's ability to escape or defend against the threat (Finlay, 2018).

Destructive harming includes theft – “appropriative harming” (Finlay, 2018, p. 11) and violence – “destructive harming” (Finlay, 2018, p.11). Data theft can evolve from appropriative harming to destructive harming (Finlay, 2018). For example, theft of medical records (cyber exploitation) begins as appropriative harm, but using information from those records, such as a penicillin allergy, to clandestinely kill a person by altering

the data in the medical record to facilitate the use of penicillin by healthcare workers (destructive cyber activity) becomes destructive harm. This concept of violent agency as the context to determine whether an attack has occurred reinforces the three types of cyberattack as defined above by Archer (2014).

The Cyberattack Phenomenon

One of the most disconcerting characteristics of cyberattack is that it transcends geography, causing virtually immediate effects from any part of the world (Brecher, 2012; Huey et al., 2012). The abstract nature of cyberspace makes it very difficult to identify the source of an attack (Brecher, 2012; Linn & Lupiccini, 2011; Farwell & Rohozinski, 2011).

“Places” in cyberspace are the product of relationships rather than waypoints on a geographic map (Balzacq & Cavelty, 2016). Baudry and Chassagnon (2012) expanded on Coase’s (1937) Theory of the Firm as it applies in an age of globalization where value chains have been relocated from within a single firm into a vertical network of firms. The Vertically Networked Organization (VNO) challenges the traditional boundaries of the firm because it is predicated on information sharing and information dissemination across multiple nodes in an orchestrated network (Baudry & Chassagnon, 2012). Defensive strategies are traditionally based on physical boundaries, but both the VNO, which redefines the boundaries of the firm, and cyberspace, which supplants boundaries altogether, make this approach wholly inadequate (Baudry & Chassagnon, 2012; Huey et al., 2012; Brecher, 2012; Linn & Lupiccini, 2011). Networks challenge boundaries and create vulnerabilities.

Vulnerabilities are created at the integration points of networks, for example, as the Internet of Things grows, and additional objects are integrated into the network, the number of entry points expands (Manworren et al., 2016). In the VNO, a hub-firm integrates partner firms using two mechanisms 1) by establishing certification processes to build trust, and 2) using information technology to connect partner firms (Baudry & Chassagnon, 2012).

Building trust through certification processes is based on an exchange of information, and cyberattackers can manipulate information. Connecting firms with information technology requires more devices on the network, and cyberattackers have more access. Cyberattacks can penetrate and disable vital corporate capabilities from anywhere in the world with very few resources (Brecher, 2012). The concept of the VNO expands the attack surface of the cyber environment by adding both cognitive and physical nodes to the network (Baudry & Chassagnon, 2012) and increasing the volume of information transiting the network.

Research Construct

Mechanics of the Cyber-Based View

The Cyber-Based View posits that cyberspace is comprised of cognitive, informational, and physical dimensions which are constantly engaged in a series of dynamic interactions. It is the constant interaction of the three dimensions that enables cyberattack, such that if any one dimension is removed from the environment, the attack falls apart.

The Cognitive Dimension

The cognitive dimension contains a firm's tacit knowledge resources and decision making capacity. The ability to assign value for decision making is a cognitive activity (Kahneman & Tversky, 1979; Bordalo et al., 2012). To ignore this dimension of the Cyber-Based View loses the concepts of knowledge – information that has been cognitively processed – as an intangible firm resource which is supported by the knowledge-based view and knowledge management theory. The minds of hackers and other rivals are also part of this dimension, strategically engaging with the firm (Cavusoglu et al., 2008). Game theory provides ample evidence of the rivalry that exists between firms and hackers, an outcome of which is cyberattack, thus the concept of rivalry, and by extension cyberattack, would be lost if the cognitive dimension was removed.

In a social engineering attack, a hacker may choose a number of approaches to gain access to a secure computing environment. The hacker (cognitive) may choose to create an email (informational) targeting a specific individual (cognitive), or they may embed malware (informational) on a USB drive (physical), and leave the USB drive somewhere that a human target will decide to pick up (cognitive) the device (physical). In each case, if the cognitive dimension is removed, the hacker, without whom there is no cyberattack, is removed from the attack scenario. In addition to the removal of the hacker, the removal of the cognitive dimension also eliminates the human target. The removal of the human target means there is no one to read the email or pick up the USB drive and plug it into the secure computing environment, allowing the malware to infect the computing environment. Thus we can posit:

P1: Cyberattacks will include a cognitive dimension.

The Physical Dimension

With respect to cyberattack, the physical dimension is critical, not simply because of its value as a target for hackers, but because the physical dimension acts as an onramp to cyberspace granting access to the informational and cognitive domain. In essence, the physical dimension offers strategic, operational, and tactical targets (Joint Pub 3-13). The physical dimension receives a great deal of attention because it is the most tangible, in that objects – the devices, wires and sensors – are visible, making it seem as though a perimeter could be established, and outcomes, such as the results of an election, shape social constructs. But physicality is an illusion. The sensors and networks reach across geographical boundaries (Brown, 2015; Kim, 2010; Haggard & Lindsay, 2015; Cavusoglu et al., 2008; Karatzogianni & Gak, 2015), regardless of what can be seen.

For example, according to Verizon’s Data Breach Digest, in March 2016, “Hackers breached a water utility and manipulated systems responsible for water treatment and flow control” (Verizon, 2016, online). What began as a hack of the billing system for the purposes of stealing customer data from the informational dimension, allowed hackers to gain access to the “valve and flow control applications used to manipulate the utility’s hundreds of programmable logic controllers (PLCs), the hackers managed to access this software and alter settings related to water flow and the amount of chemicals used to treat the water” (Kovacs, 2016, online).

In order for the human target (cognitive) to provide access to the secure computing environment, the human target must interact with a physical device. Both the sociomateriality and information systems literature conceive this physical dimension with

which humans interact (Kautz & Jensen, 2013; Orlikowski, 2007; Scott & Orlikowski, 2009; Leonardi, 2013; Leonardi & Barley, 2008; Chen et al., 015; Burmester et al., 2012). Social engineering approaches, such as a phishing attack are predicated on the concept of sociomateriality and the physical dimension of cyberspace. The human target must use a computer and monitor to read an email, a mouse to click a link or open an attachment, a printer to create a paper copy of a document, or plug one physical device, such as a laptop computer, into another, such as a server environment. If the physical dimension is removed, the concepts of sociomateriality and information systems are no longer relevant, and there is no computing environment to be infected or any network through which the malware can travel. A hacker cannot even inject malware into a computing environment because the hacker is a cognitive element of the system. Further, if the interaction between the cognitive and physical dimension does not take place, the mutual reshaping and dynamic change of social structures becomes stagnant (Gaskin, 2014; Fuchs et al., 2009). Thus we can posit:

P2: Cyberattacks will include a physical dimension.

P3: Cyberattacks will include an element of the cognitive dimension (hacker or human target) interacting with an element of the physical dimension (e.g. a tangible object or outcome of some kind, including sensors, computers, telephones, security badges, elections, product purchases, etc.)

The Informational Dimension

In a knowledge driven organization, the informational dimension is the seat of firm power. It houses explicit knowledge assets, such as patents, training, and business intelligence, additional concepts from the KBV. It contains critical software – sets of

information rules – that run the devices, networks and sensors of the physical dimension, the software that supports core business processes, and it feeds the cognitive dimension for decision making, all of which are key concepts from the information systems literature. These knowledge assets and information systems are often primary targets of cyberattack, thus the removal of the information dimension removes the purpose and the means of cyberattack and undermines the existing knowledge and information systems theory. It is impossible to defend everything, but understanding what is housed in the informational dimension allows prioritization of targets to be defended.

The informational dimension also contains clues regarding the kinds of attacks an organization experiences on a daily basis. For example, the CERT team at Carnegie Mellon University's Software Engineering Institute (SEI) identified a distinctive pattern of behavior that evolves prior to sabotage incidents (Capelli et al., 2012). Many malicious insider threat indicators are available within the informational dimension prior to an attack if you know where to look. According to the SEI CERT, they include, but are not limited to:

- IT data such as the creation of backdoor accounts, or data downloads (Capelli et al., 2012)
- Personnel data, such as disciplinary actions resulting from conflicts with colleagues, or misuse of worktime (Capelli et al., 2012)
- Travel data that reveals misuse of travel, and/or expenses (Capelli et al., 2012)
- Security data, such as entrance and exit times

Hackers select human targets through a variety of methods, including, but not limited to physical surveillance of a target organization, data searches in social media, or

by telephoning a target organization. Once a target is selected, the hacker seeks out information about both the target organization and the specific human target(s) within that organization. Social media provides a wealth of information about individuals which can be used to create emails designed to appeal to a human target, and entice the individual to click on a link or open an attachment infected with malware. Social media data, the phishing email, and malware are all elements of the informational dimension. Both the hacker and the human target interact with the informational dimension by creating informational elements and consuming informational elements. If the informational dimension is removed from cyberspace, then there is no data being created, disseminated, stored, shared, or turned into knowledge, and no software to support decision making or automate processes. Further, access to information is often the goal of a cyberattack, such as cyberespionage or cybercrime (Luppicini, 2014; Myauo, 2016; Archer, 2014). Thus we posit:

P4: Cyberattacks will include an informational dimension.

P5: Cyberattacks will include an element of the cognitive dimension (hacker, organization, human target, etc.) interacting with an element of the informational dimension (data, software, knowledge, etc.).

The lion's share of information security theory is based on the interaction between the physical and the informational dimensions (Burmester et al., 2012; Cavsoglu et al., 2009; Chen et al., 2015; Johnson & Warkentin, 2010), as is the sociomateriality literature, which proposes the concept of the *IT artefact* (Leonardi, 2013). Without the interaction between these two dimensions in cyberspace, these theoretical concepts are lost within the Cyber-Based View construct. The creation of *cyber-physical systems* also speaks

directly to an interaction between elements of the physical dimension such as computers, networks, heart monitoring devices, or transportation networks, and elements of the informational dimension, such as data and software (Nguyen, 2013; DiMase et al., 2015; Vanderhaegen, 2017; Netto & Spurgeon, 2017). The use of malware, an informational element, to impact operations of a device, such as a sensor, a computer keyboard, or a transformer (Amin, 2015; Balzacq & Cavelty, 2016; Farwell & Rohozinski, 2011; Finlay, 2018), is the most recognized outcome of cyberattack. A cyberattack consists of two major components, the computing environment vulnerability to be exploited (physical element) and the payload being delivered (informational element) (Nguyen, 2013). In fact, it is the technical effect of the malware on the physical devices that is often the first indicator that a cyberattack has taken place (Balzacq & Cavelty, 2016). Thus we posit:

P6: Cyberattacks will include an element of the informational dimension (e.g. malware or data) interacting with an element of the physical dimension (e.g. computer, network, sensor, etc.).

The multilateral relationship between the cognitive, physical, and informational dimensions is what sets the Cyber-Based View apart from other theoretical frameworks. In order for the cognitive dimension to interact with the informational dimension, there must be some kind of mediation from the physical environment. For example, written information is absorbed through the act of reading signage, a screen, or a piece of paper by using the eyes or, in the case of braille, the fingertips. Auditory information may be provided through broadcasting technologies such as radios or televisions, the use of the larynx, or the movement of physical objects through space,

such as a moving vehicle or falling tree. Auditory information is absorbed by listening with the ears, or possibly by feeling the vibrations of the soundwaves with the body.

For example, in a botnet attack, it doesn't matter in which devices (physical) the zombies for a botnet (informational) reside, but rather where the controllers (cognitive) and thus the instructions (informational) for their command-and-control networks (informational] are operated from (physical) and by whom (cognitive) (Farwell & Rohozinski, 2011).

The vector through which a cognitive attack is launched is often informational, such as with an email during a phishing attack. It can include the manipulation of data, as with the 2013 hack of the AP twitter feed, when investors, believing that an explosion had occurred at the White House, caused a 143.5-point drop in the Dow Jones Industrial Average and a loss of more than \$136 billion U.S. Dollars in the Standard and Poor's 500 Index (Prigg, 2015) – a very tangible outcome. The cognitive dimension, though always vulnerable to misinformation, has become considerably more vulnerable with the growth of cyberspace because of the wealth of information delivered to it by the physical and informational dimensions. Thus we posit:

P7: Cyberattacks will include multilateral interactions between the cognitive, physical, and informational dimensions.

Figure 10 illustrates the research construct used to examine the dynamics of cyberattacks.

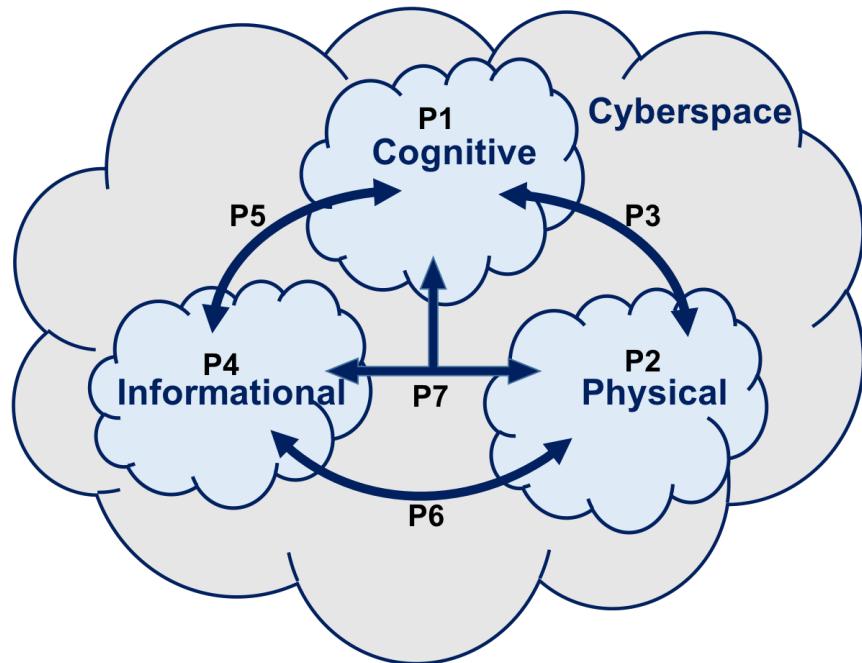


Figure 10. Cyber-Based View Research Construct

Research Design

This study employs a “failure autopsy” qualitative approach to examine successful cyberattacks, using a qualitative multi-case study analysis. In the context of an evolving phenomenon, historical analysis is useful to infer underlying patterns. This approach was chosen because it provides a way to structure a considerable amount of information into a concise narrative (Calori et al., 1997).

Case study analysis is meaningful because it employs multiple methods “to bring different epistemological perspectives together” (Almutairi et al., 2014, p. 243) to facilitate understanding of highly complex, contextual phenomena (Almutairi et al., 2014). The cyberattack case studies were developed through a combination of coding, pattern matching, and narrative techniques.

Part 1: Choosing Case Studies for Investigation

Data Collection

The broad definition for cyberattack offered by Archer (2014) which includes cyber exploitation, disruptive cyber activity, and destructive cyber activity was used to develop the initial data set. A pool of 114 candidate events was compiled using a broad internet search using the following search terms: biggest hacks of all time, notorious hackers, biggest hacks of 2013, 2014, 2015, 2016, 2017, biggest hacks of all time 2010, biggest hacks of all time 2005, biggest hacks of all time 2000, innovative hacks, biggest government hacks, cyber breaches federal government, cyber breaches critical infrastructure, cyberattack critical infrastructure, twitter facebook botnets, botnets, social engineering hacks, fake news, DDoS, ransomware, bitcoin hacks.

Method

Part 1a

In order to reduce the initial sample size, the 114 candidate events were stratified using two criteria. The first criteria was the type of cyberattack as defined by Archer (2014): cyber exploitation, which includes both cybercrime and cyberespionage; disruptive cyber, and destructive cyber. The second criteria was the type of attacker involved in the event in order to differentiate between attacks perpetrated by nation states, organized crime gangs, hacktivist organizations, terrorist networks, or individual hackers. Within each of these strata, an online random number generator tool, called *Research Randomizer*, was applied to reduce the total number of events within a category to no more than 10 candidates. Two events were removed from the list because they did

not fit the criteria of a cyberattack, reducing the sample from 114 events to 112 candidate events.

1. In 2015, there was a vulnerability discovered in the password manager “Last Pass,” which was falsely reported as a hack. This event highlighted a vulnerability that could have been used to conduct a cyberattack, but it was not a cyberattack.
2. Also in 2015, there was a data breach at the State of Georgia, Secretary of State’s office, but this was not the product of a cyberattack. It was the result of employee carelessness, when Georgia Secretary of State Brian Kemp mailed CDs containing the data of 6.2 million registered voters to 12 organizations that had purchased voting information. This event was a data breach, but not a cyberattack.

Once the remaining 112 events were classified by type of attack and type of attacker, the sample was sorted to determine how many candidate events existed within each category and sub-category. This approach was used to ensure a robust sample with a variety of cyberattack and attacker types as the sample size was reduced.

1. Sixty-six (66) events were classified as cyber exploitation, which can be further stratified as cyberespionage (39 events) and cybercrime (27 events).
 - a. Hacktivist organizations were attributed with three (3) cyberespionage events, many of which were presented as “socially conscious” behaviors.
 - b. Individual hackers were tied to twelve (12) cyberespionage events.
 - c. Nation states were identified as the perpetrators in eighteen (18) cyberespionage events.
 - d. Organized crime was attributed to six (6) cyberespionage events.
 - e. Individual hackers were responsible for five (5) cybercrime events.

- f. North Korea was the only nation state attributed with a cybercrime event
 - (1): stealing bitcoin from a South Korean bitcoin exchange.
 - g. The lion's share (21 events) of cybercrime events are attributed to organized crime.
- 2. There were forty-two (42) events that were classified as disruptive cyberattacks.
 - a. Twenty-five (25) of the disruptive cyberattacks were attributed to nation states.
 - b. Eight (8) of the disruptive cyberattacks were attributed to individual hackers.
 - c. Six (6) of the disruptive cyberattacks were attributed to organized crime.
 - d. Two (2) of the disruptive cyberattacks were attributed to terrorist networks.
 - e. One (1) disruptive cyberattack was attributed to a hacktivist organization.
- 3. There were four (4) events which were categorized as destructive cyberattacks, three of which have been attributed to nation states, and one of which was attributed to an individual hacker.

Using the website *Research Randomizer* (2018), unique sets of random numbers were generated within each category to select candidate events from the larger samples. According to the website, *Research Randomizer* is “a free resource for researchers and students in need of a quick way to generate random numbers or assign participants to experimental conditions. This site can be used for a variety of purposes, including psychology experiments, medical trials, and survey research.” Figure 11 provides an example of the output from Research Randomizer.

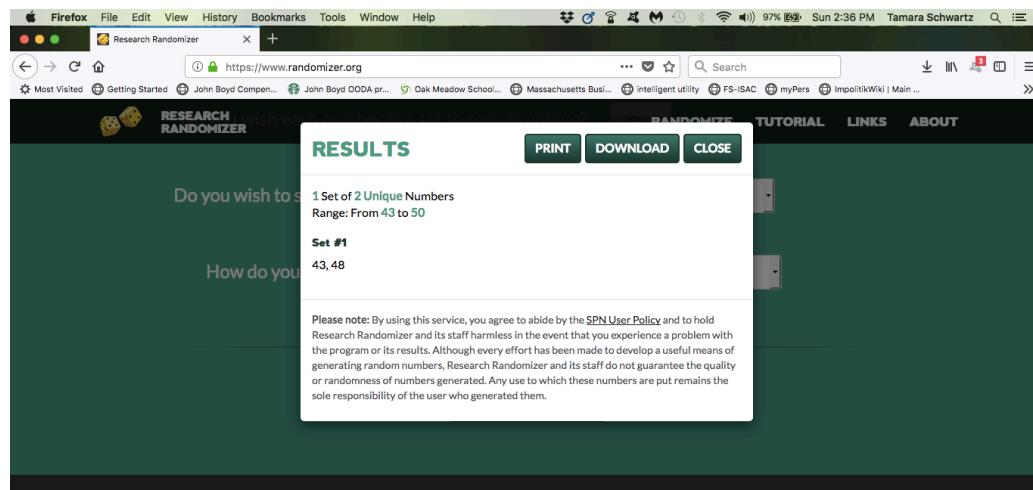


Figure 11. Output from Research Randomizer.

In areas where there were four events or less, all candidate events were retained on the survey. The outcomes of the random sampling approach were as follows:

1. *Cyberespionage* events were reduced from 39 events to 12 events.
 - a. Three hacktivist events were all kept on the survey.
 - b. Starting with 12 events attributed to individual hackers, one set of three unique numbers was generated within the range 86-97 based on the lines within the original list. Events 95, 87, and 92 were kept on the survey.
 - c. Starting with 18 events attributed to nation states, one set of three unique numbers was generated within the range 94-114. Events 101, 103, and 115 were kept on the survey.
 - d. Starting with a list of 6 events attributed to organized crime, one set of three unique numbers was generated within the range 115-120. Events 121, 118, and 119 were kept on the survey.
2. *Cybercrime* events were reduced from 27 events to 8 events.

- a. Five events were attributed to individual hackers. One set of two unique numbers was generated within the range 15-19, and events 17 and 18 were kept on the survey.
 - b. The one nation state event attributed to North Korea was kept on the survey.
 - c. Twenty-one events attributed to organized crime were reduced to a set of five events. One set of five unique numbers was generated within the range 21-41. Events 27, 33, 37, 31, and 34 were kept on the survey.
3. Disruptive cyberattack candidate events were reduced from 42 events to 11 events.
 - a. Twenty-five events attributed to nation states were reduced to four events. One set of four unique numbers was generated within the range 51-74. Events 74, 72, 54, and 69 were kept on the survey.
 - b. Eight events attributed to individual hackers were reduced to two events. One set of two unique numbers was generated within the range 43-50. Events 43 and 48 were kept on the survey.
 - c. Six events attributed to organized crime were reduced to two events. One set of two unique numbers was generated within the range 75-80. Events 77 and 80 were kept on the survey.
 - d. The two events attributed to terrorist networks were kept on the survey.
 - e. The one event attributed to a hacktivist organization was kept on the survey.

4. There were only four *destructive cyberattack* candidate events, and all four were kept on the survey.

Using this approach, the total number of events on the survey was reduced from 112 events to 35 events. Although the use of the randomizer resulted in the removal of the Melissa Virus attack which took place in 1999, this event was added back into the survey because it appeared on nearly every published list of significant cyberattacks. The reduced sample includes 36 candidate cyberattacks.

Part 1b

In order to select the events for case study from the reduced sample, a panel of experts from the Department of Defense, the National Security Agency, hackers, commercial cybersecurity specialists, and cyber operations communities was recruited to complete a survey evaluating the reduced data set. Study participants spent no more than two hours completing the survey. A questionnaire (Appendix C) was developed describing the cyberattacks identified in the reduced data sample, including the year of the cyberattack and a brief description. The survey instrument was tested with three subjects from the cybersecurity academic community, and the language in the evaluation criteria was adjusted based on feedback. Using Qualtrics to administer the survey, study participants were asked to rate the events using a 1-5 Likert-type Scale to evaluate the following criteria:

- *Success of the event (originally attack)*: organizational impacts, overcoming security measures, organizational security culture, goal achievement

- *Scale of the event (originally attack)*: number of countries affected, number of organizations affected, impact to operations within the organization, impact to organizational stakeholders
- *Novelty of the event (originally attack)* in the context of the time when it occurred: creativity/innovation, exploitation of new vulnerabilities, employment of emerging technologies, use of new tactics and techniques
- *Familiarity with the event (originally attack)*: is the panelist familiar with the event such that they are comfortable applying the evaluation criteria.

The survey captured responses from twelve experts in the cybersecurity community, including former National Security Agency hackers, Military Cyberwarriors, and commercial cybersecurity experts; however, every event was not scored by every participant. For each cyber event, Qualtrics provided a total score for each rating criteria by summing the Likert scores from each respondent. The scores for each rating criteria were then added to acquire a total score for the event. The results of the survey are captured in Appendix E. These scores were then used to rank order the cyber events, and seven of the top eight cyberattack events were developed into qualitative case studies. The Northeast Blackout of 2003 was ranked second on the list of cyberattack events, but research into this event revealed it to be a hoax (Poulsen, 2008), which is why this event was eliminated from the top eight. However, there were two blackouts in Ukraine in 2015 and 2016 which were the product of cyberattacks. The experts did not have an opportunity to evaluate these events because they had been removed from the survey by the random number generator approach. Research revealed that the 2015 and 2016 Ukrainian blackouts are the only known instances of cyberattacks of electric power

infrastructure, so the 2015 and 2016 Ukrainian Blackouts were substituted for the 2003 Northeast Blackout event and developed into a qualitative case study.

The goal was for the final sample to include at least two events for each type of attack: cyber exploitation, disruptive cyber, and destructive cyber (3 strata) and at least one, but preferably two events for each type of attacker: nation states, organized crime gangs/terrorist networks, hacktivist organizations, and individual hackers (4 strata). In order to achieve this goal, one additional hacktivist event was added to the study. Two candidates were considered for this last case study: the 2015 hack of the IRS conducted by Anonymous, which was ranked #14 with a raw score of 149 points, and the 2015 hack of the dating website Ashley Madison by The Impact Team, which was ranked #19 with a score of 142 points. Although the IRS event achieved a higher total score, the evaluators rated themselves as being less familiar with the IRS hack than they were with the Ashley Madison hack. Because they experts were more familiar with the Ashley Madison case, this score was determined to have greater validity than the score for the IRS event, and the Ashley Madison hack was selected as the ninth case study for investigation.

The purpose of this approach to select the case studies was to ensure generalizability of the sample by including all types of cyberattacks as defined in the study and all types of attackers. Table 4 shows the rank ordered list of the selected case studies classified by type of cyberattack and type of attacker. In order to further showcase the breadth of the sample, Table 5 shows the rank ordered list of the case studies classified by industry and types of technology tools employed by the attackers.

Table 4. Rank Ordered Case Studies Classified by Type of Cyberattack and Type of Attacker

Case Study	Type of Event			Type of Actor		
	Cyber Exploitation	Disruptive Cyber	Destructive Cyber	Nation State	Organized Crime	Hacktivists
Cybercrime	Cyberespionage					
Stuxnet, 2010			✓	✓		
Ukrainian Blackouts 2015 & 2016		✓	✓	✓		
Internet of Things (IoT) Botnet, 2016 - present		✓			✓	✓
Twitterbots 2016-present		✓		✓		✓
Melissa Virus, 1999		✓				✓
Hack of American Business 2005-2012	✓			✓		
(Not)Petya Ransomware, 2017	*	✓	✓	✓		
Manning Disclosure & WikiLeaks, 2010		✓			✓	✓
Ashley Madison, 2015	✓				✓	

* Ransomware is typically cybercrime, but the Petya Ransomware, 2017 event was destructive malware masquerading as ransomware.

Table 5. Rank Ordered Case Studies Classified by Industry and Employed Technology Tools

Case Study	Industry	Descriptive Details		Technology Tools	
		Critical Infrastructure			
Stuxnet, 2010	National Intelligence Community	Banking & Finance: Electricity	Banking & Finance: Consumer Credit	Communications	Information Technology
Ukrainian Blackouts 2015 & 2016	Critical Infrastructure	Postal & Shipping	Healthcare & Public Health	Governments & Elections	Nuclear Reactors, Materials, & Waste
Internet of Things (IoT) Botnet, 2016 - present	Transportation	Retail	Manufacturing & Shipping	Industrial Control Systems	Internet of Things
Twitterbots 2016-present	Postal & Shipping	Commercial Facilities: Retail	Healthcare & Public Health	Social Media	Internet Infrastructure
Melissa Virus, 1999	Healthcare & Public Health	Commercial Facilities: Manufacturing	Manufacturing & Shipping	Wikileaks	Organization IT
Hack of American Business 2005-2012	Transportation	Industrial Control Systems	Industrial Control Systems	Wikileaks	
(Not)Petya Ransomware, 2017	Postal & Shipping	Commercial Facilities: Manufacturing	Commercial Facilities: Manufacturing	Wikileaks	
Manning Disclosure & Wikileaks, 2010	Postal & Shipping	Commercial Facilities: Manufacturing	Commercial Facilities: Manufacturing	Wikileaks	
Ashley Madison, 2015	Postal & Shipping	Commercial Facilities: Manufacturing	Commercial Facilities: Manufacturing	Wikileaks	

*(Not)Petya Ransomware attack affected multiple industries, but this case study analysis focused on AP Moller-Maersk.

Part 2: Case Study Development and Analysis

Data Collection

An electronic database search in Lexis-Nexis and Google using key words related to the cyberattack event was employed to collect journal articles, academic articles, and other media. In addition to reference materials collected through electronic database searches, public documents were sourced by searching the Internet sites of relevant government agencies (e.g. General Accounting Office, Federal Bureau of Investigations, Department of Justice, Security Exchange Commission, Department of Defense, and the Information Sharing and Analysis Centers). Discussion forums from within the hacker and cyber-security communities, such as HAKIN9 Magazine were also used.

According to Saunders et al. (2018), saturation is a widely accepted qualitative research principle indicating that additional data collection and/or analysis is no longer necessary based on the data that has already been collected and analyzed. Additional data collection using the above keyword search method continued iteratively until saturation was achieved.

Data Analysis

Each cyberattack event was developed into a qualitative case study by examining, coding, and recombining the narratives within the qualitative data collected from journal articles, academic articles, public records, and other media sources.

As the data was analyzed, each step of the process was captured in a codebook as illustrated in Tables 6 and 7. Capturing the process with a step-by-step codebook for the analysis of the qualitative data (Table 6) ensured rigor and encouraged reflexivity in order to account for bias resulting from the researcher's professional experience in

information warfare. The approach to analysis was iterative, moving between the data and theory to inform the data collection and analysis until saturation was achieved.

The data was catalogued, coded, and managed using the codebook tables in conjunction with coded filenames in Dropbox (Figure 12). A unique code was assigned to each article of source material in order to have traceability from the .pdf version of the article, to the citation, to the pattern matching analysis in the code book. This approach enabled the researcher to share the status of data analysis with members of the dissertation committee while work was in progress.

Melissa Virus					
	Name	Date Modified	Size	Kind	Search
Favorites	5-1 Peterson 1999	Jan 5, 2019, 1:30 PM	293 KB	PDF Document	
	5-2 WSJ 1999	Jan 5, 2019, 1:31 PM	560 KB	PDF Document	
	5-3 NYT 2002	Jan 5, 2019, 1:31 PM	788 KB	PDF Document	
	5-4 Smothers 1999	Jan 5, 2019, 1:31 PM	1.2 MB	PDF Document	
	5-5 NYT 2002	Jan 5, 2019, 1:31 PM	443 KB	PDF Document	
	5-6 NYT 1999	Jan 5, 2019, 1:32 PM	821 KB	PDF Document	
	5-7 Taylor 1999	Jan 5, 2019, 1:32 PM	274 KB	PDF Document	
	5-8 Redmond 1999	Feb 1, 2019, 4:29 PM	574 KB	PDF Document	
	5-9 CERT 1999	Jan 5, 2019, 8:07 PM	918 KB	PDF Document	
	5-10 Cheng 1999	Jan 5, 2019, 1:32 PM	756 KB	PDF Document	
	5-11 Pearce 2002	Jan 5, 2019, 1:32 PM	79 KB	PDF Document	
	5-12 Raney 1999	Jan 5, 2019, 1:39 PM	321 KB	PDF Document	
	5-13 NYT 1999	Jan 5, 2019, 2:24 PM	400 KB	PDF Document	
	5-14 Editor 2016	Jan 5, 2019, 2:24 PM	522 KB	PDF Document	
	5-15 Strickland 2008	Jan 5, 2019, 4:20 PM	311 KB	PDF Document	
	5-16 Panda 2013	Jan 5, 2019, 4:20 PM	354 KB	PDF Document	
	5-17 Techopedia 2019	Jan 5, 2019, 4:20 PM	193 KB	PDF Document	
	5-18 McNamara 2014	Jan 7, 2019, 8:48 AM	1.9 MB	PDF Document	
	5-19 Cluley 2009	Jan 5, 2019, 4:21 PM	2.7 MB	PDF Document	
	5-20 Mills 2009	Jan 5, 2019, 4:21 PM	2.1 MB	PDF Document	
	5-21 Leyden 2002	Jan 5, 2019, 4:22 PM	231 KB	PDF Document	
	5-22 Techspirited 2019	Jan 5, 2019, 4:22 PM	342 KB	PDF Document	
	5-23 Gostev 2005	Jan 7, 2019, 2:28 PM	463 KB	PDF Document	
Devices	Deleted duplicates	Jan 5, 2019, 5:13 PM	--	Folder	
	Melissa Virus case study	Jan 7, 2019, 4:36 PM	22 KB	Micros...(docx)	
	Melissa Virus Codebook	Feb 1, 2019, 3:29 PM	57 KB	Micros...(xlsx)	

Figure 12: Example of Dropbox Filing System for Melissa Virus

Table 6: Codebook for Analysis of Documents

Data Identifier	Article Citation	Reflexivity
Unique code to identify article	Bibliography	Discussion of how prior researcher knowledge impacts understanding of coded themes
Example : 5-9	Computer Emergency Readiness Team. (1999). <i>CA-1999-04: Melissa Macro Virus</i> , 31 March 1999.	This event impacted operations in the researcher's squadron during Kosovo operations.

The analysis of the narrative data used a coding process applying specific steps developed through an examination of the Stuxnet attack. First, the specific physical, cognitive, and informational elements were identified and highlighted using a color coded scheme. Physical elements were highlighted in yellow. Cognitive elements were highlighted in blue, and informational elements were highlighted in pink (Figure 13). In addition to color coding the data, each element will be captured in Table 7 to identify recurring themes, for example, in the Melissa Virus case study, “*any mail handling system could experience performance problems*” (CERT, 1999) was captured as a physical element, and “*...a Microsoft Word 97 and Word 2000 macro virus which is propagating via email attachments*” (CERT, 1999) was captured as an informational element.

4: CA-1999-04: Melissa Macro Virus

4 CA-1999-04: Melissa Macro Virus

Original issue date: March 27, 1999
Last revised: March 31, 1999
A complete revision history is at the end of this file.

Systems Affected

- Machines with Microsoft Word 97 or Word 2000
- Any mail handling system could experience performance problems or a denial of service as a result of the propagation of this macro virus.

Overview

At approximately 2:00 PM GMT-5 on Friday March 26 1999 we began receiving reports of a Microsoft Word 97 and Word 2000 macro virus which is propagating via email attachments. The number and variety of reports we have received indicate that this is a widespread attack affecting a variety of sites.

Our analysis of this macro virus indicates that human action (in the form of a user opening an infected Word document) is required for this virus to propagate. It is possible that under some mailer configurations, a user might automatically open an infected document received in the form of an email attachment. This macro virus is not known to exploit any new vulnerabilities. While the primary transport mechanism of this virus is via email, any way of transferring files can also propagate the virus.

Anti-virus software vendors have called this macro virus the Melissa macro or W97M_Melissa virus.

In addition to this advisory, please see the Melissa Virus FAQ (Frequently Asked Questions) document available at: http://www.cert.org/tech_tips/Melissa_FAQ.html.

I. Description

The Melissa macro virus propagates in the form of an email message containing an infected Word document as an attachment. The transport message has most frequently been reported to contain the following Subject header:

Subject: Important Message From <name>

Where <name> is the full name of the user sending the message.

The body of the message is a multipart MIME message containing two sections. The first section of the message (Content-Type: text/plain) contains the following text:

1999 CERT ADVISORIES | SOFTWARE ENGINEERING INSTITUTE | CARNEGIE MELLON UNIVERSITY |
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution. 24

Figure 13: Example of Coding Approach for Melissa Virus Item 5-9

Second, the content of the entire quote was examined to explore what model elements were interacting, for example, in the Melissa Virus attack, “...analysis of this macro virus indicates that human action (in the form of a user opening an infected Word document) is required for this virus to propagate” (CERT, 1999) indicated that a person made the decision to open (cognitive) information in the form of an infected Word Document leading to the propagation of the information rules comprising Melissa (informational). These interactions, which were revealed from coding the three elements

of the model within a single quote, derived the first order themes and were captured in Table 7.

Third, the first- order themes will be summarized in the seven second-order themes captured in the Cyber-Based View: physical, informational, and cognitive elements, and physical – informational interactions, physical – cognitive interactions, cognitive – informational interactions, and physical – cognitive – informational interactions.

Table 7: Model Elements & Interactions

Data Identifier	Physical	Cognitive	Informational	P – I Interaction	P – C Interaction	C – I Interaction	P – C – I Interaction
First Order Themes							
5-9	E.g. Machines, mail handling system	E.g. Our analysis indicates human action is required	E.g. Melissa macro virus	E.g. Machines (P) with Microsoft Word 97 or Word 2000 (I)	E.g. Human use (C) of computer (P)	E.g. Human action in the form of opening (C) an attached word document (I)	E.g. Human uses (C) computer to read (C) email (I) & mouse to open (C) Word doc (I)

Finally, these first order themes were used to develop the narrative case study of the events as they unfolded during the attack. “Intertextuality refers to the condition whereby all communicative events draw on earlier events” (Jorgensen & Phillips, 2002, p. 73). Using multiple kinds of source material aided triangulation of the data by combining elements from different discourses to capture the dynamic nature of intertextuality as it relates to the understanding of cyberattack. A pattern matching logic was used to analyze and synthesize the key elements and multiple first order themes identified during the coding process. Pattern matching was of particular importance because it highlighted the strengths and limitations of the Cyber-Based View framework (Almutairi et al., 2014).

Almutairi et al. (2014) describe a pattern as an “arrangement of occurrences, incidents, behavioral actions, or outcomes...apparent in the raw data” (p. 240). Pattern matching techniques, which are intended to increase rigor, were used to identify the patterns within the raw data and compare them with the theorized patterns (Almutairi et al., 2014) of the Cyber-Based View. Pattern matching diverges from conventional hypothesis testing because “pattern matching encourages the use of more complex or detailed hypotheses and treat(s) observations from a multivariate rather than a univariate perspective” (Trochim, 1989, p. 357). The comparison process indicated whether or not the predicted patterns were evident in the cyberattacks analyzed in the failure autopsy case studies.

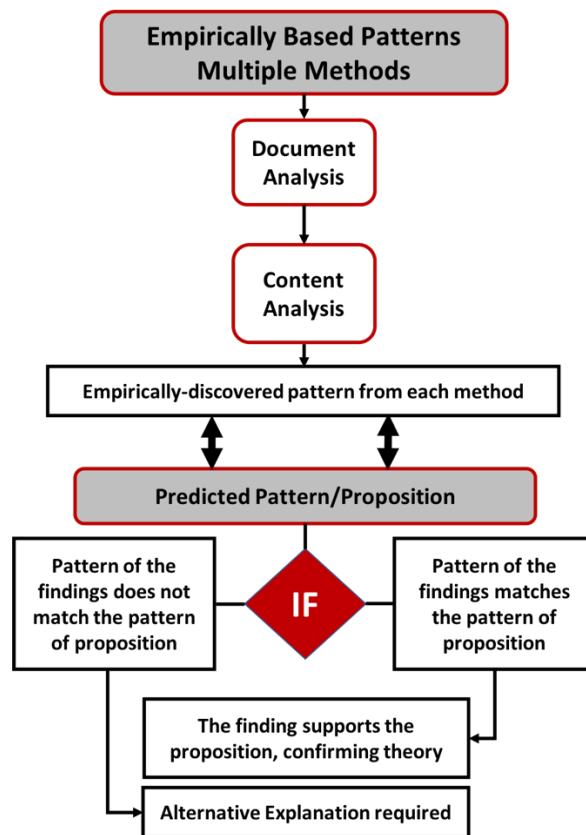


Figure 14: Pattern Matching Process, Adapted from Almutairi et al., 2014

Case Study Analyses

Analysis of the 2010 Stuxnet Attack

According to an NPR broadcast (2016), the Stuxnet Attack is recognized as “the first time to our knowledge that digital code was able to create physical destruction in the real world” (Shapiro, 2016), with many experts comparing it to the atom bomb dropped on Hiroshima and Nagasaki (Shapiro, 2016). The attack, which damaged over a thousand centrifuges at the Natanz Uranium Enrichment Facility (Lindsay, 2013; Nakashima & Warrick, 2012), has been attributed to the United States and Israel (Shapiro, 2016; Sanger, 2012; Rosenbaum, 2012; Paganini, 2016), although neither country has ever confirmed these suspicions (Rogers, 2015). At work in the Stuxnet attack was a choreographed dance leveraging the ecosystem of cyberspace, with elements at work in all three dimensions of the Cyber-Based View (Cyber-Based View) – physical, informational, and cognitive.

It is alleged that the Israelis built a replica of the Natanz enrichment facility in their Negev Nuclear Research Center in Dimona (Paganini, 2016; Broad et al., 2011) while it is speculated that the United States, which had acquired P-1 centrifuges from Libya (Broad et al., 2011), had a test facility in the Idaho National laboratory (Paganini, 2016; Broad et al., 2011). It is believed that these facilities were used to develop and test the Stuxnet cyberweapon through multiple iterations (Paganini, 2016; Nakashima & Warrick, 2012; Broad et al., 2011). An early version of Stuxnet, “Stuxnet 0.5,” was submitted to a malware scanning service in late 2007, suggesting that it was being tested to see if it could avoid detection by conventional antivirus systems (Arthur, 2013), while another

virus, “Flame” was also determined to be a precursor to Stuxnet designed to spy on infected computers and send data back to its creators (Kushner, 2013; Sanger, 2012).

Stuxnet, a set of information rules which maps to the informational dimension, entered through four “zero day Windows exploits”, which are software vulnerabilities that map to the informational dimension (Chen & Abu-Nimeh, 2011; Gjelten, 2010; Zetter, 2011; Lindsay, 2013; Farwell & Rohozinski, 2011; Kushner, 2013), including a vulnerability in the LNK file of Windows Explorer (Zetter, 2011). Stuxnet copied itself to other Windows PCs, which map to the physical dimension, through a print spooler vulnerability (MS10-061) (which maps to the informational dimension) and connected to other computers (also part of the physical dimension) through the Server Message Block protocol (an informational element) and exploited (exploitative behavior is a design characteristic and maps to the cognitive dimension), a Windows Server Service remote procedure call (RPC) vulnerability (MS08-067) (informational) (Chen & Abu-Nimeh, 2011). The Windows exploits (informational) were used as the point of entry (a hacker design decision mapping to the cognitive dimension) because Siemens SIMATIC STEP 7 software (informational), the ultimate target (targets are selected by attackers, indicating the presence of a cognitive element) (Kushner, 2013), runs on the Microsoft Windows operating systems (informational) and provides human interfaces to monitor and control, both cognitive behaviors of operating personnel, the peripheral devices that drive equipment such as centrifuge rotors, all of which are tangible physical devices mapping to the physical dimension (Lindsay, 2013).

Once the virus (informational) had infected a Windows system (physical), it would then install itself (informational) on a USB stick (physical). This technique was designed

into (cognitive) Stuxnet (informational) with the specific knowledge that humans would then connect (cognitive) their equipment, whether it was a laptop or USB drive (physical), to computers inside Natanz (physical), allowing the Stuxnet worm (informational) to “jump the air gap” (Farwell & Rohozinski, 2011; Lindsay, 2013; Zetter, 2011; Arthur, 2013). When an infected computer or USB stick (physical) was connected to (cognitive) the Siemens Programmable Logic Controllers (PLC) (physical) running Siemens SIMATIC Step 7 software (informational), a malicious .dll file (informational) was installed to operate in memory to remain hidden (techniques to remain hidden are a cognitive element), while allowing Stuxnet to monitor and intercept communication (informational) between the PC and the PLC (physical) (Chen & Abu-Nimeh, 2011; Zetter, 2011; Kushner, 2013). The use of (cognitive) two digital certificates of authenticity (informational) (Gjelten, 2010; Weinberger, 2011; Zetter, 2011) from verified sources: Realtek Semiconductor and JMicron Technology (cognitive) (Chen & Abu-Nimeh, 2011; Zetter, 2011; Lindsay, 2013) enabled installation of a rootkit which used a hard-coded password to access the SIMATIC Step7 software (informational) (Lindsay, 2013; Farwell & Rohozinski, 2011) in order to be able to inject commands (informational) into the PLC (physical).

In addition to intercepting communications (informational) between the PC and the PLC (physical), Stuxnet relayed information back (informational) to servers hosted in Malaysia and Denmark (physical), allowing its authors to update (cognitive) the software with new functionality (informational) (Zetter, 2011; Weinberger, 2011). “Stuxnet had an extensive configuration file – mdmcpq3.pnf— with a menu of more than 400 items

[informational] the attackers could tweak to control [cognitive] every aspect of the code [informational]" (Zetter, 2011).

Hidden (cognitive) within the Stuxnet code was the specific configuration (informational) of the Natanz facility (physical) (Zetter, 2011; Rosenbaum, 2012; Lindsay, 2013; Broad et al., 2011). The malware logic asked questions specific to the configuration (informational) of Natanz (physical), as if it "had been written by lawyers" designed to limit collateral damage (cognitive) (Rosenbaum, 2012). According to a cable released on Wikileaks, the intent was to design a weapon that could find even those facilities that were unknown (Paganini, 2016; Zetter, 2011; Broad et al., 2011).

Once Stuxnet was installed (informational), it would slow down and speed up the normal frequency of the frequency converters (physical) manufactured by Fararo Paya and Vacon (cognitive) (Farwell & Rohozinski, 2011; Zetter, 2011) on the centrifuges (physical), which ultimately caused the devices to fail over time, potentially causing them to fly apart (physical). (Chen & Abu-Nimeh, 2011; Zetter, 2011; Weinberger, 2011; Rosenbaum, 2012; Lindsay, 2013). Using a "man in the middle" strategy, Stuxnet would mask the malicious commands and intercept status reports (informational) sent to the PLC Step7 machine (physical) so that workers monitoring (cognitive) the PLC from the Step7 machine (physical) would see only authorized commands (informational) and normal operations (Langner, 2011; Zetter, 2011; Weinberger, 2011; Lindsay, 2013; Broad et al., 2011). Stuxnet also disabled any automated commands to prevent any automated responses (informational) designed to prevent (cognitive) catastrophic failure (physical) (Zetter, 2011; Broad et al., 2011; Langner, 2011).

The nature of the failures (physical) appeared to be random, another strategy designed with the understanding (cognitive) that a significant number of simultaneous failures (physical) “would be discovered and neutralized to early” (cognitive) (Lindsay, 2013). Random, continuing failure (physical) was intended to make the Iranians think it was due to a lack of expertise (cognitive) (Sanger, 2012; Nakashima & Warrick, 2012; Langner, 2011), a fact that was corroborated by intelligence that engineers from the Natanz facility were fired (Sanger, 2012).

Like any industrial facility, Natanz was not just an assemblage of technical equipment (physical), but also a human organization (cognitive) (Lindsay, 2013). Knowing this, (cognitive) the initial infections (informational) were spread to organizations known or suspected to work with (cognitive) the Natanz facility (physical). Stuxnet left a digital trail (informational) to a number of Iranian engineering firms: Foolad Technic, Behpajoooh, Neda Industrial Group, and Control Gostar Jahed, all of which were known providers of design, installation, and programming (cognitive) of industrial control systems (ICS), (physical) including the Siemens Step7 software (informational) which drove the centrifuges used to refine uranium at the Natanz Enrichment Facility (physical) (Zetter, 2014). The interactions between multiple organizations was a critical cognitive element of the cyberspace ecosystem because the Natanz facility was tangibly “air-gapped” (physical) meaning that it did not physically connect to the larger internet.

In order to gain access to these secondary actors (cognitive), hackers used social engineering techniques (cognitive) such as spear phishing emails (informational) to lure targeted users into clicking (cognitive) on fraudulent websites or attachments infected

with malware (informational) (Lindsay, 2013). At one point, an engineer at Neda became suspicious (cognitive) that there was malware (informational) installing itself on USB sticks (physical) and corrupting the computers (physical), but when he ran (cognitive) detection software to look for viruses (informational), no malware was identified (Zetter 2014). Stuxnet (informational) was designed with the understanding that there were both humans (cognitive) and other software (informational) which might detect its presence, employing specific techniques to remain hidden, and illustrating the strategic nature of the hackers who perpetrated the attack.

Analysis of the 2015 and 2016 Ukrainian Blackouts

In preparing the initial data set for the survey to rank cyber events, the 2003 Northeast Blackout was identified as one of the most significant cyberattacks on critical infrastructure, and was included in the survey. The theory was that the attack was an act of terrorism (Barker, 2013) and that the explanation of trees interfering with the transmission lines was a cover story (Barker, 2013; Poulsen, 2008;). When data collection examining the 2003 Northeast Blackout as a cyberattack revealed that it was just a theory that resulted from critical computer system failures (Poulsen, 2008; Barker, 2013) and the identification of malware on computers as opposed to a targeted virus (Moyer, 2011), the data collection search terms were changed from “cyberattack 2003 Northeast Blackout” to “cyberattack power outage” and the Ukrainian Blackouts of 2015 and 2016 were identified as the first known and confirmed case of power outages caused by cyberattack (Greenberg, 2017; Sullivan & Kamensky, 2017; Polityuk et al., 2017; Smith, 2018; Lee et al., 2016; Osborne, 2018). These events were the subject of significant interest in the U.S. electric power sector because they show evolving

cyberattack capabilities and dry run attacks that could be modified to attack power grids and other critical infrastructure anywhere in the world (BBC, 2017; Greenberg, 2017; Osborne, 2018; Smith, 2018; Zetter, 2017).

Since 2007 in its military clashes with Georgia, Russia has been honing its integration of cyberwarfare with traditional military and economic force (Kozlowski, 2014; Park et al., 2017). Espionage operations have always been a substantial element of Russia's political and military conflicts with Eastern Europe, and the growth of cyberspace has expanded this capability (Park et al., 2017; Kozlowski, 2014). Russia's use of hybrid warfare has become commonplace in Ukraine since the annexation of Crimea in 2014 (Greenberg, 2017; Sullivan & Kamensky, 2017; Park et al., 2017; Smith, 2018; BBC, 2017). Because of the Russian exploitation of cyberspace through hybrid warfare, both the 2015 and 2016 cyberattacks on the Ukrainian power grid have been attributed to Russia (Park et al., 2017; Harrell, 2017; Smith, 2018; Greenberg, 2017; Sullivan & Kamensky, 2017).

The first attack occurred on December 23, 2015, causing a six hour blackout that affected 225,000 customers in and around Kiev, Ukraine (BBC, 2017; Polityuk et al., 2017; Huang et al., 2018; Toecker, 2016). During this attack, operators in the control rooms watched their cursors moving around on the screen, navigating through the Industrial Control Systems and executing commands to cause the outages (Sullivan & Kamensky, 2017; Toecker, 2016). A second attack occurred almost one year later, beginning just before midnight on December 17, 2016 and lasting just one hour (Zetter, 2017; Park et al., 2017; Huang et al., 2018; BBC, 2017; Polityuk et al., 2017; Adamczyk, 2017; Harrell, 2017). Although the 2016 blackout did not last as long as the 2015

cyberattack, the tactics, techniques and software indicated a much more sophisticated hack, demonstrating an evolving capability (Osborne, 2018; Greenberg, 2017; Park et al., 2017; Huang et al., 2018; Smith, 2017).

The 2015 attack, launched on December 23rd, was conducted against three electric power distribution companies (cognitive), began with a spear phishing (cognitive) email campaign (informational) (Greenberg, 2017; Park et al., 2017; Toecker, 2016; Detsch, 2016; Smith, 2018; Zetter, 2017; Lee et al., 2016; Harrell, 2017; Osborne, 2018). The hackers weaponized (cognitive) Microsoft Office Word and Excel documents (informational) by embedding BlackEnergy3 malware (informational) (Park et al., 2017; Zetter, 2017; Lee et al., 2016; Harrell, 2017). These emails (informational) were delivered to personnel working (cognitive) in the administrative and IT networks (physical) within the companies (source). Upon opening (cognitive) the messages (informational), the users would be prompted (cognitive) by a popup message (physical – informational) to enable (cognitive) macros (informational), which allowed the malware to install BlackEnergy3 (informational) on the operator's system (physical) (Park et al., 2017; Huang et al., 2018; Sullivan & Kamensky, 2017; Lee et al., 2016; Harrell, 2017).

The BlackEnergy3 malware (informational) allowed the hacker to connect to and communicate with (cognitive) the command and control system (physical) (Park et al., 2017; Huang et al., 2018; Sullivan & Kamensky, 2017; Lee et al., 2016; Harrell, 2017). Over the course of the next six months, the hackers began to steal (cognitive) credentials (informational) and expand their privileges to move throughout the systems, blending into the environment until they had gained access (cognitive) to the Industrial Control Systems (ICS) and the Uninterruptable Power Supply (UPS) systems (physical) used to

manage (cognitive) the connected load (physical) during scheduled maintenance (cognitive) (Lee et al., 2016; Osborne, 2018; Park et al., 2017; Smith, 2017; Polityuk et al., 2017; Huang et al., 2017; Detsch, 2016).

Using these capabilities, the attackers were able to use (cognitive) the Virtual Private Network (VPN) (physical) and existing remote access tools (informational) to issue (cognitive) the necessary commands (informational) to cause the power outage (physical) (Lee et al., 2016; Park et al., 2017). Operators describe sitting (cognitive) at their supervisory control and data acquisition (SCADA) terminals (physical) watching (cognitive) their cursors move around the screen (physical) systematically opening (cognitive) breakers at 30 substations (physical) (Sullivan & Kamensky, 2017; Toecker, 2016; Park et al., 2017). Within 5 minutes, power had been cut off to 225,000 customers (physical) (Toecker, 2016).

In addition to opening (cognitive) the breakers to cause the power outage (physical), the attackers used (cognitive) corrupted firmware (informational) to disable (cognitive) remote-terminal units in the substations (physical), requiring the technicians to travel (cognitive) to the various sites (physical) and manually close (cognitive) the breakers to restore power (physical) (Zetter, 2017; Toecker). They also reconfigured (cognitive) the battery backup systems (physical) in order to thwart (cognitive) the automatic transfer functionality (informational), knocking the command and control systems offline (physical) (Toecker, 2016). The attack was rounded out with a complete wipe (cognitive) of the hard drives of the control systems (physical) using KillDisk malware (informational), which required the reinstallation of (cognitive) the operating system and

other critical software components (informational) (Toecker, 2016; Zetter, 2017; Lee et al., 2016; Park et al., 2017; Sullivan & Kamensky, 2017).

Nearly one year later, on December 17, 2016, hackers attacked (cognitive) the grid (physical) a second time, but instead of directing the attack against (cognitive) distribution stations (physical), they targeted (cognitive) a transmission facility (physical) (Zetter, 2016; Greenberg, 2017; Park et al., 2017; Smith, 2017; Harrell, 2017). Although this outage lasted only one hour (physical), it demonstrated an evolving expertise through the use of (cognitive) a malware called Industroyer (also called Crash Override), which automated the attack (informational) (Greenberg, 2017; Park et al., 2017; Huang et al., 2018; Osborne, 2018). Unlike in 2015, the hackers merely shut down (cognitive) the remote terminal units (physical) rather than breaking (cognitive) them, making it much easier to restore (cognitive) power (physical) (source). Industroyer (informational) was specifically designed to attack (cognitive) the power grid (physical), in a deliberate manner similar to the way (cognitive) Stuxnet (informational) was used to attack (cognitive) the centrifuges at the Natanz Iranian nuclear facility (physical) (Osborne, 2018).

As with the 2015 attack, this event began with a widespread phishing campaign (cognitive – informational) that targeted a number of government organizations in addition to the power companies (cognitive) (Osborne, 2018; BBC, 2017; Smith, 2018; Zetter, 2017). The hackers again conducted reconnaissance over a period of months prior to taking any action, blending in by using (cognitive) the same tools (informational) used by legitimate personnel and mimicking their behaviors (cognitive) (Zetter, 2017; Lee et al., 2016; Harrell, 2017; Park et al., 2017; Toecker, 2017).

Industroyer (informational) infiltrated (cognitive) the substation (physical) by exploiting (cognitive) the CVE-2015-5374 vulnerability (informational) in the Siemens SIPROTEC 4 and SIPROTEC Compact devices (physical) (Osborne, 2018; Greenberg, 2017). In order to persist, (cognitive) the malware made a copy of both the primary and secondary backdoors which would execute if the initial infection were uncovered (informational) (Osborne, 2018). The Industroyer malware (informational) focused on (cognitive) the industrial onsite hardware, specifically the substations' circuit breakers and protection relays (physical) (Osborne, 2018).

The malware included four different payloads (informational) which could be reconfigured to use (cognitive) the protocols defined by industry standards (informational) based on the devices present in the facility (physical) so that they could be compromised regardless (cognitive) of the device type (physical), vendor (cognitive), or configuration files (informational) (Osborne, 2018; Greenberg, 2017; Park et al., 2017). These different payloads enabled the malware to speak directly to and take control of (informational) the circuit breakers (physical) (Osborne, 2018; Greenberg, 2017; Park et al., 2017).

In addition to the communication protocols, the malware included two other components which magnified the attack (Osborne, 2018). First, a denial of service tool would attack (informational) the protection relays (physical) to prevent them from engaging (cognitive). Second, a wiper tool fixed on (informational) the command and control workstations (physical), scanned (informational) their hard drives (physical) for specific file extensions and deleted files (informational), inhibiting recovery (cognitive) if backup files (informational) were unavailable (Osborne, 2018). The malware

(informational) completed its work by crashing (cognitive) the system (physical) (Osborne, 2018).

Hidden within the malicious code, a predefined timer established (cognitive) the time and date (informational) for the power outage (physical) (Osborne, 2018). When the clock struck a few minutes before midnight, one-fifth of Kiev's power consumption was cut off (physical) (BBC, 2017; Greenberg, 2017; Adamczyk, 2017; Osborne, 2018). Operators who tried to respond to the event found (cognitive) open circuit breakers and nonresponsive protection relays (physical), and when they tried to remedy the situation, they discovered (cognitive) that their SCADA systems also failed to respond (physical) (Osborne, 2018).

Experts say the first attack in 2015 used approximately twenty people to attack three facilities, but that the improved capabilities built into Industroyer would enable those same twenty people to launch a coordinated attack on as many as ten – fifteen different facilities simultaneously (Greenberg, 2017). The Industroyer malware has grabbed the attention of the critical infrastructure industries in the United States and Europe because of its modular, automated design, which could allow it to be used not only in Ukraine, but anywhere in the world (BBC, 2017; Greenberg, 2017; Osborne, 2018; Smith, 2018; Zetter, 2017).

Analysis of the 2016 Internet of Things Botnet

Imagine Acme Corporation has purchased machines from a vendor in order to expand their capabilities. These new resources generate valuable information, assist with automation, and increase productivity, but the fine print in the vendor's sales contract explains that they come with *one small catch*. Acme's industry competitors can use the

exact resources Acme has just purchased and installed, inside the Acme facilities, whenever they choose. Not only that, any opportunist off the street who would like to use Acme's resources can also enter Acme's facilities to use them in any way they see fit, even if that means disrupting Acme's operations. This scenario is difficult to fathom. Of course, Acme would never permit anyone off the street, especially competitors or others who might disrupt operations, to enter their facility and make use of their resources, and yet, the Internet of Things (IoT) does exactly this.

A resource based view of IoT sees new resources that lead to innovative capabilities, but it ignores the fine print, because in a resource based view of the firm, these resources and capabilities belong to Acme Corp. and only Acme Corp. A Cyber-Based View of the firm recognizes that anything hooked up to the Internet is accessible to anyone with the ingenuity to gain access. A principle that is showcased in the growth of IoT botnets.

The term *botnet* is essentially a robot network – a collection of Internet-connected machines communicating with one another via software programming, and controlled by an outside party (Fruhlinger, 2018; Moriuchi & Chohan, 2018; Kolias et al., 2018). The first botnet, comprised mostly of desktop and laptop computers, was built in 2001 for the purpose of distributing spam, which became difficult to block because of the number of computers sending the messages (Fruhlinger, 2018). Since then, computers have become more difficult targets for hackers to incorporate into botnets because of more sophisticated firewalls and antivirus capabilities (Vlajic & Zhou, 2018). However, the growth of sensor capability has led to more and more devices being connected to the Internet, such as home routers, surveillance cameras, baby monitors, Fit Bits, insulin

pumps, thermostats, fish tank maintenance sensors, and the Smart Grid (Perlroth, 2016; Mansfield-Devine, 2016; Fruhlinger, 2018; Vlajic & Zhou, 2018; Moriuchi & Chohan, 2018; Schiffer, 2017), creating new resources for botnet builders.

These devices seem innocuous, afterall, what would be the purpose of gaining access to someone's fish tank (Schiffer, 2017)? As a result, vendors build little to no security built into these devices, and their vulnerabilities are well known (Sanger & Perlroth, 2016; Mansfield-Devine, 2016; Greenberg, 2017; Moriuchi & Chohan, 2018; Kolias et al., 2017). The common perception is that baby monitors and thermostats are not a computers, but the reality is, that in order to function in an Internet-connected environment, these devices must have some kind of computer operating system, often a stripped down Linux system (Fruhlinger, 2018, Trendmicro, 2017). Many devices include a default username/password, but it is rarely changed by the owner once a device is purchased (Kolias et al., 2017; Trendmicro, 2017; Greenberg, 2017; Moriuchi & Chohan, 2018; Fruhlinger, 2018), making them prime targets for hackers.

In addition to being useful for spam distribution (Fruhlinger, 2018), botnets are a valuable “weapon of mass disruption” (Sanger & Perlroth, 2016). Botnets are the tool of choice for hackers seeking to launch a distributed-denial-of-service (DDoS) attack. The first denial of service (DoS) attack was launched in 1974 by a 13-year old high school student. David Dennis who was curious about what would happen if all the computers in the Computer-Based Education Research Laboratory (CERL) at the University of Illinois Urbana-Champaign were to fail at the same time, and he created a program to do just that (Radware, 2018). The first distributed DoS (DDoS) attack, “Trinoo” enslaved machines as “masters and daemons” enabling the botmaster to send commands to a few “masters”

with instructions to forward to hundreds of “daemons” (Radware, 2018). The power of the DDoS attack was that it created a robustness because of the distribution of the devices powering the attack – a robustness that is buttressed by the Internet of Things.

IoT botnets first came to the attention of the public in October 2016, when the Mirai IoT botnet nearly brought down the Internet with DDoS firepower of 1.2 terabits per second (Liu, 2017; Vlajic & Zhou, 2018; Kolias et al., 2017).

Essentially, a DDoS attacker sends massive amounts of data traffic toward a server until the server collapses under the strain (Liu, 2017; Perlroth, 2016; Vlajic & Zhou, 2018). According to internet security expert Bruce Schneier, “If the attacker has a bigger firehose of data than the defender has, the attacker wins” (Sanger & Perlroth, 2016). The bigger the botnet, the larger the data firehose, and the IoT provides an smorgasbord of devices through which to create this capability.

The Mirai malware was built by an entrepreneurial Minecraft player hoping to generate revenue for himself by shutting down competing Minecraft hosts in order to drive traffic toward his own Minecraft game server (Fruhlinger, 2018). Ironically, Mirai’s first DDoS victim was French host OVH, which supported tools used by Minecraft server hosts to defend against DDoS attacks (Fruhlinger, 2018; Kolias et al., 2017). Not long after the September attack on OVH, the Mirai source code was released into the wild, where it has continued to evolve (Mansfield-Devine, 2016; Fruhlinger, 2018; Kolias et al., 2017; Trendmicro, 2017). Mirai IoT botnets are now available in multiple business models, including custom-made botnets and botnet-for-hire (Vlajic & Zhou, 2016; Leyden, 2017).

The botmaker begins by scanning (cognitive) the Internet for vulnerable devices (physical) using an IP search engine such as Shodan or Censys (physical), which periodically scan “all Internet facing networks (physical) to construct indexed databases (informational) of all discovered, publicly accessible (cognitive) devices/systems (physical), and provide public access (cognitive) to these databases (informational),” (Vlajic & Zhou, 2018, p. 29). A \$19.00 per month subscription to Shodan will provide a user with up to 10,000 queries (cognitive) and one-million results (informational) each month (Vlajic & Zhou, 2018).

According to Kolias et al. (2017), there are four main components to a Mirai botnet:

- The *bot*, malware (informational) that infects the device (physical)
- The *loader*, a server (physical) where potential devices (physical) are queued for malware infection (informational)
- The *command and control (C2) server*, (physical) from which the botmaster issues (cognitive) commands to the botnet (informational)
- The *report server*, (physical) which maintains a database of botnet device details (informational)

Armed with a list (informational) of candidate devices (physical), the Mirai malware begins to propagate (informational), attempting to gain access to devices (physical) by using a hardcoded (cognitive) list of 60+ possible username/password combinations (informational) (Kolias et al., 2017; Fruhlinger, 2018; Sanger & Perlroth, 2016). Once the bot identifies the right credentials (informational), it forwards device details (informational) to the report server (physical). From the C2 server (physical), the botmaster can communicate with (cognitive) the report server (physical) to retrieve

(cognitive) information (informational) about candidate devices (physical) and the status of the botnet (informational) (Moriuchi & Chohan, 2018; Koliass et al., 2017; NetLab, 2017; Greenberg, 2017). In order for the botmaster to remain anonymous (cognitive), the C2 server and the report server usually communicate via the Tor network (physical) (Koliass et al., 2017).

The botmaster will sort through (cognitive) the list of vulnerable devices (information) provided by the report server (physical) and choose which devices to recruit into the zombie army (physical) (Trendmicro, 2017; Greenberg, 2017; Leyden, 2017; Koliass et al., 2017). The botmaster then issues (cognitive) a detailed infection command (informational) to the loader (physical) to infect (informational) the device (physical) (Koliass et al., 2017; Greenberg, 2017; NetLab, 2017). The loader (physical) logs into (informational) the target (physical) and commands it to download and execute the Mirai code (informational) (Koliass et al., 2017; NetLab, 2017; Greenberg, 2017). This process is repeated until the botmaster has amassed a sufficient force to launch an attack against (cognitive) a target server (physical) (Fruhlinger, 2018; Koliass et al., 2017; Greenberg, 2017; Moriuchi & Chohan, 2018; Perlroth, 2016).

Once the botmaster issues (cognitive) an attack command (informational) through the C2 server (physical), the zombies – devices (physical) adopted into the botnet informational) – will begin to flood the target server (physical) with data (informational) (Fruhlinger, 2018; Koliass et al., 2017; Greenberg, 2017; Moriuchi & Chohan, 2018; Perlroth, 2016; Sanger & Perlroth, 2016; Perlroth, 2016). In October of 2016, one Mirai botmaster targeted Dyn, a company located in Manchester, N.H. which provides core infrastructure to the Internet (physical) by offering Domain Name System (DNS) services

(cognitive) – essentially a switchboard (physical) translating web addresses such as temple.edu into numerical addresses (informational) that enable computers to communicate with one another (physical) (Perlroth, 2016; Liu, 2017; Sanger & Perlroth, 2016). At the time of the attack (cognitive), approximately 493,000 devices hooked to the Internet (physical) were infected with Mirai malware (informational) (Perlroth, 2016; Koliass et al., 2017).

The onslaught began just prior to 9:30 AM, and initially, Dyn was able to fend off its attacker (cognitive) (Perlroth, 2016). They withstood a second strike (cognitive) around midday, but by 5:00 PM its servers (physical) were assaulted for a third time (cognitive) with record setting attack rates of 1.2 terabits per second (informational), and the servers collapsed (physical), making vast areas of the Internet, including such prominent websites as *The New York Times*, Netflix, Twitter, Tumblr, and Airbnb, inaccessible to people across the U.S. (cognitive), (Trendmicro, 2017; Liu, 2017; Greenberg, 2017; Perlroth, 2016).

Since the 2016 attack on Dyn, IoT botnet malware has continued to flourish, as the Mirai code is evolved by innovative hackers (Greenberg, 2017; Moriuchi & Chohan, 2018; Koliass et al., 2017; Vlajic & Zhou, 2018). In 2017, IoT_Reaper (also called IoTroop) emerged, which allows the botmater to perform modular software updates to infected devices (Vlajic & Zhou, 2018; Trendmicro, 2018; Greenberg, 2017; Leyden, 2017; Moriuchi & Chohan, 2018; NetLab, 2017). A second IoT botnet malware, Hajime introduces a peer-to-peer architecture, which creates greater resilience (Koliass et al., 2017; Vlajic & Zhou, 2018); however, Hajime does not exhibit malicious behavior. In fact, it actually closes device vulnerabilities exploited by other botnet malware,

suggesting that it may be the product of a white-hat hacker (Kolias et al., 2017). The financial sector was hit with a Mirai-variant botnet suspected to be IoTroop in January 2018 (Moriuchi & Chohan, 2018). With the continued growth of the Internet of Things, this threat will only continue to expand.

Analysis of the 2016 - Present Twitterbots

What happens when the authentic and the counterfeit become indistinguishable? What is *reality*, which is socially constructed (Farrell, 2018) when there are numerous rival narratives, some of which are deliberately false? False narratives are the key to influence campaigns (Kropotov & Yarochkin, 2017), whether the intent is to influence the outcome of elections (Wooley & Shout, 2016; Timberg & Dwoskin, 2018; Guilbeault & Woolley, 2016; Baraniuk, 2018; Hirsch, 2017; Curran, 2017; Confessore et al., 2018; Kropotov & Yarochkin, 2017), damage an individual's reputation (Confessore et al., 2018; Edwards et al., 2016; Krishna, 2015), steal data (Dubbin, 2013), sell products (Wojcik, 2018; Hirsch, 2017; Confessore et al., 2018; Dubbin, 2013; Timberg & Dwoskin, 2018; Edwards et al., 2016), or change behaviors. The secret to these influence campaigns is the use of specific tools to promote and propagate the spread of these false narratives (Kropotov & Yarochkin, 2017).

“The key to audience persuasion relies on an audience’s perception of information as logical and their willingness to centrally process it” (Edwards et al., 2016), a critical factor of which is to create a high level of social engagement (Kropotov & Yarochkin, 2017). Bot networks within social media, and more specifically, Twitterbots, an automated account that interacts with other Twitter accounts (Graham, 2017; Dubbin, 2013; Wooley & Shout, 2016; Wojcik, 2018; Timberg & Dwoskin, 2018; Edwards et al.,

2014; Kropotov & Yarochkin, 2017; Guilbeault & Woolley, 2016; Baraniuk, 2018; Hirsch, 2017; *The Economist*, 2017; Spence et al., 2018; Dubbin, 2013; Edwards et al., 2016), have become the tool of choice for disseminating “fake news” and other false narratives to achieve this high level of social engagement (Kropotov & Yarochkin, 2017; Hirsch, 2017; Curran, 2017; Confessore et al., 2018). According to a study by the Pew Research Center, approximately two-thirds of tweeted links are shared by suspected bot accounts (Wojcik, 2018).

According to Kropotov and Yarochkin (2017), “the manipulation of public opinion can be broken down into several steps, which can be described as the Public Opinion Cycle” (p. 62). Kropotov’s and Yarochkin’s (2017) Public Opinion Cycle includes the following steps:

- Gathering information about the target audience, including their levels of cognitive bias and knowledge
- Preparing the central narrative, including supporting stories and alternate versions
- Delivering the story through multiple venues such as traditional and social media
- Controlling the distribution of ideas to a receptive audience until the story reaches critical mass

Twitter is a micro-blogging platform that can be used to post “tweets” – notes of 140 characters or less – where users can “follow” or subscribe to one another in order to curate their individualized news feeds (Edwards et al., 2014). One key characteristic of Twitter’s interface is that it does not require a human being in order to share information (Edwards et al., 2016; Dubbin, 2013; Guilbeault & Woolley, 2016; Woolley & Shout, 2016; Graham, 2017). As a result, estimates suggest automated accounts make up over

15% of Twitter's user base (Spence et al., 2018) and non-human agents generate approximately 49% of web traffic (Hirsch, 2017). Twitterbots are relatively easy to build, and “when thousands are created and are tweeting more or less the same message, they have the ability to shape discourse on Twitter which then can influence other media discourses” (Graham, 2017, p. 2).

Many bots are designed for creative purposes, such as *Pentametron*, which searches for rhyming couplets to retweet (Dubbin, 2013), or Dubbin’s (2013) *Exosaurs*, which combined dinosaur species and exoplanets to create intergalactic dinosaur creatures. Spambots may be used to disseminate malware or advertisements (Dubbin, 2013). Still other Twitterbots are used to share public information, such as the CDC’s use of a bot to share health related information (Edwards et al., 2016), or the Weather Channel’s use of a bot to share Weather information (Spence et al., 2018). In a study comparing a Twitterbot against a professional meteorologist and an amateur meteorologist, both humans, Spence et al. (2018) found a negligible difference between the weather Twitterbot and the professional meteorologist with respect to social attractiveness, but no other statistically significant differences in perception of the Twitterbot. With respect to the amateur meteorologist, Spence et al. (2018) found that the weather Twitterbot was perceived as a better source of information than the human.

Studies show that human – machine interactions mimic traditional human social behaviors (Spence et al., 2018; Edwards et al., 2014), conflating the human and “the abhuman” (Farrell, 2018). It is this communication phenomenon where human – Twitterbot interactions mimic interpersonal relationships (Spence et al., 2018) that makes the Twitterbot cyberattack so powerful.

Twitter's application programming interface (API) (*physical*) enables bot networks (*informational*) to connect right into the Twitter mainstream where it can analyze information and engage other users, both human (*cognitive*) and bot in a code-to-code (*informational*) connection (Dubbin, 2013). In order to create a Twitterbot, which can be written in nearly any modern programming language (*cognitive*) (Dubbin, 2013), a botmaker will use some kind of programming interface, such as a Tracery editor – programming software which visualizes the way symbols and grammar interact and the kinds of outputs a bot will generate (*informational*) (Graham, 2017). The botmaker imagines the voice of the bot to be created (*cognitive*) in order to reach the chosen audience. Using a device (*physical*), the programmer will click (*physical – cognitive*) within the various editor windows on the screen (*physical*) in order to construct the computer code (*informational*) which will control the fake account (*informational*) (Graham, 2017). Once the bot has been created, a bot hosting site such as “Cheap Bots Done Quick” will allow the bot (*informational*) to live on cloud servers (*physical*) (Dubbin, 2013).

Once the bot has been created, it can be used for a variety of purposes. Most notably, it was used by the Russian government to influence (*cognitive*) the 2016 U.S. Presidential election (*physical*) (Wooley & Shout, 2016; Timberg & Dwoskin, 2018; Guilbeault & Woolley, 2016; Baraniuk, 2018; Hirsch, 2017; Curran, 2017; Confessore et al., 2018; Metz, 2018), the French Presidential election (Kropotov & Yarochkin, 2017; Baraniuk, 2018; *The Economist*, 2017) and the Brexit referendum (*physical*) (Hirsch, 2017; Baraniuk, 2018;). In fact, approximately 500,000 messages (*informational*) were generated by only 1% of 300,000 observed accounts (*informational*) in the 48 hours

before the Brexit referendum” (*physical*) (Hirsch, 2017). The automated tweets (*informational*) were heavily in favor of leaving the European Union, and many commentators believe (*cognitive*) this narrative (*informational*) had a significant impact on the final vote (*cognitive – physical*) leading to the withdrawal of the United Kingdom from the European Union (*physical*) (Hirsch, 2017).

It was a fake news story about an alleged child sex-trafficking ring run by Hilary Clinton (*informational*) circulated through the Twitterverse by numerous Twitterbots (*informational*) that led a gunman to drive (*cognitive*) to Washington D.C.’s Comet Ping Pong pizzeria (*physical*) in order to destroy what he mistakenly believed to be the coordination center of these activities (*cognitive*) (Farrell, 2018). Russian backed (*cognitive*) bots (*informational*) were also used to tweet antagonistic messages (*informational*) designed to assassinate the character of student activists and promote acrimony (*cognitive*) following the Parkland High School active shooter incident (*physical*) and fuel the gun control debate (*cognitive*) in the United States (Baraniuk, 2018).

Computer mediated (*physical*) communication encourages people to interact and communicate (*cognitive*) at a distance, enabling the injection of algorithms (*informational*) that appear human – “fake people generated by fake realities” (Farrell, 2018, p. 25), causing a breakdown in the shared understanding of reality versus make-believe (*cognitive*) (Farrell, 2018). As Artificial Intelligence continues to improve (*informational*), Twitterbots and other programs (*informational*) designed to mimic human behavior (*cognitive*) will continue to expand this threat (Metz, 2018). “Perhaps the

only way to stop misinformation is to somehow teach people to view what they see online with extreme distrust. But that may be the hardest fix of them all” (Metz, 2018).

Analysis of the 1999 Melissa Virus

While home on military leave, recovering from surgery in March 1999, this researcher heard a story on the evening news describing a computer virus that was circulating via email and causing significant disruption. She returned to Ramstein Air Base Germany the last week of March, and before she could turn on her computer, she was accosted by her fellow officers telling her not to open any emails or email attachments. As luck would have it, the news story she had heard just days earlier was all too real. The researcher’s unit, the United States Air Force in Europe (USAFE) Air Operations Squadron (AOS), which was hosting the Joint Task Force running military operations in Kosovo, was suffering a severe, week-long disruption to the deployment planning requiring the global coordination of Air Force, Army, Navy, and Marine Corps forces. The cause of this disruption was the Melissa Virus, a self-replicating macro written using Visual Basic for Applications (VBA) code (Redmond, 1999, WeLiveSecurity Editor, 2016; US CERT, 1999), which grew at an exponential rate, embedding itself in Word documents, and emailing itself around the world (NYT, 2 May 2002; Smothers, 1999).

The Melissa virus was designed by a man named David Lee Smith from New Jersey, and named for an exotic dancer in Florida who he admired (Taylor et al., 1999; NYT, 2 May 2002; NYT, 9 Apr 1999; Cheng, 1999; WeLiveSecurity Editor, 2016; Strickland, 2008; Panda, 2013; Cluley, 2009; Leyden, 2002; Techspirited Staff, 2019). At the time, financially motivated malware was rare (Cluley, 2009), and according to

Smith's court testimony, his intent was just mischief, and he had never intended or expected to cause such significant denial-of-service or damage (NYT, 7 Apr 1999; WeLiveSecurity Editor, 2016; Smothers, 1999; Techspirited Staff, 2019; WSJ Staff Reporter, 1999) – damages estimated at \$80 million - \$1.2 billion (Techspirited, 2019; NYT, 2 May 2002; Smothers, 1999; NYT, 4 May 2002; Pearce, 2002; WeLiveSecurity Editor, 2016; Panda, 2013; McNamara, 2014; Mills, 2009; Leyden, 2002). When it was released, it was the fastest-spreading virus of its time (NYT, 9 Apr 1999; McNamara, 2014; Techspirited Staff, 2019; Taylor et al., 1999; Cluley, 2009; Peterson, 1999), affecting over a million computer systems around worldwide (Smothers, 1999; NYT, 2 May 2002; NYT, 4 May 2002).

Smith had created (cognitive) the virus based on a Microsoft Word 97 macro (informational) (Peterson, 1999; Redmond, 1999; US CERT, 1999; WeLiveSecurity Editor, 2016; Strickland, 2008; Panda, 2013; Techopedia, 2019; McNamara, 2014; Cluley, 2009; Mills, 2009; Techspirited Staff, 2019; Gostev, 2005). He set it loose (cognitive) on the world wide web (physical) by embedding it in a Word document called “Passcodes 3-26-99” to Alt.sex (physical), an erotica focused Usenet newsgroup (informational) (Taylor et al., 1999; Cluley, 2009; Mills, 2009; Leyden, 2002; Gostev, 2005). This was the first time a virus was circulated by sending a Word document within an email (Panda, 2013). The document (informational) in which the Melissa virus was embedded (cognitive), appeared to be (cognitive) a list of passwords (informational) for pornography websites (physical) (Taylor et al., 1999; Cluley, 2009; Mills, 2009; Leyden, 2002; Gostev, 2005). It was posted by (cognitive) the email address skyroket@aol.com (informational), which belonged to a man named Scott Steinmetz of Lynnwood, WA

(cognitive) (Taylor et al., 1999; Cluley, 2009). Curiosity being what it is, it was not long until Melissa began her around the world tour.

The VBA code (informational) Smith developed (cognitive) was contained in a Microsoft Word document (informational) (Redmond, 1999, WeLiveSecurity Editor, 2016; US CERT, 1999). It was designed (cognitive) to query the Messaging API address lists (informational) in Microsoft Outlook stored on the Exchange server (physical) and the client (physical) (Redmond, 1999) and extract the first 50 email addresses from list (Redmond, 1999; Peterson, 1999; NYT, 9 Apr 1999; US CERT, 1999; WeLiveSecurity Editor, 2016; Strickland, 2008; Panda, 2013; Techopedia, 2019; McNamara, 2014; Cluley, 2009; Mills, 2009; Leyden, 2002; Techspirited Staff, 2019). Once Melissa had acquired the email addresses, it created the following message (informational):

Subject line: Important Message From [insert name from address book]
Message text: Here is that document you asked for...don't show anyone else ;-)
(Redmond, 1999; Strickland, 2008; McNamara, 2014; Techspirited Staff, 2019; US CERT, 1999; WeLiveSecurity Editor, 2016; Panda, 2013)

CERT Advisory CA-1999-04 (informational) stated that their analysis (cognitive) had indicated “that human action (in the form of a user opening an infected Word document) [was] required (cognitive) for this virus to propagate (informational)” (p. 24). The CERT Advisory also identified the possibility that “in some mailer configurations, a user might automatically open (cognitive) an infected document received in the form of an email attachment (informational)” (p. 24), as well as the fact that any file transfer system could also transmit the virus (informational).

Because many organizations had groups (cognitive) of email addresses at the top of the Outlook Global Address List (informational) (Redmond, 1999), Melissa grew at an alarming rate, swamping email networks (physical) and even causing Exchange servers

(physical) to shut down altogether (WeLiveSecurity Editor, 2016; McNamara, 2014; Mills, 2009; Redmond, 1999; US CERT 1999; Cluley, 2009; Leyden, 2002; Techspirited staff, 2019; Gostev, 2005; NYT, 2 May 2002). Melissa (informational) was everywhere, shutting down more than 300 computer networks (physical) (Taylor et al., 1999), including Microsoft and Intel (cognitive) (Leyden, 2002 Techspirited staff, 2019; Gostev, 2005; Panda, 2013).

Infection by the virus also put sensitive or proprietary information at risk because Melissa would infect the Normal.dot template in both Word97 and Word2000 (informational), and thus infect every document (informational) created by the victim (cognitive), which would then send itself to 50 email addresses (informational) (Redmond, 1999; Peterson, 1999; NYT, 9 Apr 1999; US CERT, 1999; WeLiveSecurity Editor, 2016; Strickland, 2008; Panda, 2013; Techopedia, 2019; McNamara, 2014; Cluley, 2009; Mills, 2009; Leyden, 2002; Techspirited Staff, 2019). Once Melissa had infected the Normal.dot template (informational), if an infected document was opened (cognitive) when the minute of the hour matched the day of the month (informational), the macro would insert a quote from an episode of *The Simpsons* (cognitive): “Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game’s over. I’m outta here.” into the document (informational) (CERT, 1999; Cluley, 2009; Techspirited Staff, 2019). US CERT advised organizations (cognitive) to have their users disable macros (cognitive) in Word97 and Word2000 (informational) in order to limit propagation (CERT, 1999).

A global manhunt ensued with everyone from malware hobbyists to the FBI searching for clues to Melissa’s creator’s whereabouts (cognitive) (Taylor et al., 1999;

Cluley, 2009). Phar Lap Software President, Richard M. Smith (unrelated to the perpetrator), examined other (cognitive) viruses (informational) posted (cognitive) from the same email address (Taylor et al., 1999), while a computer science student in Stockholm suggested (cognitive) that Melissa's code (informational) resembled other work from a hacker calling himself VicodinES (cognitive), one of several cyberpersonas (Taylor et al., 1999; Smothers, 1999). According to Peter Titppet, a computer security specialist who aided the investigation, VicodinES had bragged in the hacker underground about "creating a ruckus," (Smothers, 1999). AOL informed investigators (cognitive) that Steinmetz's email address (informational) had been hijacked (cognitive), and that the real perpetrator had dialed up (cognitive) from a telephone located in New Jersey (physical) (Taylor et al., 1999, Mills, 2009). Within a week of the Melissa virus's (informational) launch, the FBI arrested David Smith on April Fool's Day (cognitive) (Taylor et al., 1999; McNamara, 2014; Gostev, 2005; NYT, 9 Apr 1999; McNamara, 2014; Cluley, 2009).

Smith was charged with several counts related to theft of computer services, interruption of public communication, and conspiracy (WSJ Staff Reporter, 1999; NYT, 9 Apr 1999). During the arraignment, Smith's attorney Edward Borden equated his client's behavior to graffiti art (NYT, 9 Apr 1999; NYT, 7 Apr 1999), stating that "David has really been demonized throughout this. Making him out to be an international, criminal mastermind is a bit of an overstatement," (WSJ, 1999, pB10), even suggesting that Smith deserved credit for causing organizations to recognize the need to install virus protection systems (NYT, 2 May 2002). At his trial in 2002, Smith was sentenced to 10 years in prison, fined \$5000, (NYT, 2 May 2002; NYT, 4 May 2002; Pearce, 2002;

Strickland, 2008; Mills, 2009; Panda, 2013; WeLiveSecurity Editor, 2016) and directed to serve 100 hours community service (NYT, 2 May 2002). “The New Jersey attorney general for the case, John J. Farmer, Jr. called the case the ‘single most significant Internet prosecution in the nation to date,’” (Smothers, 1999). David Lee Smith spent just 20 months in prison because he cooperated with the FBI on subsequent cyber investigations (Panda, 2013; Cluley, 2009). He was also barred from the use of computer networks without court approval (Techspirited Staff, 2019; Strickland, 2008; NYT, 2 May 2002).

The Melissa virus was a wakeup call to organizations and individual users who were not using antivirus software, and a reminder to those who were using virus checkers, to keep their pattern files current (Redmond, 1999). Although it was created without monetary gains in mind, Melissa is recognized as a turning point, when malware changed from attention seeking exhibitionism to unrestrained, monetized criminality (Taylor et al., 1999).

Analysis of the 2005-2012 Hack of American Business

Estimates suggest cybercrime in 2018 generated as much as \$1.5 trillion (Nohe, 2018). Although hackers and cybercriminals are often perceived as hooded and disembodied figures operating in a virtual space, in reality, they are real people sitting in a physical location (French, 2017). Because of the challenges of attribution in the cyber realm, this aspect of cybercrime is often forgotten, but there are entire economies, such as “Hackerville” Romania, in Eastern Europe for which cybercrime is a regular occupation (Lusthaus & Varese, 2017). Romania is just one cybercrime hub, according to a 2018 Cybercrime Report by Threat Metrix Inc., 48% of cyberattacks originate from Central

and Eastern Europe. In fact, in some Eastern European countries, sophisticated hackers are national assets supporting an enormous shadow economy (Jones et al., 2013).

As of 2015, the largest international cybercrime case every prosecuted in the United States was the hack of American Business that took place of a period of seven years against a huge list of victims including: Citigroup, Nasdaq OMX Group, PNC Financial Services Group and a Visa licensee, Visa Jordan, Carrefour, 7-Eleven Inc., J.C. Penney, Hannaford Brothers Co. supermarkets, and JetBlue Airways (Bray, 2013; Bray & Yadron, 2013; Fox, 2013; Reuters, 2013; Jones & Finkle, 2013; Wood, 2018; Schwartz, 2015; DoJ, 2015; Hudson, 2013). The losses from just three of these organizations totaled over \$300 million (DoJ, 2015; DoJ, 2018; Armental, 2015; Beekman, 2013; Bray, 2013; Bray & Yadron, 2013; Reuters, 2013; Sullivan, 2013; Jones & Finkle, 2013; Schwartz, 2015). Four Russian nationals and one Ukrainian man were indicted in 2013 on charges of carrying out a computer-hacking conspiracy and conspiracy to commit wire fraud (Beekman, 2013; DoJ, 2018; Armental, 2015; Bray, 2013; Bray & Yadron, 2013; Fox, 2013; Reuters, 2013; Jones & Finkle, 2013; Wood, 2018; Schwartz, 2015; DoJ, 2015). A fifth man, Albert Gonzalez, who is currently serving a 20-year sentence for previous cybercrimes, was involved in several of the data breaches while concurrently assisting U.S. investigators with the hunt for an infamous cybercrime gang called “Shadowcrew” (Sullivan, 2013; Schwartz, 2015).

Each member of the gang had specific talents which were highly coordinated to maximize their success (Schwartz, 2015; Hudson, 2013; Fox, 2013; Jones & Finkle, 2013; Wood, 2018; DoJ, 2015; Armental, 2015; DoJ, 2018). Vladimir Drinkman and Alexandr Kalinin were gifted hackers known for their ability to penetrate (cognitive)

network security (informational) and gain access to (cognitive) corporate systems (physical) (Schwartz, 2015; Hudson, 2013; Fox, 2013; Jones & Finkle, 2013; Wood, 2018; DoJ, 2015; Armental, 2015; DoJ, 2018). Roman Kotov was the data (informational) miner who would explore (cognitive) the networks (physical) and find (cognitive) valuable knowledge and data assets (informational) (Schwartz, 2015; Hudson, 2013; Fox, 2013; Jones & Finkle, 2013; Wood, 2018; DoJ, 2015; Armental, 2015; DoJ, 2018). Mikhail Rytikov provided the team with anonymous (cognitive) webhosting services from which (physical) they could execute their attacks (cognitive) and on which (physical) they could store (cognitive) their stolen assets (informational) (Schwartz, 2015; Hudson, 2013; Fox, 2013; Jones & Finkle, 2013; Wood, 2018; DoJ, 2015; Armental, 2015; DoJ, 2018). Dmitriy Smilianets was responsible for sales, working with (cognitive) data (informational) wholesalers to sell (cognitive) the stolen information in large, profitable chunks (informational) (Schwartz, 2015; Hudson, 2013; Fox, 2013; Jones & Finkle, 2013; Wood, 2018; DoJ, 2015; Armental, 2015; DoJ, 2018). He would then distribute (cognitive) the proceeds (physical) to the various members of the team (cognitive) (Schwartz, 2015; Hudson, 2013; Fox, 2013; Jones & Finkle, 2013; Wood, 2018; DoJ, 2015; Armental, 2015; DoJ, 2018).

The team would begin with reconnaissance visits (cognitive) to retail locations (physical) to determine what kind of (cognitive) payment processing systems (physical) were being used and assess their vulnerability (cognitive) (Bray, 2013; Bray & Yadron, 2013; Sullivan, 2013). Once they had determined (cognitive) which payment system (physical) was being used, they would penetrate (cognitive) the credit card systems (physical), often by using (cognitive) an SQL-injection attack (informational) (Sullivan,

2013; Wood, 2018; Schwartz, 2015; DoJ, 2015; DoJ, 2018). “SQL, or Structured Query Language, is a type of programming language designed to manage data held in particular types of databases” (DoJ, 2015, p. 2). SQL injection methods work by entering (cognitive) bad information into a database (informational) using (cognitive) an online (physical) form (informational) and tricking (cognitive) the server (physical) into giving the attacker privileged user access (cognitive) (Sullivan, 2013). Once inside (cognitive) the network (physical), Drinkman and (allegedly Kalinin) would inject (cognitive) malware (informational) into the system (physical) to create (cognitive) a backdoor (informational) in order to maintain access (cognitive) to the network (physical) (DoJ, 2015;). The hackers would change (cognitive) the settings (informational) on the networks (physical) to disable (cognitive) mechanisms that would have logged their actions (informational), thus evading discovery (cognitive) by the security software (informational)

Then Kotov would allegedly go to work mining (cognitive) the databases for valuable information (informational) (DoJ, 2015; Schwartz, 2015; Hudson, 2013; Fox, 2013; Jones & Finkle, 2013; Wood, 2018; Armenthal, 2015; DoJ, 2018), using (cognitive) software programs called “sniffers” (informational) which were designed to identify, collect, and steal (cognitive) data (informational) from victims’ networks (physical) (DoJ, 2015; DoJ, 2018). According to Kalinin, they were overwhelmed by (cognitive) the amount of data (informational) to which they were able to gain access (cognitive) (Sullivan, 2013). The stolen data (informational) would be stored (cognitive) on an array of servers located around the globe (physical) (DoJ, 2015; DoJ, 2018; Hudson, 2013).

Using these methods, the cybercrime gang stole (cognitive) over 160 million credit card numbers (informational), which Smilianets would sell in tranches to individuals and wholesalers (cognitive) (Wood, 2018; DoJ, 2015; DoJ, 2018; Armental, 2015; Fox, 2013; Reuters, 2013; Jones & Finkle, 2013). He priced (cognitive) American credit card numbers and associated information (informational) at \$10 each, Canadian credit card numbers and associated information (informational) at \$15 each, and European credit card numbers and associated information (informational) at \$50 each (Hudson, 2013; Fox, 2013; Reuters, 2013; Sullivan, 2013; Jones & Finkle, 2013; Wood, 2018; DoJ, 2015; DoJ, 2018; Beekman, 2013). European credit information (informational) was the most valuable due to the fact that they included (cognitive) security chips on the cards (physical) (Reuters, 2013; Jones & Finkle, 2013). At the end of the value chain, the customers would encode (cognitive) the stolen data (informational) onto the magnetic strip of a blank card (physical), which they would then use to drain (cognitive) bank accounts (informational) via an ATM machine (physical) or to make fraudulent purchases (cognitive) (Hudson, 2013; Reuters, 2013; Jones & Finkle, 2013; Wood, 2018; DoJ, 2015; DoJ, 2018; Beekman, 2013).

According to an online chat record (informational), Gonzalez explained that he had set up (cognitive) Google alerts using search terms like “data breach,” “credit card fraud,” “debit card fraud,” and “atm fraud” (informational) in order to be notified when (cognitive) news stories (informational) broke about hacks he was perpetrating, and he recommended that Kalinin do the same (cognitive) (Hudson, 2013; Bray, 2013; Bray & Yadron, 2013; Sullivan, 2013; Beekman, 2013). In addition to monitoring the news for indications that their actions had been discovered, they also used encrypted

communication channels to avoid exposure (cognitive) (DoJ, 2015; DoJ, 2018; Armental, 2015).

Drinkman and Smilianets were arrested in 2012 while traveling in the Netherlands (DoJ, 2018; DoJ, 2015; Armental, 2015). Smilianets was extradited to the U.S. in September 2012, and Drinkman in 2015 (DoJ, 2015; DoJ, 2018; Schwartz, 2015; Armental, 2015). They were both convicted in February 2018. Kalinin, Kotov and Rytikov continue to elude capture (DoJ, 2018; Wood, 2018).

Analysis of the 2017 (Not)Petya Ransomware

Ransomware first appeared in 1989 at the World Health Organization's AIDS conference, when biologist Joseph Popp distributed floppy disks infected with a trojan horse virus he had developed (Scott & Spaniel, 2016). This first ransomware attack was relatively ineffective due to a very small target population, and no effective means through which to receive payment (Scott & Spaniel, 2016). The growth and expansion of the internet led to the emergence of the early forerunners of modern ransomware in 2005, where it took the form of fraudulent applications that charged a fee for cleanup tools that did nothing (Scott & Spaniel, 2016). As users gained knowledge, and anti-virus software became widely used, hackers began to develop fake anti-virus programs that would identify numerous threats to a user's computer and request payment in order to clean up the "infected files," but the malware developer had no leverage to force payment (Scott & Spaniel, 2016). The first locker malware demanding ransom payments emerged in 2008 (Scott & Spaniel, 2016), and since then, ransomware attacks have expanded at an alarming rate, growing 350% in 2017 (Cook, 2018).

The most notorious and virulent ransomware attack to strike global business was the “Petya” ransomware attack which was unleashed in June 2017 (Asia News Monitor, 2017; Collins, 2017; Daneshkhu, 2017; Chopping, 2017;), but as the Petya attack spread, experts quickly discovered that all was not as it seemed, and that this was no ordinary, criminal ransomware attack (Nott, 2017; Collins, 2017; Frenkel et al., 2017; Fruhlinger, 2017; Daneshkhu et al., 2017; Palmer, 2017). In fact, as the attack spread with no way to pay the ransom (Fruhlinger, 2017), and no way to decrypt the encrypted Master Boot Record (Fruhlinger, 2017; Tung, 2017; Hackett, 2017; Nott, 2017; DHS, 2018; Daneshkhu et al., 2017; Greenberg, 2018) even when victims did pay the ransom (Greenberg, 2018; Fruhlinger, 2017), it became evident that the motivation behind what came to be known as the “NotPetya” ransomware attack was not financial at all (Nott, 2017; Collins, 2017; Frenkel et al., 2017; Fruhlinger, 2017; Daneshkhu et al., 2017; Palmer, 2017). Welcome to the wilderness of mirrors, “where nothing is real, and all is just a reflection of some distant motive, nation, and/or ideology” (Byrne, 2014). Within six months after the NotPetya ransomware attack, the United States intelligence community and the British intelligence community had attributed this cyberattack to the Russian military (DHS, 2018; Cimpanu, 2018; Greenberg, 2018; Woo, 2018).

The cybersecurity community concluded that the NotPetya attack built on the WannaCry ransomware attack, which originated in North Korea (Newman, 2018; Palmer, 2017) and took place several weeks earlier, in May 2017 (Palmer, 2017; Reilly, 2017; Ryan, 2017; Schilling, 2017; Tung, 2017; Collins, 2017; Daneshkhu et al., 2017; Chopping, 2017; Frenkel et al., 2017; Goldsborough, 2017; Hackett, 2017; Nelson, 2017; Osborne, 2018). WannaCry combined ransomware with an alleged NSA exploit called

EternalBlue (Palmer-1, 2017; Palmer-2, 2017; Tung, 2017; DHS, 2018; Fruhlinger, 2017; Greenberg, 2018; Hackett, 2017; Osborne, 2017), that was leaked to the public by the Shadow Brokers in April 2017 (Newman, 2018). The EternalBlue exploit used a vulnerability in the Microsoft Windows implementation of the SMB-1 file sharing protocol (Tung, 2017; DHS, 2018; Fruhlinger, 2017; Hackett, 2017; Greenberg, 2018) which enabled the malware to self-propagate throughout the network with a worm-like behavior (Palmer, 2018). WannaCry was quickly halted using a “killswitch” when a researcher discovered he could buy a domain name for \$10 (Frenkel et al., 2017; Tung, 2017; Hackett, 2017). Following the WannaCry attack, Microsoft released patch MS17-010 to address the EternalBlue vulnerability, even for unsupported Windows systems such as Windows XP (Fruhlinger, 2017; Hackett, 2017), nevertheless many organizations failed to implement the patch (Fruhlinger, 2017; Hackett, 2017).

NotPetya mimicked WannaCry’s use of the EternalBlue exploit (Palmer-1, 2017; Palmer-2, 2017; Tung, 2017; DHS, 2018; Fruhlinger, 2017; Greenberg, 2018; Hackett, 2017; Osborne, 2017), but it removed the “killswitch” that had enabled WannaCry to be stopped so quickly (Frenkel et al., 2017; Tung, 2017; Hackett, 2017). Petya ransomware originally circulated via email, allowing it to be disrupted by wary users who did not consent when a request to download software message was displayed (Fruhlinger, 2017). NotPetya evolved the malware to eliminate the need for users to permit the download, by incorporating “a tool called Mimi Katz to find network administration credentials in the infected machine’s memory, and then use the PsExec and WMIC tools built into Windows to remotely access other computers on the local network” (Fruhlinger, 2017), enabling it to penetrate even those machines which had received the Microsoft patch

(Fruhlinger, 2017; Greenberg, 2018). NotPetya also expanded the Petya encryption capabilities beyond the encryption of the Master Boot Record and damaging the hard drive beyond repair (Fruhlinger, 2017). Finally, the fact that NotPetya was not ransomware, but simply masquerading as ransomware, was demonstrated by the fact that the Petya virus gave victims valid information through which they could pay the ransom, while NotPetya provided a random number that appeared to be account information but led nowhere (Fruhlinger, 2017).

WannaCry infected approximately 300,000 machines in more than 70 countries (Rayome, 2017; Palmer-2, 2017; Collins, 2017), causing approximately \$4 billion to \$8 billion (Greenberg, 2018). NotPetya also infected hundreds of thousands of machines in just 64 countries (Rayome, 2017; Landler & Shane, 2018), but the estimated damages exceeded \$10 billion (Greenberg, 2018). The NotPetya attack impacted some of the largest global businesses in the world, including the pharmaceutical company Merck (Collins, 2017; Chopping, 2017; Greenberg, 2018; Hackett, 2017; Matthews, 2017; Ryan, 2017; Tung, 2017; Woo, 2018; Chirgwin, 2018; Cimpanu, 2018) costing \$870,000,000 (Greenberg, 2018), delivery company FedEx via TNT Express, a European subsidiary (Daneshkhu et al., 2017; Matthews, 2017; Osborne, 2018; Palmer-1, 2017; Tung, 2018; Woo, 2018; Chirgwin, 2018; Cimpanu, 2018) with a cost of approximately \$400,000,000 (Greenberg, 2018), snack company Mondelez, the maker of Cadbury chocolates, (Frenkel et al., 2017; Tung, 2017; Reilly, 2017; Greenberg, 2018) with a \$188,000,000 loss (Greenberg, 2018), and British manufacturer Reckitt-Benckiser (Palmer-1, 2017; Greenberg, 2018; Ryan, 2017) at a cost of \$129,000,000 (Greenberg, 2018). The legal

firm DLA Piper also reported being impacted by the NotPetya attack (Tung, 2017; Daneshkhu et al., 2017; Frenkel et al., 2017).

Danish shipping company A.P. Moller-Maersk, which controls approximately one-fifth of the world's shipping capacity, conducts business in 130 countries around the globe, operates nearly 800 ships, and is responsible for 76 ports around the world, was brought to its knees by the NotPetya cyberattack in mere hours (Greenberg, 2018). Maersk publicly estimates their damages at \$300,000,000 (Greenberg, 2018; Matthews, 2017), but the impact could have been far more extensive were it not for a happenstance power outage in Ghana (Greenberg, 2018; Doctorow, 2018). Maersk chairman, Jim Hagemann Snabe, speaking at the World Economic Forum in January 2018, was very open about the corporate crisis caused by the NotPetya cyberattack, sounding the alarm and sharing Maersk's new philosophy that cybersecurity is about competitive advantage (Greenberg, 2018; Tung, 2018; Chirgwin, 2018; Cimpanu, 2018; Olenick, 2018; Osborne, 2018).

Patient Zero for the NotPetya attack was discovered to be the M.E. Docs update server (physical) in Ukraine (Greenberg, 2018; Frenkel et al., 2017; Fruhlinger, 2017; Cimpanu, 2018; Olenick, 2018). M.E. Docs is a tax and accounting software (informational) used by almost all Ukrainian businesses (Greenberg, 2018; Frenkel et al., 2017; Fruhlinger, 2017; Cimpanu, 2018; Olenick, 2018). The NotPetya virus (informational) was injected (cognitive) into the M.E. Docs update server (physical) via a back door (informational), and pushed out with an M.E. Docs software update (informational) (Greenberg, 2018; Frenkel et al., 2017; Fruhlinger, 2017; Cimpanu, 2018; Olenick, 2018). A Maersk finance executive in Odessa, Ukraine had asked the IT staff to

install (cognitive) M.E. Docs (informational) on a single machine (physical). It was this single instantiation of the M.E. Docs software (informational) that led to the destruction of the entire Maersk network (physical) (Greenberg, 2018; Tung, 2018; Chirgwin, 2018; Cimpanu, 2018; Olenick, 2018; Osborne, 2018). As the malware spread (informational), machines were spontaneously rebooting (physical) and the screens turned black (Greenberg, 2018). Other machines (physical) were displaying messages (informational) that read “repairing file system on C:” or demanding a \$300 ransom payment (Greenberg, 2018). Many of Maersk’s servers (physical) were still running Windows 2000 (informational), which was no longer supported by Microsoft (cognitive) because it was so old (Ryan, 2017), making their systems (physical) particularly vulnerable to the EternalBlue exploit (informational) that hackers had integrated into (cognitive) the NotPetya malware (informational) (Palmer-1, 2017; Palmer-2, 2017; Tung, 2017; DHS, 2018; Fruhlinger, 2017; Greenberg, 2018; Hackett, 2017; Osborne, 2017). Once the malware (informational) had a foothold in the network (physical), it would steal network credentials (informational) that would allow it (informational) to jump from machine to machine (physical) (Fruhlinger, 2017; Greenberg, 2018; Schilling, 2017), where it would encrypt and wipe files (informational) and destroy the hard drive (physical) (Matthews, 2017; Palmer-1, 2017; Nott, 2017; Schilling, 2017; Doctorow, 2018; Greenberg, 2018).

It took a little over two hours for Maersk to shut down their entire global infrastructure – computers, servers, routers, and desk phones (physical) to stop the spread of the malware (informational) (Greenberg, 2018). Then the real problems began. Gates at the port terminals would not work (physical) turning away tens of thousands of trucks (physical) and creating a miles long back up of 18-wheelers (physical) at the port in

Elizabeth, New Jersey (Greenberg, 2018). Maerskline.com (informational), the central booking website (physical), was down, and employees were not answering (cognitive) their phones (physical) (Greenberg, 2018; Asia News Monitor, 2017). Although the ships onboard computers (physical) were working, they could not exchange shipping content data (informational) with the ports, thwarting loading/unloading operations (cognitive) at the ports (Greenberg, 2018; Ryan, 2017; Asia News Monitor, 2017; Daneshkhu et al., 2017).

Maersk confiscated (cognitive) all computer equipment (physical) and sent its employees to local electronics stores to buy up (cognitive) computers (physical) and WIFI hotspots (physical) to ensure that the virus (informational) could not continue to spread (Greenberg, 2018). The staff located (cognitive) backups (informational/physical) for everything except its domain controllers (physical), “the servers (physical) that function as a detailed map (informational) of Maersk’s network (physical) and set the basic rules that determine which users are allowed access to which systems” (Greenberg, 2018). Because the 150 domain controllers (physical) were designed to synchronize with one another (cognitive), theoretically, any server could be a backup to any other server (informational/physical), but there was no plan for the simultaneous destruction of every domain controller (Greenberg, 2018).

Maersk’s administrators finally located one surviving domain controller in Ghana (physical), where a power outage had shut down the machine (physical) before the cyberattack hit (informational) (Greenberg, 2018; Doctorow, 2018). The several hundred gigabytes of domain controller data (informational) proved too cumbersome to transmit, so Maersk employees hand-carried (cognitive) the priceless hard drive (physical) from

Ghana to Nigeria to London (Greenberg, 2018; Doctorow, 2018). Because of a chance power outage, it took Maersk only 10 days to restore (cognitive) 4,000 servers (physical) and 45,000 computers (physical), and about 2 months to completely restore (cognitive) 2,500 applications (informational) (Tung, 2018; Chirgwin, 2018; Cimpanu, 2018; Olenick, 2018; Osborne, 2018), a process that should have taken 6 months (Olenick, 2018).

After determining the location (cognitive) of the initial NotPetya infection (informational), Ukrainian Police seized (cognitive) the servers (physical) from M.E. Docs during the first week of July 2017 (Sayer, 2017).

Prior to the NotPetya attack, the IT administrators could not get the management to make the necessary investments in cybersecurity, but since the June 2017 cyberattack, Maersk's philosophy has changed, and they now perceive cybersecurity as a competitive advantage (Greenberg, 2018; Tung, 2018; Chirgwin, 2018; Cimpanu, 2018; Olenick, 2018; Osborne, 2018). Although NotPetya has been determined to be a Russian attack on Ukraine (Tung, 2018; Greenberg, 2018; DHS, 2018; Woo, 2018), the attack highlights the absolute irrelevance of nation state boundaries in the virtual world of cyberspace (Greenberg, 2018; Arquilla & Rondfeldt, 1999; Brown, 2015; Baudry & Chassagnon, 2012; Kim, 2010; Haggard & Lindsay, 2015; Cavusoglu et al., 2008; Karatzogianni & Gak, 2015).

Analysis of the 2010 Manning Disclosure to WikiLeaks

When Private Manning leaked a huge trove of classified information during the summer of 2010, both the United States Department of Defense and the United States Department of State were affected by the disclosure of the information through

WikiLeaks (Sangarasivam, 2013; Nita, 2014; Berghel, 2012; Jones, 2013; Garnett & Hughes, 2019; Somashekhar, 2017; Cadwalladr, 2018; Zavis, 2017; Booth et al., 2010; McGreal, 2010; Tate, 2013; Zetter & Poulsen, 2010). Private Manning's motivation, and the competing narratives (AP, 2013; Berghel, 2012) that both demonize (Somashekhar, 2017; Zavis, 2017; Tate, 2013) and celebrate Manning's actions (Chan, 2017; Jones, 2013; Cadwalladr, 2018; Sangarasivam, 2013; Nita, 2014; Jones, 2013; Garnett & Hughes, 2019; Booth et al., 2010) demonstrate the polarizing nature of the event. From the perspective of the Cyber-Based View, this strongly reinforces the cognitive elements of the model, highlighting the fact that the cognitive element of motivation is present and central to the event.

An article by Sangarasivam (2013), of Nazareth College, highlights the inflammatory nature of the event, when the author celebrates Manning's "quintessential example of cyber rebellion" (p. 69), applauding Manning's disclosure for "radically revising global historic archives that document the hegemonic construction of 'terrorism,' which empowers a dystopic democracy," (p. 70). He goes on to say that "The United States government continues to detain, torture, and proceeds to prosecute Pvt. Manning," (Sangarasivam, 2013, p. 70).

A less provocative version of the celebratory narrative is that of those who see informational leaks as a natural consequence of free speech and a free press (Berghel, 2012; Tate, 2013; Sangarasivam, 2013; Chan, 2017). "Republican presidential contender Ron Paul suggested that Private Manning might be a 'political hero...a true patriot who reveals what is going on in government,' (Berghel, 2012, p. 71). The celebration of Manning's actions is further clouded by her self-identification as transgender and her

request to be called Chelsea Elizabeth (AP, 2017;). Once this element of the story came to public attention, the LGBTQ community began to laud Manning for her bravery as a transgender-female, and that acclaim was conflated with her actions related to the information disclosure (Chan, 2017; Garnett & Hughes, 2019; Somashekhar, 2017; Zavis, 2017; Nita, 2014). To Manning’s credit, she specifically stated that “I don’t want to make that connection. I didn’t leak because I’m trans. That’s not it.” (Cadwalladr, 2018).

One lesser discussed narrative that was offered by Zbigniew Brzezinski, the former National Security Advisor to President Jimmy Carter, suggested that Manning and WikiLeaks’ Assange were merely pawns in the spy game. He proposed that the “leaked documents might be background noise that overshadows the more important and damaging ‘seeded’ documents,” (Berghel, 2012, p. 71).

Last but not least is the narrative that resonates with the majority of mainstream media – the narrative that Private Manning committed treason (Tate, 2013; Franceschi-Bicchieri, 2018; AP, 2013; Berghel, 2012). But the divided opinion with respect to the morality of Manning’s actions (Jones, 2013) is immaterial. Whether Private Manning is vilified as a traitor (Tate, 2013; Franceschi-Bicchieri, 2018; AP, 2013; Berghel, 2012), pitied as a clueless dupe (Berghel, 2012), or celebrated as whistleblower (Chan, 2017; Jones, 2013; Cadwalladr, 2018; Sangarasivam, 2013; Nita, 2014; Jones, 2013; Garnett & Hughes, 2019; Booth et al., 2010) and leader of the transgender community (Chan, 2017; Garnett & Hughes, 2019; Somashekhar, 2017; Zavis, 2017; Nita, 2014), is ultimately irrelevant with respect to the Cyber-Based View. What matters is that Private Manning’s cognitive, decision making behaviors are a central element of the Cyber-Based View.

While United States Army Private Bradley Manning was serving as an intelligence analyst in Baghdad, Iraq, his position gave him access to (cognitive) a vast amount of sensitive information, including (but not limited to): classified videos, U.S. Department of State diplomatic cables, operational field reports, detainee reports, incident reports, and threat assessments (informational) (Zetter & Poulsen, 2010; Sangarasivam, 2013; Jones, 2013; Somashekhar, 2017; Cadwalladr, 2018; McGreal, 2010; Tate, 2013). In January 2010, while serving in this position, Private Manning downloaded 251,287 dispatched cables (informational) from more than 250 United States embassies and consulates (cognitive), 391,832 documents (informational) related to military operations in Iraq (cognitive), dubbed the *Iraq War Logs* (Garnett & Hughes, 2019; Nicks et al., 2011; Somashekhar, 2017; Cadwalladr, 2018; Zavis, 2017; Booth et al., 2010; McGreal, 2010; Tate, 2013; Zetter & Poulsen, 2010), and another 77,000 documents (informational) related to operations in Afghanistan, titled the *Afghan War Diary* (cognitive) (Garnett & Hughes, 2019; Berghel, 2012). He also included a video (informational) taken from an Apache helicopter (physical) showing US personnel firing upon civilians (cognitive) (Sangarasivam, 2013; Garnett & Hughes, 2019; Nita, 2014; Zavis, 2017; Booth et al., 2010; Tate, 2013; Zetter & Poulsen, 2010).

Manning downloaded (cognitive) this information (informational) from CIDNE-I (physical) and CIDNE-A (physical) (Garnett & Hughes, 2019), specific data stores (informational) to which he had access (cognitive) via the Secret Internet Protocol Router Network (SIPRNet) (physical) (Berghel, 2012; Jones, 2013; Zetter & Poulsen, 2010; Nicks et al., 2011) and saved (cognitive) the data (informational) to a CD-RW (physical) titled *Lady Gaga* (cognitive), (Sangarasivam, 2013; Garnett & Hughes, 2019; AP, 2017;

Zetter & Poulsen). He then released (cognitive) it (informational) through WikiLeaks (physical) (Sangarasivam, 2013; Nita, 2014; Berghel, 2012; Jones, 2013; Garnett & Hughes, 2019; Somashekhar, 2017; Cadwalladr, 2018; Zavis, 2017; Booth et al., 2010; McGreal, 2010; Tate, 2013; Zetter & Poulsen, 2010).

Smuggling (cognitive) the CD-RW (physical) out of the Security Compartmented Information Facility (physical), Manning brought (cognitive) it (physical) back to the United States (physical) while home on leave (cognitive), where he sought out a platform through which to disclose (cognitive) the data (informational) (Garnett & Hughes, 2019; Zetter & Poulsen, 2010; Nicks et al., 2011). He contacted both *The Washington Post* and *The New York Times* (cognitive), neither of which replied to his contacts (cognitive), (Garnett & Hughes, 2019; Cadwalladr, 2018; Zetter & Poulsen, 2010).

In chats with hacker Adrian Lamo, Manning bragged about how he had access (cognitive) to both Secret and Top Secret information (informational) through two different laptops, one connected to the SIPRNet and the other connected to the Joint Worldwide Intelligence Communications System (physical) (Zetter & Poulsen, 2010). He said that despite the networks being “air-gapped,” (physical) it was easy to smuggle (cognitive) data (informational) out because of lax security measures (Zetter & Poulsen, 2010).

Shortly after returning to Iraq in February, Manning conducted a dry run to determine how to move (cognitive) encrypted data (informational) to the public Internet (physical) by sending (cognitive) a diplomatic cable related to Iceland (informational) to WikiLeaks (physical) (Booth et al., 2010). WikiLeaks, with servers hosted in multiple

countries (physical), provides sources secure anonymity (cognitive) with an encrypted document submission process (informational) (Zetter & Poulsen, 2010).

In 2008, WikiLeaks (physical) was placed on (cognitive) a list of enemies of the state (informational) by the U.S. Army Counterintelligence Center (cognitive) (Nicks et al., 2011). Although WikiLeaks (physical) was founded in 2006 (Nita, 2014; Zetter & Poulsen, 2010), it was not until the Manning disclosure (cognitive) that Assange (cognitive) and WikiLeaks (physical) gained their current notoriety (cognitive), specifically with the 2010 publication of (cognitive) the Apache helicopter video (informational) released by Manning (cognitive) and posted on WikiLeaks (physical) under the title *Collateral Murder* (informational) (Nita, 2014; Booth et al., 2010; Berghel, 2012; Garnett & Hughes, 2019; Cadwalladr, 2018; McGreal, 2010; Zetter & Poulsen, 2010).

From March – May 2010, Manning began to download (cognitive) additional documents (informational), which he also sent (cognitive) to WikiLeaks (physical) (Garnett & Hughes, 2019; Booth et al., 2010; Zetter & Poulsen, 2010; Nicks et al., 2011). Manning reached out for support (cognitive) through an online forum (physical), where he met hacker Adrian Lamo (cognitive) (Cadwalladr, 2018). Testimony during Manning’s Article 32 hearing described a Manning user account (informational) created on (cognitive) an unclassified computer located in a supply closet (physical) (Nicks et al., 2011). Manning disclosed to Lamo that he had been hunting through (cognitive) classified government and military networks (physical) for over a year and had found (cognitive) information (informational) which he found disturbing, and which he believed belonged (cognitive) in the public domain (physical) (Zetter & Poulsen, 2010; Tate,

2013). A record of (informational) their online chats (cognitive) discloses an increasing sense of isolation (cognitive) and the belief that the safest place Manning could find (cognitive) was the Internet (physical) (Cadwalladr, 2018; Thompson, 2010; Zetter & Poulsen, 2010).

Lamo reported Manning to the military and the FBI (cognitive) because Manning had boasted (cognitive), “Hillary Clinton, and several thousand diplomats around the world, are going to have a heart attack when they wake up one morning, and find (cognitive) an entire repository of classified foreign policy is available, in a searchable format (informational), to the public (cognitive),” (McGreal, 2010). Manning was subsequently arrested and sent to (cognitive) prison in Kuwait (physical) (Sangarasivam, 2013; Booth et al., 2010; McGreal, 2010; Tate, 2013; Zetter & Poulsen, 2010; Peralta, 2013; Nicks et al., 2011). During a search of Manning’s home (his Aunt’s house), agents from Army Criminal Investigation Command found (cognitive) an SD card (physical) with a “read me” text file (informational) explaining Manning’s desire to remove the “fog of war” (Nicks et al., 2011). Following his arrest, Manning asked his Aunt to post (cognitive) the following message on his Facebook page (informational): “Some of you may have heard that I have been arrested for disclosure of classified information to unauthorized persons. See CollateralMurder.com” in order to increase traffic (cognitive) to the WikiLeaks site (physical) (Zetter & Poulsen, 2010).

In an attempt to control the leak (cognitive) of information (informational) Senator Joe Lieberman approached Amazon CEO Jeff Bezos to request (cognitive) that Amazon Web Services stop hosting (physical) WikiLeaks content (informational), which was located on servers in North America (physical) at the time of the leak (cognitive)

(Berghel, 2012). Although Amazon removed the WikiLeaks.org content (informational) from its servers (physical), WikiLeaks was hosted in multiple sites around the world (physical), and pulling content (informational) from the Amazon servers in North America (physical) did nothing to halt the propagation of the sensitive information (informational) throughout cyberspace (Berghel, 2012).

When an alleged DDoS attack (informational) directed against (cognitive) the WikiLeaks.org website (physical) threatened other subscribers (cognitive), EveryDNS removed (cognitive) the domain name server (DNS) entry (informational) related to WikiLeaks' IP address (informational) for North America (physical), but that too failed because DNS records (informational) began to multiply for other WikiLeaks hosting sites (physical) (Berghel, 2012).

Following the removal of (cognitive) the DNS records (informational), WikiLeaks announced (cognitive) via Twitter (informational) that they had created (cognitive) WikiLeaks.ch (informational), which, though it implied (cognitive) a location in Switzerland (physical), led to a Swedish server (physical) that “redirected traffic (informational) to a French host (physical), which assigned an IP address (informational) that was part of a 16-address server cluster located in France (physical) but registered in Melbourne, Australia.” (Berghel, 2012, p. 72).

Private Manning was convicted and sentenced to 35 years in prison, but President Obama commuted her sentence after she had served 7 years (Zavis, 2017; Somashekhar, 2017; Cadwalladr, 2018; Chan, 2017; AP, 2017). Manning has become a vocal activist for LGBTQ rights and transparency in government (Chan, 2017). Her recent activities

include running for a Maryland Senate seat in 2018 (Cadwalladr, 2018; Franceschi-Bicchieri, 2018).

The 2010 Manning release to WikiLeaks was the largest leak of sensitive information in history (Nita, 2014; Tate, 2013; Thompson, 2010; Zetter & Poulsen, 2010). It is also recognized as a significant historical event which ushered in the era of weaponized information leaks (Cadwalladr, 2018).

Analysis of the Ashley Madison Hack

Ashley Madison is an online dating website owned and operated by a company called Avid Life Media, which offers to facilitate extramarital affairs for its clientele (Rogers, 2015; *Economist*, 2015; George-Cosh, 2015; Tuttle, 2015; Murdock, 2015; Hackett, 2015; Koller, 2016; Cox, 2015; Schwartz, 2015; Basu, 2015). The image on the front page features a woman with a finger to her lips implying secrecy and discretion (*Economist*, 2015). In July 2015, hackers calling themselves “The Impact Team” (*Economist*, 2015; Rogers, 2015; Tuttle, 2015; Gauthier, 2015; *CNNMoney Staff*, 2015; Wright, 2015; Dewey 1, 2015; *ICT Monitor*, 2015; Hackett, 2015; *Panda Security*, 2015; Solomon, 2015; Chirgwin, 2016; Ragan, 2015; Cox, 2015; Schwartz, 2015; *PIPEDA Report*, 2016; Basu, 2015), announced to the employees of Avid Life Media that they had hacked the website and stolen vast amounts of data, which they threatened to release if the Ashley Madison website, and another site called Established Men, were not shut down (George-Cosh, 2015; Gauthier, 2015; *CNNMoney*, 2015; Basu, 2015; *PIPEDA Report*, 2016).

The Ashley Madison event is an example of hacktivist vigilantism (Basu, 2015) where the hackers, sought to hold Avid Life Media accountable for what they perceived

as unethical business practices (Cox, 2015). Although the Ashley Madison hack was not particularly innovative from a technical perspective, the exposure of the data, a practice known as “doxing” (Michelsen, 2015) for the purposes of naming and shaming (Arvanitidis, 2016; Ong, 2012), brought attention to the fact that data theft can have significant consequences for customers that go well beyond financial fraud or identity theft (*Economist*, 2015; Tuttle, 2015). In fact, the data that was exposed is attributed to be the cause of two suicides (George-Cosh, 2015; Rogers, 2015; *CNNMoney*, 2015), became evidence in divorce proceedings (*CNNMoney*, 2015), laid a foundation for blackmail schemes by other criminal actors (*Panda Security*, 2015), and created conditions from which nation states sought to coerce government employees to share state secrets (Basu, 2015).

To reinforce the implication that Ashley Madison was a private space, as conveyed by the woman with a finger to her lips, the website featured a “Trusted Security Award” logo (Solomon, 2017; Chirgwin, 2016), which implied that an objective third party had audited the websites security practices and found them to be at or above industry standard (Solomon, 2017; Chirgwin, 2016). In fact, this award was a fabrication of Avid Life Media designed to fool users into believing their data and their behavior would be kept private (Chirgwin, 2016). This was the one of several behaviors The Impact Team sought to expose (Cox, 2015).

As with all online dating websites, the revenue model on the Ashley Madison website is based on economies of scale within the application (Gauthier, 2017), so “fembots,” automated accounts which send sexy messages to potential male clients, feature heavily in the experience (Tuttle, 2015; Gauthier, 2017). In order for a paid dating

site to be worth the investment, prospective customers need to believe there is a huge pool of potential mates (Dewey 2, 2015; Gauthier, 2017). Ashley Madison created this impression through a program called “Ashley’s Angels” which paid ALM employees to develop messages that could be sent from sexy female profiles to visitors on the site (Dewey 2, 2015; Tuttle, 2015). In order to respond to these messages, the user would have to create an account and pay a service fee for various levels of participation (Dewey 2, 2015;). This baiting of male customers was one of the business practices with which The Impact Team took exception (Cox, 2017), describing this behavior during an interview with *Motherboard*, as blackmail (Cox, 2015).

Another ALM business practice which The Impact Team found unethical was the offering of a fraudulent “Full Delete” service, which purportedly erased all traces that a person had used the site when they paid a fee of \$19.00 (Cox, 2015; Tuttle, 2015; Schwartz, 2015; Hackett, 2015; Ragan, 2015; Gauthier, 2017). The data exposed by The Impact Team provided evidence that even when members paid for the full delete service, ALM retained user data and credit card information on its servers dating back as far as 2007 (Cox 2015; Tuttle, 2015).

According to an interview with The Impact Team, Avid Life Media had very poor security practices, allowing the hackers to “use Pass1234 (informational) from the internet (physical) to root on all servers (physical)” (Cox, 2015). It is believed that the hack began with the compromise of an employee’s Avid Life Media credentials (informational) (Murdock 1, 2015; Schwartz, 2015; *PIPEDA Report*, 2016). Although the hackers did not use an anonymity capability (cognitive) such as *Tor* (informational) (Hackett, 2015), by employing a proxy service (physical) to enter the Avid Life Media

virtual private network (VPN) (physical) (Chirgwin, 2016; Cox, 2015; *PIPEDA Report*, 2016; Basu, 2015; Englander, 2015; Solomon, 2017), the hackers were able to use a pseudonymity capability by “spoofing” (cognitive) a Toronto IP address (informational) in order to mask their whereabouts (cognitive) (Solomon, 2017; *PIPEDA Report*, 2016). It was later identified that the box initiating the attack “was located at 94.102.63.121,” (physical) (Hackett, 2015).

The attackers accessed (cognitive) the data (informational) over time in order to minimize unusual activity (cognitive), growing their understanding (cognitive) of network topography (physical), and expanding their privileges (informational) while they exfiltrated (cognitive) user data (informational) without discovery (*PIPEDA Report*, 2016). Eventually, the hackers gained (cognitive) administrative privileges (informational), which allowed them to erase (cognitive) evidence of their presence from the VPN log files (informational) (*PIPEDA Report*, 2016). Although Avid Life Media used (cognitive) the bcrypt hashing algorithm (informational) to “hash” passwords (informational) (*Panda Security*, 2015; Schwartz, 2015; *CynoSure Prime*, 2015; *PIPEDA Report*, 2016; Tuttle, 2015;), programming errors undermined the implementation (Tuttle, 2015), and the passwords (informational) could still be cracked by experts using (cognitive) an MD5 algorithm (informational) (*CynoSure*, 2015), and over 11 million passwords were cracked using this technique (*CynoSure*, 2015; Englander, 2015; *CNNMoney*, 2015).

The Impact Team announced themselves on 12 July 2015 (cognitive) by delivering a message (informational) to Avid Life Media Employees (cognitive) via their corporate computers (physical) (George-Cosh, 2015; Rogers, 2015; Tuttle, 2015; Gauthier, 2017;

Panda Security, 2015; Cox, 2015; *PIPEDA Report*, 2016). The message threatened to release (cognitive) the stolen data (informational) onto the Internet (physical) if Avid Life Media did not shutter (cognitive) their Ashley Madison and Established Men websites (physical) (Rogers, 2015; *PIPEDA Report*, 2016; George-Cosh, 2015). When Avid Life Media refused to shut down (cognitive) their websites (physical), The Impact Team released (cognitive) three tranches of data linked to approximately 37 million users (informational) (Michelsen, 2015; Koller, 2016; Tuttle, 2015; Cox, 2015; Schwartz, 2015, *CNNMoney*, 2015; Wright, 2015; Dewey 1, 2015; *ICT Monitor*, 2015; Hackett, 2015), including names, addresses, credit card information, and even more personal details such as sexual preferences and fantasies (informational) (Tuttle, 2015; Gauthier, 2017; Dewey 1, 2015; *ICT Monitor*, 2015; *Panda Security*; 2015; Wright, 2015; Hackett, 2015; Ragan, 2015; Cox, 2015; Schwartz, 2015; Englander, 2015).

The available data (informational) led to the creation of multiple websites (physical) which provided indexing and search services (informational) (Rogers, 2015; Michelsen, 2015; Koller, 2015), while other sites (physical) offered to delete data (informational) in order to lure visitors (cognitive), infecting them with malware (informational) designed for other purposes (Rogers, 2015). Other opportunists used the data to blackmail Ashley Madison users (cognitive) (*Panda Security*, 2015; Basu, 2015; George-Cosh, 2015; *CNNMoney*, 2015).

Although the morality of the Ashley Madison website users raised eyebrows, the issue of data privacy and the morality of Avid Life Media's data retention practices drew the most attention (Gauthier, 2017; Cox, 2015; *Panda Security*, 2017; Basu, 2015). The lack of respect for client data (Cox, 2015), a negligent security culture (Tuttle, 2015;

Gauthier, 2017; *Panda Security*, 2015; Basu, 2015), and a business model designed to exploit clientele (Cox, 2015; Gauthier, 2017; Dewey 2, 2015) have been used to highlight the importance of cybersecurity culture and showcase the ramifications of data theft.

Results

Each of nine case studies was examined using a pattern matching technique to examine the correctness of the propositions. The propositional patterns were compared to the empirically based patterns that emerged within each case. Although the specific physical, informational, and cognitive elements were different for each case study, the comparison process indicated that the patterns within the nine cases matched the predicted patterns. Tables 8-14 show samples of the empirical patterns for each case study. Appendix F provides an expanded version of the tables capturing the empirical patterns.

Cognitive Dimension

The propositional pattern expected was:

P1: Cyberattacks will include a cognitive dimension.

As evidenced in studies applying Game Theory to the cyber domain (Cavusoglu et al., 2008; Do et al., 2017; Hausken & Bier, 2011; Liu et al., 2017; Njilla et al., 2016; Perea & Puerto, 2013; Rao et al., 2016; Spyridopoulos et al., 2013; Wang et al., 2016), the nine case studies provided ample evidence that the cognitive skills of both the attackers and the people within the organizations being attacked were fundamental in each event. Decision making, creativity, and knowledge were critical elements for both attackers and victims. For example, were it not for the single individual in the Finance department at Maersk deciding to install M.E. Docs software on his laptop, the NotPetya malware

would never have gotten into the Maersk infrastructure (Greenberg, 2017). Table 8 provides empirical examples of actors in the cognitive dimension from each case study to support this proposition.

Table 8. Examples of the Cognitive Dimension from Nine Case Studies

P1: Cyberattacks will include a cognitive dimension.		
Case Study	Examples	References
Stuxnet	<i>Nation state governments (Iran, United States and Israel):</i> People who make decisions to benefit the security and prosperity of their country, in this case, Iran, the United States and Israel.	Paganini, 2016; Broad et al., 2011; Nakashima & Warrick, 2012; Kushner, 2013; Sanger, 2012; Arthur, 2013; Rogers, 2015
	<i>Engineers at Natanz nuclear facility:</i> People using their knowledge and skills to make operational decisions related to the enrichment of uranium.	Sanger, 2012; Nakashima & Warrick, 2012; Langner, 2011
Ukrainian Blackouts	<i>Hackers/Attackers (possibly Sandworm or Fancy Bear):</i> People who apply their knowledge and skills to gain unauthorized access to computing environments.	BBC, 2017; Greenberg, 2017; Park et al., 2017; Polityuk et al., 2017; Sullivan & Kamensky, 2017; Detsch, 2016; Smith, 2018; Zetter, 2017; Lee et al., 2016; Harrell, 2017; Toecker, 2016; Osborne, 2018
	<i>Electric Power Operations Personnel:</i> People who monitor, manage, and make decisions related to the transmission and distribution of electric power.	Park et al., 2017; Sullivan & Kamensky, 2017; Toecker, 2016; Detsch, 2016; Smith, 2017; Harrell, 2017; Greenberg, 2017; Osborne, 2018
Internet of Things (IoT) Botnet	<i>"Paras Jha, an undergraduate at Rutgers, became interested in how DDoS attacks could be used for profit."</i> The person who created the Mirai malware.	Fruhlinger, 2018
	<i>Dyn:</i> An Internet Service Provider company. People at Dyn use their skills and knowledge to defend their organization against cyberattack.	Mansfield-Devine, 2016; Liu, 2017; Perlroth, 2016; Sanger & Perlroth, 2016; Trendmicro, 2017; Greenberg, 2017; Leyden, 2017; Fruhlinger, 2018
Twitterbots	<i>Bot makers:</i> People who use their creativity to make bots.	Hirsch, 2017; Confessore et al., 2018; Dubbin, 2013; Guilbeault & Woolley, 2016
	<i>Voters & Public Sentiment:</i> People who make decisions and share opinions about complex issues such as national leadership or alliances.	Woolley & Shout, 2016; Timberg & Dwoskin, 2018; Baraniuk, 2018
Melissa Virus	<i>David Lee Smith:</i> The person who created the malicious software, which he named Melissa after an exotic dancer he had liked.	WSJ, 1999; NYT, Dec 1999; Smothers, 1999; Taylor et al., 1999; Pearce, 2002; Strickland, 2008; Panda Security, 2013; McNamara, 2014; Cluley, 2009; Mills, 2009; Raney, 1999
	<i>Victim organizations and users:</i> Groups of people whose abilities to do their jobs were impacted.	Peterson, 1999; McNamara, 2014; CERT, 1999; NYT, Apr 1999; Redmond, 1999; Panda Security, 2013; McNamara, 2014; Mills, 2009

Hack of American Business 2005-2012	<p><i>Vladimir Drinkman:</i> A person who was a member of the cybercrime gang.</p>	Hudson, 2013; Bray, 2013; Bray & Yadron, 2013; Fox, 2013; Reuters, 2013; Sullivan, 2013; Jones & Finkle, 2013; Wood, 2018; Schwartz, 2015; DoJ, 2015, 2018; Armental, 2015
	<p><i>Cashers:</i> People who were customers of the cybercrime gang.</p>	Hudson, 2013; Reuters, 2013; Sullivan, 2013; Jones & Finkle, 2013; Beekman, 2013; DoJ, 2015, 2018
(Not)Petya Ransomware	<p><i>Russian Government:</i> People who make decisions to benefit the security and prosperity of the Russian Nation State.</p>	Greenberg, 2018; Hackett, 2017; Palmer, 2017; Reilly, 2017; Tung, 2018; USCERT, 2017; Woo, 2018; Doctorow, 2018; Cimpanu, 2018; Fruhlinger, 2017
	<p><i>AP Moeller-Maersk:</i> People who make decisions for the company related to the global shipping services that move 20% of the world's cargo.</p>	Ryan, 2017; Tung, 2017, 2018; Cimpanu, 2018; Collins, 2017; Daneshkhoo et al., 2017; Chopping, 2017; Greenberg, 2018; Hackett, 2017; Matthews, 2017; Olenick, 2018; Osborne, 2018; Ryan, 2017
WikiLeaks & the Manning Disclosure	<p><i>Private Manning:</i> The person who served as an intelligence analyst, who made the decision to steal classified data and release it to the public domain.</p>	Sangarasivam, 2013; Nita, 2014; Berghel, 2012; Jones, 2013; Garnett & Hughes, 2019; Somashekhar, 2017; Cadwalladr, 2018; Zavis, 2017; Booth et al., 2010; McGreal, 2010; Tate, 2013; Zetter & Poulsen, 2010; Peralta, 2013; Bumiller, 2010; Thompson, 2010; Chan, 2017; Nicks et al., 2011
	<p><i>U.S. Government:</i> People who make decisions to benefit the security and prosperity of the United States Nation State.</p>	Sangarasivam, 2013; Berghel, 2012; Garnett & Hughes, 2019; Tate, 2013; McGreal, 2010; Zetter & Poulsen, 2010
Ashley Madison	<p><i>"Impact Team":</i> The people who exposed the Ashley Madison clientele and business model.</p>	<i>Economist</i> , 2015; Rogers, 2015; Tuttle, 2015; Gauthier, 2017; <i>CNNMoney</i> , 2015; Wright, 2015; Dewey, 2015; <i>ICTMW</i> , 2015; Hackett, 2015; <i>Panda</i> , 2017; Solomon, 2017; Chirgwin, 2016; Ragan, 2015; Cox, 2015; Schwartz, 2015; <i>PIPEDA Report</i> , 2016; Basu, 2015
	<p><i>Avid Life Media:</i> The people who made decisions for the parent company which owned and operated the Ashley Madison website.</p>	George-Cosh, 2015; Tuttle, 2015; Gauthier, 2017; <i>CNNMoney</i> , 2015; Murdock, 2015; Hackett, 2015; Solomon, 2017; <i>PIPEDA Report</i> , 2016

Physical Dimension

The propositional pattern expected was:

P2: Cyberattacks will include a physical dimension.

The physical dimension offers strategic, operational, and tactical targets (Joint Pub 3-13),

such as the tangible industrial control systems that distribute electric power, as in the

Ukrainian Blackouts or the tangible outcomes of an election to determine regional economic integration, as in the Brexit Referendum. The physical dimension also encompasses the tools that act as an onramp to the virtual world, such as the sensors and networks that reach across geographical boundaries (Brown, 2015; Kim, 2010; Haggard & Lindsay, 2015; Cavusoglu et al., 2008; Karatzogianni & Gak, 2015). Table 9 provides empirical examples from each case study of the tangible objects and outcomes of the physical dimension that link the material world and the virtual world to support this proposition.

Table 9. Examples of the Physical Dimension from Nine Case Studies

P2: Cyberattacks will include a physical dimension.		
Case Study	Examples	References
Stuxnet	<i>Natanz centrifuges:</i> The tangible devices used to refine uranium to weapons grade.	Chen & Abu-Nimeh, 2011; Zetter, 2011; Weinberger, 2011; Rosenbaum, 2012; Lindsay, 2013
	<i>USB thumb drives:</i> Tangible devices used to transfer and store data.	Farwell & Rohozinski, 2011; Lindsay, 2013; Zetter, 2011; Arthur, 2013
Ukrainian Blackouts	<i>Supervisory Control and Data Acquisition (SCADA) Systems:</i> Tangible computer systems that operate industrial controls within the electric power infrastructure.	Polityuk et al., 2017; Park et al., 2017; Huang et al., 2018; Detsch, 2016; Smith, 2017; Lee et al., 2016; Harrell, 2017; Osborne, 2018
	<i>Power outage:</i> The absence of electric power resulting in the tangible loss of heat and light.	Osborne, 2018; BBC, 2017; Greenberg, 2017; Polityuk et al., 2017; Park et al., 2017; Sullivan & Kamensky, 2017; Detsch, 2016; Smith, 2018; Adamczyk, 2017; Huang et al., 2018; Zetter, 2017; Lee et al., 2016; Harrell, 2017
Internet of Things (IoT) Botnet	<i>IoT Devices (webcams, routers, baby monitors, etc.):</i> Tangible devices that are connected to the Internet.	Kolias et al., 2017; Greenberg, 2017;
	<i>Report Server and Command & Control Server:</i> The tangible computer server that contains information about the various devices in the IoT botnet, and the tangible terminal from which commands can be issued to control the IoT botnet.	Kolias et al., 2017; Greenberg, 2017; Moriuchi & Chohan, 2018; Fruhlinger, 2018;
Twitterbots	<i>Bot hosting site, cloud servers:</i> Tangible computing tools where bots are stored.	Graham, 2017; Dubbin, 2013
	<i>Elections (for example presidential elections, Brexit referendum):</i> The Brexit vote had a tangible impact on the UK/European Union legal	Timberg & Dwoskin, 2018; Baraniuk, 2018; Confessore et al., 2018; Hirsch, 2017; Curran, 2017; Metz, 2018;

	and economic relationship. Presidential elections change the direction of government policy and the people involved in the government.	Woolley & Shout, 2016; Gu et al., 2017; Guilbeault & Woolley, 2016
Melissa Virus	<i>Mail servers:</i> Tangible computer servers that manage electronic mail systems.	Redmond, 1999; We Live Security, 2016; McNamara, 2014; Mills, 2009; Raney, 1999; Cheng, 1999
	<i>Telephone:</i> Tangible device used to dial into the Internet.	Mills, 2009; Taylor et al., 1999;
Hack of American Business 2005-2012	<i>Anonymous Web Hosting:</i> Tangible computer servers positioned all over the world.	Armental, 2015; Beekman, 2013; Hudson, 2013; DoJ, 2015, 2018; Fox, 2013; Reuters, 2013; Jones & Finkle, 2013; Schwartz, 2015
	<i>Magnetic Strips on Blank Plastic Cards:</i> Tangible object used to interface with payment processing systems and banking machines.	Hudson, 2013; Wood, 2018; DoJ, 2015, 2018
(Not)Petya Ransomware	<i>M.E. Doc's Update Server:</i> The tangible computer server used to push software updates to users over the Internet.	Tung, 2017, 2018; Fruhlinger, 2017; Greenberg, 2018; Nott, 2017; Sayer, 2017; Chirgin, 2018; Cimpanu, 2018; Frenkel et al., 2017; Olenick, 2018
	<i>Security gates at Maersk shipping ports:</i> The tangible physical boundaries that were unable to be operated once the computer systems were corrupted.	Greenberg, 2018; Tung, 2017; <i>Asia News Monitor</i> , 2017; Daneshkhuh et al., 2017; Chopping, 2017; Frenkel et al., 2017; Olenick, 2018
Wikileaks & the Manning Disclosure	<i>CD-RW:</i> The tangible object used by Manning to move data from one location to another.	Sangarasivam, 2013; Garnett & Hughes, 2019; Zetter & Poulsen, 2010
	<i>Apache Helicopter:</i> The tangible weapon system which fired weapons in Iraq.	Sangarasivam, 2013; Nita, 2014; Zavis, 2017; Booth et al., 2010; Tate, 2013; Zetter & Poulsen, 2010
Ashley Madison	<i>Avid Life Media data servers:</i> Tangible servers that belong to the parent company, Avid Life Media on which the company's core knowledge assets are stored.	Chirgin, 2016; Ragan, 2015; Cox, 2015; <i>PIPEDA Report</i> , 2016; Basu, 2015; Englander, 2015
	<i>Divorce proceedings, job loss, suicides:</i> Tangible events that occurred following the Ashley Madison hack.	George-Cosh, 2015; Rogers, 2015; <i>CNNMoney</i> , 2015

Cognitive – Physical Interaction

The propositional pattern expected was:

P3: Cyberattacks will include an element of the cognitive dimension (hacker or human target) interacting with an element of the physical dimension (e.g. a tangible object, including sensors, computers, telephones, security badges, etc. or tangible outcome, including elections, immunizations, absence of light & heat, etc.)

As evidenced in the sociomateriality and information systems literature, people and technology are constantly interacting (Kautz & Jensen, 2013; Orlikowski, 2007; Scott & Orlikowski, 2009; Leonardi, 2013; Leonardi & Barley, 2008; Chen et al., 015; Burmester et al., 2012). Hackers use a combination of tactics, techniques, and tools to conduct cyberattacks. Tactics and techniques, such as the use of spear phishing or SQL injection techniques require specific knowledge, creativity, and skills, all of which are cognitive in nature, placing them in the cognitive dimension, while the tools, such as desktop computers or networked servers reside in the physical dimension. Target organizations also use tactics, techniques, and tools to conduct their operations, generate revenue, and to defend or secure their organizations.

Decision making, a cognitive behavior, figures heavily in the tangible outcomes of events such as elections, as evidenced in the Twitterbots case study (Timberg & Dwoskin, 2018; Baraniuk, 2018; Confessore et al., 2018; Hirsch, 2017; Curran, 2017; Metz, 2018; Woolley & Shout, 2016; Gu et al., 2017; Guilbeault & Woolley, 2016), or divorce proceedings, as evidenced in the Ashley Madison hack (George-Cosh, 2015; Rogers, 2015; CNNMoney, 2015). Table 10 provides empirical examples from each case study of the interaction between the cognitive dimension – people as either attackers or victims – and the physical dimension – tangible objects and outcomes at the intersection of the virtual and the material.

Table 10. Examples of the Cognitive – Physical Interaction from Nine Case Studies

P3: Cyberattacks will include an element of the cognitive dimension (hacker or human target) interacting with an element of the physical dimension (e.g. a device of some kind, including sensors, computers, telephones, security badges, etc.)		
Case Study	Examples	References
Stuxnet	<i>“Iranians were apparently caught off guard and surprised by the degree to which their defences could be penetrated, even against highly protected air-gap systems.”</i>	Farwell & Rohozinski, 2011

	People from Iran had designed the defense strategy to include (c) a tangible “air gap” between the tangible devices in the Natanz facility and the global Internet. (p)	
Ukrainian Blackouts	<i>“Taking control of the facilities’ SCADA systems, malicious actors opened breakers at some 30 distribution substations...”</i> Malicious people used their skills to gain unauthorized access (c) to tangible industrial control systems and electric power breakers (p).	Park et al., 2017
Internet of Things (IoT) Botnet	<i>“IoT devices have become the ‘new favorite’ for DDoS hackers because a very large percentage of administrators and users of IoT devices think of them as plug-and-play solutions and, as a result, do not take even the most basic steps to protect these devices from malicious hacking...”</i> Malicious people understand that most people do not decide to secure (c) IoT devices. (p)	Vlajic & Zhou, 2018
Twitterbots	<i>“...public sentiment on contentious issues including gun control and the 2016 U.S. presidential election.”</i> People have strong opinions (c) about the tangible impacts of gun regulations and other government policies (p).	Baraniuk, 2018
Melissa Virus	<i>“Eventually,’ says deputy attorney general Christopher Bubb, ‘we were able to trace it back to the specific telephone that was being used.’”</i> People investigating the cyber disruption were able to identify (c) the specific tangible telephone that connected to the Internet. (p)	Taylor et al., 1999
Hack of American Business 2005-2012	<i>“...identified Drinkman and Kalinin as “sophisticated” hackers who specialized in penetrating the computer networks of multinational corporations, financial institutions and payment processors.”</i> Two people, Drinkman & Kalinin who were part of the cybercrime gang were highly skilled at using their knowledge to gain illegal access to (c) tangible computer networks. (p)	Hudson, 2013
(Not)Petya Ransomware	<i>“One staffer from the Ghana office flew to Nigeria to meet another Maersk employee in the airport to hand off the very precious hard drive.”</i> People from Maersk’s leadership made the decision to have two people, one from Ghana and another from Nigeria, hand-carry (c) the tangible hard drive that functioned as the domain controller for Maersk’s entire global operation. (p)	Greenberg, 2018; Doctorow, 2018
Wikileaks & the Manning Disclosure	<i>“...the only safe place I seem to have (c) is this satellite internet connection.””</i> In this person’s – Manning’s – own words, the only time she experienced a sense of safety was when communicating with other people (c) via the tangible equipment comprising the satellite connection to the Internet.	Cadwalladr, 2018
Ashley Madison	<i>“Ashley Madison is a website that arranges extramarital liaisons.””</i> The tangible servers that comprise the Ashley Madison website are a location (p) where users can go when they make the decision to engage in an extramarital affair. (c)	Economist, 2015

Informational Dimension

The propositional pattern expected was:

P4: Cyberattacks will include an informational dimension.

Because it houses explicit knowledge assets, such as patents, training, and business intelligence, the informational dimension also offers viable targets for attackers, such as the media narratives related to gun control and other contentious political issues (Baraniuk, 2018), or information being fed to operations personnel related to orchestration of port loading and unloading operations (Ryan, 2017). The critical software that supports core business processes, or runs the devices, networks and sensors of the physical dimension are also conspicuous targets. In addition to providing targets for hackers, the information dimension also provides tools for hackers, such as the messages contained in phishing emails, or the information rules contained in malware. Table 11 provides empirical examples of the types of data, information, and software which make up the informational dimension from each case study to support this proposition.

Table 11. Examples of the Informational Dimension from Nine Case Studies

P4: Cyberattacks will include an informational dimension.		
Case Study	Examples	References
Stuxnet	<i>Stuxnet malware:</i> Set of malicious information rules tailored to communicate with Industrial Control Systems.	Lindsay, 2013; Nakashima & Warrick, 2012; Shapiro, 2016; Sanger, 2012; Rosenbaum, 2012; Paganini, 2016; Rogers, 2015; Broad et al., 2011; Arthur, 2013; Zetter, 2011, 2014; Kushner, 2013; Chen & Abu-Nimeh, 2011; Gjelten, 2010; Farwell & Rohozinski, 2011
	<i>Siemens WinCC/Step7 software:</i> Set of information rules used to program Siemens Simatic Programmable Logic Controllers.	Chen & Abu-Nimeh, 2011; Zetter, 2011; Kushner, 2013
Ukrainian Blackouts	<i>Email & Email attachments:</i> Information delivered in electronic mail form with attached Microsoft Word or Microsoft Excel documents.	Greenberg, 2017; Park et al., 2017; Toecker, 2016; Detsch, 2016; Smith, 2018; Zetter, 2017; Lee et al., 2016; Harrell, 2017

	<i>Malware (BlackEnergy3, KillDisk & Crash Override):</i> Information rules of that subvert the proper system information rules allowing unauthorized access and actions.	BBC, 2017; Greenberg, 2017; Polityuk et al., 2017; Park et al., 2017; Huang et al., 2018; Sullivan & Kamensky, 2017; Toecker, 2016; Smith, 2018; Smith, 2017; Zetter, 2017; Lee et al., 2016; Harrell, 2017; Osborne, 2018
Internet of Things (IoT) Botnet	<i>Mirai & Reaper Malware:</i> Information rules that orchestrate a botnet.	Mansfield-Devine, 2016; Vlajic & Zhou, 2018; Trendmicro, 2017, 2018; Greenberg, 2017; Leyden, 2017; Moriuchi & Chohan, 2018; NetLab, 2017; Fruhlinger, 2018; Liu, 2017; Perlroth, 2016; Kolias et al., 2017
	<i>Username/password combinations:</i> Information used to connect to an IoT device.	Kolias et al., 2017; Greenberg, 2017; Moriuchi & Chohan, 2018; NetLab, 2017; Fruhlinger, 2018; Sanger & Perlroth, 2016
Twitterbots	<i>Twitterbots:</i> Information rules (software) to control information accounts about a fake person that looks like information about a real person and imitates human behavior.	Woolley & Shout, 2016; Wojcik, 2018; Graham, 2017; Timberg & Dwoskin, 2018; Edwards et al., 2014; Gu et al., 2017; Guilbeault & Woolley, 2016; Baraniuk, 2018; Farrell, 2018; Hirsch, 2017; Spence et al., 2018; Confessore et al., 2018; Dubbin, 2013; Edwards et al., 2016; Krishna, 2014; Metz, 2018
	<i>Propaganda & disinformation:</i> Information that is not objective, and is sometimes false, which is used to influence an audience.	Woolley & Shout, 2016; Guilbeault & Woolley, 2016; Baraniuk, 2018; Hirsch, 2017; Economist, 2017; Timberg & Dwoskin, 2018; Curran, 2017; Gu et al., 2017
Melissa Virus	<i>Melissa Computer Virus:</i> Information rules contained in macros within a Word document.	Taylor et al., 1999; Redmond, 1999; CERT, 1999; Cheng, 1999 ; Pearce, 2002 ; Raney, 1999 ; NYT, Apr 1999; Strickland, 2008; Peterson, 1999; WSJ, 1999; Smothers, 1999
	<i>Word document with a list of passwords to pornography websites:</i> Information in the form of passwords.	McNamara, 2014; Cluley, 2009; Mills, 2009; Techspirited, 2019; Taylor et al., 1999
Hack of American Business 2005-2012	<i>Credit Card Numbers:</i> Information that ties to financial accounts.	Hudson, 2013; Bray, 2013; Bray & Yadron, 2013; Fox, 2013; Reuters, 2013; Sullivan, 2013; Jones & Finkle, 2013; Wood, 2018; Schwartz, 2015; DoJ, 2015, 2018; Armental, 2015; Beekman, 2013
	<i>Structured Query Language & SQL Injection:</i> Information in the form of a programming language designed to manage data held in specific kinds of databases. SQL injection is bad information that gets input into the databases.	DoJ, 2015, 2018; Sullivan, 2013; Wood, 2018; Schwartz, 2015
(Not)Petya Ransomware	<i>M.E. Docs software:</i> Information rules in the form of tax and accounting software used by Ukrainian businesses.	Tung, 2017, 2018; Fruhlinger, 2017; Greenberg, 2018; Nott, 2017; Sayer, 2017; Chirgwin, 2018; Cimpanu, 2018; Frenkel et al., 2017; Olenick, 2018

	<i>EternalBlue & EternalRomance Exploits:</i> Vulnerabilities within the information rules of the Microsoft Windows Operating System.	Tung, 2018; USCERT, 2017; Fruhlinger, 2017; Greenberg, 2018; Hackett, 2017; Osborne, 2018; Palmer, 2017, 2018
WikiLeaks & the Manning Disclosure	<i>"Collateral Murder" Video:</i> Information stored in the form of full motion video of an airstrike that took place in Iraq.	Sangarasivam, 2013; Nita, 2014; Berghel, 2012; Somashekhar, 2017; Cadwalladr, 2018; Zavis, 2017; Booth et al., 2010; McGreal, 2010; Tate, 2013; Zetter & Poulsen, 2010
	<i>Chat Logs:</i> The information record of the conversations between Private Manning and Adrian Lamo.	Nita, 2014; Cadwalladr, 2018; Zetter & Poulsen, 2010
Ashley Madison	<i>Pictures & Conversations:</i> Information in the form of email exchanges between clientele, photographs of people in various states of dress, and other private exchanges of information.	Dewey, 2015; <i>ICTMW</i> , 2015; Cox, 2015; <i>CNNMoney</i> , 2015; Wright, 2015
	<i>Fembots:</i> Information rules attached to fake Ashley Madison female accounts that generated sexy, enticing digital interactions with male clients.	Dewey, 2015; Tuttle, 2015

Cognitive – Informational Interaction

The propositional pattern expected was:

P5: Cyberattacks will include an element of the cognitive dimension (hacker, organization, human target, etc.) interacting with an element of the informational dimension (data, software, knowledge, etc.).

Access to information is often the goal of a cyberattack, such as cyberespionage or cybercrime (Luppincini, 2014; Myauo, 2016; Archer, 2014). For example, the Hack of American Business involved the theft of credit and debit card information, while the Ashley Madison hack and the Manning disclosure to WikiLeaks involved the theft and exposure of sensitive data to the general public.

Manipulation of information is another tactic used in cyberattacks, such as the circulation of propaganda and disinformation with Twitterbots (Woolley & Shout, 2016; Guilbeault & Woolley, 2016; Baraniuk, 2018; Hirsch, 2017; Economist, 2017; Timberg

& Dwoskin, 2018; Curran, 2017; Gu et al., 2017), or the man-in-the-middle manipulating data sent to centrifuge operators in the Stuxnet attack (Zetter, 2014; Sanger, 2012).

Because information is crucial for decision making, organizations also use informational capabilities to expand their customer base, generate revenue, and execute core capabilities, for example Maersk's online booking capability Maerskline.com (Greenberg, 2018; Asia News Monitor, 2017). Table 12 provides empirical examples from each case study of the interaction between the cognitive dimension – people as either attackers or victims – and the physical dimension – tangible objects and outcomes at the intersection of the virtual and the material.

Table 12. Examples of the Cognitive – Informational Interaction from Nine Case Studies

P5: Cyberattacks will include an element of the cognitive dimension (hacker, organization, human target, etc.) interacting with an element of the informational dimension (data, software, knowledge, etc.).		
Case Study	Examples	References
Stuxnet	<p><i>“...when it [Stuxnet] attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally.”</i></p> <p>Operations personnel made decisions based on receiving (c) information indicating that everything was within normal parameters (i).</p>	Sanger, 2012
Ukrainian Blackouts	<p><i>“Four elements of the payload targeted particular communication protocols specified in the standards IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OLE for Process Control Data Access (OPC DA).”</i></p> <p>People learned about and targeted (c) specific information communication protocols defined in written information standards with four specific information rules called the “payload” (i).</p>	Osborne, 2018
Internet of Things (IoT) Botnet	<p><i>“...custom-made botnets, but also to botnets-for-hire...”</i></p> <p>Entrepreneurial people will use their knowledge and skills to market their services to operate or create customized (c) information rules in the form of botnet software, such as Mirai or Reaper malware. (i)</p>	Vlajic & Zhou, 2018
Twitterbots	<p><i>“...people report similar levels of information seeking, cognitive elaboration, affective learning, and motivation behaviors when receiving information from a Twitterbot when compared to a human agent.”</i></p> <p>People learn, form associations with their existing understanding based on, and are motivated to seek (c) information from Twitterbots (i).</p>	Edwards et al., 2016, p. 669

Melissa Virus	<p><i>"In Stockholm, computer-science grad Fredrik Bjorck suggested that Melissa's code bore a strong resemblance to the work of a virus writer called VicodinES."</i></p> <p>A person, Fredrik Bjorck, examined (c) the information rules in the Melissa virus (i) and he thought he recognized the work of a person calling himself VicodinES (c).</p>	Taylor et al., 1999
Hack of American Business 2005-2012	<p><i>"Drinkman and Smilianets not only stole over 160 million credit card numbers from credit card processors, banks, retailers, and other corporate victims, they also used their bounty to fuel a robust underground market for hacked information..."</i></p> <p>Two people from the cybercrime gang, Drinkman and Smilianets used their knowledge and skills to steal and sell (c) information in the form of over 160 million credit card numbers, (i), and their decisions and actions contribute to the growth of other people making the decisions to participate in the illegal purchase and sale of (c) information. (i)</p>	DoJ, 2018
(Not)Petya Ransomware	<p><i>"an attack designed by and for a state (Ukraine was the target: the malware was put in a malicious update to MeDoc, the country's most popular accounting software)."</i></p> <p>People from Ukraine have concluded that the attack was part of hybrid warfare, and that people from Russia corrupted (c) the information rules for the M.E. Docs software with the information rules that comprise the NotPetya malware. (i)</p>	Chirgwin, 2018
Wikileaks & the Manning Disclosure	<p><i>"The reaction to the video gave me immense hope..."</i></p> <p>Information recorded in the chat logs captured (i) Manning telling Adrian Lamo about her emotional state, and feeling hopeful about people's reactions to (c) the information released in the full motion video "Collateral Murder."</p>	Booth et al., 2010
Ashley Madison	<p><i>"'ALM confirmed that the 'trusted security award' trust-mark on their home page was simply their own fabrication rather than a validated designation by any third party,' it notes."</i></p> <p>People made the decision to trust the people of Avid Life Media with (c) their personal information because of a fake "trusted security award" seal (i) that was fabricated by Avid Life Media to fool users. (c)</p>	Chirgwin, 2016

Informational – Physical Interaction

The propositional pattern expected was:

P6: Cyberattacks will include an element of the informational dimensions (e.g.

malware or data) interacting with an element of the physical dimension (e.g. computer, network, sensor, etc.).

The interaction between the informational and physical dimension is well researched, with ample evidence provided in information security theory (Burmester et al., 2012; Cavsoglu et al., 2009; Chen et al., 2015; Johnson & Warkentin, 2010) and the concept of the information artefact in sociomateriality theory (Leonardi, 2013). Cyber-physical systems, such as the Uranium refinement centrifuges in the Stuxnet case study (Zetter, 2014) or the electric power distribution center or the electric power transmission stations in the case study of the Ukrainian blackouts (Greenberg, 2017), speaks directly to the automation of physical systems through the use of software, which is comprised of information rules and executes specific operations based on data (Nguyen, 2013; DiMase et al., 2015; Vanderhaegen, 2017; Netto & Spurgeon, 2017). In each of these cases, malware, a set of malicious information rules, was used to impact the operations of the physical devices (Zetter, 2014; Greenberg, 2017; Amin, 2015; Balzacq & Cavelty, 2016; Farwell & Rohozinski, 2011; Finlay, 2018). Table 13 provides empirical examples from each case study of the interaction between the informational dimension and the physical dimension, confirming existing research.

Table 13. Examples of the Informational – Physical Interaction from Nine Case Studies

P6: Cyberattacks will include an element of the informational dimensions (e.g. malware or data) interacting with an element of the physical dimension (e.g. computer, network, sensor, etc.).		
Case Study	Examples	References
Stuxnet	<p><i>“Stuxnet seized the controls of the machine running the centrifuges and in a delicate, invisible operation, desynchronized the speeds at which the centrifuges spun, causing nearly a thousand of them to seize up, crash and otherwise self-destruct.”</i></p> <p>The information rules in the Stuxnet malware sent instructions to (i) the tangible centrifuges, which spun at incorrect speeds, causing them to break. (p)</p>	Rosenbaum, 2012
Ukrainian Blackouts	<p><i>“Commands were then sent to the circuit breakers and protection relays which only opened circuit breaker switches...”</i></p> <p>Information triggers in the form of commands operated (i) tangible grid equipment such as circuit breaker switches and protection relays. (p)</p>	Osborne, 2018

Internet of Things (IoT) Botnet	<p><i>IoT Botnet:</i></p> <p>Tangible devices connected to the Internet that are connected to one another (p) through a set of information rules. (i)</p>	Greenberg, 2017; Mansfield-Devine, 2016; Vlajic & Zhou, 2018; Trendmicro, 2017, 2018; Leyden, 2017; Moriuchi & Chohan, 2018; NetLab, 2017; Fruhlinger, 2018; Liu, 2017; Koliias et al., 2017
Twitterbots	<p><i>“...nearly half of the Tweets, some 500,000 messages, were generated by just 1 per cent of the 300,000 sampled accounts, clearly suggesting these were automated. In the last 48 hours before the referendum, these comments leaned heavily in favor of Leave...”</i></p> <p>500,000 information messages generated by automated accounts (i) in the 2 days prior to a tangible event – the Brexit referendum (p).</p>	Hirsch, 2017
Melissa Virus	<p><i>“...the virus backed up and at times incapacitated computer networks...”</i></p> <p>Information rules comprising the Melissa virus transmitted so much information (i) that tangible computer networks broke down. (p)</p>	NYT, Apr 1999
Hack of American Business 2005–2012	<p><i>“...\$50 for European cards, which are more expensive because they have computer chips...”</i></p> <p>European credit card numbers (i) had a tangible value of \$50 because they included a tangible computer chip (p)</p>	Reuters, 2013
(Not)Petya Ransomware	<p><i>“...(a key piece of data was wiped out on seven mirrored servers and only survived on a system in Ghana due to a freak blackout that shut down the data-center so that the system was knocked offline before it could be infected).”</i></p> <p>The tangible data center in Ghana was shut down by the tangible loss of power, so it was not connected to the tangible Maersk networks, which protected it from (p) being corrupted by the information rules of the NotPetya malware and preserved the critical data and information rules (i) the tangible computer server contained. (p)</p>	Doctorow, 2018
Wikileaks & the Manning Disclosure	<p><i>“The video showed a deadly 2007 U.S. helicopter air strike in Baghdad...”</i></p> <p>The tangible Apache helicopter was equipped with a video camera to record tangible missions, such as an airstrike in Iraq (p) in the form of full motion video information. (i)</p>	Zetter & Poulsen, 2010
Ashley Madison	<p><i>“...threatening message” on their computer screens...”</i></p> <p>Information in the form of a threatening message (i) appeared on the tangible computer screens. (p)</p>	George-Cosh, 2015

Cognitive – Physical – Informational Interaction

The propositional pattern expected was:

P7: Cyberattacks will include multilateral interactions between the cognitive, physical, and informational dimensions.

In each case study, the human was central to the success of the attack. Human knowledge and creativity were responsible for the creation of the information rules comprising malware used to penetrate tangible devices in the eight of the nine cases studies, providing ample evidence that the three dimensions are in a constant state of interaction. Although the Manning disclosure to WikiLeaks was not predicated on malware, Manning's ingenuity to figure out how to export data from classified networks and to mask the data theft by labeling it as a music CD, again speaks to the cognitive element of cyberattack, while the use of tangible devices to exfiltrate information speaks to the multilateral interactions between the three dimensions. What makes the IoT botnet attack so powerful is not the set of information rules connecting the tangible devices, but the human controlling the botnet and directing it against selected targets (Farwell & Rohozinski, 2011; Fruhlinger, 2018).

Sometimes the cognitive dimension is the target for the attack, and the tool of choice is information, for example the use of phishing emails in the Stuxnet attack (Zetter, 2014) and the Ukrainian blackouts (Detsch, 2016), or the use of Twitterbots to circulate disinformation and propaganda to impact public sentiment (source). The man-in-the-middle approach used in Stuxnet manipulated the data in such a way as to manipulate the person responsible for reviewing the data to believe the tangible machinery was operating properly (Sanger, 2012). Table 14 provides empirical examples from each case study of the multilateral interaction between the informational dimension and the physical dimension, confirming existing research.

Table 14. Examples of the Multilateral Cognitive – Physical – Informational Interaction from Nine Case Studies

P7: Cyberattacks will include multilateral interactions between the cognitive, physical, and informational dimensions.		
Case Study	Examples	References
Stuxnet	<p><i>"To get Stuxnet to its target machines, the attackers first infect computers belonging to five outside companies that are believed to be connected in some way to the nuclear program."</i></p> <p>The tangible computers operating the Natanz equipment had a tangible “air gap” from the Internet (p), so the people who developed the strategy started their attack at organizations of people who worked with the Natanz personnel by injecting (c) the information rules within the Stuxnet malware (i) into tangible computers (p) at five outside companies (organized groups of people). (c)</p>	Zetter, 2014
Ukrainian Blackouts	<p><i>"...includes swappable, plug-in components that could allow it to be adapted to different electric utilities, easily reused, or even launched simultaneously across multiple targets."</i></p> <p>Information rules (i) were created by people to enable them to change and tailor their attack tactics and techniques (c) to different tangible electric utility equipment environments. (p)</p>	Greenberg, 2017
Internet of Things (IoT) Botnet	<p><i>"The Mirai source code was released in a cybercrime forum recently, since when it has been used to build large botnets created from compromised Internet of Things (IoT) devices such as digital video recorders, CCTV systems and so on."</i></p> <p>A person made the decision to post (c) to a cybercrime information-sharing forum a set of information rules called Mirai, a type of malware that connects (i) tangible Internet connected devices such as video recorders or CCTV systems. (p)</p>	Mansfield-Devine, 2016
Twitterbots	<p><i>"...Russia-backed bots programmed to automatically tweet animosity-stoking messages in the U.S. gun control debate following last month's school shooting in Parkland, Fla."</i></p> <p>After the tangible school shooting in Parkland, FL (p), people from Russia wrote (c) information rules (computer programs) for Twitterbots to automatically tweet information (i) designed to make American people angry in order to influence their decision making behaviors (c) related to tangible legal controls relating to tangible guns (p).</p>	Baraniuk, 2018
Melissa Virus	<p><i>"While none of the three companies would divulge its post-Melissa sales figures, they all reported fourfold to fivefold increases in traffic to their Web sites."</i></p> <p>The people at three antivirus companies would not disclose (c) sales information, but the data traffic increased substantially (i) on the tangible servers comprising their Websites (p) because people were trying to protect or repair (c) their tangible computers (p) from the malicious information rules in the Melissa virus.(i)</p>	Raney, 1999

Hack of American Business 2005-2012	<p><i>"The cashers would encode the information onto the magnetic strips of blank plastic cards and cash out the value, by either withdrawing money from ATMs in the case of debit cards, or running up charges and purchasing goods in the case of credit cards."</i></p> <p>People made the decision to purchase (c) information in the form of credit and debit card numbers (i) which the people, "cashers," would then use their knowledge and expertise to encode (c) onto the tangible magnetic strips of the blank plastic cards, which interfaced with the tangible ATMs which would disburse tangible bank notes. (p)</p>	Hudson, 2013
(Not)Petya Ransomware	<p><i>"...one single infection would become particularly fateful for Maersk: In an office in Odessa, a port city on Ukraine's Black Sea coast, a finance executive for Maersk's Ukraine operation had asked IT administrators to install the accounting software M.E.Doc on a single computer."</i></p> <p>One person who worked for Maersk's Ukrainian operations as a finance executive made the decision to request that the people from the IT staff install (c) the information rules comprising the M.E. Docs tax and accounting software (i) in his tangible computer which exposed the rest of the tangible infrastructure (p) to the malicious information rules contained in NotPetya. (i)</p>	Greenberg, 2018
WikiLeaks & the Manning Disclosure	<p><i>"I would come in with music on a CD-RW labeled with something like 'Lady Gaga,' erase the music then write a compressed split file..."</i></p> <p>In Manning's own words, he devised a strategy that involved misdirection and specific knowledge and skills to write (c) specific information rules that captured data on (i) tangible rewritable CDs (p) that he could carry with him. (c)</p>	Zetter & Poulsen, 2010
Ashley Madison	<p><i>"You could use Pass1234 from the internet to VPN to root on all servers. "</i></p> <p>In an interview with a person who was a reporter, the people (hackers) who called themselves "Impact Team" said that used (c) default password information "Pass1234" which provided access (i) to the tangible servers via the Virtual Private Network. (p)</p>	Cox, 2015

Summary

This research further develops the Cyber-Based View as a forensic tool by using it to conduct failure autopsies of successful cyberattacks. The nine case studies represent all three types of cyberattacks as defined in the study and four different types of attackers in a wide variety of industry contexts employing a wide variety of technology tools. The breadth of these case studies illustrates the generalizability of the Cyber-Based View

framework. The use of a pattern matching technique provides evidence that the anticipated interactions amongst the dimensions are in fact present in actual cyberattacks, demonstrating that the Cyber-Based View accurately captures the dynamics of cyberspace at work during a cyberattack.

CHAPTER 5

CONCLUSIONS, IMPLICATIONS, & FUTURE RESEARCH

Information Warfare in the Twenty-First Century

In October 2016, a massive distributed denial of service (DDoS) attack took down internet sites all over the Eastern United States (Sanger & Perlroth, 2016). The culprit, a piece of malware that had been designed by a college student with the intent to drive Minecraft gamers to his online game server (Fruhlinger, 2018). In June 2017, Maersk, which operates 20% of the global transportation network was brought to its knees by what appeared to be ransomware (malware designed to encrypt files until a ransom is paid to decrypt the files and make them accessible) but was in fact collateral damage from an attack by Russia on Ukraine (Osborne, 2018). The Melissa virus, which flooded networks around the world in 1999 inspired the weaponization of Microsoft Word and Excel documents embedded in phishing emails (Cluley, 2009), which, today, deliver 92% of malware (Verizon, 2018).

Cyberwarfare has traditionally been deemed a national security issue, and thus a military issue, but circumstances have changed (Al-Ahmad, 2013). The multiple cases of cyberattack examined with the Cyber-Based View as part of this study, indicate the convergence of global information warfare and corporate information warfare.

Information warfare is *the use of information and communication technologies to achieve a competitive advantage* (Joint Pub 3-13). Cybersecurity has been mischaracterized as a technical problem with a technical solution. At its core, cyberattack is not a technical problem. It is a strategic problem focused on achieving competitive advantage.

Business strategy models of the past, which examine the boundaries of the firm and dynamic capabilities in a Resource Based View are designed for material world enterprises, and fail to maximize performance in the virtual world (Dastikop, 2005).

Speaking about the 2017 NotPetya Ransomware attack at the 2018 World Economic Forum, A.P. Moeller-Maersk chairman, Jim Haggeman Snabe said, “It is time to stop being naive when it comes to cybersecurity. I think many companies will be caught if they are naive. Even size doesn’t help you...The next level of dependency is everything will be digital — all the documents will be digital, the boats will be autonomous and hence the criticality of the infrastructure becomes even more urgent and you cannot overcome with human resilience anymore.” (Tung, 2018).

The emergence of new technologies and resources has generally amplified organizational capacity and generated new business models, and cyber is no exception (Dastikop, 2005). Cyberspace, with its ever growing data streams, data/software/platform as a service business models, autonomous vehicles, and electronic store fronts, offers boundless opportunity, but the very absence of boundaries significantly shifts organizational exposure. “While cybersecurity is a topic of discussion all over the world today – little is heard about broader notions of cyber strategy” (Guzdial 2016, p11).

By deriving, testing, and applying the Cyber-Based View of the Firm, this dissertation set out to explore the broader notions of business strategy by answering the following questions:

1. How do people, machines, and data interact during a cyberattack?

They interact both bilaterally and multilaterally, exploiting an organization’s strategic vulnerabilities in infrastructure and human behavior.

2. How can capturing those interactions enable a firm to build strategic adaptive cyber capabilities?

- Examining successful cyberattacks with the Cyber-Based View showed the critical importance of knowledge in order to build adaptive cyber capability
- Hackers are highly engaged in knowledge sharing to remain agile and adaptable
- Organizations can tap into hacker knowledge to understand and enhance areas of strategic vulnerability to gain strategic competitive advantage

Deriving, Testing, and Applying the Cyber-Based View of the Firm

The Cyber-Based View conceives cyberspace as a multidimensional construct of dynamic bilateral and multilateral interactions amongst its cognitive, informational, and physical aspects. The continuous interaction of the three dimensions facilitates and accelerates cyberattack, which will fail if any one dimension is eliminated.

A comprehensive literature review and broad meta-analysis went well beyond the cybersecurity literature, delving into a broad range of theoretical research examining cyberspace phenomena across a multitude of disciplines. Using a theory testing framework that can be applied to both existing theory and emergent theory, a significant theoretical gap was discovered and bounded, confirming that there is scant theory available to study the nature of the firm in cyberspace.

In order to validate and refine the Cyber-Based View as a forensic tool, to explore how cyberattack has affected an organization, a multi-case study was used in conjunction with a pattern matching technique. The framework was used to conduct “failure

autopsies” of nine successful cyberattacks and develop each event into a qualitative case study.

The nine cyberattacks were selected for analysis by surveying a panel of 12 experts from the cybersecurity practitioner and academic communities. The sample represents the three forms of cyberattack: cyber exploitation, which combines cybercrime and cyberespionage; disruptive cyberattack, and destructive cyberattack (Archer, 2014; Roberds & Schreft, 2008). The various types of attackers: individuals, organized crime gangs/terrorist networks, nation states, and hacktivists, are also represented in the sample.

Public records, media, and academic articles regarding each event were analyzed by coding the data to look for empirical patterns. Multiple types of source material were used in order to triangulate the data, and the iterative process of coding, studying the narratives, and looking for patterns continued until saturation was reached. Once the empirical patterns were identified, the first-order themes were used to develop the nine narrative case studies to capture the events as they unfolded during each cyberattack.

The Significance of the Cognitive Dimension: Adaptive Cyber Capability

In addition to providing evidence of the dynamic interactions between the physical, cognitive, and informational dimensions of the Cyber-Based View, using this framework to investigate a broad sample of cyberattacks revealed evidence of a cognitive pattern related to the evolution of cyberthreat across multiple case studies. Evolving cyberthreat is often characterized individually, such as ransomware trends (Cook, 2018) or phishing trends (Verizon, 2018), but examining multiple case studies of cyberattacks with the Cyber-Based View exposed a very specific growth pattern that occurs over time across multiple events: ***an individual creates a capability, organized crime monetizes that***

capability, and nation states weaponize the capability. Although there are exceptions to this rule, such as the current inability to monetize attacks on industrial control systems, and weapons created within organizations such as the NSA, the pattern is evident when multiple events are examined across time.

An example of this pattern is visible in the Melissa Virus, WikiLeaks, and NotPetya Ransomware case studies. Joseph Popp created (cognitive) the first ransomware (informational) in 1989 and distributed it via floppy disk (physical) at the World Health Organization's AIDS conference (Scott & Spaniel, 2016). The precursors to modern ransomware began in 2005 with fraud applications that could be removed for a fee (Scott & Spaniel, 2016). Fraud applications evolved into monetized ransomware beginning in 2013 (Cook, 2018). The most common approach to installing (implies a physical device) ransomware is the use of a macro virus infected Microsoft Word or Excel document distributed with a phishing email (informational) (Cook, 2018), an approach created in 1999 by David Smith (cognitive) with the *Melissa Virus* (Cluley, 2009; McNamara, 2014).

The Petya ransomware in 2016 evolved the attack vector from encryption of specific file types to encryption of the Master Boot Record, a part of the hard drive which manages the storage location of the operating system (Fruhlinger, 2017; DHS, 2018; Greenberg, 2018). Finally, the *NotPetya ransomware* attack weaponized the Petya Ransomware by integrating the EternalBlue exploit, a vulnerability which was shared through *WikiLeaks* following the Shadow Brokers' cyberattack at the NSA, and the Mimikatz exploit, another vulnerability, which was developed in 2011 by a French security researcher (Greenberg, 2017). Table 15 captures the learning behaviors that have

led to the expansion of cyberthreat, illuminating this pattern of individual invention, criminal monetization, and nation state weaponization that evolves over time across multiple attacks.

Table 15. Adaptive Cyber Capability in the Hacker Community of Practice

Year	Events in Growth of Adaptive Cyber Capability				Source	Learning
	Botnets & DDoS	Twitterbots	WikiLeaks Adoption	Ransomware		
1974	First Denial of Service (DoS) attack, by David Dennis, age 13				Radware, 2018	Individual wrote a program to power off all terminals in a computer laboratory at one time to see if it could be done and what would happen
1989			Floppy Disk Ransomware, by Joseph Popp		Scott & Spaniel, 2016	Individual wrote trojan horse virus and passed it out at the WHO AIDS Conference
March, 1999			Melissa Virus & embedded macro viruses, created by David Smith		Cluley, 2009	Phishing email for circulation of macro virus malware embedded in Microsoft Documents, exposed impacts of denial of service in a global scenario
August, 1999	First Distributed Denial of Service Attack (DDoS)				Radware, 2018	Advanced the 1974 attack by networking machines as “masters” and “daemons” with a tool called “Trinoo”
2001	Botnets used for spam delivery				Fruhlinger, 2018	Botnet introduction
2005			Introduction of Fraud Applications with offer to remove them for a fee		Scott & Spaniel, 2016	Monetization of malware removal, but antivirus software solved this problem
2006			WikiLeaks Created by Julian Assange		Nita, 2014	
April, 2010			Bradley Manning uses WikiLeaks to share stolen		Nita, 2014	Draws attention to WikiLeaks as a prominent location for distribution of stolen information, naming & shaming a nation by hacktivist

	U.S. Gov't Secrets	Stuxnet	Zetter, 2014	First known case of malware to jump an air gap using firm relationships. First known case of malware automatically manipulating industrial control systems and damaging physical devices
2010				
2011	Mimikatz created by Benjamin Delpy	Greenberg, 2018	Infiltration of network servers to gain access to credentials to enter any networked computer	
2013	Twitterbots emerge	Dubbin, 2013	Automated accounts within the Twitterverse can share information on an individual basis	
2013 – 2014	Criminal use of Ransomware Grows 350%	Cook, 2018	Russian attack on Ukraine. Malware designed to encrypt files and demand a ransom for decryption key, monetizes malware in a way not easily defeated by antivirus software	
2013- 2016	Phishing grows over 400%	APWG 2013, 2016	Phishing and weaponized Microsoft Documents used to inject malware, including ransomware and remote access malware	
2015	BlackEnergy3 remote access malware used to manipulate Ukrainian distribution centers and cause power outage, KillDisk malware used to break computers	Lee et al., 2016	Russian attack on Ukraine. Malware used to allow remote access of industrial control systems in the electric power grid to create specific targeted effects.	

2015		Impact Team releases Ashley Madison data over WikiLeaks		Gauthier, 2017	WikiLeaks used for naming & shaming individuals and a company by hacktivists
2016		Petya Ransomware emerges	Hackett, 2017		Instead of encrypting specific file types, this malware encrypts the master boot record, making the entire computer inaccessible
2016		Disclosure of DNC documents	Abramson & Walshe, 2016		
2016		Botnets of Twitterbots emerge and are used to disseminate fake news, propaganda, and direct people to WikiLeaks	Graham, 2017		Botnets were previously used to disseminate spam, then networked for DDoS attacks, now used to network automated Twitter accounts to manipulate public opinion
September, 2016	Mirai IoT botnet created by Paras Jha and shared on Hacker Forum		Fruhlinger, 2018		
October , 2016	Mirai IoT botnet used to launch a DDoS attack against Dyn		Sanger & Penroth, 2016		Mirai IoT botnet created to launch a DDoS attack against a DNS provider and bring down the Internet on the east coast of the U.S.
December, 2016		Industroyer Malware used to attack Ukrainian Transmission Station and cause a blackout	Osborne, 2018		Unlike BlackEnergy3 this malware automates the targeted manipulation and includes four different modules that can tailor the malware to specific electric power infrastructure design
April, 2017	Shadow Brokers release hacker tools stolen from the NSA via WikiLeaks, includes EternalBlue exploit		Palmer, 2017		WikiLeaks becomes a repository for hacker tools

May, 2017		Wannacry Ransomware attack	Reilly, 2017	Ransomware integrated with EternalBlue exploit and weaponized by North Korea, brings down British Healthcare system and many others around the world, thwarted by X when he registers a domain name within the Wannacry code (kill switch)
May, 2017	Mirai IoT botnet used in DDoS attack against the Wannacry killswitch	Wannacry hackers attempt to get malware working by DDoSing killswitch	Hack Read, 2017	Integration of DDoS attack to thwart killswitch to ransomware
June, 2017		NoPetya Ransomware attack	Daneshkhу et al., 2017	Russian attack on Ukraine. Used Petya virus, EternalBlue exploit, Mimikatz exploit, and removed killswitch in Wannacry.
Present	Customized IoT Botnets and DDoS as a Service		Vlajic & Zhou, 2016; Leyden, 2017	Darknet economy monetizes DDoS and IoT botnet services
Present	Twitterbotnets used to disseminate fake news and propaganda		Kropotov & Yarochkin, 2017	Nation States weaponize information and botnets of automated twitter accounts
Present		WikiLeaks continues to be the venue of choice for exposing valuable data	Nita, 2014	
Present		Ransomware as a Service	Archer, 2014	Darknet economy monetizes ransomware services

The Convergence of Corporate and Global Information Warfare

Because the nine case studies provided a broad sample of cyberattacks and cyberattackers across multiple contexts, the elimination of boundaries in cyberspace was clearly visible. Furthermore, the stark absence of boundaries highlighted the convergence of global information warfare with corporate information warfare, placing global organizations of all kinds, whether they be nation states, organized crime gangs, or multinational companies in direct competition with one another – a rivalry for strategic competitive advantage that is revealed when the cognitive dimension is included in the construct of cyberspace.

This is a significant shift from the past. Global information warfare – “war against industries, global economic forces, or against entire countries or states” (Al-Ahmad, 2013, p. 1) is historically the responsibility of nation states. The case studies reveal a clear connection between cybercrime and state action, as evidenced in the cyberthreat evolution pattern across multiple events of individual invention, criminal monetization, and nation state weaponization. In fact, the pervasiveness of cybercrime enables concealment of a host of nation state activities by enabling the outsourcing of cyberattacks to non-attributable third parties (Farwell & Rohozinski, 2011), or the disguising of an act of hybrid warfare as criminal activity.

The NotPetya attack on the Ukraine – appeared to be an ordinary, albeit global, criminal ransomware event (informational) with significant operational and financial impacts (tangible physical outcomes) on companies like Maersk and Merck (cognitive), although it was later determined to be collateral damage from a Russian attack on Ukraine (DHS, 2018; Cimpanu, 2018; Greenberg, 2018; Woo, 2018). China felt entirely

justified in their use of the PLA and private hacking groups (cognitive) to steal Google's source-code (informational) and other technical secrets such as pharmaceutical formulas, bioengineering designs, nanotechnology, and weapons systems (physical) in order to accelerate economic development (Hartnett, 2011). The exploitation of organizational relationships in a vertically networked organization, as with the Stuxnet (informational) injection into the Natanz nuclear facility (physical) through Iranian engineering firms (cognitive) (Zetter, 2014), provides yet another example of nation states in conflict with corporations in order to realize national security goals.

Contributions to Theory

A Novel Definition of Cyberspace

Organizations have been expanding their virtual presence through the introduction of technology, electronic commerce, automation, and digitization. Meanwhile, cyberthreat has changed from curious individuals asking the question, "what would happen if..." to organized groups of criminals, activists, and nation states asking the question, "how can I leverage the access I have to profit, manipulate people, and gain power?" Despite the expansion of digital technologies and the escalation of information warfare, there is currently no strategic view of the firm with which to investigate the repositioning of vast swaths of an organization into the virtual terrain of cyberspace. Thus, this dissertation began with a review of current literature to derive a "Cyber-Based View" of the firm to enable the exploration of the dynamic interactions of cyberspace, concluding that ***cyberspace is comprised of three, interdependent physical, informational, and cognitive dimensions which continuously interact between systems, individuals, and organizations both within and beyond the firm.***

The novelty of this definition lies in the inclusion of a *cognitive dimension*, which includes a firm's individuals and groups responsible for information processing, perception, judgement, creativity, decision making, and knowledge growth. In essence, taking into account how humans access, use, and grow the *informational dimension* with its spectrum of data, information, and information rules (software). Of further note, is the definition of the *physical dimension* as the tangible connections between the material world and the virtual world, including both objects *and outcomes that result from humans engaged in the dynamic change of social structures with their cognitive behaviors.*

Defining the Literature Gap Filled by the Cyber-Based View

The bulk of existing cybersecurity literature falls within the computer science specialty, which focuses on securing the devices and data by attempting to create boundaries in an environment without borders. While information security technologies are necessary, they provide only tactical, technical capabilities, which are an insufficient replacement for firm strategy to gain competitive advantage. Although a wide range of academic disciplines have explored the cognitive – informational interaction, how modes of information delivery affect this cognitive – informational link is limited to information security research in the information systems and computer science communities.

Competing discourses (Jorgensen, 2016) – the competition to control both the data and the narrative – is also evident in the literature that examines the cognitive – informational interaction. Unfortunately, the investigation of how tools are used to manipulate and control the informational dimension, and by extension, the cognitive dimension, is restricted to the computer science community, which proposes technical solutions for what is inherently a human challenge.

This examination of existing theory further revealed a lack of available theory to illuminate the simultaneous bilateral and multilateral interactions amongst the physical – informational – cognitive dimensions of cyberspace. For example, the use of the people – process – technology model to address data loss in business operations uses a resource based view, with human resources, technology resources, and capabilities (Cotescu, 2016). This RBV of people, process, and technology is buttressed by the Cyber-Based View, which separates the physical and informational aspects of the technology resources, and further dissects process into the interactions between cognitive processing of data and information (informational) through the use of tools (physical), providing additional insight into how the cognitive, informational, and physical dimensions are interacting.

The introduction of a multilateral interaction between people, information, and the physical devices that mediate information delivery is a fresh approach to the cybersecurity dilemma. Although there is ample research investigating the bilateral interactions between these three dimensions, there is no theory that looks at the multilateral and simultaneous bilateral interactions taking place. This study contributes to the existing literature by shaping that gap, and introduces a Cyber-Based View of the firm to fill this theoretical void and complement the institutional-based resource-based, and knowledge-based views of the firm common to strategy literature.

Generalizability of the Cyber-Based View

Applying a pattern matching technique to the empirical patterns in the nine case studies revealed evidence of the propositional patterns. Although the specific physical, informational, and cognitive elements engaged in dynamic bilateral and multilateral

interactions were different for each case, the propositional patterns were evident in each case study. The breadth of the sample group across the various types of cyberattack and types of attackers further supports the generalizability and the utility of the Cyber-Based View framework.

For example, after the school shooting in Parkland, FL, a tangible event (physical), hackers working on behalf of the Russian nation state created (cognitive) propaganda and information rules for Twitterbots to automatically circulate the propaganda (informational) designed to make Americans angry in order to influence their decision making behaviors (cognitive) related to tangible legal controls relating to guns and gun ownership (physical) (Baraniuk, 2018). This is a very different type of attack from the Ukrainian blackouts, where flexible information rules functioning as interchangeable components (informational) were created by the hackers in order to enable them to change and tailor their attack tactics and techniques (cognitive) to different tangible electric utility equipment environments (physical) (Greenberg, 2017), and yet the dynamics of the Cyber-Based View are evident in both events.

In each of the previous instances, the attacker was the Russian nation state, but the same pattern is evident in the Mirai Internet of Things botnet, which was created by a college student (cognitive) for the purpose of driving Minecraft traffic (informational) to his game hosting server (physical) (Fruhlinger, 2018). The student made the decision to post (cognitive) to a cybercrime information-sharing forum the set of information rules comprising the Mirai malware, which connects (informational) tangible Internet connected devices such as video recorders or CCTV systems (physical) (Mansfield-Devine, 2016, Fruhlinger, 2018). His decision to create and then share the malware led its

use in a Distributed Denial of Service attack against Dyn, a company that supports Internet infrastructure with Domain Name Server hosting services, bringing down the Internet in much of the Eastern United States (Perlroth, 2016; Sanger & Perlroth, 2016).

From an academic perspective, this adds a new theoretical tool for examining the dynamics at work during a cyberattack. This in turn, enables the development of better game theory models, social engineering models, and other research algorithms. Integrating the human behavior and the need for information to be physically mediated for consumption provides greater insight related to how the human fits into the cyberspace environment as a vulnerable piece of the ecosystem.

New Evolutionary Pattern of Cyberthreat Revealed by the Cyber-Based View

Applying the Cyber-Based View of the Firm in this study revealed a new pattern in the evolution of cyberthreat over time across multiple events: individuals create a capability, criminals monetize that capability, and nation states weaponize it. There are exceptions to this pattern, such as tools created by the NSA or the current inability for criminals to monetize attacks on industrial control systems, but the learning is still evident, even in these contexts, for example the increase in automation between BlackEnergy3 malware used to attack the Ukrainian power grid in 2015 and the Industroyer malware used to attack the Ukrainian power grid in 2016 (Zetter, 2017; Lee et al., 2016; Harrell, 2017; Greenberg, 2017; Park et al., 2017; Huang et al., 2018; Osborne, 2018). Although popular opinion conceives of hacking and cybercrime as anonymous activity taking place in cyberspace (Lusthaus & Varese 2017), this ordered growth of cyberthreat shows evidence of a hacker community of practice – “groups of experts who share a common interest or topic and collectively want to deepen their

knowledge" (Paasivaara & Lassenius, 2014, p. 1556), an insight gleaned by examining the interactions of the cognitive, physical, and informational dimensions within the Cyber-Based View.

The identification of this pattern in cyberthreat evolution firmly illustrates the opportunistic and strategic nature of cyberthreat and opens new avenues of inquiry for the development of threat prediction models, going well beyond the statistical growth of malware. Capturing the knowledge growth patterns within the hacker community of practice also provides a model for the study of adaptive cyber behavior, which could be used to develop adaptive cyber capabilities in support of firm strategies.

Corporations and Nation States Become Competitive Rivals

Finally, the Russian NotPetya disruptive cyberattack and the U.S. – Israeli Stuxnet destructive cyberattack provide clear evidence of the convergence of global and corporate information warfare because of the absence of boundaries in the cyberspace realm which resulted in the malware from both attacks affecting private industry in locations across the globe, well outside the target area. Applying the Cyber-Based View to multiple cyberattacks highlights the emergence of the multinational company as one of several entities engaged in a strategic global rivalry for competitive advantage. Furthermore, the rise of hybrid warfare, which combines conventional military and special operations with information warfare (Park et al., 2017) highlights the need for theoretical research to understand the strategic impact to organizations due to the inevitable fallout and collateral damage from a cyberattack unbounded by geography.

Contributions to Practice

Characterizing Cyberattack

The threat of cyberattack is often misunderstood by organizations' top management. It is important to include the interaction of the cognitive dimension with the physical and informational dimensions when examining cyberspace, otherwise cyber vulnerabilities can be mischaracterized as just a technology problem, when it is really a strategic competitive advantage problem. Examining the physical, informational, and cognitive dimensions and the bilateral and multilateral interactions amongst these dimensions provides new insights related to cyberthreat.

- Cyberthreat is *increasing at an exponential rate* consistent with the speed of technological change.
- Cyberthreat is *increasing because of knowledge sharing* in the hacker community.
- Hackers are highly agile, adapting their behavior to respond to changes in the cyberspace environment to gain and maintain a competitive advantage.
- Cyberthreat follows a specific growth pattern where one set of individuals create a capability, followed by criminals who monetize that capability, followed by nation states that figure out how to weaponize that capability to achieve global power.

A Tool to Examine Tradeoffs to Achieve Competitive Advantage

The Cyber-Based View is not intended to be a tactical tool for cybersecurity. From a practitioner perspective, this investigation bridges the gap between theory and application by providing ***a lens that can be applied to generate strategic advantage and to expose vulnerabilities*** by examining the synergy created amongst the physical,

cognitive, and informational dimensions of cyberspace, aiding in the development of strategic adaptive cyber capabilities. By using the Cyber-Based View to explore the dynamic interactions amongst the physical, informational, and cognitive that are created with digitalization, enhanced decision making, and process automation, this perspective can be used in tradeoff analyses related to the implementation of technological solutions, training programs, and human resources.

For example, from a capability perspective the Cyber-Based View can justify the value of employing wireless medical devices and closed circuit TV monitors, both elements of the physical dimension, in nursing homes to enable seniors to maintain their independence (Mortenson et al., 2015) because the devices send healthcare data to the medical decision makers (informational and cognitive elements). The Cyber-Based View can also reveal vulnerabilities that puts seniors at risk because of the use of these technologies in nursing homes, for example if the networked devices fail, such as an insulin device (physical) with corrupted data (informational) or when cybercriminals gain access (cognitive) to the information about patients daily routines, enabling that information to be exploited for criminal enterprises. By highlighting both the capabilities generated and the vulnerabilities created, the Cyber-Based View can enable better tradeoff analyses.

One of the reasons that current cybersecurity approaches are tactical, is that the early theoretical literature examined only the bilateral physical – informational interaction. More recent literature examines two or three bilateral interactions, which is facilitating movement toward more operational cyber defense strategies. The Cyber-Based View

framework provides a macro view revealing the multilateral interactions taking place, such as the example above regarding seniors living independently.

From a practitioner perspective, having the proper tool to explore a cyberattack in a victimized firm will enable a more comprehensive approach to remediation strategies. The Cyber-Based View can highlight vulnerabilities. Current tools explore only those elements of the physical and informational elements in a firm, but few remediation strategies address the cognitive and cultural elements of organizational security. The use of the Cyber-Based View tool will highlight the role played by the various actors in the cognitive dimension. This in turn, will enable the creation of new training programs and internal processes to address vulnerabilities that result from the human element. Further, as the Cyber-Based View begins to reveal patterns through employment as a forensic tool, it can begin to identify common vulnerabilities that are created by traditional information technology strategies, introduction of new technologies, and specific organizational behaviors. Understanding these vulnerabilities is the first step to developing defense and remediation strategies.

Although it was not the focus of this study, there was evidence of how the Cyber-Based View might be used to explore revenue generating capabilities. For example, an analysis of the Ashley Madison attack revealed that Avid Life Media used “fembots” – accounts automated by a set of information rules which sent sexy messages (informational) to entice male users to spend (cognitive) their financial resources (physical) in order to engage in conversation with what they thought were real women (cognitive) (Tuttle, 2015; Gauthier, 2017). Twitterbots, which are also accounts automated by a set of information rules (informational) are regularly used by

organizations to drive consumers (cognitive) to website storefronts (informational) in an effort to drive purchasing decisions (cognitive) resulting in product sales (physical) (Wojcik, 2018; Hirsch, 2017; Confessore et al., 2018; Dubbin, 2013; Timberg & Dwoskin, 2018; Edwards et al., 2016). Finally, the NotPetya Ransomware event halted operations at Maersk ports because the ships and the port computer systems (physical) could not exchange the data (informational) used by the people responsible for decision making related to loading and unloading (cognitive) the cargo from ships (physical) (Greenberg, 2018; Ryan, 2017; Asia News Monitor, 2017; Daneshkhu et al., 2017), highlighting how this operational, revenue generating capability hinges on the multilateral interactions of the Cyber-Based View construct.

Organizations Need to Engage in Continuous Learning Related to Cyberspace

Cyberattack cannot be prevented. The most an organization can do is to become agile and adaptive in order to limit the breadth of the impact. ***In order to become agile and adaptive, organizations must be able to assess their own vulnerabilities. The Cyber-Based View is a new tool to make this assessment.*** An adaptive cyber strategy integrates multiple capabilities within the full spectrum of a firm's operations (Schwartz & Schuff, 2018). The nature of the cyber firm is contextual, with every activity increasingly driven by knowledge, and in need of a knowledge interaction interface (Dastikop, 2005). Because cyberthreat has a visible pattern of evolution, cyberattacks can be anticipated with the right knowledge capabilities. CIOs and CISOs need to ask questions of their staff such as:

- What is the technical skill level of our staff related to state-of-the-art hacking abilities?

- What are we doing to maintain and grow our hacking skills, for example who are we sending to the *Black Hat Conference*?
- What resources are we using to maintain knowledge and awareness of the latest attack vectors and hacker exploits?
- What are the top ranked open source software security communities, and in which ones are we participating? (for example OWASP)
- What are the current top 10 vulnerabilities being identified in these open source communities?

There is a need for business intelligence in order to achieve competitive advantage against rivals in cyberspace. Just as an organization develops specific business intelligence for competition in a hostile marketplace (Caltone et al., 1997), firms need people who develop the strategy for competition in the hostile cyber domain, in other words, firms need people who can think like hackers. As the following story explains, there is not a shortage of technical solutions, there is a shortage of strategic operational knowledge.

During the survey of cyberattacks, one of the panel experts observed that the Shadow Brokers hack of the NSA and subsequent release of the various exploits through WikiLeaks would likely to lead to other cyberattacks. Several months later, in early 2019, this panel expert was contacted by a client who was victimized by the EternalBlue exploit – the same exploit that was shared through WikiLeaks in April 2017 and weaponized in both the WannaCry ransomware attack in May 2017 and the NotPetya ransomware attack in June 2017 (Tung, 2017; DHS, 2018; Fruhlinger, 2017; Greenberg, 2018; Hackett, 2017; Osborne, 2017). Microsoft offered patch MS17-010 in March 2017 when they were

notified of the stolen exploit by the NSA (Fruhlinger, 2017; Hackett, 2017), but despite the available patch and the fact that all three events were well publicized, making the national news cycle, the client had no knowledge of this threat. The client's staff possessed all the industry standard certifications and prided themselves on their technical expertise, but despite all their training, they were missing critical strategic operational knowledge.

Think Like a Hacker – The Knowledge is Accessible

The evolutionary pattern of individual invention, criminal monetization, and nation state weaponization, which emerges over time across multiple events, reveals critical knowledge transfer in the hacker community of practice, and this information is available to anyone – according to the panel expert, he found the source code for the attack his client experienced on Github. ***Organizations must make cybersecurity a strategic priority. They must have people dedicated to the acquisition of this knowledge for the purposes of gaining a competitive advantage in cyberspace.*** The purpose of adding operational expertise to the cyber strategy team is not to have someone warning that the sky is falling, but rather to have deep expertise in how transformative technologies can be used by both the firm and the hacker community. Hackers are constantly changing their behaviors to achieve competitive advantage, an adaptive behavior fed by the robust knowledge sharing within the community. The way to defend against new cyberattack techniques is to follow and incorporate the widely shared information within the hacker communities about new attack methods. ***Organizations can grow their own adaptive cyber capabilities by learning from and emulating the knowledge and agility of the hacker community.***

Table 16. Takeaways for Top Management

Takeaways	Implications
Cyberthreat has been mischaracterized as a technical problem, when it is really <i>an issue of strategic competitive advantage</i> .	Cyberattack cannot be prevented, and cyberthreat will continue to expand because of the exponential rate of technological change and the continuous learning behaviors of hackers.
Organizations must engage in continuous learning to be aware of the latest cyberthreats and hacker exploits	CIOs/CISOs should be asking their staff: <ul style="list-style-type: none"> • What resources are we using to maintain knowledge and awareness of the latest attack vectors and hacker exploits? • What are the top ranked open source software security communities, and in which ones are we participating? (for example OWASP) • What are the current top 10 vulnerabilities being identified in these open source communities?
Organizations must learn to think and behave like hackers	CIOs/CISOs should be honing their organizations' skills and asking: <ul style="list-style-type: none"> • What is the technical skill level of our staff related to state-of-the-art hacking abilities? • What are we doing to maintain and grow our hacking skills, for example who are we sending to the Black Hat Conference?

Without Boundaries, Understanding Hybrid Warfare is Critical

Hybrid warfare, being perfected by Russia in the Ukraine is a foreshadowing of what's to come in the cyber realm (Park et al., 2017). The spread of the NotPetya ransomware that caused financial damages in excess of \$10 billion in numerous industries, including the pharmaceutical, transportation, and manufacturing industries, began in the Ukraine (Greenberg, 2018). The 2015 Ukrainian blackout required human operation of the industrial control systems through the use of remote access malware, but the 2016 Ukrainian blackout automated the operation of the industrial control systems and added an agile reconfiguration capability to the Industroyer malware that threatens both privately owned and state owned critical infrastructure companies all over the world (Greenberg, 2017; Park et al., 2017; Huang et al., 2018; Osborne, 2018).

In the past companies could count on their national governments to keep them safe. In the age of the Internet, this is no longer the case. As companies amass power that puts them on equal footing with nation states, it also engages them in the rivalry for power on the global stage, particularly in cyberspace. Physical distance and national borders are irrelevant, and governments cannot protect organizations from attack. This global information warfare between nation states has become inseparable from information warfare between corporate competitors. Living in a world of constant information warfare demands that top management teams need to maintain awareness of significant cyberattacks and their impact in order to remain competitive in the cyber landscape.

Table 17. Three Cyberattacks Every CEO/CIO/CISO Should Know About

Cyberattack	Significance
The Shadow Brokers	Hacking tools and exploits stolen from the NSA and released through WikiLeaks by a cybercrime gang suspected of Russian origin. Many of the exploits have patches and other remediations available, but they are still being used successfully.
(Not)Petya Ransomware Attack	A cyberattack that began as an act of hybrid warfare when Russia attacked Ukraine. The absence of boundaries in cyberspace sent this attack global (using exploits from the Shadow Brokers), impacting firms like Maersk (\$300M) and Merck (\$800M) with huge operational impacts, such as shutting down 20% of the global shipping industry.
Mirai Botnet	The mirai botnet software infects a multitude of devices connected to the internet, creating “internet of things botnets” which are used to launch distributed denial of service attacks (DDoS) attacks. Organizations should be aware of how these attacks work, and they should be asking: how are we protecting mission critical services applications from DDoS attacks?

With organizations positioning significant organizational key terrain in cyberspace – the phenomenon of becoming cyborg – the need for companies to be able to see themselves through a Cyber-Based View is imperative.

Study Limitations and Future Research

This dissertation was limited to the examination of the Cyber-Based View as a forensic tool. The dynamics of the Cyber-Based View will become yet more valuable if it can be validated in a predictive and/or preventive capacity. Subsequent action research could explore the utility of the Cyber-Based View as it relates to the development of a dynamic adaptive cyber capability by using the Cyber-Based View to identify firm vulnerabilities and new opportunities for digital strategies.

Although this study was limited to a sample size of nine case studies, the emergence of a threat evolution pattern from individual invention, to criminal monetization, to nation state weaponization, suggests that the Cyber-Based View can be used to highlight other interesting phenomena for study, specifically because of the cognitive dimension. The theoretical lens of the Cyber-Based View sheds light on the hacker community of practice and the knowledge sharing that enables a dynamic cyber capability. Because this study was limited to the validation of the theoretical model, the illumination of a dynamic, adaptive cyber capability in the hacker community offers new avenues of research to develop this strategic capability within the firm.

According to a 2016 report by McKinsey Global Institute, Globalization is entering “a new phase defined by soaring flows of data and information. [These] digital flows—which were practically nonexistent just 15 years ago—now exert a larger impact on GDP growth than the centuries-old trade in goods” (Manyika et al, 2016). Following the NotPetya ransomware attack, Maersk’s chairman, speaking at the 2018 World Economic Forum, said, “It was an important wake-up call. We were basically average when it comes to cybersecurity, like many companies. And this was a wake-up call to become not

just good —we actually have a plan to come in a situation where our ability to manage cybersecurity becomes a competitive advantage” (Cimpanu, 2018). Adaptive cyber capability is about value creation and competitive advantage, calling for deep knowledge and business intelligence to compete in a hostile environment, demanding a Cyber-Based View of the Firm as a necessary tool for developing firm strategy in the digital economy.

REFERENCES

- (1999). Lawyer Likens the Melissa Virus to Graffiti. *The New York Times*, 9 Apr 1999, pB2.
- (1999). Melissa Virus Defendant to Plead Not Guilty. *The New York Times*, 7 Apr 1999, p. B7.
- (2002). Creator of Melissa Virus Gets 20 Months in Jail. *The New York Times*, 2 May 2002, p. B8.
- (2002). No Extra Jail Time For Man Sentenced in Melissa Virus. *The New York Times*, 4 May 2002, p.B4
- (2013). The Most Famous Virus in History. *PandaSecurity.com*. Retrieved 5 Jan 19 from: <https://www.pandasecurity.com/mediacenter/malware/most-famous-virus-history-melissa/>.
- (2017). Denmark: Cyberattack Stops Shipper Maersk Taking New Orders, Causes Delays. *Asia News Monitor*. Retrieved 15 Dec 2018 from: <https://search.proquest.com/docview/1914566092?accountid=14270>.
- (2017). Hackers Trying to Bring Back WannaCry Attacks by DDoSing its KillSwitch. HackRead.com. Retrieved 16 February 2019 from: <https://www.hackread.com/wannacry-killswitch-ddos-via-mirai-botnet/>.
- (2017). History of DDoS Attacks. *Radware Website*. Retrieved 16 February 2019 from: <https://security.radware.com/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/>.
- (2017). IoT_Reaper: A Rapid Spreading New IoT Botnet. *NetLab Website*. Retrieved 11 Jan 2019 from: http://blog.netlab.360.com/iot_reaper-a-rapid-spreading-new-iot-botnet-en/.
- (2017). Securing Your Routers Against Mirai and Other Home Network Attacks. *Trendmicro.com*. Retrieved 11 Jan 2019 from: <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-routers-against-mirai-home-network-attacks>.
- (2017). Shadow Puppets: Russian Meddling in Europe. *The Economist*, 423(9036), 44.
- (2017). Ukraine Power Cut 'Was Cyber-Attack.' *BBC News*. Retrieved 17 Jan 2019 from: <https://www.bbc.com/news/technology-38573074>.

- (2018). New Rapidly-Growing IoT Botnet - Reaper. *Trendmicro.com*. Retrieved 11 Jan 2019 from: <https://success.trendmicro.com/solution/1118928-new-rapidly-growing-iot-botnet-reaper>.
- (2019). Technology Dictionary: What Does Melissa Virus Mean? *Techopedia.com*. Retrieved 5 Jan 19 from: <https://www.techopedia.com/definition/15808/melissa-virus>.
- Aaron, G. and Manning, R. (2013). *APWG Phishing Activities Trends Report, 2nd Quarter 2013*. Retrieved 22 February 2019 from: http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf.
- Aaron, G. and Manning, R. (2016). *APWG Phishing Activities Trends Report, 2nd Quarter 2016*. Retrieved 22 February 2019 from: http://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf.
- Abramson, A. and Walshe, S. (2016). The 4 Most Damaging Emails from the DNC WikiLeaks Dump. *abc News Website*. Retrieved 18 February 2019 from: <https://abcnews.go.com/Politics/damaging-emails-dnc-wikileaks-dump/story?id=40852448>.
- Adamczyk, E. (2017). December Power Outage in Kiev was Cyberattack, Investigators Say. *UPI News Current, 11 Jan 2017*. Retrieved 17 Jan 2019 from: http://link.galegroup.com/apps/doc/A477113860/ITOF?u=temple_main&sid=ITOF&xid=10517ad2.
- Ahmed, M., Mahmood, A., and Hu, J. (2016). A Survey of Network Anomaly Detection Techniques. *Journal of Network and Computer Applications, 60*, 19-31.
- Al-Ahmad, W. (2013). A Detailed Strategy for Managing Corporation Cyber War Security. *International Journal of Cyber-Security and Digital Forensics, 2(4)*, 1-9.
- Aleroud, A. and Karabatis, G. (2017). Contextual Information Fusion for Intrusion Detection: A Survey and Taxonomy. *Knowledge Information Systems, 52*, 563-619.
- Alexy, O., George, G., and Salter, A. (2013). Cui Bono? The Selective Revealing of Knowledge and Its Implications for Innovative Activity. *Academy of Management Review, 38(2)*, 270-291.
- Al-Muhtadi, J. (2017). Misty Clouds – A Layered Cloud Platform for Online User Anonymity in Social Internet of Things. *Future Generation Computer Systems, 40*, 1-9.
- Almutairi, A.F., Gardner, G.E., and McCarthy, A. (2014). Practical Guidance for the Use of a Pattern-Matching Technique in Case Study Research: A Case Presentation. *Nursing & Health Sciences, 16*, 239-244.

- Alnuaimi, T. and George, G. (2016). Appropriability and the Retrieval of Knowledge After Spillovers. *Strategic Management Journal*, 37, 1263-1279
- Ambs, K. et al. (2000). Optimizing Restoration Capacity in the AT&T Network. *Interfaces*, 30 (1), 26-44.
- Amin, S.M. (2015). Power and Energy Infrastructure: Cyber Security, Defense, and Resilience. *Georgetown Journal of International Affairs*, Fall 2015, 70-82.
- Angst, C. et al. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly*, 41(3), 893-916.
- Anonymous. (2015). An Affair to Remember: The Ashley Madison Hack. *The Economist*, 416, 14-17.
- Anonymous. (2015). How We Cracked Millions of Ashley Madison bcrypt Hashes Efficiently. *CynoSure Prime Blogsite*. Retrieved online 26 November 2018: <https://blog.cynosureprime.com/2015/09/how-we-cracked-millions-of-ashley.html>.
- Anonymous. (2015). Tech Analyst on Ashley Madison Hack: 'Internet Security is an Oxymoron - It Does Not Exist. *ICT Monitor Worldwide*. Retrieved online 26 November 2018: http://link.galegroup.com/apps/doc/A422451281/ITOF?u=temple_main&sid=ITOF&xid=7f516479.
- Anonymous. (2017). A Dating Site and Corporate Cyber-Security Lessons to Be Learned. *Panda Security Website*. Retrieved online 26 November 2018: <https://www.pandasecurity.com/mediacenter/security/lessons-ashley-madison-data-breach/>.
- Aragon-Correa, J. and Sharma, S. (2003). A Contingent Resource Based View of Proactive Corporate Environmental Strategy. *Academy of Management Review*, 28 (1), 71-88.
- Archer, E.M. (2014). Crossing the Rubicon: Understanding Cyber Terrorism in the European Context. *The European Legacy*, 19(5), 606-621.
- Argote, L. and Fahrenkopf, E. (2016). Knowledge Transfer in Organizations: The Roles of Members, Tasks, Tools, and Networks. *Organizational Behavior and Human Decision Processes*, 136, 146-159.
- Armental, M. (2015). Russian Man Admits to Conspiring to Hack Nasdaq, Others. *Dow Jones Institutional News*. Retrieved 21 Jan 2019 from: <https://search.proquest.com/docview/2064021296?accountid=14270>.

Arquilla, J., and Ronfeldt, D. (1999). *The Emergence of Noopolitik: Toward an American Information Strategy*. Santa Monica, CA: National Defense Research Institute-RAND.

Arvanitidis, T. (2016). Publication Bans in a Facebook Age: How Internet Vigilantes Have Challenged the Youth Criminal Justice Act's "Secrecy Laws" Following the 2011 Vancouver Stanley Cup Riot. *Canadian Graduate Journal of Sociology and Criminology*, 5(1), 18-32.

Associated Press. (2013). Bradley Manning: 25 Years in Prison? Or 60? *USA Today*. Retrieved 7 Jan 19 from:
<https://www.usatoday.com/story/news/nation/2013/08/19/bradley-manning-wikileaks/2674457/>.

Associated Press. (2013). Key Dates in the Case of WikiLeaks Source Chelsea Manning. *APNews.com*. Retrieved 7 Jan 19 from:
<https://www.apnews.com/b6a31ec6aee74f7bb972e579af0e64ac>.

Balzacq, T. and Covely, M.D. (2016). A Theory of Actor-Network for Cyber-Security. *European Journal of International Security*, 1(2), 176-198.

Bannard, C., Rosner, M., and Matthews, D. (2017). What's Worth Talking About? Information Theory Reveals How Children Balance Informativeness and Ease of Production. *Psychological Science*, 28(7), 954-966.

Bansal, P. (2003). From Issues to Actions: The Importance of Individual Concerns and Individual Values in Responding to Natural Environmental Issues. *Organizational Science*, 14(5), 510-527.

Baraniuk, C. (2018). How Twitter Bots Help Fuel Political Feuds. *Scientific American*. Accessed online 8 Nov 2018: <https://www.scientificamerican.com/article/how-twitter-bots-help-fuel-political-feuds/>.

Barnard, S. (2016). 'Tweet or Be Sacked': Twitter and the New Elements of Journalistic Practice. *Journalism*, 17(2), 190-207.

Basu, E. (2015). Cybersecurity Lessons Learned From the Ashley Madison Hack. *Forbes*. Retrieved online 26 November 2018:
<https://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/#90819af4c82b>.

Baudry, B. and Chaussagnon, V. (2012). The Vertical Network Organization as a Specific Governance Structure: What Are the Challenges for Incomplete Contracts Theories and What Are the Theoretical Implications for the Boundaries of the (Hub-) Firm? *Journal of Management & Governance*, 16, 285-303.

- Beekman, D. (2013). Hacker Hit Companies Like Nasdaq, 7-Eleven for \$300 Million, Prosecutors Say. *NY Daily News*. Retrieved 21 Jan 2019 from: <https://www.nydailynews.com/news/national/russians-ukrainian-charged-largest-hacking-spree-u-s-history-article-1.1408948>.
- Behal, S. and Kumar, K. (2017). Detection of DDoS Attacks and Flash Events Using Novel Information Theory Metrics. *Computer Networks*, 116, 96-110.
- Belanger, F. et al. (2017). Determinants of Early Conformance with Information Security Policies. *Information & Management*, 54, 887-901.
- Bennett, H. (Executive Producer) and Johnson, K. (Producer). (1973-1978). *The Six Million Dollar Man*. Los Angeles, CA. American Broadcasting Corporation.
- Benoit, S. et al. (2016). Explaining Social Exchanges in Information-Based Online Communities (IBOCs). *Journal of Service Management*, 27(4), 460-480.
- Berghel, H. (2012). WikiLeaks and the Matter of Private Manning. *Computer, March 2012*, 70-73.
- Berman S. and Marshall, A. (2014). The Next Digital Transformation: From an Individual-Centered to an Everyone-to-Everyone Economy. *Strategy & Leadership*, 42 (5), 9-17.
- Beresford, A. (2003). Fouault's Theory of Governance and the Deterrence of Internet Fraud. *Administration & Society*, 35(1), 82-103.
- Bharadwaj, A. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly*, 24(1), 169-196.
- Booth, R., Brooke, H., and Morris, S. (2010). WikiLeaks Cables: Bradley Manning Faces 52 Years in Jail. *The Guardian*. Retrieved 7 Jan 19 from: <https://www.theguardian.com/world/2010/nov/30/wikileaks-cables-bradley-manning>.
- Bordalo, P., Gennaioli, N. and Shleifer, A. (2010). Salience Theory of Choice Under Risk. *Quarterly Journal of Economics*, 127(3), 1243-1285.
- Bourreau, M. et al. (2012). "Selling Less of More?" The Impact of Digitization on Record Companies. *Journal of Cultural Economics*, 37, 327-346.
- Bray, C. (2013). Nasdaq, Others, Targeted by Hackers; Data Breach Resulted in 'Hundreds of Millions' of Dollars in Losses. *Wall Street Journal*. Retrieved 21 Jan 2019 from: <https://search.proquest.com/docview/1413183541?accountid=14270>.

- Bray, C. and Yadron, Y. (2013). Nasdaq, Others, Targeted by Hackers. *Dow Jones Institutional News*. Retrieved 21 Jan 2019 from:
<https://search.proquest.com/docview/2092682026?accountid=14270>.
- Brecher, A.P. (2012). Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations. *Michigan Law Review*, 111(3), 423-452.
- Bressler, M.S. and Bressler, L. (2015). Protecting Your Company's Intellectual Property Assets from Cyber-Espionage. *Journal of Legal, Ethical, and Regulatory Issues*, 18(1), 21-34.
- Bronco, M. and Rodrigues, L. (2006). Corporate Social Responsibility and Resource Based Perspectives. *Journal of Business Ethics*, 69, 111-132.
- Brown, C. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 9 (1), 55-119.
- Bruce, C., S. Hick, & J. Cooper. (Eds.). (2004). Exploring crime analysis: Readings on essential skills. (2nd ed.). North Charleston, South Carolina: BookSurge, LCC.
- Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: an Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34(3), 523-548.
- Bumiller, E. (2010). Army Leak Suspect is Turned in, by Ex-Hacker. *The New York Times*. Retrieved 7 Jan 19 from:
<https://www.nytimes.com/2010/06/08/world/08Leaks.html>.
- Burmester, M., Magkos, E., and Chrissikopoulos, V. (2012). Modeling Security in Cyber-Physical Systems. *International Journal of Critical Infrastructure Protection*, 5, 118-126.
- Byrne, M. (2014). Lawrence English's 'Wilderness of Mirrors': A Cold War Truth in Dark Drones: A Favorite Saying from the Dawn of Domestic Surveillance Finds Sonic Life. *Motherboard*. Retrieved 4 Jan 19 from:
https://motherboard.vice.com/en_us/article/ae334b/lawrence-englishs-wilderness-of-mirrors-a-cold-truth-in-ambient-darkness.
- Cadwalladr, C. (2018). Interview: "I Spent Seven Years Fighting to Survive": Chelsea Manning on Whistleblowing and WikiLeaks. *The Guardian*. Retrieved 7 Jan 19 from: <https://www.theguardian.com/us-news/2018/oct/07/chelsea-manning-wikileaks-whistleblowing-interview-carole-cadwalladr>.

- Calori R. et al. (1997). Modelling the Origins of Nationally-Bound Administrative Heritages: A Historical Institutional Analysis of French and British Firms. *Organization Science*, 8 (6), 681-696.
- Caltone, R., Schmidt, J. and DiBenedetto, A. (1997). New Product Activities and Performance: The Moderating Role of Environmental Hostility. *Journal of Product Innovation Management*, 14, 179-189.
- Cappelli, D., Moore, A., and Trzeciak, R. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. New York: Pearson Education Inc.
- Carlo, J., Lyytinen, K. and Boland, J. (2012). Dialectics of Collective Minding: Contradictory Appropriations of Information Technology in a High-Risk Project. *MIS Quarterly*, 36(4), 1081-1108.
- Cavusoglu, H., Raghunathan, S. and Yue, W. (2008). Decision-Theoretic and Game Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, 25(2), 281-304.
- Cavusoglu, H., Raghunathan, S., and Cavusoglu, H. (2009). Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. *Information Systems Research*, 20(2), 198-217.
- Cecez-Kecmanovic, D. et al. (2014). The Sociomateriality of Information Systems: Current Status, Future Directions. *MIS Quarterly*, 38(3), 809-830.
- Cerullo, V. and Cerullo, M. (2006). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management*, 21(3), 70-78.
- Ceruzzi, P. (2005). Moore's Law and Technological Determinism: Reflections on the History of Technology. *Technology and Culture*, 46(3), 584-593.
- Chan, M. (2017). What to Know about Chelsea Manning as Whistleblower Is Released from Prison. *Time*. Retrieved 7 Jan 19 from: <http://time.com/4768943/chelsea-manning-release-prison/>.
- Chatterji, A. and Fabrizio, K. (2012). How Do Product Users Influence Corporate Invention? *Organization Science*, 23(4), 971-987.
- Chen, A., Hwang, Y., and Raghu, T. (2010). Knowledge Life Cycle, Knowledge Inventory, and Knowledge Acquisition Strategies. *Decision Sciences*, 41(1), 21-47.
- Chen, H., Beaudoin, C., and Hong, T. (2017). Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors. *Computers in Human Behavior*, 70, 291-302.

- Chen,P., Len, D., and Yin, S. (2015). The Classification of Information Assets and Risk Assessment: An Exploratory Study Using the Case of C-Bank. *Journal of Global Information Management*, 23(4), 26-54.
- Chen, P., Kataria, G., and Krishnan, R. (2011). Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quarterly*, 35(2), 397-422.
- Cheng, K. (1999). Melissa Virus Spooks Users. *Brandweek*, 13 Sep 1999, p 40.
- Cheong, P. and Gong, J. (2010). Cyber Vigilantism, Transmedia Collective Intelligence, and Civic Participation. *Chinese Journal of Communication*, 3(4), 471-487.
- Cherner, L. (2017). None of Your Business: Protecting the Right to Write Anonymous Business Reviews Online. *Columbia Journal of Law & the Arts*, 40, 471-501.
- Chirgwin, R. (2016). Hacked Hookup Site Ashley Madison's Security Was Laughable: Canadian and Australian Privacy Watchdogs Bite, Hard. *The Register*. Retrieved online 26 November 2018:
https://www.theregister.co.uk/2016/08/24/canada_oz_privacy_watchdogs_bite_ashley_madison/.
- Chirgwin, R. (2018). IT 'Heroes' Save Maersk from NotPetya with Ten-Day Reinstallation Bliz. *The Register*. Retrieved 15 Dec 2018 from:
https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/.
- Choo, K. (2011). The Cyber Threat Landscape: Challenges and Future Research Directions. *Computers and Security*, 30, 719-731.
- Chopping, D. (2017). Fallout From Global Cyberattack Extends Into Second Day. *Dow Jones Institutional News*. Retrieved 15 Dec 2018 from:
<https://search.proquest.com/docview/1914399316?accountid=14270>.
- Christin, D., Mogre P. and Hollick, M. (2010). Survey on Wireless Sensor Network Technologies for Industrial Automation: The Security and Quality of Service Perspectives. *Future Internet*, 2, 96-125.
- Cimpanu, C. (2018). Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack. *Bleeping Computer*. Retrieved 15 Dec 2018 from:
<https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/>.
- Clinton, L. (2011). A Relationship on the Rocks: Industry – Government Partnership for Cyber Defense. *Journal of Strategic Security*, 4(2), 97-112.

- Cluley, G. (2009). Memories of the Melissa Virus. *Naked Security*. Retrieved 5 Jan 19 from: Retrieved 5 Jan 19 from:
<https://nakedsecurity.sophos.com/2009/03/26/memories-melissa-virus/>.
- CNN Money Staff. (2015). The Ashley Madison Hack...in 2 Minutes. *CNN Wire*. Retrieved online: 26 November 2018:
http://link.galegroup.com/apps/doc/A432548318/AONE?u=temple_main&sid=AONE&xid=89ee937c.
- Coase, R.H. (1937). The Nature of the Firm. *Economica*, 4(16), 386-405.
- Collins, K. (2017). The Petya Ransomware Attack Made \$20K Less than WannaCry in its First 24 Hours. *Quartz*. Retrieved 15 Dec 2018 from:
<https://qz.com/1016525/the-petya-ransomware-cyberattack-has-earned-hackers-20k-less-than-wannacry-in-its-first-24-hours/>.
- Computer Emergency Readiness Team. (1999). *CA-1999-04: Melissa Macro Virus*, 31 March 1999.
- Confessore, N. Dance, G.J.X., Harris, R., and Hansen, M. (2018). The Follower Factory. *The New York Times*. Accessed online 27 Jan 2018:
<https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html?mtrref=undefined>.
- Contreras, F., Oliveira, F., and Muller, E. (2012). Internet: Monitored Freedom. *Journal of Information Systems and Technology Management*, 9(3), 459-472.
- Coteneanu, V.M. (2016). People, Process, and Technology; a Blend to Increase an Organization Security Posture. *Scientific Bulletin "Mircea cel Batran" of Naval Academy*, 19(2), 580.
- Cook, S. (2018). 2017-2019 Ransomware Statistics and Facts. *Comparitech Website*. Retrieved 4 Jan 19 from: <https://www.comparitech.com/antivirus/ransomware-statistics/>.
- Cooper, P. (2010). Data, Information and Knowledge. *Informatics*, 505-506.
- Couldry, N. (2003). Media Meta-Capital: Extending the Range of Bourdieu's Field Theory. *Theory and Society*, 32(5/6), 653-677.
- Cox, J. (2015). Ashley Madison Hackers Speak Out: 'Nobody Was Watching': The Company's Security Was Bad, the Hackers Say. *Motherboard*. Retrieved online 26 November 2018: https://motherboard.vice.com/en_us/article/bmjqyz/ashley-madison-hackers-speak-out-nobody-was-watching.
- Crossler, R. et al. (2012). Future Directions for Behavioral Information Security Research. *Computers & Security*, 32, 90-101.

- Crump, C. (2003). Data Retention: Privacy, Anonymity, and Accountability Online. *Stanford Law Review*, 56, 191-229.
- Cuganesan, S., Steele, C., and Hart, A. (2018). How Senior Management and Workplace Norms Influence Information Security Attitudes and Self Efficacy. *Behaviour & Information Technology*, 37(1), 50-65.
- Curran, J. (2017). Senators Open Hearing on Russia Hacking by Pledging Bipartisanship. Cybersecurity Policy Report. Retrieved from <https://search-proquest-com.libproxy.temple.edu/docview/1936156117?accountid=14270>.
- Daneshkhu, S., Jones, S., Rovnick, N. (2017). Reckitt's [Pounds Sterling] 110M Hit Hints at Scale of 'Petya' Attack Damage; *UK Group Reveals Malware's Impact* Maersk and WPP Struggle to Recover. *The Financial Times*. Retrieved 15 Dec 2018 from: http://link.galegroup.com/apps/doc/A497847571/AONE?u=temple_main&sid=AO_N&xid=826282a9.
- Danzi, P., et al. (2018). Software-Defined Microgrid Control for Resilience Against Cyber Attacks. *IEEE Transactions on Smart Grid*, 2018, 1-9.
- Dastikop, R. (2005). The Nature of the Cyber Firm: Contextual Model of Business for Cyber World. *Proceedings of the 2005 International Conference on Cyberworlds*, 1-5.
- de Laat, P. (2012). Coercion or Empowerment? Moderation of Content in Wikipedia as 'Essentially Contested' Bureaucratic Rules. *Ethics of Information Technology*, 14, 123-135.
- de Muth, S. (2012). Twitter Fake Followers and a Fatwa. *Middle East*, 436, 58-59.
- Denegri-Knott, J. (2006). Consumers Behaving Badly: Deviation or Innovation? Power Struggles on the Web. *Journal of Consumer Behavior*, 5, 82-94.
- Department of Energy. (2016) Cybersecurity. *Department of Energy Official Website*, Retrieved 15 July 2017 from: <https://energy.gov/national-security-safety/cybersecurity>.
- Department of Homeland Security. (2016). Mission. *Department of Homeland Security Official Website*, Retrieved 15 July 2017 from: <https://www.dhs.gov/mission>.
- Department of Justice, Office of Public Affairs. (2015, February 17). *Russian National Charged in Largest Known Data Breach Prosecution Extradited to United States* [Press Release]. Retrieved 21 Jan 2019 from: <https://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states>.

- Department of Justice, Office of Public Affairs. (2018, February 15). *Two Russian Nationals Sentenced to Prison for Massive Data Breach Conspiracy* [Press Release]. Retrieved 23 Jan 2019 from: <https://www.justice.gov/opa/pr/two-russian-nationals-sentenced-prison-massive-data-breach-conspiracy>.
- Detsch, J. (2016). Hard Lessons Emerge from Cyberattack on Ukraine's Power Grid. *The Christian Science Monitor*. Retrieved 17 Jan 2019 from: <https://search.proquest.com/docview/1761909747?accountid=14270>.
- Dewey, C.1 (2015). Let the Ashley Madison Hack Remind You That No 'Secrets' Are Safe Online. *The Washington Post*. Retrieved online 24 November 2018: https://www.washingtonpost.com/news/the-intersect/wp/2015/07/20/let-the-ashley-madison-hack-remind-you-that-no-secrets-are-safe-online/?utm_term=.4db988cf7c6b.
- Dewey, C.2 (2015). Ashley Madison Faked Female Profiles to Lure Men in, Hacked Data Suggest. *The Washington Post*. Retrieved online 26 November 2018: https://www.washingtonpost.com/news/the-intersect/wp/2015/08/25/ashley-madison-faked-female-profiles-to-lure-men-in-hacked-data-suggest/?utm_term=.d5146e76cccd5.
- DiMase, D., et al. (2015). Systems Engineering Framework for Cyber Physical Security and Resilience. *Environmental Systems Decisions*, 35, 291-300.
- Dinh, L et al. (2011). Resilience Engineering of Industrial Processes: Principles and Contributing Factors. *Journal of Loss Prevention in the Process Industries*, 25, 233-241.
- Doctorow, C. (2018). The True Story of Notpetya: a Russian Cyberweapon that Escaped and Did \$10B in Worldwide Damage. *Boing Boing*. Retrieved 15 Dec 2018 from: <https://boingboing.net/2018/0822/andy-greenberg.html>.
- Dor, D. and Elovici, Y. (2016). A Model of the Information Security Investment Decision-Making Process. *Computers & Security*, 63, 1-13.
- Dubbin, R. (2013). The Rise of Twitter Bots. *The New Yorker*. Accessed online 8 Nov 2018: <https://www.newyorker.com/tech/annals-of-technology/the-rise-of-twitter-bots>.
- Ebeling, M. (2003). The New Dawn: Black Agency in Cyberspace. *Radical History Review*, 87, 96-108.
- Editor. (2016). Flashback Friday: The Melissa Virus. *We Live Security*. Retrieved 5 Jan 19 from: <https://www.welivesecurity.com/2016/07/15/flashback-friday-melissa-virus/>.

- Edwards, C., Beattie, A. J., Edwards, A., and Spence, P.R. (2016). Differences in Perceptions of Communication Quality Between a Twitterbot and Human Agent for Information Seeking and Learning. *Computers in Human Behavior*, 65, 666-671.
- Edwards, C., Edwards, A., Spence, P.R., and Shelton, A.K. (2014). Is That a Bot Running the Social Media Feed? Testing the Differences in Perceptions of Communication Quality for a Human Agent and a Bot Agent on Twitter. *Computers in Human Behavior*, 33, 372-376.
- Edwards, M. et al. (2017). Panning for Gold: Automatically Analysing Online Social Engineering Attack Surfaces. *Computers & Security*, 69, 18-34.
- Englander, A. (2015). Ashley Madison Lessons Learned: Security Lessons Learned from the Most Famous PHP Site Ever to Be Hacked. *LinkedIn SlideShare Website*. Retrieved online 26 November 2018:
<https://www.slideshare.net/AdamEnglander/ashley-madison-lessons-learned>.
- Ezhei, M. and Ladani, B. (2017). Information Sharing vs. Privacy: A Game Theoretic Analysis. *Expert Systems with Applications*, 88, 327-337.
- Farrell, G. (2013). Five Tests for a Theory of the Crime Drop. *Crime Science*, 2(5), 1-8.
- Farrell, H. (2018). Philip K. Dick and the Fake Humans. *Amass*, 22(3), 24-26.
- Farwell, J.P. and Rohzenski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, 53(1), 23-40.
- Fielder, A. et al. (2016). Decision Support Approaches for Cyber Security Investment. *Decision Support Systems*, 86, 13-23.
- Finlay, C.J. (2018). Just War, Cyber War, and the Concept of Violence. *Philosophy & Technology*, January 2018, 1-21.
- Fitzgerald, C. and Brantly, A. Subverting Reality: The Role of Propaganda in 21st Century Intelligence. *International Journal of Intelligence and Counterintelligence*, 30(2), 215-240.
- Fitzpatrick, W. and Dilullo, S. (2015). Cyber Espionage and the S.P.I.E.S. Taxonomy. *Competition Forum*, 13(2), 307-336.
- Flores, W. and Ekstedt, M. (2016). Shaping Intention to Resist Social Engineering Through Transformational Leadership, Information Security Culture and Awareness. *Computers & Security*, 59, 26-44.
- Forbes, D. (2007). Reconsidering the Strategic Implications of Decision Comprehensiveness. *Academy of Management Review*, 32(2), 361-376.

- Fox, E.J. (2013). 5 Charged with Hacking 160 Million Cards Over 7 Years. *CNN.com*. Retrieved 21 Jan 2019 from: <https://money.cnn.com/2013/07/25/pf/credit-card-hacking-scheme/index.html>.
- Franceschi-Bicchieri, L. (2018). Alleged CIA Leaker Tweeted That Chelsea Manning 'Should Be Executed.' *Motherboard*. Retrieved 7 Jan 19 from: https://motherboard.vice.com/en_us/article/xwmxyj/joshua-schulte-cia-leaker-chelsea-manning-wikileaks.
- Frenkel, S., Scott, M., and Mozur, P. (2017). Mystery of Motive for a Ransomware Attack: Money, Mayhem or a Message? *The New York Times*. Retrieved 15 Dec 2018 from: <https://www.nytimes.com/2017/06/28/business/ramsonware-hackers-cybersecurity-petya-impact.html>.
- Fruhlinger, J. (2017). Petya Ransomware and NotPetya Malware: What You Need to Know Now. *CSO Online*. Retrieved 15 Dec 2018 from: <https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html>.
- Fruhlinger, J. (2018). The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought Down the Internet. *CSO Online*. Retrieved 11 Jan 2019 from: <https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html>.
- Fuchs, C., Bichler, R., and Raffl, C. (2009). Cyberethics and Co-operation in the Information Society. *Science and Engineering Ethics*, 15(4), 447-466.
- Gal-Or, E., and Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research*, 16(2), 186-208.
- Gao, J. and Bansal, P. (2013). Instrumental and Integrative Logics in Business Sustainability. *Journal of Business Ethics*, 112(2), 241-255.
- Garnett, P. and Hughes, S.M. (2019). Obfuscated Democracy? Chelsea Manning and the Politics of Knowledge Curation. *Political Geography*, 68, 23-33.
- Gaskin, J. et al. (2014). Toward Generalizable Sociomaterial Inquiry: A Computational Approach for Zooming In and Out of Sociomaterial Routines. *MIS Quarterly*, 38(3), 849-871.
- Gauthier, M. (2017). (Un)ethical Practices: Intimacy and Internet in the Media Coverage of the Ashley Madison Hack. *Feminist Media Studies*, 17(6), 941-956.

- Geletkanycz, M. (1997). The Salience of 'Culture's Consequences': The Effects of Cultural Values on Top Executive Commitment to the Status Quo. *Strategic Management Journal*, 18(8), 615-634.
- George-Cosh, D. (2015). Canadian Police Call Ashley Madison Hack Criminal; Toronto Police Working with U.S. Authorities to Find Intruders. *The Wall Street Journal*. Retrieved online 24 November 2018:
<https://search.proquest.com/docview/1706286259?accountid=14270>
- Gisladottir, V. et al. (2016). Resilience of Cyber Systems with Over- and Underregulation. *Risk Analysis*, 37(9), 1644-1651.
- Gladstein, D. and Reilly, N. (1985). Group Decision Making Under Threat: The Tycoon Game. *Academy of Management Journal*, 28(3), 613-627.
- Goldsborough, R. (2017). The Increasing Threat of Ransomware. *Personal Computing*, 61-63.
- Gordon, L. et al. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, 34(3), 567-594.
- Gordon, L. et al. (2015). The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective. *Journal of Accounting Public Policy*, 34, 509-519.
- Gostev, A. (2005). The Melissa Virus Struck 6 Years Ago Today. *Kaspersky Lab Website*. Retrieved 5 Jan 19 from: <https://securelist.com/the-melissa-virus-struck-6-years-ago-today/29986/>.
- Graham, S. (2017). An Introduction to Twitterbots with Tracery. *The Programming Historian Website*. Accessed 8 Nov 2018:
<https://programminghistorian.org/en/lessons/intro-to-twitterbots>
- Greenberg, A. (2017). 'Crash Override': The Malware that Took Down a Power Grid. *Wired*. Retrieved 17 Jan 2019 from: <https://www.wired.com/story/crash-override-malware/>.
- Greenberg, A. (2017). The Reaper IoT Botnet Has Already Infected a Million Networks. *Wired*. Retrieved 11 Jan 2019 from: <https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/>.
- Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. Retrieved 15 Dec 18 from:
<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

- Gregor, S. and Jones, K. (1999). Beef producers online: diffusion theory applied. *Information Technology & People*, 12(1), 71-85.
- Gu, L. Kropotov, V., and Yarochkin, F. (2017). The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public. *Trend Labs Research Paper*, 1-80.
- Guilbeault, D. and Woolley, S. (2016). How Twitter Bots are Shaping the Election. *The Atlantic*. Accessed online 8 Nov 2018: <https://www.theatlantic.com/technology/archive/2016/11/election-bots/506072/>.
- Gwynne, J. (2013). “The Lighter that Fuels a Blaze of Change”: Agency and (Cyber)spatial (Dis)embodiment in *Girls of Riyadh. Women’s Studies International Forum*, 37, 46-52.
- Hackett, R. (2015). What to Know About the Ashley Madison Hack. *Fortune*. Retrieved online 26 November 2018: <http://fortune.com/2015/08/26/ashely-madison-hack/>
- Hackett, R. (2017). Everything to Know About the Latest Worldwide Ransomware Attack. *Fortune*. Retrieved 15 Dec 18 from: <http://fortune.com/2017/06/27/petya-ransomware-cyber-attack/>.
- Haggard, S. and Lindsay, J. (2015). North Korea and the Sony Hack: Exporting Instability Through Cyberspace. *Analysis from the East-West Center*, 117, 1-8.
- Handley, R. and Rutigliano, L. (2012). Journalistic Field Wars: Defending and Attacking the National Narrative in a Diversifying Journalistic Field. *Media, Culture & Society*, 34(6), 744-760.
- Harknett, R. (2003). Integrated Security: A Strategic Response to Anonymity and the Problem of the Few. *Contemporary Security Policy*, 24(1), 13-45.
- Harrell, B. (2017). Why the Ukraine Power Grid Attacks Should Raise Alarm. *CSO Online*. Retrieved 17 Jan 2019 from: <https://www.csionline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html>.
- Hartwick, R. P. and Wilkinson, C. (June, 2014). *Cyber Risks: The Growing Threat*. Retrieved from the Insurance Information Institute website: http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf
- Hatfield, J. (2018). Social Engineering in Cybersecurity: The Evolution of a Concept. *Computers & Security*, 73, 102-113.
- Hausken, K. (2014). A Strategic Analysis of Information Sharing Among Cyber Hackers. *Journal of Information Systems and Technology Management*, 12(2), 245-270.

- Hemsath, D. (2014). Efficient Code to Counter Dying Moore's Law. *Communications of the ACM*, 57(6), 9.
- Henry, D. and Ramirez-Marquez, J.E. (2016). On the Impacts of Power Outages During Hurricane Sandy—A Resilience-Based Analysis. *Systems Engineering*, 19 (1), 59-75.
- Hernandez-Ardieta, J., et al. (2013). A Taxonomy and Survey of Attacks on Digital Signatures. *Computers & Security*, 34, 67-112.
- Herrington, L. and Aldrich, R. (2013). The Future of Cyber-Resilience in an Age of Global Complexity. *Politics*, 33(4), 299-310.
- Herzenstein, M., Posavac, S. and Brakus, J. (2007). Adoption of New and Really New Products: The Effects of Self-Regulation Systems and Risk Salience. *Journal of Marketing Research*, 44 (2), 251-260.
- Hillebrandt, A. and Barclay, L. (2017). Comparing Integral and Incidental Emotions: Testing Insights from Emotions as Social Information Theory and Attribution Theory. *Journal of Applied Psychology*, 102(5), 732-752.
- Hiller, J. and Russell, R. (2017). Privacy in Crises: The NIST Privacy Framework. *Journal of Contingencies and Crisis Management*, 25(1), 31-37.
- Hirsch, P.B. (2017). Windmills in Cyberspace. *Journal of Business Strategy*, 38(3), 48-51.
- Hirsch-Kreinsen, H. (2016). Digitization of Industrial Work: Development Paths and Prospects. *Journal for Labour Market Research*, 49(1), 1-14.
- Holt, T. (2013). Exploring the Social Organisation and Structure of Stolen Data Markets. *Global Crime*, 14(2-3), 155-174.
- Hong, L. and Chen, W. (2014). Information Theory and Cryptography Based Secured Communication Scheme for Cooperative MIMO Communication in Wireless Sensor Networks. *Ad Hoc Networks*, 14, 95-105.
- Hornstein, M. (Executive Producer) and Frakes, J. (Director). (1996). *Star Trek - First Contact*. United States: Paramount Pictures.
- Hovav, A. and D'Arcy, J. (2003). The Impact of Denial-of-Service Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, 6(2), 97-121.

- Howard, J. and Longstaff, T. (1998). A Common Language for Computer Security Incidents. Pittsburgh, PA, CERT Coordination Center at Carnegie Mellon University: 1-33.
- Howard, M., Withers, M., and Tihanyi, L. (2013). Knowledge Dependence and the Formation of Director Interlocks. *Academy of Management Journal*, 60(5), 1986-2013.
- Hsu, I. and Sabherwal, R. (2012). Relationship Between Intellectual Capital and Knowledge Management: An Empirical Investigation. *Decision Sciences*, 43(3), 489-524.
- Htun, N. (1990). The Environmental Challenge and the Impact on the Oil Industry. *Energy Policy*, 18 (1), 5-10.
- Huang, B., Majidi, M., and Baldick, R. (2018). Case Study of Power System Cyber Attack Using Cascading Outage Analysis Model. *2018 IEEE Power & Energy Society General Meeting*, 1-5.
- Huang, C. and Behara, R. (2013). Economics of Information Security Investment in the Case of Concurrent Heterogeneous Attacks with Budget Constraints. *International Journal of Production Economics*, 141, 255-268.
- Hudson, T. (2013). 5 Charged in Massive Hacking Group That Targeted J.C. Penney, 7-Eleven. *Dallas News*. Retrieved 21 Jan 2019 from: <https://www.dallasnews.com/business/business/2013/07/25/5-charged-in-massive-hacking-group-that-targeted-j.c.-penney-7-eleven>.
- Huey, L., Nhan, J., and Broll, R. (2012). ‘Uppity Civilians’ and ‘Cyber-Vigilantes’: The Role of the General Public in Policing Cyber-Crime. *Criminology and Criminal Justice*, 13(1), 81-97.
- Hult, G. (2003). An Integration of Thoughts on Knowledge Management. *Decision Sciences*, 34(2), 189-195.
- Iqbal, S., et al. (2016). On Cloud Security: A Taxonomy and Intrusion Detection and Prevention as a Service. *Journal of Network & Computer Applications*, 74, 98-120.
- Izquierdo-Yusta, A. and Martinez-Ruiz, M. (2011). Assessing the Consumer’s Choice of Purchase Channel in the Tourism Sector. *EuroMed Journal of Business*, 6(1), 77-99.
- Jane, E. (2016). Online Misogyny and Feminist Digital Activism. *Continuum: Journal of Media and Cultural Studies*, 30(3), 284-297.

- Jansson, A. (2016). How to Become an 'Elite Cosmopolitan': The Mediatized Trajectories of United Nations Expatriates. *European Journal of Cultural Studies*, 19(5), 465-480.
- Jardine, E. (2018). Tor, What is it Good for? Political Repression and the Use of Online Anonymity-Granting Technologies. *New Media & Society*, 20(2), 435-452.
- Jing, Q. et al. (2014). Security of the Internet of Things. *Wireless News*, 20, 2481-2501.
- Jinyang, L. (2015). Knowledge Sharing in Virtual Communities: A Social Exchange Theory Perspective. *Journal of Industrial Engineering and Management*, 8(1), 170-183.
- Johnston, A. and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3), 549-566.
- Joint Publication 3-13: Information Operations*. Department of Defense, 27 November 2012, Incorporating Change 1, 20 November 2014.
- Joint Publication 3-12 (R): Cyberspace Operations*. Department of Defense, 5 February 2013.
- Jones, D. and Finkle, J. ((2013). Largest Hacking Fraud Case Launched After Credit Card Info Stolen from J.C. Penney, Visa Licensee. *Huffington Post*. Retrieved 21 Jan 2019 from: https://www.huffingtonpost.com/2013/07/25/credit-card-stolen-visa_n_3653274.html.
- Jones, M. (2014). A Matter of Life and Death: Exploring Conceptualizations of Sociomateriality in the Context of Critical Care. *MIS Quarterly*, 38(3), 895-925.
- Jones, S.L. (2013). The Passion of Bradley Manning: The Story Behind the WikiLeaks Whistle-Blower. *Journal of Military Ethics*, 12(2), 195-196.
- Jordan, T. and Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review*, 46(4), 757-780.
- Jorgensen, A. (2016). Competing Visions of eDemocracy in Greenland: Negotiations of Power in Online Political Participation. *Policy and Internet*, 9(2), 210 – 231.
- Jorgensen, M. and Phillips, L. (2002). Discourse Analysis as Theory and Method. Thousand Oaks, CA: SAGE Publications Ltd.
- Junger, M., Montoya, L., and Overink, F.J. (2017). Priming and Warnings are not Effective to Prevent Social Engineering Attacks. *Computers in Human Behavior*, 66, 75-87.

- Kahneman, D. and Tversky, A. (1979). Prospect Theory: An Analysis of Decision Under Risk. *Econometrica*, 47, 263-292.
- Kalia, D. and Aleem, S. (2017). Cyber Victimization Among Adolescents: Examining the Role of Routine Activity Theory. *Journal of Psychological Research*, 12(1), 223-232.
- Karatzogianni A. and Gak, M. (2015). Hack or Be Hacked: The Quasi-Totalitarianism of Global Trusted Networks. *New Formations*, 84/85, 130-147.
- Kautz, K. and Jensen, T.B. (2012). Sociomateriality – More Than Jargon Monoxide? Questions from the Jester to the Sovereigns. *ECIS 2012 Proceedings, Paper 54*, 1-13.
- Kim, W., et al. (2010). The Dark Side of the Internet: Attacks, Costs, and Responses. *Information Systems*, 36, 675-705.
- Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer*, 50(7), 80-84.
- Koller, M.S. (2016). Tales from the Trenches: Lessons Learned from the Ashley Madison Data Breach. *Data Privacy Monitor*. Retrieved online 26 November 2018: <https://www.dataprivacymonitor.com/data-breaches/tales-from-the-trenches-lessons-learned-from-the-ashley-madison-data-breach/>.
- Kostakis, V. (2012). The Political Economy of Information Production in the Social Web: Chances for Reflection on Our Institutional Design. *Contemporary Social Science*, 7(3), 305-319.
- Kovacs, E. (2016, March 22). Attackers Alter Water Treatment Systems in Utility Hack: Report. *Security Week*. Retrieved from: <http://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report>
- Kozlowski, A. (2014). Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal*, 3, 237.
- Krishna, G. (2014). Using Social Media Threats for Benefit. *Hakin9*. Accessed online 9 Nov 2018: <https://hakin9.org/using-social-media-threats-for-benefits/>.
- Krombholz, K. et al. (2015). Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, 22, 113-122.
- Lallie, H.S., Debattista, K., and Bal, J. (2018). An Empirical Evaluation of the Effectiveness of Attack Graphs and Fault Trees in Cyber-Attack Perception. *IEEE Transaction on Information Forensics and Security*, 13(5), 1110-1122.

- Landler, M. and Shane, S. (2018). U.S. Condemns Russia for Cyberattack, Showing Split in Stance on Putin. *The New York Times*. Retrieved 4 Jan 19 from:
<https://www.nytimes.com/2018/02/15/us/politics/russia-cyberattack.html>.
- Latour, B. (2005). *Reassembling the social. An introduction to actor-network-theory*. Oxford: Oxford University Press.
- Lee, C., Lee, C., and Kim, S. (2016). Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity. *Computers & Security*, 59, 60-70.
- Lee, R.M., Assante, M.J., and Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. *SANS Report*. Electricity - Information Sharing and Analysis Center, Washington, D.C. Retrieved 17 Jan 2019 from: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
- Leonardi, P. (2007). Activating the Informational Capabilities of Information Technology for Organizational Change. *Organization Science*, 18(5), 813-831.
- Leonardi, P. (2010). Digital Materiality? How Artifacts Without Matter, Matter. *First Monday*, 15(6-7), 1-22.
- Leonardi, P. (2011). When Flexible Routines Meet Flexible Technologies: Affordance, Constraint, and the Imbrication of Human and Material Agencies. *MIS Quarterly*, 35(1), 147-167.
- Leonardi, P. (2013). Theoretical Foundations for the Study of Sociomateriality. *Information and Organization*, 23, 59-76.
- Leonardi, P. and Barley, S. (2008). Materiality and Change: Challenges to Building Better Theory About Technology and Organizing. *Information and Organization*, 18, 159-176.
- Lewis, K., Belliveau, M., Herndon, B., and Keller, J. (2007). Group Cognition, Membership Change, and Performance: Investigating the Benefits and Detriments of Collective Knowledge. *Organizational Behavior and Human Decision Processes*, 103, 159-178.
- Leyden, J. (2002). Melissa Virus Author Jailed for 20 Months: Long Time Coming. *The Register*. Retrieved 5 Jan 19 from: Retrieved 5 Jan 19 from:
https://www.theregister.co.uk/2002/05/01/melissa_virus_author_jailed/.
- Leyden, J. (2015). Les Unsporting Gits! French Spies BUGGED Concorde Passengers. *The Register*. Retrieved 3 June 2018 from:
https://www.theregister.co.uk/2015/06/09/french_spied_concorde_passengers/.

- Leyden, J. (2017). Reaper IoT Botnet Ain't So Scary, Contains Fewer than 20,000 Drones. *The Register*. Retrieved 11 Jan 2019 from: https://www.theregister.co.uk/2017/10/27/reaper_iot_botnet_follow_up/.
- Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A.K., and Choo, K.K.R. (2018). A Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments. *Journal of Network and Computer Applications*, 103, 194-204.
- Lindsay, J. (2011). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3), 365-404.
- Linn, X. and Luppincini, R. (2011). Socio-Technical Influences of Cyber Espionage: A Case Study of the GhostNet System. *International Journal of Technoethics*, 2(2), 65-77.
- Lioukas, C., Reuer, J., and Zollo, M. (2016). Effects of Information Technology Capabilities on Strategic Alliances: Implications for the Resource-Based View. *Journal of Management Studies*, 53(2), 161-183.
- Liu, C. (2017). Distributed-Denial-of-Service Attacks and DNS. *Forbes*. Retrieved 11 Jan 2019 from: <https://www.forbes.com/sites/forbestechcouncil/2017/11/15/distributed-denial-of-service- attacks-and-dns/#1218d0cf6076>.
- Liu, S.D. (2013). The Cyberpolitics of the Governed. *Inter-Asia Cultural Studies*, 14(2), 252-271.
- Liu, Z., Min, Q., Zhai, Q., and Smyth, R. (2016). Self-Disclosure in Chinese Micro-Blogging: A Social Exchange Theory Perspective. *Information and Management*, 53, 53-63.
- Lockett, A., Moon, J. and Visser, W. (2006). Corporate Social Responsibility in Management Research: Focus, Nature, Salience and Sources of Influence. *Journal of Management Studies*, 43(1), 115-136.
- Love, V. (2011). IT Security Strategy: Is Your Health Care Organization Doing Everything It Can to Protect Patient Information? *Journal of Health Care Compliance*, 13(6), 21-28.
- Luo, X. and Donthu, N. (2007). The Role of Cyber-Intermediaries: a Framework Based on Transaction Cost Analysis, Agency, Relationship Marketing, and Social Exchange Theories. *Journal of Business & Industrial Marketing*, 19(6), 452-458.

- Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal*, 7(1), 35-49.
- Lusthaus, J. and Varese, F. (2017). Offline and Local: The Hidden Face of Cybercrime. *Policing: A Journal of Policy and Practice*, 1(1), 1-11.
- Mahowald, K., et al. (2013). Info/Information Theory: Speakers Choose Shorter Words in Predictive Contexts. *Cognition*, 126, 313-318.
- Majda, A. and Gershgorin, B. (2011). Improving Model Fidelity and Sensitivity for Complex Systems Through Empirical Information Theory. *Proceedings of the National Academy of Sciences of the United States of America*, 108(25), 10044-10049.
- Mansfield-Devine, S., ed. (2016). Major ISPs Targeted in Internet of Things Botnet Attacks. *Network Security Newsletter*, Dec 2016, 1-2.
- Manyika, J. et al. (2016). Digital Globalization: The New Era of Global Flows. *McKinsey Global Institute Report*, 1-4.
- Manworren, N., Letwat, J., and Daily, O. (2016). Why You Should Care about the Target Data Breach. *Business Horizons*, 59, 257-266.
- Matthews, L. (2017). NotPetya Ransomware Attack Cost Shipping Giant Maersk Over \$200 Million. *Forbes*. Retrieved 15 Dec 18 from: <https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#43746fc64f9a>.
- Mayadunne, S. and Park, S. (2016). An Economic Model to Evaluate Information Security Investment of Risk-Taking Small and Medium Enterprises. *International Journal of Production Economics*, 182, 519-530.
- Mayor, S. (2018). Sixty Seconds on...the WannaCry Cyberattack. *British Medical Journal*, 361, 1.
- McCormac, A. et al. (2017). Individual Differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151-156.
- McGinn, H. (1994). Information Assets. *The Bottom Line*, 7(2), 40-41.
- McGreal, C. (2010). US Private Bradley Manning Charged with Leaking Iraq Killings Video. *The Guardian*. Retrieved 7 Jan 19 from: <https://www.theguardian.com/world/2010/jul/06/bradley-manning-charged-iraq-killings-video>.

- McIver, D. et al. (2013). Understanding Work and Knowledge Management from a Knowledge-in-Practice Perspective. *Academy of Management Review*, 38(4), 597-620.
- McNamara, P. (2014). Melissa Virus Turning 15... (Age of Stripper Still Unknown). *Network World*. Retrieved 5 Jan 19 from: <https://www.networkworld.com/article/2226599/security/melissa-virus-turning-15--age-of-the-stripper-still-unknown-.html>.
- McNichol, T. (2006). *AC/DC: The Savage Tale of the First Standards War*. San Francisco, CA: Josey Bass.
- Melville, N., Kraemer, K., and Gurbaxani, V. (2004). Review: Information Technology and Organizational Performance: An Integrative Model of IT Business Value. *MIS Quarterly*, 28(2), 283-322.
- Member ISACs. (2016). *National Council of ISACs Web Page*. Retrieved 2 July 2017 from: <https://www.nationalisacs.org>.
- Metz, C. (2018). How Will We Outsmart A.I. Liars? *The New York Times*. Accessed online 20 Nov 2018: <https://www.nytimes.com/2018/11/19/science/artificial-intelligence-deepfakes-fake-news.html>.
- Michelsen, J. (2015). Ashley Madison Hack Brings Issues to Light. *UWIRE Text*, 3 Sept 2015, 1. Retrieved online 26 November 2018: http://link.galegroup.com/apps/doc/A433789175/AONE?u=temple_main&sid=AO NE&xid=4d1edebc.
- Mihailidis, P. and Viotti, S. (2017). Spreadable Spectacle in Digital Culture: Civic Expression, Fake News, and the Role of Media Literacies in “Post-Fact” Society. *American Behavioral Scientist*, 61(4), 441-454.
- Miller, C. (2018). Ukraine Rearrests Alleged Mastermind of Global Cybercrime Gang. *Radio Free Europe Radio Liberty*. Retrieved 21 January 2019 from: <https://www.rferl.org/a/ukraine-rearrests-alleged-mastermind-global-cybercrime-gang-kapkanov/29063336.html>.
- Mills, E. (2009). Melissa Virus Turns 10. *CNET Website*. Retrieved 5 Jan 19 from: Retrieved 5 Jan 19 from: <https://www.cnet.com/news/melissa-virus-turns-10/>.
- Mitchell, R., Agle, B. and Wood, D. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *The Academy of Management Review*, 22(4), 853-886.
- Moore, G.E. (1965). Cramming More Components onto Integrated Circuits. *Electronics*, 38 (8), 114-117.

- Moriuchi, P. and Chohan, S. (2018). Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018. *Recorded Future Cyber Threat Analysis Report*. Retrieved 11 Jan 2019 from: <https://www.recordedfuture.com/mirai-botnet-iot/>.
- Mortenson, W., Sixsmith, A., and Woolrych, R. (2015). The Power(s) of observation: theoretical perspectives on surveillance technologies and older people. *Aging and Society*, 35, 512-530.
- Mouton, F., Malan, M., and Venter, H. (2012). Development of Cognitive Functioning Psychological Measures for the SEADM. *Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance*, 40-51.
- Mouton, F. et al. (2014). Social Engineering Attack Framework. *IEEE Conference Paper*, DOI: 10.1109/ISSA.2014.6950510.
- Mouton, F., Leenen, L., and Venter, H. (2016). Social Engineering Attack Examples, Templates and Scenarios. *Computers and Security*, 59, 186-209.
- Murdock, J.1 (2015). Ashley Madison Hack, Apple Ins0mnia and Adobe Flash: the Week in Security. *V3.co.uk*. Retrieved online 26 November 2018:
http://link.galegroup.com/apps/doc/A427383022/ITOF?u=temple_main&sid=ITOF&xid=5dbeb53b.
- Murdock, J.2 (2015). Ashley Madison hack, Kaspersky Allegations and Stagefright 2: The Week in Security. *v3.co.uk*. Retrieved online 26 November 2018:
http://link.galegroup.com/apps/doc/A426238036/ITOF?u=temple_main&sid=ITOF&xid=37ba37a0.
- Myaauo, M. (2016). The U.S. Department of Defense Cyber Strategy: A Call to Action for Partnership. *Georgetown Journal of International Affairs*, 17(3), 21-29.
- Nakashima, E. and Warrick, J. (2012). Stuxnet Was Work of U.S. and Israeli Experts, Officials Say. *The Washington Post*, Retrieved 6 November 2017 from:
https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.1097ea516e47.
- National Institute of Standards. (2016). Cybersecurity. *NIST Official Website*, Retrieved 15 July 2017 from: <https://www.nist.gov/topics/cybersecurity>.
- Neal, P. and Ilsever, J. (2016). Protecting Information: Active Cyber Defence for the Business Entity: A Prerequisite Corporate Policy. *Academy of Strategic Management Journal*, 15(2), 15-35.

- Nelson, S.D., Simek, J.W., and Maschke, M.C. (2017). Risk Management. *ABA Journal*, 103(10), 28-31.
- Netto, M. and Spurgeon, S. (2017). Special Section on Cyber-Physical & Human Systems (CPHS). *Annual Reviews in Control*, 44, 249-251.
- Newman, L.H. (2018). The Leaked NSA Spy Tool that Hacked the World. *Wired*. Retrieved 4 Jan 19 from: <https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/>.
- Ng, A. (1) (2017). Lights out: How Crash Override Hits Power Grids – Hard. The Malware is Designed to Take Advantage of the World’s Outdated Power Grids to Shut Off Electricity in Entire Cities. *CNet.com*. Retrieved 3 July 2017 from: <https://www.cnet.com/news/lights-crash-power-grid-industry-malware-blackout-override/>.
- Ng, A. (2) (2017). The Global Ransomware Epidemic Is Just Getting Started. *CNet.com*. Retrieved 2 July 2018 from: <https://www.cnet.com/news/petya-goldeneye-wannacry-ransomware-global-epidemic-just-started/>.
- Nguyen, R. (2013). Navigating Jus Ad Bellum in the Age of Cyber Warfare. *California Law Review*, 101(4), 1079-1130.
- Nicks, D. et al. (2011). Chelsea Manning/WikiLeaks Timeline. *Shadow Proof Website*. Retrieved 7 Jan 19 from: <https://shadowproof.com/bradley-manning-wikileaks-timeline/>.
- Nita, B.O. (2014). The Truth is Out There. *Metro Magazine*, 179, 75-77.
- Nohe, P. (2018). Re-Hashed: 2018 Cybercrime Statistics: A Closer Look at the “Web of Profit.” *TheSSLStore.com*. Retrieved 21 January 2019 from: <https://www.thesslstore.com/blog/2018-cybercrime-statistics/>.
- Nott, G. (2017). Petya 'Ransomware' Ruse for Something More Sinister: Researchers. Computerworld Hong Kong. Retrieved 15 Dec 18 from: <https://search.proquest.com/docview/1933315620?accountid=14270>.
- Nycyk, M. (2016). The New Computer Hacker’s Quest and Contest with the Experienced Hackers: A Qualitative Study Applying Pierre Bourdieu’s Field Theory. *International Journal of Cyber Criminology*, 10 (2), 92-109.
- Office of the Privacy Commissioner of Canada. (2016). Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner. *PIPEDA Report of Findings #2016-005*. Ottawa, Ontario, Canada. Retrieved online 28 November

- 2018: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/#c>.
- Oldroyd, J. and Morris, S. (2012). Catching Falling Stars: A Human Resource Response to Social Capital's Detrimental Effect of Information Overload on Star Employees. *Academy of Management Review*, 37(3), 396-418.
- Olenick, D. (2018). NotPetya Attack Totally Destroyed Maersk's Computer Network: Chairman. *SC Magazine*. Retrieved 15 Dec 18 from: <https://www.scmagazine.com/home/security-news/ransomware/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/#main>.
- Ong, R. (2012). Online Vigilante Justice Chinese Style and Privacy in China. *Information & Communications Technology Law*, 21(2), 127-145.
- Orlikowski, W. (2006). Material Knowing: The Scaffolding of Human Knowledgeability. *European Journal of Information Systems*, 15(5), 460-471.
- Orlikowski, W. (2007). Sociomaterial Practices: Exploring Technology at Work. *Organization Studies*, 28 (9), 1435-1448.
- Orlikowski, W. (2010). The Sociomateriality of Organizational Life: Considering Technology in Management Research," *Cambridge Journal of Economics*, 34(1), 125-141.
- Orlikowski, W. and Scott, S. (2008). Sociomateriality: Challenging the Separation of Technology, Work and Organization. *The Academy of Management Annals*, 2(1), 433-474.
- Orlikowski, W. and Scott, S. (2015). Exploring Material-Discursive Practices. *Journal of Management Studies*, 52(5), 697-705.
- Ortiz-De-Mandojana, N. and Bansal, P. (2016). The Long-Term Benefits of Organizational Resilience Through Sustainable Business Practices. *Strategic Management Journal*, 37, 1615-1631.
- Osborne, C. (2018). Industroyer: An In-Depth Look at the Culprit Behind Ukraine's Power Grid Blackout. *ZDNet.com*. Retrieved 17 Jan 2019 from: <https://www.zdnet.com/article/industroyer-an-in-depth-look-at-the-culprit-behind-ukraines-power-grid-blackout/>.
- Osborne, C. (2018). NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs. *ZDNet Website*. Retrieved 15 Dec 18 from: <https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/>.

- Paasivaara, M. and Lassenius, C. (2014). Communities of practice in a large distributed agile software development organization – Case Ericsson. *Information and Software Technology*, 56, 1556-1577.
- Palmer, D. (2017). Petya Ransomware: Cyberattack Costs Could Hit \$300m for Shipping Giant Maersk. *ZD Net Website*. Retrieved 15 Dec 18 from:
<https://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/>.
- Palmer, D. (2017). Ransomware Turns Even Nastier: Destruction, Not Profit, Becomes the Real Aim. *ZD Net Website*. Retrieved 15 Dec 18 from:
<https://www.zdnet.com/article/ransomware-turns-even-nastier-destruction-not-profit-becomes-the-real-aim/>.
- Palmer, D. (2018). WannaCry Ransomware Crisis, One Year on: Are We Ready for the Next Global Cyber Attack? *ZDNet*. Retrieved 4 Jan 19 from:
<https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/>.
- Park, D., Summers, J., and Walstrom, M. (2017). Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks. *Jackson School of International Studies, University of Washington Website*. Retrieved 17 Jan 2019 from:
<https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/>.
- Pavlou, P. , Liang, H., and Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal – Agent Perspective. *MIS Quarterly*, 31(1), 105-136.
- Pearce, J. (2002). 'Melissa' Virus. *The New York Times*. Retrieved 5 Jan 19 from:
http://link.galegroup.com/apps/doc/A85460943/AONE?u=temple_main&sid=AON_E&xid=84cdd831.
- Pemberton, M. (1993). 'You Manage What?' RIM and the Meaning of Information. *Records Management Quarterly*, 27(1), 50-53.
- Peralta, E. (2013). The Bradley Manning Trial: A Short(ish) Guide to Understanding the Case. National Public Radio Website. Retrieved 7 Jan 19 from:
<https://www.npr.org/sections/thetwo-way/2013/06/05/188938313/the-bradley-manning-trial-a-short-ish-guide-to-understanding-the-case>.
- Perlroth, N. (2016). Hackers Used New Weapons to Disrupt Major Websites Across U.S. *The New York Times*. Retrieved 11 Jan 2019 from:
<https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html>.
- Peterson, I. (1999). Looking Beyond the Melissa Virus. *Science News*, 155(19), 303.

- Polityuk, P., Vukmanovic, O., and Jewkes, S. (2017). Ukraine's Power Outage was a Cyber Attack: Ukrrenergo. *Reuters.com*. Retrieved 17 Jan 2019 from: <https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA>.
- Posey, C. et al. (2013). Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors. *MIS Quarterly*, 37 (4), 1189-1210.
- Prigg, M. (2015). The Tweet That Cost \$139 BILLION: Researchers Analyse Impact of Hacked 2013 Message Claiming President Obama Had Been Injured by White House Explosion. *DailyMail.com*. Retrieved 3 July 2017 from: <http://www.dailymail.co.uk/sciencetech/article-3090221/The-tweet-cost-139-BILLION-Researchers-analyse-impact-hacked-message-claiming-President-Obama-injured-White-House-explosion.html>.
- Qui, Y., Ma, M., and Chen, S. (2017). An Anonymous Authentication Scheme for Multi-Domain Machine-to-Machine Communication in Cyber-Physical Systems. *Computer Networks*, 129, 306-318.
- Ragan, S. (2015). Ashley Madison Hack Exposes IT Details and Customer Records. *CSO Online*. Retrieved online 26 November 2018: <https://www.csionline.com/article/2949902/vulnerabilities/ashley-madison-hack-exposes-it-details-and-customer-records.html>.
- Ramirez, R. and Chourcri, N. (2016). Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review. *IEEE Access*, 4, 2216-2243.
- Raney, R.F. (1999). Market Place: the Melissa Virus on the Internet Gives Software Developers a Chance to Increase Their Brand Exposure. *The New York Times*, 5 Apr 1999. Retrieved 5 Jan 19 from: http://link.galegroup.com/apps/doc/A150020325/AONE?u=temple_main&sid=AONE&xid=b33edb04.
- Ranganathan, R. and Rosenkopf, L. (2014). Do Ties Really Bind? The Effect of Knowledge and Commercialization Networks on Opposition to Standards. *Academy of Management Journal*, 57(2), 515-540.
- Ravichandran, T., Lertwongsatien, C., and Lertwongsatien, C. (2014). Effect of Information Systems Resources and Capabilities on Firm Performance: A Resource-Based Perspective. *Journal of Management Information Systems*, 21(4), 237-276.

- Ray, G., Barney, J., and Muhanna, W. (2004). Capabilities, Business Processes, and Competitive Advantage: Choosing the Dependent Variable in Empirical Tests of the Resource-Based View. *Strategic Management Journal*, 25, 23-37.
- Reagans, R. and McEvily, B. (2003). Network Structure and Knowledge Transfer: The Effects of Cohesion and Range. *Administrative Science Quarterly*, 48(2), 240–267.
- Redmond, T. (1999). Lessons from the Melissa Virus. *ITPro Today*. Retrieved 5 Jan 19 from: <https://www.itprotoday.com/microsoft-exchange/lessons-melissa-virus>.
- Reilly, C. (2017). Cadbury Chocolate Factory Shut Down by Petya Cyberattack. *CNet Website*. Retrieved 15 Dec 18 from: <https://www.cnet.com/news/petya-goldeneye-malware-hits-cadbury-chocolate-factory/>.
- Reuters. (2013). US Charges Six in Biggest Credit Card Hack on Record. *CNBC.com*. Retrieved 21 Jan 2019 from: <https://www.cnbc.com/id/100913932>.
- Reyns, B. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, 50(2), 216-238.
- Riolli, L. and Savicki, V. (2003). Information System Organizational Resilience. *The International Journal of Management Science*, 31, 227-233.
- Roberds, W. and Schreft, S.L. (2008). Data Breaches and Identity Theft. *Journal of Monetary Economics*, 56, 918-929.
- Robnett, B. and Feliciano, C. (2011). Patterns of Racial-Ethnic Exclusion by Internet Daters. *Social Forces*, 89(3), 807-828.
- Rogers, K. (2015). After Ashley Madison Hack, Police in Toronto Detail a Global Fallout. *The New York Times*. Retrieved online 24 November 2018: <https://www.nytimes.com/2015/08/25/technology/after-ashley-madison-hack-police-in-toronto-detail-a-global-fallout.html>.
- Rogers, M. (2015). Remarks by Admiral Michael S. Rogers at the New America Foundation Conference on Cybersecurity, Washington, D.C. *NSA.gov*, Retrieved 6 November 2017 from: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/022315-new-america-foundation.shtml>.
- Rohle, T. (2005). Power, Reason, Closure: Critical Perspectives on New Media Theory. *New Media & Society*, 7(3), 403-422.
- Rosenbaum, R. (2012). Richard Clarke on Who Was Behind the Stuxnet Attack: America's Longtime Counterterrorism Czar Warns that the Cyberwars Have Already Begun—And that We Might Be Losing. *Smithsonian Magazine*, Retrieved

5 November 2017 from: <https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/>.

- Rosenberg, Y. (2017). Confessions of a Digital Nazi Hunter. *The New York Times*. Accessed online 8 Nov 2018: <https://www.nytimes.com/2017/12/27/opinion/digital-nazi-hunter-trump.html>.
- Rosoff, H., Cui, J., and John, R. (2013). Heuristics and Biases in Cyber Security Dilemmas. *Environmental Systems Decisions*, 33, 517-529.
- Ryan, V. (2017). Data Held Hostage. *CFO.com*. Retrieved 15 Dec 18 from: <https://search.proquest.com/docview/1943868906?accountid=14270>.
- Sabherwal, R. and Sabherwal, S. (2005). Knowledge Management Using Information Technology: Determinants of Short-Term Impact on Firm Value. *Decision Sciences*, 36(4), 531-567.
- Safa, N. and Von Solms, R. (2016). An Information Security Knowledge Sharing Model in Organizations. *Computers in Human Behavior*, 57, 442-451.
- Safa, N., Von Solms, R., and Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers & Security*, 56, 70-82.
- Sahebjamnia, N., Torabi, S., and Mansouri, S. (2015). Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience. *European Journal of Operational Research*, 242, 261-273.
- Sanchez, R. and Mahoney, J. (1996). Modularity, Flexibility, and Knowledge Management in Product and Organization Design. *Strategic Management Journal*, 17, 63-76.
- Sangarasisvam, Y. (2013). Cyber Rebellion: Bradley Manning, WikiLeaks, and the Struggle to Break the Power of Secrecy in the Global War on Terror. *Perspectives on Global Development and Technology*, 12, 69-79.
- Sanger, D. (2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*, Retrieved 5 November, 2017 from: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>.
- Sanger, D. and Perlroth, N. (2016). A New Era of Internet Attacks Powered by Everyday Devices. *The New York Times*. Retrieved 11 Jan 2019 from: <https://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html>.

- Saunders, B. et al. (2018). Saturation in Qualitative Research: Exploring Its Conceptualization and Operationalization. *Quality & Quantity*, 52(4), 1893-1907.
- Saydjari, O. (2004). Cyber Defense: Art to Science. *Communications of the ACM*, 47 (3), 52-57.
- Schiffer, A. (2017). How a Fish Tank Helped Hack a Casino. *The Washington Post*. Retrieved 26 July 2017 from: https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?utm_term=.2189d00e6773.
- Schwartz, A. et al. (2006). Brain-Controlled Interfaces: Movement Restoration with Neural Prosthetics. *Neuron*, 52 (1), 205-220.
- Schillebeeckx, S. et al. (2016). What Do I Want? The Effects of Individual Aspiration and Relational Capability on Collaboration Preferences. *Strategic Management Journal*, 37, 1493-1506.
- Schilling, J. (2017). Ransomware 101--How to Face the Threat. *Petroleum Accounting and Financial Management Journal*, 36(2), 6-8.
- Schwartz, A., Cui, X.T., Weber, D.J., and Moran, D.W. (2006). Brain-Controlled Interfaces: Movement Restoration with Neural Prosthetics. *Neuron*, 52(1), 205-220.
- Schwartz, M.J. (2015). Alleged Russian Mega-Hacker Extradited. *BankInfoSecurity.com*. Retrieved 21 Jan 2019 from: <https://www.bankinfosecurity.com/alleged-300m-hacker-extradited-to-us-a-7928>.
- Schwartz, M.J. (2015). Ashley Madison Breach: 6 Essential Lessons. *Banking Info Security*. Retrieved online 26 November 2018: <https://www.bankinfosecurity.com/life-after-ashley-madison-6-essential-lessons-a-8503>.
- Schwartz, T. and Schuff, D. (2018). The Cyber-Based View of the Firm: A Framework for Survival in the Information Economy, *The IBIT Report*, p. 1-28.
- Scott, J. and Spaniel, D. (2016). *The ICIT Ransomware Report: 2016 Will Be the Year Ransomware Holds America Hostage*. Retrieved from Institute for Critical Infrastructure Technology website: <http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf>
- Scott, S. and Orlikowski, W. (2007). Entanglements in Practice: Performing Anonymity Through Social Media. *MIS Quarterly*, 38(3), 873-893.

- Scott, S. and Orlikowski, W. (2009). ‘Getting the Truth’: Exploring the Material Grounds of Institutional Dynamics in Social Media. IDEAS Working Paper Series from RePEc. Retrieved 29 January 2018 from:
<https://search.proquest.com/docview/1698351009?accountid=14270>.
- Scott, S. and Orlikowski, W. (2013). Sociomateriality – Taking the Wrong Turning? A Response to Mutch. *Information and Organization*, 23, 77-80.
- Sears, J. and Hoetker, G. (2014). Technological Overlap, Technological Capabilities, and Resource Recombination in Technological Acquisitions. *Strategic Management Journal*, 35, 48-67.
- Serracino-Inglott, P. (2013). Is it OK to be an Anonymous? *Ethics & Global Politics*, 6(4), 217-244.
- Shalf, J. M. and Leland, R. (2015). “Computing Beyond Moore’s Law.” *Computer*, 48(12), 14-23.
- Shapiro, A. (Host and Editor). (2016, July 4). Documentary Explores the Cyberwar Secrets of Stuxnet. *All Things Considered, National Public Radio*. United States.
- Sharma, S. and Vrendenburg, H. (1998). Proactive Corporate Environmental Strategy and the Development of Competitively Valuable Organizational Capabilities. *Strategic Management Journal*, 19(8), 729-753.
- Shtatfeld, R. and Barak, A. (2009). Factors Related to Initiating Interpersonal Contacts on Internet Dating Sites: A View From the Social Exchange Theory. *Interpersona*, 3, 19-37.
- Siponen, M., Mahmood, M., and Pahnila, S. (2014). Employees’ Adherence to Information Security Policies: An Exploratory Field Study. *Information & Management*, 51, 217-224.
- Smart, C. and Vertinski, I. (1984). Strategy & the Environment: A Study of Corporate Responses to Crises. *Strategic Management Journal*, 5, 199-213.
- Smith, A.C. (2018). Ukraine Warns of Coming Large-Scale Cyberattack by Russia. *SNL Power Policy Week*. Retrieved 17 Jan 2019 from:
<https://search.proquest.com/docview/2064582120?accountid=14270>.
- Smith, S. (2017). Gas Utilities Alerted to Malware Threat Months After Cyberattack on Ukraine Grid. *SNL Power Policy Week*. Retrieved 17 Jan 2019 from:
<https://search.proquest.com/docview/1919019758?accountid=14270>.

- Smith, S. et al. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security “De Jure” Standard in a Government Organization. *MIS Quarterly*, 34 (3), 463-486.
- Smathers, R. (1999). Man Pleads Guilty to Creating Melissa Virus. *The New York Times*, 10 Dec 1999, pB14.
- Snediker, D., Murray, A., and Matisziw, T. (2007). Decision Support for Network Disruption Mitigation. *Decision Support Systems*, 44, 954-969.
- Solon, O. and Hern, A. (2017). 'Petya' Ransomware Attack: What Is It and How Can It Be Stopped? *The Guardian*. Retrieved 3 July 2017 from:
<https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how>.
- Somani, G., et al. (2017). DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions. *Computer Communications*, 107, 30-48.
- Somashekhar, S. (2017). Chelsea Manning, Who Gave Trove of U.S. Secrets to WikiLeaks, Leaves Prison. *The Washington Post*. Retrieved 7 Jan 19 from:
https://www.washingtonpost.com/national/chelsea-manning-who-gave-trove-of-us-secrets-to-wikileaks-to-leave-prison/2017/05/17/c988b6f8-399a-11e7-a058-ddbb23c75d82_story.html?noredirect=on&utm_term=.0ad3e9fc9e94.
- Spence, P.r., Edwards, A., Edwards, C., and Jin, X. (2018). "The Bot Predicted Rain, Grab an Umbrella": Few Perceived Differences in Communication Qualtiy of a Weather Twitterbot versus Professional and Amateur Meteorologists. *Behaviour & Information Technology*, 37. Accessed online 9 Nov 2018: <https://doi-org.libproxy.temple.edu/10.1080/0144929X.2018.1514425>.
- Staff Reporter. (1999). Melissa Virus Suspect is Expected to Plead Innocent in New Jersey. *Wall Street Journal*, 7 Apr 1999, p. B10.
- Staff. (2019). Things You Need to Know About the Melissa Virus. *Techspirited.com*. Retrieved 5 Jan 19 from: <https://techspirited.com/things-you-need-to-know-about-melissa-virus>.
- Steinmetz, K. and Gerber, J. (2015). “It Doesn’t Have to Be This Way”: Hacker Perspectives on Privacy. *Social Justice*, 41(3), 29-51.
- Stevenson, M. (2016). The Cybertultural Moment and the New Media Field. *New Media & Society*, 18(7), 1088-1102.
- Stone, E. et al. (2003). Foreground:Background Salience: Explaining the Effects of Graphical Displays on Risk Avoidance. *Organizational Behavior and Human Decision Processes*, 90, 19-36.

- Strawn, G. and Strawn C. (2015). Moore's Law at Fifty. *IT Professional*, 17 (6), 69-72.
- Strickland, J. (2008). 10 Worst Computer Viruses of All Time. *HowStuffWorks.com*. Retrieved 5 Jan 19 from: <https://computer.howstuffworks.com/worst-computer-viruses10.htm>
- Sullivan, B. (2013). 160 Million Credit Cards Later, 'Cutting Edge' Hacking Ring Cracked. *NBC News Website*. Retrieved 21 Jan 2019 from: <https://www.nbcnews.com/technology/160-million-credit-cards-later-cutting-edge-hacking-ring-cracked-8c10751970>.
- Sullivan, J.E. and Kamensky, D. (2017). How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid. *The Electricity Journal*, 30, 30-35.
- Sung, S. and Choi, J. (2012). Effects of Team Knowledge Management on th Creativity and Financial Performance of Organizational Teams. *Organizational Behavior and Human Decision Processes*, 118, 4-13.
- Surroca, J., Tribo, J. and Waddock, S. (2010). Corporate Responsibility and Financial Performance: The Role of Intangible Resources. *Strategic Management Journal*, 31(5), 463-490.
- Tappin, B., Van Der Leer, L. and McKay, R. (2017). The Heart Trumps the Head: Desirability Bias in Political Belief Revision. *Journal of Experimental Psychology: General*.
- Tate, J. (2013). Bradley Manning Sentenced to 35 Years in WikiLeaks Case. *The Washington Post*. Retrieved 7 Jan 19 from: https://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html?utm_term=.434e9137e3d1.
- Taylor, C., Dowell, W., and Shannon, E. (1999). How They Caught Him. *Time*, 153(14), p. 66.
- Taylor, S. and Thompson, S. (1982). Stalking the Elusive Vividness Effect. *Psychological Review*, 89, 155-181.
- Tayouri, D. (2015). The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. *6th International Conference on Applied Human Factors and Ergonomics and the Affiliated Conferences, Procedia Manufacturing*, 3, 1096-1100.
- Teilhard de Chardin, P; translated by Wall B, introduction by Huxley, J. (1959). *The Phenomenon of MAN*. New York: Harper & Row Publishers.

- Tetri, P. and Vuorinen, J. (2013). Dissecting Social Engineering. *Behavior and Information Technology*, 32(10), 1014-1023.
- Thellefsen, T. Thellefsen, M., and Sørensen, B. (2013). Emotion, Information, and Cognition, and Some Possible Consequences for Library and Information Science. *Journal of the American Society for Information Science and Technology*, 64(8), 1735–1750.
- Thompson, G. (2010). Early Struggles of Soldier Charged in Leak Case. The New York Times. Retrieved 7 Jan 19 from:
<https://www.nytimes.com/2010/08/09/us/09manning.html>.
- Threat Matrix. (2017). *2017 Cybercrime Report: Global Insights from the ThreatMatrix Digital Identity Network*. Retrieved 21 January 2019 from:
<https://www.threatmatrix.com/digital-identity-insight/cybercrime-report/q4-2017-cybercrime-report/>.
- Timberg, C. and Dwoskin, E. (2018). Twitter is Sweeping Out Fake Accounts Like Never Before, Putting User Growth at Risk. *The Washington Post*. Accessed online 8 Nov 2018: https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?utm_term=.5ad5a1d34759
- Toecker, M. (2016). Why Power Generators Can't Ignore the Ukraine Cyberattack. *Power*, 160(5), 1-6.
- Trochim, W. (1989). An Introduction to Concept Mapping for Planning and Evaluation. In W. Trochim (Ed.), A Special Issue of Evaluation and Program Planning, 12, 1–16.
- Tsvetkova, M. et al. (2017). Understanding Human-Machine Networks: A Cross-Disciplinary Survey. *ACM Computing Surveys*, 50(1), 12:1-12:35.
- Tung, L. (2017). New Ransomware Strikes After WannaCry. *Computerworld Hong Kong*. Retrieved 15 Dec 18 from:
<https://search.proquest.com/docview/1933318076?accountid=14270>.
- Tung, L. (2018). Maersk Took Just 10 Days to Replace 45,000 PCs Wiped by NotPetya Attack. *CSO Online*. Retrieved 15 Dec 18 from:
<https://www.cso.com.au/article/632622/maersk-took-just-10-days-install-4k-servers-45k-pcs-after-notpetya-attack/>.
- Turner, K. and Makhija, M. (2006). The Role of Organizational Controls in Managing Knowledge. *Academy of Management Review*, 31(1), 197-217.

- Tuttle, H. (2015). Implications of the Ashley Madison Hack. *Risk Management Magazine*, 62(8), 6-9.
- Tversky, A. and Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, 211, 453-458.
- United States Department of Homeland Security, National Cybersecurity and Communications Integration Center. *Alert (TA 17-181A)*. Washington D.C.: Original release date: 1 July 2017. Last revised: 15 Feb 2018. Retrieved 15 Dec 18 from: <https://www.us-cert.gov/ncas/alerts/TA17-181A>.
- United States Department of State. (2014). Office of the Coordinator for Cyber Issues. *U.S. Department of State Official Website*, Retrieved 15 July 2017 from: <https://www.state.gov/s/cyberissues/>.
- United States Strategic Command. (2015). U.S. Cyber Command (USCYBERCOM). *U.S. Strategic Command Official Website*, Retrieved 15 July 2017 from: <https://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/>.
- Uzunov, A. and Fernandez, E. (2014). An Extensible Pattern-Based Library and Taxonomy of Security Threats for Distributed Systems. *Computer Standards & Interfaces*, 36, 734-747.
- Vanderhaegen, F. (2017). Towards Increased Systems Resilience: New Challenges Based on Dissonance Control for Human Reliability in Cyber-Physical & Human Systems. *Annual Reviews in Control*, 44, 316-322.
- van Ginkel, W. and van Knippenberg, D. (2008). Group Information Elaboration and Group Decision Making: The Role of Shared Task Representations. *Organizational Behavior and Human Decision Processes*, 105, 82-97.
- van Schie, E. and van der Pligt, J. Influencing Risk Preference in Decision Making: The Effects of Framing and Salience. *Organizational Behavior and Human Decision Processes*, (63)(3), 264-275.
- Verizon. (2016). *Data Breach Digest: Scenarios from the Field*. Retrieved 18 November 2016 from: http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf.
- Verizon. (2018). *2018 Data Breach Investigations Report*. Retrieved 21 February 2019 from:
https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf.

- Vlajic, N. and Zhou, D. (2018). IoT as a Land of Opportunity for DDoS Hackers. *Computer*, 51(7), 26-34.
- Walshaw, M. (2015). Confirmations and Contradictions: Investigating the Part that Digital Technologies Play in Students' Everyday and School Lives. *Waikato Journal of Education*, 19(1), 237-247.
- Wang, W. and Lu, Z. (2013) "Cyber Security in the Smart Grid: Survey & Challenges," *Computer Networks*, 57, 1344-1371.
- Wang, Y., Meister, D., and Gray, P. (2013). Social Influence and Knowledge Management Systems Use: Evidence from Panel Data. *MIS Quarterly*, 37(1), 299-313.
- Weinberger, S. (2011). Is This the Start of Cyberwarfare? *Nature*, 474(7350), 142-145.
- Wojcik, S. (2018). 5 Things to Know about Bots on Twitter. *Pew Research Center Website*. Accessed 8 Nov 2018: <http://www.pewresearch.org/fact-tank/2018/04/09/5-things-to-know-about-bots-on-twitter/>
- Woo, S. (2018). London Blames Russia for Cyberattack -- Last Year's 'Petya' Malware Hit Networks at FedEx, Maersk and Other Multinationals. *Wall Street Journal, Eastern Edition*. Retrieved 15 Dec 18 from: <https://search.proquest.com/docview/2002110343?accountid=14270>.
- Wood, S. (2018). Two Russians Sentenced in Camden in Massive Hacking Scheme. *The Philadelphia Inquirer*. Retrieved 21 Jan 2019 from: <http://www.philly.com/philly/business/two-russians-hackers-hacking-sentenced-camden-hacking-cybercrimes-20180214.html>.
- Wooley, S. and Shout, P.H. (2016). Twitterbots United. *Wired*. 25(5), p. 17.
- Workman, M., Ford, R., and Allen, W. (2008). A Structuration Agency Approach to Security Policy Enforcement in Mobile Ad Hoc Networks. *Information Security Journal: A Global Perspective*, 17, 267-277.
- Wright, A.D. (2015). Ashley Madison Hack: A Cautionary Tale for HR. *HR News*. Retrieved online 26 November 2018: <https://search.proquest.com/docview/1706225189?accountid=14270>.
- Xifra, J. and McKie, D. (2012). From Realpolitik to Noopolitik: The Public Relations of (Stateless) Nations in an Information Age. *Public Relations Review*, 38, 819-824.
- Yuxiao, Z. (1988). Definitions and Sciences of Information. *Information Processing and Management*, 24(4), 479-491.

- Zajko, M. (2016). Telecom Responsibilization: Internet Governance, Surveillance, and New Roles for Intermediaries. *Canadian Journal of Communication*, 41(1), 75-93.
- Zavis, A. (2017). Chelsea Manning Leaves Prison After Serving 7 Years for Handing U.S. Secrets to WikiLeaks. *LA Times*. Retrieved 7 Jan 19 from: <https://www.latimes.com/nation/la-na-army-chelsea-manning-20170517-story.html>.
- Zetter, K. (2011). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. *Wired*, Retrieved 3 November 2017 from: <https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/>.
- Zetter, K. (2014). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *Wired*, Retrieved 3 November 2017 from: <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>.
- Zetter, K. (2017). The Ukrainian Power Grid Was Hacked Again. *Motherboard*. Retrieved 17 Jan 2019 from: https://motherboard.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report.
- Zetter, K., and Poulsen, K. (2010). U.S. Intelligence Analyst Arrested in WikiLeaks Video Probe. *Wired*. Retrieved 7 Jan 19 from: <https://www.wired.com/2010/06/leak/>.
- Zhang, X. (2017). Knowledge Management System Use and Job Performance: A Multilevel Contingency Model. *MIS Quarterly*, 41(3), 811-840.
- Zhang, X. and Venkatesh, V. (2017). A Nomological Network of Knowledge Management System Use: Antecedents and Consequences. *MIS Quarterly*, 41(4), 1275-1306.
- Zobel, C. and Khansa, L. (2012). Quantifying Cyberinfrastructure Resilience Against Multi-Event Attacks. *Decision Sciences*, 43 (4), 687-710.

APPENDIX A

TEST CASE STUDY: STUXNET

A1. Analysis of the Stuxnet Attack

According to an NPR broadcast (2016), the Stuxnet Attack is recognized as “the first time to our knowledge that digital code was able to create physical destruction in the real world” (Shapiro, 2016), with many experts comparing it to the atom bomb dropped on Hiroshima and Nagasaki (Shapiro, 2016). The attack, which damaged over a thousand centrifuges at the Natanz Uranium Enrichment Facility (Lindsay, 2013; Nakashima & Warrick, 2012), has been attributed to the United States and Israel (Shapiro, 2016; Sanger, 2012; Rosenbaum, 2012; Paganini, 2016), although neither country has ever confirmed these suspicions (Rogers, 2015). At work in the Stuxnet attack was a choreographed dance leveraging the ecosystem of cyberspace, with elements at work in all three dimensions of the Cyber-Based View (Cyber-Based View) – physical, informational, and cognitive.

It is alleged that the Israelis built a replica of the Natanz enrichment facility in their Negev Nuclear Research Center in Dimona (Paganini, 2016; Broad et al., 2011) while it is speculated that the United States, which had acquired P-1 centrifuges from Libya (Broad et al., 2011), had a test facility in the Idaho National laboratory (Paganini, 2016; Broad et al., 2011). It is believed that these facilities were used to develop and test the Stuxnet cyberweapon through multiple iterations (Paganini, 2016; Nakashima & Warrick, 2012; Broad et al., 2011). An early version of Stuxnet, “Stuxnet 0.5,” was submitted to a malware scanning service in late 2007, suggesting that it was being tested to see if it avoid detection by conventional antivirus systems (Arthur, 2013), while another virus,

“Flame” was also determined to be a precursor to Stuxnet designed to conduct spy on infected computers and send data back to its creators (Kushner, 2013; Sanger, 2012).

Stuxnet entered through four “zero day Windows exploits” (Chen & Abu-Nimeh, 2011; Gjelten, 2010; Zetter, 2011; Lindsay, 2013; Farwell & Rohozinski, 2011; Kushner, 2013), including a vulnerability in the LNK file of Windows Explorer (Zetter, 2011). “It copie[d] itself to other Windows PCs through a print spooler vulnerability (MS10-061) and connect[ed] to other computers through the Server Message Block protocol and exploit[ed] a Windows Server Service remote procedure call (RPC) vulnerability (MS08-067)” (Chen & Abu-Nimeh, 2011). The Windows exploits were used as the point of entry because Siemens SIMATIC STEP 7 software, the ultimate target (Kushner, 2013), “runs on the Microsoft Windows operating systems and provides human interfaces to monitor and control the peripheral devices that drive equipment such as centrifuge rotors” (Lindsay, 2013).

Once the virus had infected a Windows system, it would then install itself on a USB stick. This technique was designed into Stuxnet with the specific knowledge that humans would then connect their equipment, whether it was a laptop or USB drive, to computers inside Natanz, allowing the Stuxnet worm to “jump the air gap” (Farwell & Rohozinski, 2011; Lindsay, 2013; Zetter, 2011; Arthur, 2013). When an infected computer or USB stick was connected to the Siemens Programmable Logic Controllers (PLC) running Siemens SIMATIC Step 7 software, a malicious .dll file was installed to operate in memory to remain hidden, while allowing Stuxnet to monitor and intercept communication between the PC and the PLC (Chen & Abu-Nimeh, 2011; Zetter, 2011; Kushner, 2013). The use of two digital certificates of authenticity (Gjelten, 2010;

Weinberger, 2011; Zetter, 2011) from verified sources: Realtek Semiconductor and JMicron Technology (Chen & Abu-Nimeh, 2011; Zetter, 2011; Lindsay, 2013) enabled installation of a rootkit which used a hard-coded password to access the SIMATIC Step7 software (Lindsay, 2013; Farwell & Rohozinski, 2011) in order to be able to inject commands into the PLC.

In addition to intercepting communications between the PC and the PLC, Stuxnet relayed information back to servers hosted in Malaysia and Denmark, allowing its authors to update the software with new functionality (Zetter, 2011; Weinberger, 2011). “Stuxnet had an extensive configuration file – mdmcpq3.pnf— with a menu of more than 400 items the attackers could tweak to control every aspect of the code” (Zetter, 2011).

Hidden within the Stuxnet code was the specific configuration of the Natanz facility (Zetter, 2011; Rosenbaum, 2012; Lindsay, 2013; Broad et al., 2011). The malware logic asked questions specific to the configuration of Natanz, as if it “had been written by lawyers” designed to limit collateral damage (Rosenbaum, 2012). According to a cable released on Wikileaks, the intent was to design a weapon that could find even those facilities that were unknown (Paganini, 2016; Zetter, 2011; Broad et al., 2011).

Once Stuxnet was installed, it would slow down and speed up the normal frequency of the frequency converters manufactured by Fararo Paya and Vacon (Farwell & Rohozinski, 2011; Zetter, 2011) on the centrifuges, which ultimately caused the devices to fail over time, potentially causing them to fly apart (Chen & Abu-Nimeh, 2011; Zetter, 2011; Weinberger, 2011; Rosenbaum, 2012; Lindsay, 2013). Using a “man in the middle” strategy, Stuxnet would mask the malicious commands and intercept status reports sent to the PLC Step7 machine so that workers monitoring the PLC from the

Step7 machine would see only authorized commands and normal operations (Langner, 2011; Zetter, 2011; Weinberger, 2011; Lindsay, 2013; Broad et al., 2011). Stuxnet also disabled any automated commands to prevent any automated responses designed to prevent catastrophic failure (Zetter, 2011; Broad et al., 2011; Langner, 2011).

The nature of the failures appeared to be random, another strategy designed with the understanding that a significant number of simultaneous failures “would be discovered and neutralized to early” (Lindsay, 2013). Random, continuing failure was intended to make the Iranians think it was due to a lack of expertise (Sanger, 2012; Nakashima & Warrick, 2012; Langner, 2011), a fact that was corroborated by intelligence that engineers from the Natanz facility were fired (Sanger, 2012).

“Natanz, like any industrial facility, was not just an assemblage of technical equipment, but also a human organization” (Lindsay, 2013). Knowing this, the initial infections were spread to organizations known or suspected to work with the Natanz facility. Stuxnet left a digital trail to a number of Iranian engineering firms: Foolad Technic, Behpajoooh, Neda Industrial Group, and Control Gostar Jahed, all of which were known providers of design, installation, and programming of industrial control systems (ICS), including the Siemens Step7 software which drove the centrifuges used to refine uranium at the Natanz Enrichment Facility (Zetter, 2014). The interactions between multiple organizations was a critical element of the cyberspace ecosystem because the Natanz facility was “air-gapped” meaning that it did not connect to the larger internet.

In order to gain access to these secondary actors, “social engineering techniques such as “spear phishing” emails disguised as communications from trusted colleagues to lure targeted users into clicking on fraudulent websites or running infected programs”

(Lindsay, 2013) were used. At one point, an engineer at Neda became suspicious that there was malware installing itself on USB sticks and corrupting the computers, but when he ran detection software to look for viruses, no malware was identified (Zetter 2014). Stuxnet was designed with the understanding that there were both humans and other software which might detect its presence, employing specific techniques to remain hidden, and illustrating the strategic nature of the hackers who perpetrated the attack.

Cognitive Dimension Elements

1. Nation states: Iran (known), United States and Israel (suspected)
2. Engineers at Natanz nuclear facility in Iran
3. Foolad Technic
4. Behpajoooh, an engineering firm, responsible for installing & programming ICS
5. Neda Industrial Group, design & install ICS
6. Control Gostar Jahed, design & install ICS
7. Realtek Semiconductor (trusted source of software)
8. JMicron Technology (trusted source of software)

Physical Dimension Elements

1. Natanz Uranium Enrichment Facility
2. Siemens S7-400 Programmable Logic Controllers (PLCs)
3. USB thumb drives
4. Laptop computers used for programming PLCs
5. Networked printers
6. Internet

7. P-1 and P-2 Centrifuges used to enrich uranium
8. Valves on centrifuges
9. Profibus network card
10. Frequency converters manufactured by Vacon and Fararo Paya

Informational Dimension Elements

1. Malware: the Stuxnet worm, “Stuxnet 0.5,” and Flame
2. Stolen digital certificates from Realtek Semiconductor and JMicron Technology
3. Looped operational information via “man-in-the-middle” exploit
4. Siemens WinCC/Step7 used to program Siemens Simatic PLCs
5. Profibus Communication Modules
6. Detailed specifications of the Natanz uranium enrichment facility in the code
7. Expiration date included in the code: 24 June 2012
8. Information released via Wikileaks announced a “serious” nuclear incident at Natanz
9. Virus searched for a specific value: the part number for a Profibus network card
10. Commands to operate the Vacon and Fararo Paya frequency converters
11. Searched for the number: 19790509 (speculated to be a date critical to the Jewish exodus from Iran) and if found, passed over the system

A2. Theory Testing

To begin testing the Cyber-Based View framework three questions specific to the elements of the Cyber-Based View are asked:

1. Does the event include effects in the physical, informational, and cognitive dimensions?
2. Were the effects in different dimensions interacting?
3. What interactions were taking place amongst the dimensions?

Table A1. Analysis of the Stuxnet Case Study in the Context of the Cyber-Based View

Event	Physical	Info	Cog	Interactions			
				P – I	P – C	I – C	P – I – C
Stuxnet	✓	✓	✓	✓	✓	✓	✓

Having confirmed the presence of various elements of the attack in the three dimensions of cyberspace as it has been defined, this phenomenon must be examined through the lens of existing theories to determine if current knowledge can explain the relationships amongst the physical, informational and cognitive dimensions. In order to make this determination, four questions are asked:

4. Does this theory explain the interaction between the physical and informational dimensions?
5. Does this theory explain the interaction between the physical and cognitive dimensions?
6. Does this theory explain the interaction between the cognitive and informational dimensions?
7. Does this theory explain the interaction amongst all three of the physical, informational, and cognitive dimensions?

Information Theory specifically differentiates between information and the devices on which it is presented, which can explain elements of the Natanz infrastructure environment such as the Siemens PLCs and the Siemens SIMATIC Step 7 software (a P

– I interaction). *Information Security* also addresses this relationship by defining security methods to secure the physical devices using physical security measures and to secure the software that runs the devices with approaches such as malware detection.

Information Theory and Knowledge Management can explain the iterative development of the Stuxnet cyberweapon which involved a feedback loop to turn information into knowledge (an I – C interaction), enabling the hackers who developed the weapon to design – build – test the malware to create specific capabilities.

Social Engineering explains how humans can be exploited as social entry points such as the use of USB drives to cross the “air-gap” at Natanz (a P – C interaction), or the use of “phishing” emails to entice a person to click on a link that downloads malware (an I – C interaction). *Salience* can explain the complacency of the engineers who did not perceive any risk to their “air-gapped” systems (an I – C interaction), and thus did not monitor their behavior related to the use of USB drives, an organization-wide behavior that could be explored by applying *Organizational Theory*. *Social Engineering* is predicated on humans engaging with and being immersed in technology, a phenomenon that is explained by *Sociomateriality*, but neither *Social Engineering* nor *Sociomateriality* offer a view of the cyber ecosystem.

Resilience Theory explores the ability of the individual domains to recover from failure, such as the recovery of the Natanz uranium enrichment process by replacing the failed centrifuges, but it does not explore the relationships that led to the failure. The *Resource Based View* looks at the cognitive (the engineers), physical assets (centrifuges), and informational assets (Siemens SIMATIC Step 7 software) within the organization, but it does not explain the interactions amongst these elements, it merely explores how

those resources relate to firm performance. *Game Theory* can explain the rivalry between the United States, Israel, and Iran, but that rivalry is contained within the cognitive dimension. But despite speculations that the United States and Israel were responsible for the attack, full attribution is not possible, a factor that can be explored using *Anonymity* theory.

Taxonomy is the use of specific language to discuss cyberattacks, and *Moore's Law* explains the speed of technological change, but neither explains the interactions amongst the various elements of cyberspace. *Agency Theory*, *Power/Resistance*, *Social Exchange*, *Routine Activity Theory*, *Weberian Theory*, *Totalitarianism/Quasitotalitarianism*, *Vigilantism*, and *Bourdieu's Field Theory*, can be used to explain why hackers behave as they do, but these theories do not explain how the Stuxnet attack was successful.

The Stuxnet attack was successful because it orchestrated the interactions between the humans (cognitive), the devices (physical), and the data and software (informational) with iterative behaviors, including the “man-in-the-middle” approach that fed malicious commands to the physical devices, while feeding false information to the engineers to influence their decision making. The software also masked its behavior by causing the physical devices to fail over time in order to keep the engineers confused regarding the cause of the failures. These interactions involved feedback amongst all three of the physical, informational, and cognitive dimensions in an iterative and simultaneous dance. Though several of these theories can explain interactions between two of the dimensions, only the Cyber-Based View captures both the bilateral interactions and the multidimensional interactions.

Table A2. Stuxnet Case Study: Testing Existing Theory & the Cyber-Based View

Theory	Question 4	Question 5	Question 6	Question 7
Information Theory	✓	X	✓	X
Information Security	✓	X	X	X
Knowledge Management	X	X	✓	X
Social Engineering	X	✓	✓	X
Sociomateriality	X	✓	✓	X
Moore's Law	X	X	X	X
Taxonomy	X	X	X	X
Resilience	X	X	X	X
RBV	X	X	X	X
Salience	X	X	✓	X
Game Theory	X	X	X	X
Agency Theory	X	X	X	X
Power/Resistance	X	X	X	X
Social Exchange	X	X	X	X
Routine Activity Theory	X	X	X	X
Organizational Theory	X	X	X	X
Weberian Theory	X	X	X	X
Totalitarianism/ Quasitotalitarianism	X	X	X	X
Vigilantism	X	X	X	X
Bourdieu's Field Theory	X	X	X	X
Anonymity	✓	X	✓	X
Cyber-Based View	✓	✓	✓	✓

- * 1. Does this theory explain the interaction between the physical and informational dimensions?
- 2. Does this theory explain the interaction between the physical and cognitive dimensions?
- 3. Does this theory explain the interaction between the cognitive and informational dimensions?
- 4. Does this theory explain the interaction amongst all three of the physical, informational, and cognitive dimensions?

Figure A1. Cyber-Based View of the Stuxnet Attack

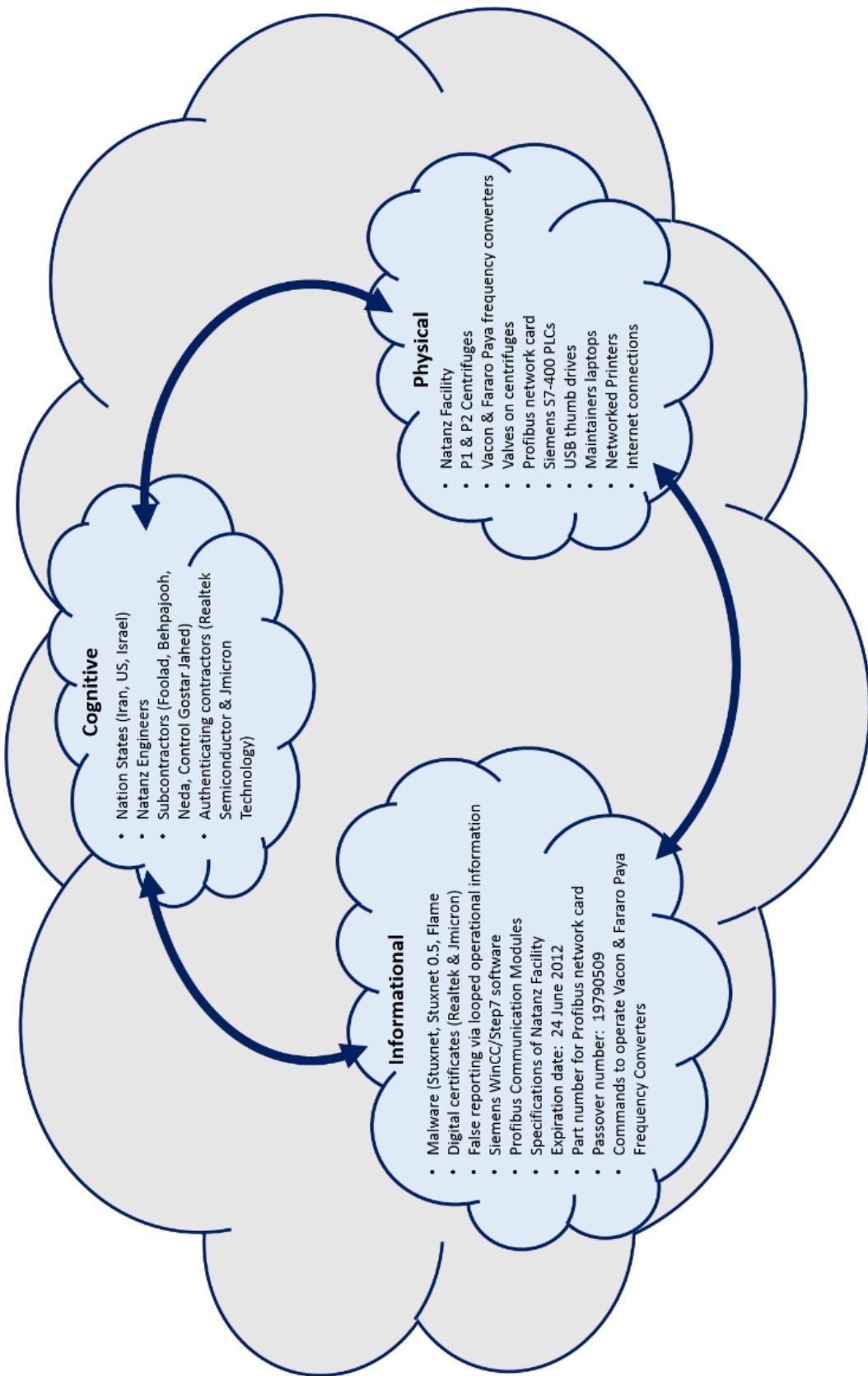


Table A3. Steps in the Data Collection and Analysis Process

Use Case	Analysis & data used	Purpose
Stuxnet, first use case to test methodology	Data collection via Google search using search term “Stuxnet”	To find news articles, practitioner analyses, and other media discussing the Stuxnet attack
Stuxnet	Data collection via library search for academic articles using search term “Stuxnet”	To find academic analyses of the Stuxnet attack
Stuxnet	Coding the 24 pieces of content listed in Table 5 for the Stuxnet Event	Test coding methodology to determine if this was a viable way to find the elements of the Cyber-Based View
Stuxnet	Development of the case study to autopsy how the event unfolded	Describe the event and how it happened to determine what the relevant factors were in the failure
Stuxnet	Identifying the elements at work in the attack and mapping them to the three dimensions of the Cyber-Based View	Theory testing to determine if the dimensions of the Cyber-Based View are present in the event and whether interactions took place
Stuxnet	Tested the relationships in the Stuxnet attack to determine applicability of existing theories	Theory testing to determine if existing theory can explain what happened in Stuxnet, or if new theory is required

Table A4. Data Analyzed for case studies

Event	Timeframe	News articles	Academic articles	Practitioner analysis	Public documents	Other
Stuxnet	September 2010 – April 2017	8	4	3	1 interview with NSA commander	<ul style="list-style-type: none"> • 3 podcasts • 1 TED talk

A3. Stuxnet Case Study Data Sources

News Articles

Arthur, C. (2013). Symantec discovers 2005 US computer virus attack on Iran nuclear plants, *The Guardian*, Retrieved 6 November 2017 from:
<https://www.theguardian.com/technology/2013/feb/26/symantec-us-computer-virus-iran-nuclear>.

Broad, W., Markoff, J. and Sanger, D. (2011). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *The New York Times*, Retrieved 6 November 2017 from:
<http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>.

Franceschi-Bicchieri, L. (2017). The New Shadow Brokers Leak Connects the NSA to the Stuxnet Cyber Weapon Used on Iran. *Motherboard*, Retrieved 6 November 2017 from: https://motherboard.vice.com/en_us/article/8qpnzp/shadow-brokers-nsa-stuxnet-iran.

Menn, J. (2015). Exclusive: U.S. Tried Stuxnet-style Campaign Against North Korea but Failed – Sources. *Reuters*, Retrieved 3 November 2017 from:
<https://www.reuters.com/article/us-usa-northkorea-stuxnet/exclusive-u-s-tried-stuxnet-style-campaign-against-north-korea-but-failed-sources-idUSKBN0OE2DM20150529>.

Nakashima, E. and Warrick, J. (2012). Stuxnet Was Work of U.S. and Israeli Experts, Officials Say. *The Washington Post*, Retrieved 6 November 2017 from:
https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.1097ea516e47.

Paganini, P. (2016). Some Facts that Probably You Still Ignore on the Stuxnet attack. *Security Affairs*, Retrieved 6 November 2017 from:
<http://securityaffairs.co/wordpress/43677/malware/new-revelations-stuxnet-attack.html>.

Rosenbaum, R. (2012). Richard Clarke on Who Was Behind the Stuxnet Attack: America's Longtime Counterterrorism Czar Warns that the Cyberwars Have Already Begun—And that We Might Be Losing. *Smithsonian Magazine*, Retrieved 5 November 2017 from: <https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/>.

Sanger, D. (2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*, Retrieved 5 November, 2017 from:
<http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>.

Academic Articles

- Farwell J. and Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, 53(1), 23-40.
- Kushner, D. (2013). The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program. *IEEE Spectrum*, 50(3), 48-53.
- Lindsay, J. (2011). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3), 365-404.
- Weinberger, S. (2011). Is This the Start of Cyberwarfare? *Nature*, 474, 142-145.

Practitioner Analysis

- Chen, T. and Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*, 44(4), 91-93.
- Zetter, K. (2011). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. *Wired*, Retrieved 3 November 2017 from: <https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/>.
- Zetter, K. (2014). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *Wired*, Retrieved 3 November 2017 from: <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>.

Public Documents

- Rogers, M. (2015). Remarks by Admiral Michael S. Rogers at the New America Foundation Conference on Cybersecurity, Washington, D.C. *NSA.gov*, Retrieved 6 November 2017 from: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/022315-new-america-foundation.shtml>.

Other

- Gibney, J. (Writer/Director). (2016). *Zero Days*. United States: Showtime Networks.
- Gjelten, T. (Host and Editor). (2010, September 27). Cyberworm's Origins Unclear, But Potential Is Not. *All Things Considered*, National Public Radio. United States.
- Gjelten, T. (Host and Editor). (2010, October 1). Stuxnet Computer Worm Has Vast Repercussions. *All Things Considered*, National Public Radio. United States.

Langner, R. (2011). *Ralph Langner: Cracking Stuxnet, a 21st-century Cyber Weapon* [Video File]. Retrieved 6 November 2017 from:
https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyber_weapon.

Shapiro, A. (Host and Editor). (2016, July 4). Documentary Explores the Cyberwar Secrets of Stuxnet. *All Things Considered, National Public Radio*. United States.

APPENDIX B

REVIEW OF LITERATURE IN FIVE THEORETICAL CATEGORIES RELATING TO THE Cyber-Based View

B1. Scope, Collection, and Organization of the Literature on Five Categories of Theory

Twenty-one theories were explored in the literature review and used to shape the Cyber-Based View of the Firm. These twenty-one theories were reduced to twenty theories by consolidating Weberian Theory with theories of Organizational Structures. They were then organized into five categories of theoretical research in order to apply a methodology derived from Farrell's (2013) Five Tests for a Theory of the Crime Drop. As cyberattack continues to increase exponentially and technology becomes ever more integrated into daily experience, it is expected that the list of applicable theory will expand as researchers seek to understand the cyber phenomenon.

In order to organize the literature within these five categories, the primary substantive focus of each individual article was considered, and where there were different theoretical perspectives, those perspectives were identified to ensure robust application of the testing methodology to the particular category of theory. The literature examined is from 1960 – 2018 and includes 339 articles. As the literature continues to grow, it should be possible to classify new theories within one of these five categories, or to create additional categories and apply the same testing method.

To ensure a detailed review and integration of the large set of articles across the five overarching categories, specific theories are identified; these theories are then further differentiated by areas of focus within the literature stream when required. Each article

was classified under the research area that was deemed to be the article's main focus. The four tests were then applied to each theory, and specific citations from reviewed articles were provided as evidence to demonstrate whether the test had been passed or failed.

B2. Category 1: Technological Growth Theories (66 articles)

Technological growth theories seek to explain the growth of cyberspace with respect to technological change, technology immersion, and language.

B2.1 Sociomateriality (28 articles)

Sociomateriality is gaining popularity among information system scholars seeking new ways to explore and theorize about information systems in organizations and society in general (Kautz & Jensen, 2013). It is important to note that materiality is not synonymous with physical items, nor limited to information technology (Mutch, 2013). Further, there have emerged two contrasting camps in the sociomateriality literature. The first uses a critical realist perspective, for which Leonardi (2007, 2010, 2011, 2013) and Leonardi and Barley (2008, 2010) are the leading proponent, and the second takes an agential realist perspective, with Orlikowski (2006, 2007, 2009), Orlikowski and Scott (2008, 2015), and Scott & Orlikowski (2007, 2009, 2013) as the recognized principals.

Critical Realism Perspective (9 articles)

The fundamental underpinning of the critical realist perspective maintains an analytical dualism between structure and action (Leonardi, 2013). Unlike the agential realist perspective, this camp differentiates between the social and the material, instead exploring the importance of the relationship between them (Mutch, 2013). Through a "process of imbrication," Leonardi (2011, p. 150) recognizes that human and material agencies are different but interdependent. Leonardi (2007, 2010) proposed that

materiality is not limited to physical objects, but that intangibles like software can also be described as material because they are not merely conceptual in nature.

Agential Realism Perspective (12 articles)

The agential realism perspective suggests that the dualism of treating the social and material as separate limits understanding of sociomaterial phenomena (Orlikowski, 2007; Orlikowski & Scott, 2008). Scott and Orlikowski (2009) suggest that people and technology are reciprocally and emergently intertwined, and that the boundaries between them are not fixed, but enacted in practice.

Agnostics: Neither Critical Realism nor Agential Realism (7 articles)

A third stream in the literature acknowledges the value of both the critical realist and agential realist perspectives. This stream of literature contrasts the two perspectives to seek out new insights and gain a deeper understanding and how it might be applied in the Information Systems discipline (Kautz & Jensen, 2013). Without choosing between the two camps, these researchers explore the sociomaterial phenomenon in specific environments to explore “the ways in which information technologies are active participants in sociomaterial reconfigurations” (Mazmanian et al., 2014, p. 846). Osterlie (2012) suggests an integration of the two perspectives by proposing a concept of dual materiality where technology not only represents physical phenomena but also creates physical phenomena. A reflection that correlates with Mazmanian et al’s (2014) observation regarding dynamic reconfigurations, which is the concept of the technology changing how people behave, and the way people use technology influencing how it evolves.

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

Sociomateriality proposes materiality as both tangible and intangible (Leonardi & Barley, 2008; Orlikowski, 2007), a proposition shared by both the critical and agential realists. Agential realists explore materiality as it relates to social and organizational behaviors, because “organizational practices become increasingly entangled with emerging sociomaterialities” (Orlikowski, 2007, p. 1444). “Practices from this perspective are not tasks undertaken by people in roles, but material-discursive practices enacted through apparatus that simultaneously constitute and organize phenomena” (Scott & Orlikowski, 2013, p. 78).

Critical realists see organizations and technology as distinct entities (Mutch, 2013). Leonardi (2011) explores how the social and the material become interwoven and continue to become more interlocked in ways that produce infrastructures to help people accomplish their work.

Regardless of whether sociomateriality is explored from a critical realist or agential realist perspective, it is not intended to explore how the physical and informational dimensions interact with one another, but rather how the material becomes entangled with the social. Therefore, the sociomateriality literature does not pass this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

Leonardi and Barley (2008) explore the routine interaction of individuals and organizations with information technologies, and explain “most information technologies are software rather than solid physical objects” (p. 162). However, despite the lack of physical properties, “software clearly does not exist in the conceptual domain because it provides hard constraints and affordances in much the same way as physical artifacts do” (Leonardi, 2010, p. 3 of 22). But they go beyond the bilateral interaction between the cognitive and the informational dimensions because they discuss *technological artifacts* as a bundle of material such as hardware and software, again merging the informational and physical dimensions. However, if the merger of the IT artifact is ignored, it can be concluded that the sociomateriality (critical realist) perspective passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

The agential realist's perspective of strong sociomateriality fails to acknowledge the criticality of the subtle interactions between the social and the material in “sociomaterial assemblages” (Orlikowski, 2007, p. 1440). It is within the integration points of a system that vulnerabilities exist. For example an agential realist would suggest that a person wearing a fit bit is a sociomaterial assemblage, and that there is no boundary between the person and the device, which in partnership creates fitness data. However, the integration

of the person and the device, which leads to the creation of positioning data, can be used by a threat actor to track the person's movements. It is the very integration and interaction of the person with the device which creates a vulnerability that can be exploited by another cognitive actor.

The critical realist's perspective of weaker sociomaterial imbrications (Leonardi, 2013), acknowledges the interdependence of the social and the material, but the imbrication of technology and human is one of dualism. Materiality is understood as both tangible – device, and intangible – software (Leonardi, 2010), merging elements of the physical dimension with elements of the informational dimension into a single entity "material." Again, if the merger of the IT artifact is ignored, it can be concluded that the sociomateriality (critical realist) perspective passes this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

Sociomaterial imbrication of technology and human is one of dualism; while sociomaterial assemblages suggest unity. The critical realist perspective addresses interactions between the human elements and the material elements, but because it merges the informational dimension with the physical and explores the interaction of human and material as dualism, it is insufficient to explain the dynamic multilateral interactions amongst the *three* physical, informational and cognitive dimensions.

The growth of sociomaterial constructs, whether considered as assemblages (Orlikowski, 2007) or imbrications (Leonardi, 2013), creates the need for a Cyber-Based View. Sociomateriality provides neither a framework for the material assemblages nor a framework for the sociomaterial assemblages that fall within the Cyber-Based View. It is the difference between looking at the face of the clock to tell the time, or opening the clock and looking at the gears inside, which allow the device to keep time. Each gear is critical, and how the gears fit together is significant. Thus the sociomateriality literature does not pass this test.

B2.2 Moore's Law (21 articles)

In its purest form, Moore's Law is an empirical observation "In a forecasting exercise, Gordon Earle Moore, co-founder of Intel, plotted data on the number of components—transistors, resistors, and capacitors—in chips made from 1959 to 1965. He saw an approximate straight line on log paper. Extrapolating the line, he speculated that the number of components would grow from 26 in 1965 to 216 in 1975, doubling every year. His 1965–1975 forecast came true" (Denning & Lewis, 2017, p. 54). According to Denning and Lewis (2017) since that time, Moore's Law has come to be equated with everything in technology that experiences exponential growth rates.

Moore's prediction that the number of transistors that could be placed on an integrated circuit would continue to double at short, regular intervals has held true for over 50 years. During that time computer-disk memory capacity and fiber-optic cable bandwidth have also increased at exponential rates (Ceruzzi, 2005). Further, analysts have been predicting the end of Moore's Law due to the limits of quantum physics for years (Ceruzzi, 2005; Wu et al, 2012; Schuster, 2016; Denning & Lewis 2017).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

Emerging literature explores on-board limitations of Moore's Law with respect to the input/output devices (Wu et al, 12; Denning & Lewis, 2017), which is creating bottlenecks due to data transfer properties. Hemsath (2014) describes a “bloatware phenomenon fueled by the expectation that Moore's Law would mask inefficient software” (p. 9). While Moore's Law focuses primarily on the physical properties of circuit boards, the literature extrapolates Moore's Law to include the exponential growth rate of other physical devices that are used for data storage (Ceruzzi, 2005) software (Hemsath, 2014) and networking technologies such as fiberoptic cables used to send data (Ceruzzi, 2005). The extension of Moore's Law, and the properties of circuit boards as they relate to data processing and data storage implies a relationship between the physical and information dimensions. Moore's Law is an empirical observation which is often used by theorists to explain changes in physical devices as they relate to information processing, thus there is some evidence to suggest that it passes this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

Moore's Law does not imply any bilateral relationship between the cognitive and informational dimensions.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

Moore's Law does not imply any bilateral relationship between the cognitive and physical dimensions.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

Moore's Law does not explore this multilateral relationship.

B2.3 Taxonomy Development (17 articles)

While the research leading to the development of taxonomies does not directly relate to technological growth theories, it is indicative of the phenomenon of technological growth, thus this stream of literature is captured within *Category 1*. A significant portion of the cybersecurity literature explores the development of taxonomies. There are many taxonomies emerging with respect to classification of attacks and threats (Iqbal et al, 2016; Hernandez-Ardiet, 2013; Fitzpatrick & Dilulio, 2015; Aleroud & Karabatis, 2017; Uzunov & Fernandez, 2014; Somani et al, 2017;

Howard & Longstaff, 1998; Kim et al, 2010). The other area of emerging taxonomies relates to operational risk assessment (Cebula & Young, 2010; Shameli-Sendi, 2016). “A taxonomy intends to permit the classification of observed phenomena” (Hernandez-Ardiet, 2013, p. 70), thus it is no surprise that the research motivation for the cybersecurity taxonomy literature is driven by an exponential increase in cyberattack, a phenomenon which has captured the attention of researchers, but for which there is yet to emerge a common language (Ramirez & Choucri, 2016).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The vast majority of emerging taxonomies explore the cyberattack phenomenon, seeking to classify the different types of attacks (Iqbal et al, 2016; Hernandez-Ardiet, 2013; Fitzpatrick & Dilulio, 2015; Aleroud & Karabatis, 2017; Uzunov & Fernandez, 2014; Somani et al, 2017; Howard & Longstaff, 1998; Kim et al, 2010). Many of these taxonomies explore specific types of attacks, such as Distributed Denial of Service attacks (Somani et al, 2017) or attacks on digital signatures (Hernandez-Ardiet, 2013), attacks on specific computing environments such as cloud computing (Somani et al, 2017; Iqbal et al, 2016), or the use of patterns and data-mining for identifying threats and predicting attacks (Aleroud & Karabatis, 2017; Uzunov & Fernandez, 2014). These taxonomies seek to explain the relationship between elements of the informational dimension and the physical dimension; therefore it passes this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

“An interesting property of a taxonomy is that it is used to classify a particular area of knowledge” (Hernandez-Ardiet, 2013, p. 71). While some of the literature classifies humans as “assets” within a firm in order to conduct a risk analysis (Cebula & Young, 2010; Shameli-Sendi, 2016), these taxonomies do not explore how humans use information as it relates to decision-making. These specific papers could have been captured under *Category 3: Information and Physical Assets Theories*, but due to the taxonomic nature of the research, they were classified in Category 1. Taxonomy is an outcome of studying a phenomenon and not a theory in and of itself, therefore it does not pass this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

One taxonomy identifies subclasses of human action such as *accidents* or *sabotage* (Cebula & Young, 2010), which explains how humans can damage physical assets within the firm. While this specific paper could have been captured under *Category 3: Information and Physical Assets Theories*, due to the taxonomic nature of the research, it was classified in Category 1. Taxonomy is an outcome of studying a phenomenon and not a theory in and of itself, therefore it does not pass this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

“Taxonomies are a useful tool for system designers as they provide a systematic way of understanding, identifying, and addressing security risks” (Iqbal et al, 2016, p. 98). The basic purpose of a taxonomy is to enable classification of a phenomenon (Hernandez-Ardiet, 2013), but classification is different from exploration of interactive relationships. As such, the taxonomic category of cybersecurity literature does not specifically address dynamic multilateral *physical – informational – cognitive* interactions.

B2.4 Summary of Category 1 Theory

Table B1. Four Tests of Category 1: Technology Growth Theories

Theory	Test 1 P – I	Test 2 I – C	Test 3 P – C	Test 4 P – I – C
Sociomateriality (Critical Realism)	X	✓	✓	X
Sociomateriality (Agential Realism)	X	X	X	X
Moore's Law	✓	X	X	X
Taxonomies	✓	X	X	X

B3. Category 2: Decision Making Theories (54 articles)

Decision Making theories explore the relationship between human beings and information with respect to how information is cognitively processed and how data is turned into information and knowledge for decision making.

B3.1 Totalitarianism/Quasitotalitarianism (13 articles)

There are two major themes in the totalitarian literature with respect to cyber: surveillance and propaganda. “The internet, our greatest tool of emancipation, has been transformed into the most dangerous facilitator of totalitarianism we have ever seen.” (Assange, 2016, p. 1).

Propaganda (7 articles)

Totalitarian regimes, which fail to recognize a meaningful distinction between state and civil society attempt to control information reaching the citizenry (Flood, 2006). Propaganda plays an important role with respect to extending ideology to gain totalitarian control (Cassinelli, 1960), and although the propaganda tool has changed in the information age (Fitzgerald & Brantly, 2017), a study of China’s “Fifty-Cent Army” conducted by Rongbin (2015) illustrates the “state’s attempts to manipulate online expression without resorting to censorship” (p. 105).

Surveillance (5 articles)

The kinds of surveillance experienced by people who came of age in authoritarian regimes post World War II, has entered entirely new horizons in the digital age (Herrara, 2015). According to Deibert (2016), there has been a growth of new technologies in totalitarian regimes to enable greater internet control on content and information. Further, there exists a lack of clarity regarding what is public and what is private when software bots can comb the web for information to search through millions of intercepted communications with little oversight (Bouman, 2003).

Both Surveillance & Propaganda (1 article)

Baehr (2014) analyzes previous research that suggested the United States under Woodrow Wilson was the first totalitarian regime of the twentieth century. He explores how Wilson used both propaganda and surveillance and contrasts the use of these tools in a democracy with the use of these tools in a totalitarian regime.

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

Bassett (2007) alludes to the physical - informational interaction by making a link between the use of ecommerce models and surveillance because the use of ecommerce models creates digital dust that enables the state to subdue or entrap an individual. While Bouman (2003) references software robots, an element of the informational dimension, scouring the web and sorting through vast amounts of information generated by cellular and fiberoptic networks which is stored on servers throughout the world – elements of the physical domain. Deibert (2016) references the relationship between cyberspace and authoritarian rule and the growth of an industry fueled by “a global market for sophisticated surveillance and other security tools” (p. 7 of 10). Karatzogianni and Gak (2015) refer to a quasitotalitarian behavior in democracies where the Internet enables surveillance of the citizenry in the name of security. However, the purpose of the totalitarian theory in each case, is not to explain the link between the information and the physical devices, but rather how the information can be accessed and grant control. Essentially, the totalitarian literature explores how the phenomenon of cyber interactions

is an enabler to totalitarian rule, rather than trying to explain those interactions; therefore it does not pass this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

Fitzgerald and Brantly (2017) explore the use of propaganda and disinformation in the age of the Internet. Propaganda can be used to overcome dissent (Baehr, 2014), because it is often rooted in widespread values (Adinolfi, 2012). The Fitzgerald and Brantly (2017) study illustrates that specific propaganda campaigns are less effective, but that the overall power of propaganda and disinformation has “become magnified by an increasing number of information streams, resulting in in a reality distortion effect both within the targeted area and beyond” (Fitzgerald & Brantly, 2017, p. 218). They also identify a link between information manipulation and its power to skew cognitive biases and affect how humans make decisions. This is a specific reference to the interaction between the cognitive and informational dimensions, and it passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

There is no reference to this bilateral interaction in the totalitarian literature.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

There is no reference to this multilateral interaction in the totalitarian literature.

B3.2 Game Theory (20 articles)

Game Theory is explored in the context of cyber with respect to two major areas. The first application is rivalry between attackers and defenders (Cavusoglu et al., 2008; Do et al., 2017; Hausken & Bier, 2011; Liu et al., 2017; Njilla et al., 2016; Perea & Puerto, 2013; Rao et al., 2016; Spyridopoulos et al., 2013; Wang et al., 2016) which uses two-player game models to explore the interactions between firms trying to defend their cyber – physical systems and hackers trying to penetrate those defenses (Do et al., 2017). The second application of game theory is the exploration of knowledge spillover effects within industries related to cybersecurity investment and information sharing(Ezhai & Ladani, 2017; Gal-Or & Ghose, 2005; Gladstein & Reilly, 1985; Gordon et al., 2015; Lin et al., 2005; Reniers & Soudan, 2010; Tosh et al., 2016; Wu et al., 2015).

Hackers vs. Defenders (9 articles)

Depending on motivation, hackers may behave opportunistically or strategically (Wu et al., 2015). Profit minded hackers behave very differently from sport-minded hackers (Cavusoglu et al., 2008). In general, the hacker attempts to inflict maximum damage to cyberspace, while the defender attempts to minimize that damage, and the defense mechanism is dependent on the strategic behaviors of both the hacker and the defender (Do et al., 2017). Game-theoretic models used to explore the strategic

interaction between hackers and defenders are often two-player games (Cavusoglu et al., 2008; Do et al., 2017; Kannan et al., 2016; Liu et al., 2017; Perea & Puerto, 2013), but several researchers have explored multi-player games (Hausken & Bier, 2011; Hausken, 2017; Njilla et al., 2016)

Industrial knowledge Sharing & Investment Spillover (8 articles)

Game theory is applied in both two-player games (Wu et al., 2015) and multi-player game models (Ezhai & Ladani, 2017; Gal-Or & Ghose, 2005; Gladstein & Reilly, 1985; Gordon et al., 2015) to explore the interactions amongst firms within an industry. Lin et al. (2005) explores the use of a game theoretic model to understand what can be done to facilitate optimal knowledge transfer. Others explore the incentives to share information through government-led Information Sharing and Analysis Centers (ISACs) (Do et al., 2017; Gal-Or & Ghose, 2005; Gordon et al., 2015). Do et al. (2017) concludes that information sharing helps firms to increase their overall resilience by both decreasing cybersecurity risk and preventing attacks. While Gladstein and Reilly (1985) found that in high threat scenarios, information exchange within a group decreases. Wu et al. (2015) found that without the right economic incentives to motivate them, firms “are not always willing to invest in security and often offload problems onto others” (p. 6132).

Combination of Attacker – Defender & Information Sharing (3 articles)

There were several articles that applied game theory in a slightly different framework from the traditional attacker – defender approach. A study by Kannan et al. (2016) explored how software vendors can be impacted both positively and negatively by hackers through the strategic exploitation of hacker behavior in pricing and software maintenance decisions. Hausken (2017) explored information sharing amongst hackers,

concluding that the cumulative attack level was unaffected by information sharing amongst them, but that hackers compete with one another, affecting individual hackers' decisions to compete with other hackers for access to the same target. Finally, Laszka et al. (2014) surveyed the existing cybersecurity game theory literature to develop a research agenda exploring the interactions both among firms, and in attacker – defender scenarios.

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The game theory literature is specifically focused on the interactions between strategic rivals, such as firms within an industry, or hackers and defenders. Although the tools of the rivalry fall into these domains, the game theory literature expressly explores the human behavior, and does not address the interaction of physical devices and information; therefore, it fails this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

Game theoretic models take into account knowledge about the capabilities and locations of infrastructure, or incidental degradations (Rao et al., 2016), as well as what information about strategic behavior is known to only one actor in a scenario, and

incorporate that knowledge into the decision-making framework. Further, they explore how firms share knowledge (Wu et al., 2015; Ezhai & Ladani, 2017; Gal-Or & Ghose, 2005; Gladstein & Reilly, 1985; Gordon et al., 2015) or how rival hackers share information (Hausken, 2017) in order to make better decisions, thus it passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

While it is assumed that hackers and defenders are challenging one another for control over cyber-physical systems (Do et al., 2017; Liu et al., 2017) in the models, game theory is being applied to *explore the interaction between the attackers and defenders* (Cavusoglu et al., 2008; Do et al., 2017; Hausken & Bier, 2011; Liu et al., 2017; Njilla et al., 2016; Perea & Puerto, 2013; Rao et al., 2016; Spyridopoulos et al., 2013; Wang et al., 2016) or *amongst firms* in industries to inform decision-making as it relates to defensive strategies and investment strategies. Therefore, the game theory literature does not pass this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

Game theory is specifically interested in the interactions between actors in the cognitive dimension. Knowledge of one another's actions informs that behavior, and actions taken may involve the use of informational or physical assets, but the focus of the investigation is the rivalry. However, while game theory is not designed to explain the phenomenon of the interactions in cyberspace, it can be used to model those interactions once they are understood and captured. The game theory literature does not pass the multilateral physical – informational – cognitive interaction test.

B3.3 Salience (21 articles)

The preponderance of salience literature delves into Prospect Theory (Kahneman & Tversky, 1979; Tversky & Kahneman, 1992). But there are several other areas that explore salience with respect to specific contexts other than Prospect Theory applications. This includes stakeholder salience in the Corporate Social Responsibility (CSR) literature (Madsen & Rodgers, 2015; Mitchell et al., 1997; Lockett et al., 2006), strategic action and managerial attention (Shepherd et al., 2017; Keil et al., 2000); salience in the wisdom of crowds (Chartier & Abele, 2017); attention and cultural identity (Gelekanycz, 1997); transferring cognitive processes from automatic processing to active thinking (Louis & Sutton, 1989); and salience based on the graphical presentation of risk information (Stone et al., 2003).

Prospect Theory (13 articles)

Prospect Theory is widely explored in the context of decision under risk (Abdellaoui & Kemel, 2014; Kahneman & Tversky, 1979; Tversky & Kahneman, 1992; Bordalo et al., 2012; Darke & Freedman, 1993; He & Zhou, 2011; Herzenstein et al., 2007; Nagarajan & Shechter, 2014; Rosoff Cui & John, 2013; Schmidt, 2015; van Schie

& van der Pligt, 1995; Weyman & Clarke, 2003), but while there are investigations in the security literature, there has not been significant application of Prospect Theory in the cybersecurity literature (Rosoff Cui & John, 2013). Kahneman and Tversky (1979) explain that people compensate for a limited ability to comprehend and evaluate extreme probabilities by simplifying the choices to only those components that distinguish one from another. Salience is the phenomenon of directing attention to one part of the environment rather than the other, and given that part of the environment greater weighting in the subsequent judgements (Taylor & Thompson, 1982). Initially Prospect Theory explored the salience of risk (Kahneman & Tversky, 1979; Taylor & Thompson, 1982), but later applications explore the framing of the question (Tversky & Kahneman, 1992; Rosoff Cui & John, 2013; van Schie & van der Pligt, 1995) as it related to risk perception. Other applications of Prospect Theory include new product adoption (Herzenstein et al., 2012), behavior during cyber dilemmas (Rosoff Cui & John, 2013), insurance and risk (Schmidt, 2015), and perception of risk with respect to organizational role (Weyman & Clarke, 2003).

Corporate Social Responsibility (2 articles)

Mitchell et al. (1997) proposed the concept of stakeholder salience to explain to whom and to what managers actually pay attention. Stakeholder salience, which is defined as the conditions under which managers consider certain people to be stakeholders (Mitchell et al., 1997) is the primary line of inquiry in the CSR literature. Stakeholder salience is predicated on three elements: power, urgency, and legitimacy (Mitchell et al., 1997; Madsen & Rodgers, 2015). Madsen & Rodgers (2015) examines

stakeholder attention to firm CSR behavior during crisis events, examining the link between power, urgency and legitimacy as antecedents.

Strategic Action & Managerial Attention (2 articles)

Shepherd et al. (2017) propose that radical opportunity beliefs differ from incremental opportunity beliefs, and they argue that managers have limited time and attention, distinguishing among various modes of attentional engagement, and recognizing that the allocation of sustained attention is what informs strategic action. Keil et al. (2000) propose that in software projects of sunk costs, the decision makers' willingness to continue a project is predicated on the salient factor of sunk costs, where higher sunk costs result in the decision to continue the project.

The Wisdom of Crowds (1 article)

Chartier and Abele (2017) explore salience as it relates to the wisdom of crowds, identifying two kinds of salience in group decision making: consensual salience and disjunctive salience. "Consensual salience derives from the fact that an initial majority in a group is likely to support the focal point in the population. Thus, groups' consensus is likely to converge on a small set of highly efficacious responses" (Chartier & Abele, 2017, p. 80), while "disjunctive salience derives from the self-evident nature of focal points. If a group member mentions the focal point, it is likely that the focal point will become the group response" (Chartier & Abele, 2017, p. 80).

Attention and Cultural Identity (1 article)

Gelekanycz (1997) applies a Hofstede framework to understand the effect of cultural identity and salience in executive decision making, finding that cultures with high uncertainty avoidance have a greater commitment to the status quo.

Transferring Cognitive Processes (1 article)

Louis and Sutton (1989) explore factors that garner attention, such as *novelty*, *discrepancy*, or *deliberate initiative*. They explain that actors will switch cognitive behaviors from automatic processing to active thinking when their attention is captured by something out of the ordinary (novel), frustrating (discrepancies), or when asked a question or trying something new (deliberate) (Louis & Sutton, 1989).

Graphical Presentation of Risk (1 article)

Stone et al. (2003) investigates foreground: background salience in the presentation of risk information. The results of several experiments provide evidence that there is a salience effect related to whether information is in the foreground or background, where the key factor is how attention is directed to either the risk of harm or actual damage (Stone et al., 2003).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The salience literature does not explore this bilateral interaction.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

The salience literature specifically investigates the interaction between the cognitive and information dimensions, seeking to explain how information is processed cognitively for the purposes of decision-making. Prospect Theory examines how risk is perceived based on the framing of questions (Tversky & Kahneman, 1992; Rosoff Cui & John, 2013; van Schie & van der Pligt, 1995), presentation of risk information (Stone et al., 2003), cultural background (Gelekanycz, 1997), or perception of risk (Kahneman & Tversky, 1979; Taylor & Thompson, 1982). The CSR literature examines how firms prioritize stakeholder value based on the salient factors of power, urgency, and legitimacy (Mitchell et al., 1997; Madsen & Rodgers, 2015), while others examine how managerial attention informs strategic action (Shepherd et al., 2017; Keil et al., 2000), how disjunctive or consensual salience informs group decision making in the wisdom of crowds (Chartier & Abele, 2017), or how novelties, discrepancies, and specific activities will garner attention and cause a shift in cognitive behavior from automatic processing to active thinking (Louis & Sutton, 1989). The salience literature passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

The salience literature does not explore this bilateral interaction.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational

capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

The salience literature does not explore this multilateral interaction.

B3.4 Summary of Category 2 Theory

Table B2. Four Tests of Category 2: Decision Making Theories

Theory	Test 1 P – I	Test 2 I – C	Test 3 P – C	Test 4 P – I – C
Totalitarian/Quasitotalitarian	X	✓	X	X
Game Theory	X	✓	X	X
Salience	X	✓	X	X

B4. Category 3: Informational & Physical Assets Theories (101 articles)

Information & physical asset theories characterize information and/or machines as firm resources and explore the defense and resilience of assets as it relates to firm performance.

B4.1 Knowledge Management (24 articles)

The preponderance of the knowledge management literature falls into two disciplines, strategy and organizational theory. Organizational theorists gravitate toward the investigation of intra-organizational knowledge sharing (Argote & Fahrenkopf, 2016; Chen A. et al., 2010; Hsu & Sabherwal, 2012; Lewis et al., 2007; McIver et al., 2013; Oldroyd & Morris, 2012; Sanchez & Mahoney, 1996; Sears & Hoetker, 2014; Sung & Choi, 2012; van Ginkel & van Knippenberg, 2008), while the strategists explore leveraging knowledge as it relates to resources and capabilities (Turner & Makhija, 2006; Howard et al., 2013; Forbes, 2007; Hult, 2003), innovation (Alexy et al., 2013; Chatterjee & Fabrizio, 2012; Ranganathan & Rosenkopf, 2014), and strategic interorganizational

alliances (Alexy et al., 2013; Chatterjee & Fabrizio, 2012; Ranganathan & Rosenkopf, 2014; Alnuaimi & George 2016; Howard et al., 2013; Schillebeeckx et al., 2016).

Internal Knowledge Sharing (8 articles)

The internal knowledge sharing literature focuses on how to optimally capture, disseminate, and leverage information across an organization, recognizing that humans are “knowledge repositories” (Argote & Fahrenkopf, 2016, p. 146). Because humans possess knowledge, the distribution of people across teams within the organization is explored as a means to distribute knowledge (Argote & Fahrenkopf, 2016; Sung & Choi, 2012). Training is also an important aspect of internal knowledge management for the purposes of growing and sharing new knowledge to avoid knowledge obsolescence (Chen, A. et al., 2010). Studies of team behaviors as related to knowledge sharing finds that often, the knowledge that arrives with team newcomers is not effectively accessed because newcomers conform to existing group behaviors (Lewis et al., 2007). Accessing knowledge within the team often depends upon the leader’s cognitive style (Sung & Choi, 2012) and whether or not groups understand that knowledge sharing and integration are critical task elements (van Ginkel & van Knippenberg, 2008). Knowledge sharing and integration also depends on social capital and networking behavior, and high-performing, visible employees often “build up an abundance of ties leading to nonredundant knowledge, though these same ties can lead to information overload (Oldroyd & Morris, 2012, p. 397).

Accessing External Knowledge Through Firm Ties (7 articles)

External knowledge sharing can allow a firm to access new knowledge to fuel innovation (Alexy et al., 2013; Chatterjee & Fabrizio, 2012; Alnuaimi & George 2016).

Firms can access external knowledge through strategic alliance with other firms (Howard et al., 2013; Ranganathan & Rosenkopf, 2014; Schillebeeckx et al., 2016), or through relationships with users (Chatterjee & Fabrizio, 2012), but it is necessary to understand what is driving the collaboration in order to facilitate joint knowledge creation (Schillebeeckx et al., 2016). Alnuaimi and George (2016) use patent data to explore knowledge spillover and knowledge retrieval behaviors. Design complexity reduces spillover effects, making it difficult for external firms to appropriate knowledge (Alnuaimi & George, 2016), while allowing focal firms to share strategically in order to create new knowledge (Alnuaimi & George 2016) or access external knowledge to reduce uncertainty (Howard et al., 2013).

Knowledge-Based View of the Firm (6 articles)

The Knowledge-Based View defines knowledge as “credible information that is of potential value to an organization,” a critical, intangible, strategic asset to be leveraged (Hult, 2003, p. 189). “Knowledge-based arguments suggest that organizational knowledge provides a synergistic advantage not replicable in the marketplace” (Brown & Duguid, 1998, p. 90). Sabherwal and Sabherwal (2005) found that a firm’s ability to manage knowledge could be a source of competitive advantage, finding a link between the use of knowledge management systems and stock market value. A firm’s ability to build competitive advantage stems from the creation and acquisition new knowledge, dissemination it to appropriate players within the firm, and the ability to interpret and integrate with existing knowledge so that it can be used for superior performance (Turner & Makhija, 2006). This ability to exploit intellectual capital – the knowledge used for competitive advantage – with good knowledge management practices will facilitate

dynamic capabilities and innovation (Hsu & Sabherwal, 2012) by ensuring that the right information is available in an accessible form at the right time (Hult, 2003).

Knowledge Management Systems (3 articles)

Knowledge management systems (KMS) leverage information technology to provide a platform for “knowledge articulation, codification, and communication” (Wang et al., 2013, p. 299). Sabherwal & Sabherwal (2005) found that KMS could improve knowledge sharing across firms. Zhang (2017) proposes that knowledge management systems that employ social technologies to facilitate collaborative work among employees can be beneficial to organizations by contributing to economic growth, reducing training costs, and enhancing job performance. As with all technology, adoption of KMS is a critical indicator of whether or not an organization will benefit from implementation. While exploring the impact of KMS on organizational performance, Zhang & Venkatesh (2017) discovered a positive relationship between the implementation of large-scale collaborative systems and systems use for help-seeking and help-providing, which led to better job performance and greater job satisfaction. However, the value of a KMS is largely dependent on whether or not employees use it (Wang et al., 2013).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The KMS literature explores the use of information technology as it relates to the creation, capture, and dissemination of information within the firm (Zhang & Venkatesh, 2017; Zhang, 2017; Sabherwal & Sabherwal, 2005; Wang et al., 2013), illustrating the link between the physical and informational dimensions. It passes this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

The relationship between human beings as repositories of information (Argote & Fahrenkopf, 2016) and the distribution of knowledge occurring as a result of human interactions illuminates the cognitive – informational interaction. Further, the knowledge management literature explores the human ability to exploit information for strategic advantage (Hsu & Sabherwal, 2012), again reinforcing the link between the cognitive and informational dimensions. The knowledge literature passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

There is a weak allusion to this link in the KMS investigations, primarily with respect to the idea that KMS are only valuable when employees use them (Wang et al., 2013). The KM literature passes this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

While integration of the knowledge management literature can begin to infer that this interaction exists, it does not explicitly investigate this multilateral interaction, and it fails this test.

B4.2 Resource-Based View (18 articles)

While the Knowledge-Based View of the firm explores information and knowledge as strategic assets (Argyres & Mostafa, 2016; Gardner et al., 2012), the Resource-Based View (RBV) explores information technology (IT) as a strategic asset (Melville et al., 2004; Wade & Hulland, 2004; Wade & Gravill, 2003). The RBV has been selected as the primary theoretical context for understanding the impact of IT investment on business competence (Son et al., 2014). The potential of IT to create competitive advantage has been of interest to both academics and practitioners, specifically trying to link strategic value of IT with competitive gain and operational efficiencies (Ravichandran et al., 2014; Son et al., 2014). Nevo and Wade (2010) define IT assets as “widely available, off the shelf or commodity like information technologies that are used to process, store and disseminate information” (p. 163).

Because of the off-the-shelf nature of IT, the focus of the RBV literature explores the synergistic behaviors of IT resources used in conjunction with other resources (Nevo & Wade, 2010) such as IT governance (Wu et al., 2015), skilled personnel (Ravichandran et al., 2014; Bharadwaj, 2000; Ray et al., 2004; Lioukas et al., 2016). The integration of

IT assets with other resources can also create valuable capabilities, such as customer service support (Nevo & Wade, 2010), supply chain (Chae et al., 2014), manufacturing strategy (Paiva et al., 2008), or e-commerce capabilities (Zhu, 2014; Zhuang & Lederer, 2006). This RBV research approach is critical from a cost-justification perspective because managers are often focused on the business value of tangible assets rather than the abstract notion of intangible resources (source). Because of its off-the-shelf nature, IT resources are sometimes perceived as being a strategic necessity (Nevo & Wade, 2010) since investments in IT are easily duplicated by competitors (Bharadwaj, 2000). Rather, it is how firms leverage their investments to create unique IT resources and skills that determine a firm's overall effectiveness.

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The RBV literature explores the business value of the “IT artifact” which Melville et al. (2004) suggests has five conceptualizations:

1. *“The tool view* where an engineered tool does what it’s designers intended
2. *The proxy view* which is rooted in individual perceptions of usefulness
3. *The ensemble view* which takes the sociomaterial perspective of people and technology being mutually reshaping
4. *The computational view* which is predicated on algorithm and system development

5. *The nominal view* which explores technology indirectly to determine its impact” (p. 286)

What is important about these conceptualizations is that they all conflate the informational and physical dimensions in the construct of the IT artifact. The RBV is not interested in the interactions between the intangibles such as software and data with the tangibles such as cloud infrastructure, but how the whole generates competitive advantage. The RBV does not explore the interaction between the physical and information dimensions and fails this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm’s decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

The RBV literature does not explore this bilateral interaction.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm’s decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

Ray et al. (2004) found that intangible resources such as managerial IT knowledge are positively related to the impact of technology resources. Other RBV literature suggests that IT resources generate the greatest amount of capability when used in conjunction with human resources (Ravichandran et al., 2014; Bharadwaj, 2000; Ray et al., 2004; Lioukas et al., 2016), suggesting that the RBV has been used to explore this

bilateral interaction for the potential to generate strategic advantage; therefore, it passes this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

Because the RBV literature conflates the physical and informational dimensions into the concept of the IT artifact, the RBV literature does not explore this multilateral interaction and fails this test.

B4.3 Information Security (23 articles)

The information security literature differentiates into three streams of investigation: technical information security (Burmester et al., 2012; Cavusoglu et al., 2009; Chen et al., 2015; Johnston & Warkentin, 2010), behavioral information security (Belanger et al., 2017; Bulgurcu et al., 2010; Crossler et al., 2013; Cuganesan et al., 2017; Lee et al., 2016; McCormac et al., 2017; Posey et al., 2013; Safa & Solms, 2016; Safa et al., 2016; Siponen et al., 2014), and information security economics (Angst et al., 2017; Chen et al., 2016; Dor & Elovici, 2016; Gordon et al., 2002; Hovav & D'Arcy, 2003; Huang & Behara, 2013; Love et al., 2011; Mayadunne & Park, 2016). Technical information security orients around using technology to secure information technology environments (Lee et al., 2016), while both behavioral information security and information security economics focus on human behavior as it relates to information security attitudes (Lee et al., 2016; Safa & Solms, 2016; Safa et al., 2016; Belanger et al., 2017; Bulgurcu et al.,

2010; Cuganesan et al., 2017) and decision-making related to information security investments (Dor & Elovici, 2016; Huang & Behara, 2013; Mayadunne & Park, 2016; Angst et al., 2017; Chen et al., 2011) respectively. Lundgren and Moller (2017) attempt to bridge the gap between the technical and human behavior avenues of research by redefining information security, settling on the *appropriate access* definition, which “describes a relation between an object of security, an agent, and a stakeholder” (p. 10)

Technical Information Security (4 articles)

Technical information security focuses on the use of information technologies (Burmester et al., 2012; Cavusoglu et al., 2009), governance structures (Johnston & Warkentin, 2010), and threat frameworks (Burmester et al., 2012) for the defense of information systems and cyber-physical systems (Chen et al., 2015). Following a cryptographic security paradigm, Burmester et al. (2012) propose a threat framework for cyber-physical systems to identify system vulnerabilities. Because of the rapid growth of information technology, networked computer systems have expanded to automate real world physical processes by connecting the cyber world to physical entities, resulting in the creation of *cyber-physical systems* (Burmester et al., 2012). This integration makes proper configuration of security technologies critical to protect systems (Cavusoglu et al., 2009). Determining how to prioritize assets for defense becomes an essential element of making progress toward successful risk control (Chen et al., 2015).

Behavioral Information Security (11 articles)

Human beings are understood to be the weakest link in a security environment (Bulgurcu, 2010; Crossler et al., 2013) thus, understanding the vital role of human behavior as it relates to information security becomes highly visible (Safa & Solms,

2016). Investigations of end-user behavior become especially important because conformance to information security policies is necessary to improve organizational information security (Belanger et al., 2017). One of the primary findings is the mediating effect of employee attitudes toward information security policy and conformance behaviors (Belanger et al., 2017; Bulgurcu, 2010; Cuganesan et al., 2017). Cultural norms (Siponen et al., 2014; Cuganesan et al., 2017; Safa & Solms, 2016) and self-efficacy (Bulgurcu, 2010; Cuganesan et al., 2017; Johnston & Warkentin, 2010;) have also been found to have a mediating effect on compliance with information security policies. McCormac et al., (2017) explore the relationship between personality and information security compliance behavior, finding evidence that suggests conscientiousness and agreeableness explain the majority of variance in behavior.

Information Security Economics (8 articles)

Given budget limitations and myriad threats, the economics of information security is of particular interest, traveling along two avenues, the first exploring decision-making in the context of financial investments in information security (Dor & Elovici, 2016; Huang & Behara, 2013; Mayadunne & Park, 2016; Angst et al., 2017; Chen et al., 2011) and the second examining the impact of information security disclosures on firm market value (Gordon et al., 2002; Hovav & D'Arcy, 2003). Angst et al. (2017) explore the impact of public policy and regulation on security investment behavior in the healthcare industry finding that information security investments are not irrelevant, but “necessary for a firm's survival” (p. 911). Huang and Behara (2013), Dor and Elovici (2016), and Mayadunne and Park (2016) develop models to inform and understand investment allocation of a fixed budget. Once those information security investments have been

made, the findings of a study by Gordon et al. (2002) provide significant evidence that voluntary disclosure of information security investments have a positive effect on market value, while Hovav and D'Arcy (2003) found evidence of a fall in market value for *internet specific companies* who voluntarily disclose being victims of a denial of service attack.

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

Cyber-Physical systems are entities in the physical environment that are monitored and controlled by integrating them into a distributed computing environment (Burmester et al., 2012). The term *cyber-physical systems* speaks directly to the bilateral interaction between the physical and informational dimensions, and passes this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

Both the behavioral information security and the information security economic streams specifically explore the interaction between people and information, passing this test. Belanger et al. (2017) and Cuganesan et al. (2017) provide evidence of employee-related information security breaches and explain the critical need to understand what inspires end-user conformance to organizational information security policies in order to

improve organizational information security. The information security economics literature goes further, attempting to understand and inform how organizations make decisions related to information security investments (Dor & Elovici, 2016; Huang & Behara, 2013; Mayadunne & Park, 2016; Angst et al., 2017; Chen et al., 2011).

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

Appropriate access, as defined by Lundgren and Moller (2017) speaks to this bilateral cognitive – physical interaction by defining appropriate access as being the relationship between an object of security (physical device), an agent (human), and a stakeholder (human). This definition has not been widely adopted, but it showcases emerging understanding of the human aspect of cyber, and it passes this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

The current information security literature looks only at the bilateral interactions among the three domains, which is evidenced by the divergent streams of literature, one taking a technical path and the other exploring the human path; therefore, it does not pass this test.

B4.4 Information Theory (12 articles)

Information theory is a subset of information science, which includes applications such as library sciences (McGinn, 1994; Yuexiao, 1988) and records management (Pemberton, 1993). It is mathematical theory related to the probability of events separate from the situation in which they, although they need not be free of context – events in context can have conditional likelihoods applied (Bannard et al., 2017). One of the basic concepts of information theory is entropy, “which measures the uncertainty of a collection of data elements” (p. 25), making it particularly useful for exploring anomalies in extremely large datasets collected through data mining (Ahmed et al., 2016). It has been used in physics to explore Quantum Theory (D’Ariano & Perinotti, 2016) and in biology to explore genetic mutation (Wagner 2017). From a cybersecurity perspective, this makes information theoretic models and algorithms extremely useful, and there are a number of studies taking this approach to address cyberthreats (Ahmed et al., 2016; Behal & Kumar, 2017; Hong & Chen, 2014; Majda & Gershgorin, 2011). Another interesting application of information theory is natural language and word choice, which has implications for the exploration of semantics in computing (Bannard et al., 2017; Hillebrandt & Barclay, 2017; Mahowald et al., 2013; Yuexiao, 1988).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

Yuexiao (1988) explains, “Information is a manifestation of the interrelation and interaction among physical objects” (p. 482). But he and other information science researchers differentiate between the containers of information, such as books, newspapers, and records and the data or information contained within them (Yuexiao, 1988; Pemberton, 1993; McGinn, 1994). Yuexiao (1988) goes on to explain, “there are binary scales, which are nonbiological, semantic information; and electrons, which are nonbiological, nonsemantic information” (p. 482). This leads other researchers to apply information-theoretical models to detect compromised nodes in wireless sensor networks (Hong & Chen, 2014), perform in-time detection of DDoS attacks and flash events (Behal & Kumar, 2017), perform anomaly detection for identifying network intrusions (Ahmed et al., 2016). The Information theory literature passes this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm’s decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

Yuexiao (1988) describes information as “a human phenomenon” (p. 479) and describes “knowledge in transmission” (p. 482) as a “human-mental” (p. 487) construct of advanced semantic information. Hillebrandt & Barclay (2017) found evidence to support how others infer information about the behavioral intentions of others by observing their emotional states and using this to inform decision making. The relationship between information human decisions, and the extent to which the right information enables the reduction of uncertainty to support optimal decision making was the subject of inquiry for Pemberton (1993), while Bannard et al. (2017) found evidence

that even young children who are still building their vocabulary would choose a more informative adjective even if they have only recently been exposed to the word chosen. Thus, it passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

The information theory literature does not explore this bilateral interaction.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

The information theory literature does not explore this multilateral interaction.

B4.5 Resilience (24 articles)

The concept of resilience takes numerous forms and is applied in numerous contexts, from individuals to organizations to processes and capabilities to systems (Davis, 2015; Henry & Ramirez-Marquez, 2016; Ortiz-de-Mandojana et al., 2016; Park et al., 2015; Riolli & Savicki, 2003; Tran et al., 2016). Cyber-resilience as a sociomaterial concept most closely aligns with the cyber resilience literature, thus this study adopts the definition offered by Caralli et al. (2010) as “a sociotechnical concept encompassing people, information, technology, and facilities that work interdependently for developing strategies and processes for protecting high-value services and associated assets” (Park et

al., 2015, p. 320). The majority of the literature used in this study was exploring resilience from an information systems perspective. In the articles where the literature was not specifically addressing information systems, the investigation was related to business continuity, disaster response, or critical infrastructure. Because of the interdisciplinary construct, there was significant breadth in the resilience literature. Even limiting the exploration to business continuity, cyber-resilience, and critical infrastructure, it branched off into a number of areas: capability development; human factors; policy, standards and regulations; security and resilience frameworks, and practitioner recommendations.

Capability Development (7 articles)

Baham et al. (2017) conducted action research to explore the application of agile software development methods to a disaster recovery scenario focusing on decision-making, organizational learning, and course of action development. They found that agile capabilities parallel a number of information systems recovery methodologies (Baham et al., 2017). Ambs et al. (2000) offers a case study of AT&T, which uses a linear programming model in conjunction with network theory to develop excess capacity that can be leveraged during outages. Interestingly, a 2004 survey exploring cyber-resilience in the context of business continuity found that while organizations plan for natural disasters, a number of business continuity plans at the time ignored the potential for internal systems threats (Cerullo & Cerullo, 2004). Resilience capabilities in supply chains was the subject of a *Technology Innovation Management Review* special issue, with Davis (2015) exploring developing greater resilience by hardening information systems, and Urciuoli (2015) advising how to leverage information and communication

technology in order to create more resilient supply chains. Although measuring resilience capability cannot be accomplished directly, Ortiz-de-Mandojana et al. (2016) was able to demonstrate that resilience gives firms an agility that improves its viability, which is visible in lower financial volatility, higher long-term growth, and higher firm survival.

Human Factor Frameworks (4 articles)

The resilience literature introduces the concept of cyber-physical and human systems (Netto & Spurgeon, 2017; Vanderhaegen, 2017), an emerging investigative construct, and offers a number of frameworks to explore the human factor in cyber-physical systems. More specifically, when human factors are explored in the resilience construct, it is with respect to how humans make decisions to work within the security constructs. Park et al. (2015) examined the perceptions of healthcare workers regarding cyber-resilience in hospital information systems, finding that disaster experience led employees to over- or under-value resilient information systems, and concluding that knowledge and awareness based on disaster experiences should be included in business continuity planning. Rioli and Savicki (2003) explored resilience as a quality of the people who manage an organization's technology infrastructure, finding that information systems personnel bring knowledge and creativity to enable organizations to capitalize on the opportunities new technology offer. This resilience as a quality of individuals and organizations enables them to respond to rapid change through an agile, flexible culture.

Security & Resilience Frameworks (5 articles)

Building resilience through the use of systems architectures and frameworks is a prominent area of research. DiMase et al. (2015) proposes the use of a multi-scale systems engineering framework to address resilience in cyber-physical systems, the

security of which they describe as poorly understood. Denzi et al. (2018) proposes a systems architecture for the electric power grid, physically separating communication interfaces of software monitoring agents within microgrids to build resilience in critical electric power infrastructure. Hamacher (2012) explores the impact of a WikiLeaks-type event using a mathematical framework to model the complexity of networks, finding that a competitor can leverage leaked information as a tactical weapon to attack rivals. Sahebjamnia et al. (2015) proposed an integrated business continuity and disaster recovery-planning framework that includes multiple decision levels in a crisis event, while Tran et al. (2016) look specifically at a zero-day (unknown vulnerability) malware outbreak in a closed system and propose a dynamic cyber resilience recovery model to ensure business continuity.

Policy, Standards, & Regulations (5 articles)

There are a number of investigations exploring how resilience could be created through organizational policies (Gisladottir et al., 2017), national and international standards bodies (Jensen, 2015), and government regulation (Joiner, 2017; Herrington & Aldrich, 2013). These studies are particularly interested in the effect of regulation and policy on compliance behavior (Gisladottir et al., 2017) and implementation of physical resilience mechanisms (Jensen, 2015; Joiner, 2017; Herrington & Aldrich, 2013).

Practitioner Recommendations (3 articles)

The practitioner literature explores cyberthreat (Amin, 2015) and offers recommendations to address vulnerabilities (Tambo & Adama, 2017; Perakslis, 2014). For all of these practitioner articles, human behavior is a significant part of the discussion related to vulnerabilities in information systems, whether it takes the form of criminals

and terrorists leveraging cyberspace (Amin, 2015; Tambo & Adama, 2017) or because an active learning approach is critical to developing prioritized cyber-protection strategies (Perakslis, 2014).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

There is a robust area of inquiry exploring cyber-physical systems, which specifically explores the physical – informational interaction. Two examples of this area of inquiry include Denzi et al. (2018) and DiMase (2015). Denzi et al. (2018) proposes systems architecture specifically tailored to separate informational elements across multiple physical devices in order to build resilience by eliminating single points of failure within microgrids. DiMase (2015) references the need for a multi-lateral framework for robust inquiry, but in the short-term he proposes a traditional systems engineering framework including electronic and physical security; information assurance and data security; asset management and access control; life cycle management, diminishing manufacturing sources, and material shortages; anti-counterfeit and supply chain risk management; software assurance and application security; forensics, prognostics, and recovery plans; track and trace network tools; anti-tamper measures, and information sharing and reporting tools. In the absence of a multilateral framework, he addresses only the physical – informational interactions. Resilience passes this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

In an examination of the impact of cybersecurity regulatory models on human behavior, Gisladottir et al. (2017) found that for most people, the objective is to complete their mission, not to stay secure. As a result, when security rules inhibit job completion, security rules will be disregarded, thus “a select number of well-framed rules are the key to minimizing human factor risks” (Gisladottir et al., 2017). This satisfies the test criteria.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

The emergence of the cyber-physical & human systems literature stream explores the integration of technology and people through such things as neural prosthetics and computer – brain interfaces (Netto & Spurgeon, 2017; Vanderhaegen, 2017; Herrington & Aldrich, 2013). It passes this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

DiMase et al. (2015) identify a future need for a framework that integrates an “approach across physical, information, cognitive and social domains to ensure

resilience” (p. 291). In the absence of such an integrated framework, they propose the use of a multi-scale systems engineering framework that addresses only the physical – informational bilateral interaction, and does not meet the criteria for the multilateral physical – informational – cognitive interaction test.

Tran et al. (2016) model a zero-day infection of a closed network. The model explores how software enters through a social engineering attack, and how the malware propagates throughout an organization’s information systems based on human behavior and compliance with organizational policies. This research seeks to model the interactions taking place, using incident rate (infection by zero-day malware on a computer (physical)) as a dependent variable, and security awareness training frequency (human), intrusion detection methods (informational) and quarantine methods (informational) as independent variables. This particular model does examine the way software (informational) infects computers (physical) due to human error (cognitive); however, the model is being used to explore a specific type of cyberattack. It is not being used to explore the interactions between decision-making, process automation, data consumption and human action, and therefore it does not pass this test.

B4.6 Summary of Category 3 Theory

Table B3. Four Tests of Category 3: Informational & Physical Asset Theories

Theory	Test 1 P – I	Test 2 I – C	Test 3 P – C	Test 4 P – I – C
Knowledge Management & Knowledge Based View (KBV)	✓	✓	✓	X
Resource Based View (RBV)	X	X	✓	X
Information Security	✓	✓	✓	X
Information Theory	✓	✓	X	X
Resilience	✓	✓	✓	X

B5. Category 4: Online Behavior Theories (67 articles)

Online behavior theories investigate how online communities are formed, how people relate to one another online, how hackers gain access to secure environments, and what motivates human social behavior in cyberspace.

B5.1 Anonymity (14 articles)

Research regarding anonymity falls into three categories: technology to enable anonymity (Qui et al., 2017; Li et al., 2018; Jardine, 2016; Haughey et al., 2016; Al-Muhtadi et al., 2018), online anonymity as it relates to the Bill of Rights (Cherner, 2017; Crump, 2003), and how anonymity influences users' social behavior (Amaya, 2017; Boyd & Field, 2016; Misoch, 2015; Tounsi & Rais, 2018; Unger, 2015; van der Nagel, 2015; Wright, 2014). The constitutional investigations revolve around data retention by internet companies as it relates to both the 1st Amendment (Cherner, 2017; Crump, 2003), which protects anonymous free speech, and the 4th Amendment (Crump, 2003), which prohibits illegal search and seizure. The technology studies explore the use of specific technologies and architectures to maintain anonymity (Al-Muhtadi et al., 2018; Jardine, 2016; Haughey et al., 2016) and technologies to create anonymity in machine – to – machine communications (Li et al., 2018; Qui et al., 2017). The largest segment of the anonymity literature focuses on how the ability to remain anonymous in cyberspace impacts human behavior from political dissent to cyber aggression.

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The literature exploring identity management and anonymity technologies explores architectures to enable anonymity (Al-Muhtadi et al., 2018; Jardine; Li et al., 2018), exploring how data is exchanged among systems in a machine to machine interactions (Qui et al., 2017). This avenue of research is specifically investigating this bilateral interaction, and it passes this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

The constitutional investigations explore the legality of data retention legislation as it relates to a right to privacy both for the purpose of anonymous free speech (Cherner, 2017; Crump, 2003) and prevention of illegal search and seizure (Crump, 2003). The literature discusses the link between user generated data and identity. Crump (2003) explains that data retention transforms the internet “from a context of relative obscurity to one of greater transparency” (p. 229), making it easier to link behaviors to individuals, which enables accountability at the expense of privacy and anonymity. The perception of anonymity specifically influences how humans choose to behave online either because of a perception of safety (Amaya, 2017; Jardine, 2016; Misoch, 2015; van der Nagle & Frith, 2015), because of low accountability (Wright, 2014; Unger, 2015; Boyd & Field, 2016), and dehumanization of others in the absence of face – to – face interaction

(Wright, 2014; Unger, 2015). Not only does anonymity affect individual behaviors and decision making, but also firm decision making. Tounsi and Rais (2018) found that offering anonymity to firms in information sharing environments, such as government sponsored Information Sharing and Analysis Centers, resulted in greater information sharing. These avenues of investigation speak specifically to this bilateral interaction between the cognitive and information dimensions and passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

The anonymity literature does not explore this bilateral interaction, but rather focuses on the behavior of people online, such as self-disclosure (Misoch, 2015; van der Nagel & Frith, 2015), cyber aggression (Wright, 2014; Unger, 2015), and political dissent (Amaya, 2017; Jardine, 2016). In order to enter an online community, users must interact with an IT artifact, but this is not the focus of the studies; therefore, the anonymity literature does not pass this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

The anonymity literature does not explore this multilateral interaction.

B5.2 Bourdieu's Field Theory (11 articles)

Researchers apply Bourdieu's Field Theory to cyberspace with respect to two constructs: new media (Vos et al., 2012; Stevenson, 2016; Jansson, 2016; Handley & Rutigliano, 2012; Barnard, 2014; Couldry, 2003)) and emerging social structures (Buchholz, 2016; Fuchs et al., 2009; Helsper, 2012; Nycyk, 2016; Walshaw, 2015). The term field refers to spheres of influence in everyday life and as frames of reference for individual action, for example, an economic digital field draws on a collection of resources, such as income, employment, education, information and digital resources, and actions in this field can be observed in questions such as participation in ecommerce, online banking, distance learning, and online information seeking (Helsper, 2012).

Media (6 articles)

The internet and cyberspace has caused a significant disruption in the journalistic field as new media challenges traditional news media sources (Vos et al., 2012). Couldry (2003) explores the use of the media to extend national narratives, also an object of study for Hendley and Rutigliano (2012) who explore this relationship with a qualitative study of how WikiLeaks was presented in both new media and traditional news sources. They found that new media viewed WikiLeaks as a whistleblower, while the traditional news media described WikiLeaks as a national security threat (Hendley & Rutigliano, 2012). New media and social media are not only competing with traditional journalism, but offering new tools to journalists who use new media sources such as Twitter to find, fact check, and disseminate news stories (Barnard, 2014). In addition to journalists, the consumption of media is explored by Jansson (2016), who found a link between the mastery of online media and social networks such as LinkedIn or Facebook to

accumulate cosmopolitan social capital and the creation of a cosmopolitan elite in the international political community.

Social Structures (5 articles)

Of particular interest in the Bourdieu's Field Theory literature is the examination of the link between digital technologies and the rise of transnational (Buchholz, 2016; Fuchs et al., 2009; Jansson, 2016) and extranational (Hendley & Rutigliano, 2012) communities and organizations. Field Theory is also applied to explore how information and communication technologies (ICTs) are impacting the social structures of younger generations (Walshaw, 2015), both in the physical world and through the growth of online communities (Nycyk, 2016) with respect to how they engage with ICTs and the resulting digital and social exclusion or inclusion (Helsper, 2012).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The Bourdieu's field theory literature does not explore this bilateral interaction.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

Bourdieu defines cultural capital as “accumulated knowledge” (Stevenson, 2016, p. 1095). The internet has given rise to globalized communication flows that provide

“unparalleled opportunities for obtaining diverse information and expressing contrary political opinions” (Hendley & Rutigliano, 2012, p. 746). Although the causal relationship between people’s beliefs and “media-channeled ideology” is abstract and intangible, the relationship between media system and social system is observable (Couldry, 2003, p. 654). Barnard (2014) found journalists use Twitter for information collection, news dissemination, sourcing, public note taking, public engagement, and other professional interactions. Jansson (2016) found that the cosmopolitan elite of the United Nations depend on email for professional communications and social media to connect with the right global professional network. These avenues of investigation speak specifically to this bilateral interaction between the cognitive and information dimensions, and passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm’s decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

The literature using Bourdieu’s field theory to explore the impact of ICTs captures the phenomenon of people using IT artifacts in order to communicate with one another (Walshaw, 2015; Fuchs et al., 2009) or acquire and disseminate information (Barnard, 2014; Jansson, 2016; Hendley & Rutigliano, 2012). The use of IT artifacts to communicate implies this bilateral test, although the IT artifact itself does conflate the physical and informational dimensions. However, it can be concluded that it passes this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

Fuchs et al. (2009) proposes that the nation state has been transcended by the phenomenon of global informational capitalism, which is based on a transnational organizational model that goes across national boundaries to create organizations and social networks that are globally distributed, and that the flows of capital, power, money, commodities, people, and information are rapidly processed across the globe. Although this speaks to the various dimensions being engaged in global informational capitalism, it does not specifically explore the simultaneous interactions amongst the cognitive, physical and informational dimensions, but rather the outcomes of this phenomenon, thus, it does not explore this multilateral interaction, and it fails this test.

B5.3 Routine Activity Theory (14 articles)

Routine Activity Theory (RAT) posits that there are three factors that must be present for a crime to occur: a suitable target, a motivated offender, and a lack of capable guardianship (Marcum et al., 2010; Kalia & Aleem, 2017; Nasi, 2017; Nasi et al., 2015; Pratt et al., 2010; Reyns et al., 2016). With cybercrime increasing, RAT is frequently applied to explore routine online behaviors and victimization (Chen et al., 2017; Choi & Lee, 2017; Kalia & Aleem, 2017; Kigerl, 2012; Kleemans et al., 2012; Leukfeldt & Yar, 2016; Leukfeldt, 2014; Marcum et al., 2010; Nasi, 2017; Nasi et al., 2015; Pratt et al., 2010; Reyns et al., 2016; Choo, 2011). Behaviors such as online banking, online shopping, downloading from the Internet, and participation in social media are found to

increase target suitability (Marcum et al., 2010; Pratt et al., 2010; Reyns et al., 2016; Chen et al., 2017; Choi & Lee, 2017; Kalia & Aleem, 2017).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

Choo (2011) explored financially motivated cybercrime, specifically emerging attack vectors such as the use of smart devices as launching points for attacks, automated teller machines (ATMs) and other point of sale devices, and how they can be exploited to inject malicious software. The exploration of physical devices is specifically related to the bilateral physical – informational interaction, and passes this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

The vast majority of the RAT literature is exploring the relationship between sharing of information as it relates to victimization. For example, Kalia and Aleem (2017) found that when parents monitored the online activities of their children, it reduced the risk of disclosing personal information, which is directly related to the RAT target suitability criteria. Reyns (2013) and Chen et al. (2017) found evidence of a link between online behaviors such as banking, shopping, and communicating, and victimization. One type of victimization in particular, identity theft, is a crime in which

the victim and the offender seldom meet face-to-face, but the offender steals the victim's identification information (Reyns, 2013). These avenues of investigation speak specifically to this bilateral interaction between the cognitive and information dimensions, and passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

The RAT literature does not explore this bilateral interaction.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

The RAT literature does not explore this multilateral interaction.

B5.4 Vigilantism (15 articles)

Cyber vigilantism, which builds upon the interactive properties of emerging media to facilitate collective intelligence (Cheong, 2010) has much in common with crowdsourcing approaches for police work (Arvantidis, 2016; Juliano, 2012). Vigilante justice often indicates serious governance problems (Phillips, 2017). Governance and law enforcement is very difficult in the wild west of cyberspace (Change et al., 2018), with governments having limited ability to keep pace with the online criminal element (Kosseff, 2016; Jane, 2016; Change et al., 2018; Serracino-Inglott, 2013). Two particular

phenomenon are of interest in the literature, the first is vigilante groups, such as Anonymous or LulzSec, and whether or not these groups are morally acceptable (Padmanabhan, 2012; Serracino-Inglott, 2013; Winters, 2009; Klein, 2015; Dysart, 2011) and the second is social media naming and shaming campaigns (Arvantidis, 2016; Cheong, 2010; Jane, 2016; Juliano, 2012; Kosseff, 2016; Ong, 2012). In both types of cyber vigilante justice, those seeking justice use information and informational tools to influence public opinion about individuals (Arvantidis, 2016; Ong, 2012) or organizations (Padmanabhan, 2012; Serracino-Inglott, 2013; Klein, 2015; Dysart, 2011) or disrupt online capabilities (Padmanabhan, 2012; Serracino-Inglott, 2013; Klein, 2015; Dysart, 2011).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The vigilantism literature does not explore this bilateral interaction.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

According to Cheong (2010), “cyber vigilantism involves the transmediation of information across multiple media platforms as online participants engage with media and with each other to spread information” (p. 474). For example, in China, *Renrou*

Sousuo or *human flesh search* involves naming and shaming corrupt public officials by tracking down their personal information and publishing it on the internet (Ong, 2012; Cheong, 2010). Naming and shaming is a common form of cyber vigilantism (Jane, 2016; Arvanitidis, 2016; Ong, 2012). The use of personal information – naming, to influence opinions – shaming, illuminates the bilateral interaction between the cognitive and the informational, and passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

The vigilanism literature does not explore this bilateral interaction.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

The vigilanism literature does not explore this multilateral interaction.

B5.5 Social Engineering (13 articles)

Oxford English Dictionary offers two definitions of social engineering: 1) the use of centralized planning in an attempt to manage social change and regulate the future development and behavior of a society or 2) the use of deception in order to induce a person to divulge private information or unwittingly provide unauthorized access to a computer system or network. The literature divides along these two definitions, with the

majority of recent literature exploring the use of social engineering to gain access to computer systems (Hatfield, 2018, p. 102).

Rutherford (2017) compares and contrasts B.F. Skinner's (1948) vision of a technology nation with Harold Loeb's (1933/1996) vision of a technocracy. The central concept of each of these visions is that government would ultimately be supplanted by technical experts who would solve society's problems by treating problems of government as technical challenges to be solved rationally (Rutherford, 2017). This approach to social engineering is also explored in Jones (2018) study of the United Arab Emirates, where social engineering approaches are being used to develop a patriotic citizenry.

Hatfield (2018) analyzes a history of the definitions of social engineering beginning in the late nineteenth century, identifying the transition point from social engineering as an economic and political concept, to social engineering as a tool of hackers, in the late 1960s with *phone phreaking*. The phone phreaking movement began when John Draper discovered that the plastic whistle offered as a prize in a Cap'n Crunch cereal box could be used to trick the telephone networks because it resonated at the same tonal frequency (Hatfield, 2018). Draper and his associates used the term *social engineering* to describe the techniques they used to gain needed information from Bell Telephone employees (Hatfield, 2018). Ultimately, Hatfield (2018) concludes that the definitions reference the same phenomenon: "Before phone phreaking, the term 'social engineering' had only been applied to the activities of powerful policy planners. Phone phreakers inverted this power structure. Here were relatively powerless individuals – often teenagers – gaining epistemic asymmetry and technocratic dominance over the powerful phone companies,

which they then used for their own purposes through a process of teleological replacement” (p. 105).

The Hatfield (2018) study offers a natural transition to the majority of recent literature studying the phenomenon of social engineering. The passive mining of information from social media is a common approach for hackers to gain access to confidential information (Edwards et al., 2017; Junger et al., 2017; Tayouri, 2015). Information is also collected through dumpster diving (Tetri & Vuorinen, 2013; Krombholz, 2015) or through socio-technical approaches (Krombholz, 2015), such as borrowing a victim’s computer to check email. Ultimately, a social engineering attack is predicated on the ability to influence people to share sensitive information (Mouton et al., 2016).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The social engineering literature does not explore this bilateral interaction.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm’s decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

A study by Junger et al. (2017) found that 80% of subjects disclosed information upon request because humans tend to trust one another. A number of studies found that

the use of social media to share information about oneself is a common source of information used to socially engineer targets and gain access to secure systems (Edwards et al., 2017; ; Junger et al., 2017; Tayouri, 2015). Other studies explored how to provide an adequate level of training to convey information about how social engineering works in order to address information security in organizations (Flores & Ekstedt, 2016; Junger et al., 2017; Mouton et al., 2016; Schaab et al., 2017; Tayouri, 2015; Thompson, 2006). These studies indicate a strong interest in the bilateral interaction between the cognitive and informational dimensions, and passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

Physical methods for gathering information include dumpster diving (sorting through organizational trash to find information) or theft of credentials (e.g. identification badges) (Krombholz, 2015; Tetri & Vuorinen, 2013). Socio-technical approaches, such as lending a USB drive also depend on physical devices being used by human targets (Krombholz, 2015). These elements of the social engineering literature specifically address the bilateral cognitive – physical interaction, passing this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

The social engineering literature does not explore this multilateral interaction.

B5.6 Summary of Category 4 Theory

Table B4. Four Tests of Category 4: Online Behavior Theories

Theory	Test 1 P – I	Test 2 I – C	Test 3 P – C	Test 4 P – I – C
Anonymity	✓	✓	X	X
Bourdieu's Field Theory	X	✓	✓	X
Routine Activity Theory	✓	✓	X	X
Vigilantism	X	✓	X	X
Social Engineering	X	✓	✓	X

B6. Category 5: Organizational Theories (51 articles)

Organizational theories explore the interaction of cyberspace and organizational structures, culture, and behavior as it relates to the impact of technology on existing organizations, and the emergence of organizations within cyberspace, including themes of agency, power, and social exchange.

B6.1 Organizational Structure Theories (13 articles)

Because of its virtual nature, cyberspace is both a host of new kinds of organizations and a capability affecting the structure within organizations. The *social web* or *Web 2.0* both terms for the media technologies that enable user generated content (Kostakis, 2012), are enabling organizations to change internal and external interactions (Harknett, 2003; Alfano, 2011; Coates, 2002; Contreras et al., 2012; Thatch & Woodman, 1994; Welp et al., 2007). The transformational nature of cyberspace challenges traditional organizational controls and existing power structures, causing a rivalry for governance of cyberspace and information in order to maintain dominance (Drissel, 2007; Okediji, 2003). The anarchical nature of cyberspace makes governance of the domain very difficult; however, these same Web 2.0 technologies are enabling individuals to interact

with one another to form new kinds of networked virtual organizations (Kostakis, 2012; de Laat, 2012; Harknett, 2003; O’Neil, 2014; Tynes, 2007; Holt, 2013).

Impact on organizations (6 articles)

A number of researchers explored how government bureaucracies are using social web technologies to interact with their citizenry (Alfano, 2011; Welp et al., 2007; Coates, 2002). Alfano (2011) conducted a qualitative study of the Venetian government’s use of the social web to improve services; Welp et al. (2007) studied the use of the social web in Catalonia, and Coates (2002) explored the implementation of e-business services in the United States government. In all three cases, they found that the use of web technologies increased the speed and flexibility of bureaucratic response to the citizenry (Alfano, 2011; Coates, 2002; Welp et al., 2007), although this often created a greater burden on the employees (Alfano, 2011; Welp et al., 2007) because of information systems that were not integrated (Welp et al., 2007), resulting in the rise of the “Web-level bureaucrat” (Coates, 2002, p. 38). Another impact to organizations is *hyper-connectivity* and the expansion of workaholism that results from devices that allow employees to work from anywhere, anytime (Contreras et al., 2012). Harknett (2003) explores the changing nature of bureaucracies due to the access, availability and speed of information, which runs counter to hierarchical, bureaucratic information flows and communication patterns. The changes in information flows shift the locus of knowledge within organizations, which in turn threatens the existing power structures (Thatch & Woodman, 1994).

Rivalry for governance (2 articles)

Cyberspace threatens existing power structures by democratizing information flows and distributing power across multiple locations (O’Neil, 2014). Further, the ability to

interact in a virtual domain enables the rise of transnational and transcorporate organizations (Drissel, 2007). The loss of power is a threat to self-interest, resulting in an attempt by nation states and corporations to control cyberspace (Drissel, 2007) or information (Okediji, 2003).

Growth of new organizations (5 articles)

The social web has enabled the growth of new organizations, such as Wikipedia (de Laat, 2012; Kostakis, 2012; O’Neil, 2014) or black market e-commerce sites (Holt, 2013). Tynes (2007) conducted a study of the virtual nation of Sierre Leone, where the citizenry maintained their nation through an online community called *Leonenet* when the structural integrity of the nation state collapsed. Within these seemingly anarchic organizations, structure emerges as members implement self-governance through roles such as moderators (Kostakis, 2012) or technology controls (de Laat, 2012). One of the structural markers of these online, virtual organizations is the network of networks (Kostakis, 2012; O’Neil, 2014; Harknett, 2003; Thatch & Woodman, 1994), or *heterarchy*, which is a “looser environment allowing for the existence of multiple teams of participants working simultaneously in a variety of possibly opposing directions” (Kostakis, 2012, p. 313). Interestingly, even in these anarchic environments, participants will accept a measure of control (de Laat, 2012; Harknett, 2003; Kostakis, 2012; O’Neil, 2014).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The organizational structures literature does not explore this bilateral interaction.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

When organizational leaders emerge in the virtual communities of cyberspace, their emergence is predicated on the concept of “hacker-charisma” (O’Neil, 2014, p. 876), which is dictated by demonstrated expertise and competency, making technical skills and knowledge contributions critical (Kostakis, 2012; Harknett, 2003; de Laat, 2012; O’Neil, 2014; Holt, 2013). In bureaucratic organizations, the locus of knowledge is equated with the locus of power (Thatch & Woodman, 1994). These organizations structure themselves around knowledge flows (Thatch & Woodman, 1994) and derive their power from the control of knowledge, for example intellectual property (Okediji, 2003) or governance of knowledge exchanges (Drissel, 2007). In both cases, power is derived from and the organization is structured around the interaction between cognitive and informational dimensions, and passes this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

The introduction of physical devices, such as smart phones and portable computers, which allow workers to connect from anywhere at any time has led to a notable increase in workload and office hours (Contreras et al., 2012). This change in work behavior is directly related to the cognitive – physical interaction, and passes this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

The organizational structures literature does not explore this multilateral interaction.

B6.2 Agency Theory (12 articles)

Agency is defined in social – cognitive theory as existing on three levels: direct personal agency; proxy agency, where an intermediary is engaged to secure a desired result; and collective agency, which is an interdependent and socially coordinated effort (Workman et al., 2008). Cyberspace has had several impacts on agency and principal – agent relationships.

Because of the borderless nature of cyberspace, it enables transnational communities to emerge (Ebeling, 2003) enabling geographically distributed populations to meet and exchange information to organize politically and build new virtual communities, allowing marginalized groups to increase their collective agency, something that was not possible prior to the dawn on the Internet (Ebeling, 2003; Gwynne, 2013). This borderless environment has also created questions regarding employee – employer relationships with respect to liability for the outcomes of online

behavior such as sexual harassment (Gelms, 2012), insider threat (Malone, 2013), and employee monitoring (White, 1992).

The spatial and temporal separation in online environments has created a great deal of uncertainty in economic exchange (Pavlou et al., 2007) because of information asymmetries, particularly with respect to e-commerce models (Izquierdo-Yusta et al., 2011; Luo & Donthu, 2007; Vaidyanathan et al., 2012; Pavlou et al., 2007). This uncertainty can be mitigated with the implementation of information security approaches (Pavlou et al., 2007; Vaidyanathan et al., 2012), but trying to build information security culture presents its own set of principle – agent challenges (Karanja, 2016; Knapp & Ferrante, 2014), such as how to incentivize employee compliance with security policies (Knapp & Ferrante, 2014) or where to position the role of Chief Information Security Officer (CISO) within the organization (Karanja, 2016).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

Workman et al. (2008) proposed using agency theory to develop security ontologies in mobile ad hoc networks to create agents that enable a self-healing approach in wireless networks. Security policies can be codified into information and communication system to create dynamically organized computational models that will simultaneously perform multiple operations to interact with the environment in which they operate (Workman et

al., 2008). This approach to securing wireless networks speaks directly to the physical – informational interaction, and passes this test.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

Ebeling (2003) Through the use of networked computer-based media, Africa-descended populations throughout the world can meet and exchange information in cyberspace and organize politically, as well as forge new, virtual communities that previously may not have been possible without the aid of the Internet. While Gwynne 2013 A narrative analysis of the book Girls of Riyadh to explore the story in the context of the Women's movement in Saudi Arabia. Agency is both greater on the internet because of the transnational space and the disembodiment within the virtual community, but social structures follow the young women onto the internet with respect to male dominance.

The open nature of the Internet and the associated threats to information security creates uncertainty in e-commerce models (Vaidyanathan et al., 2012; Pavlou et al., 2007). Key sources of this uncertainty in buyer – seller relationship stem from information asymmetry, and fears of seller opportunism (Pavlou, 2007; Lou & Donthu, 2007; Izquierdo-Yusta et al., 2011). Luo & Donthu (2007) explored the use of cyber-intermediaries in electronic markets where proxy agents were used to deal with asymmetric information and information overload to sort through and present the best information regarding price and product quality to support decision making. Izquierdo-

Yusta et al. (2011) examined this proxy agent approach in the context of how travel sites are used to enable consumer decision-making, finding that trust in the source of the mediated information is a prime factor in the decision to purchase.

Pavlou et al. (2007) found that when buyers encounter a website information they perceive as useful regarding the seller's characteristics, the products, and the seller's information practices, this helps them to overcome the uncertainty created by the online relationship.

These applications of agency theory and the principal – agent perspective highlight the cognitive – informational interaction, passing this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

The agency theory literature does not explore this bilateral interaction.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

The agency theory literature does not explore this multilateral interaction.

B6.3 Power/Resistance Theories (12 articles)

From a Foucaultian perspective, knowledge and power are connected and mutually reshaping, and examples of this power – knowledge effect can be found throughout the

internet (Beresford, 2003). The balance of power in cyberspace is a tension between discourses (Denegri-Knott, 2006; Jorgensen, 2017; Liu, 2013; Rohle, 2005), where “the nonmaterial nature of the Internet renders ‘reality’ and ‘illusion’ indistinguishable” (Beresford, 2003, p. 84). In an environment of pure communication and virtual identities, the direct association between words, symbols and meaning is ambiguous (Beresford, 2003; Brickell, 2012), but the familiarity of these symbols provides legitimacy in a world where “there is no physical form to play the role of ‘real’” (Beresford, 2003, p. 84) leaving it up to individuals “to sort through the wealth of information according to aesthetic and ethical values, and the greater the amount of available information, the greater is the challenge” (Nuyen, 2001, p. 54).

Power and discourse are inherently intertwined because they legitimize, construct and provide meaning (Jorgensen, 2017). There is no power without resistance (Liu, 2013), because resistance is a form of agency (Smith et al., 2010) which is played out on the internet through competing narratives (Denegri-Knott, 2006; Jorgensen, 2017; Liu, 2013; Rohle, 2005).

The internet also enables surveillance to an extraordinary degree, leading to mistrust of government (Steinmetz & Gerber, 2015) and privacy concerns (Steinmetz & Gerber, 2015; Mortenson et al., 2015). Ultimately surveillance is about power, which can be seen in both positive terms where a health care provider is monitoring a patient’s health with wireless devices, and negative terms where information is used to manipulate and control others (Mortenson et al., 2015).

The ability to control the internet is a constant source of tension between individuals and the nation state because of the intertwinement of technological mediation,

power, and resistance (Rao et al., 2015). The internet challenges national power, driving nation states to seek out ways to target the privately operated technological points of control within the infrastructure (Zajko, 2016).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The power literature does not explore this bilateral interaction.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

Jorgensen (2017) examined eDemocracy in Greenland exploring competing discourses between the government and the citizenry. The government discourse “constructs and legitimizes eDemocracy” (p. 213) as a way to facilitate citizen – legislator – administration dialog, while the citizens often exploit social media for political purposes to challenge the democratic establishment (Jorgensen, 2017). Denegri-Knott (2006) explores the use of social media by customers as a means to challenge firm market power. These examples speak directly to the interaction between cognitive and informational interactions, passing this test.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

According to Zajko (2016), the organizations who operate the Internet's points of control, such as the undersea cables and switching infrastructure will continue to gain power as dependence on the infrastructure and thus the organizations which control it increases. These organizations will "mediate interactions with a host of networked devices" (Zajko, 2016, p. 90). This observation about the power Internet companies will accrue speaks specifically to the cognitive interaction with the physical infrastructure, passing this test.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

Mortenson et al. (2015) examines the use of technologies in senior living arrangements. He explains that by sharing data with caregivers, health monitoring devices and closed circuit TV monitors that observe people movements can allow seniors to maintain their independence, while at the same time forcing them to sacrifice privacy (Mortenson et al., 2015). However, the purpose of this example is to study the impact of surveillance technologies as they relate to privacy and independence for seniors. The purpose is not to examine the interactions amongst the devices, people and information.

Therefore, it does not pass the multilateral cognitive – informational – physical interaction test.

B6.4 Social Exchange Theory (14 articles)

Social Exchange Theory (SET) proposes that human actions and relationships are motivated by expectations of returns and based on the perception that rewards will exceed the expected costs (Benoit et al., 2016; Clinton, 2011). When the expected rewards do not exceed the costs, people will seek alternative avenues of exchange which prove to be more beneficial (Benoit et al., 2016; Clinton, 2011). This social exchange phenomenon is visible in online communities such as ecommerce sites (Shiau & Luo, 2012; Luo, 2002; Hidayanto et al., 2017; Chen, M.J. et al., 2010; Liu et al., 2011; Willer et al., 2012) bartering sites, (Hsu et al., 2017; Willer et al., 2012), Internet dating sites (Shtatfeld & Barak, 2009; Robnett & Feliciano, 2011), and social media (Benoit et al., 2016; Liu et al., 2016; Jinyang, 2015). Social exchange has also been used to explore issues of cybersecurity compliance, both at the public – private partnership level (Clinton, 2011) and at the employer – employee level (Teh et al., 2015).

In online communities, social exchange relationships build trust over time and develop based on communications interactions between members of the virtual community (Chen, M.J. et al., 2010). Because of the asymmetric distribution of information between transactional partners, online environments create a great deal of uncertainty, which is a critical barrier to purchase decisions (Shiau & Luo, 2012; Luo, 2002; Hidayanto et al., 2017; Chen, M.J., et al., 2010; Liu et al., 2011; Willer et al., 2012; Hsu et al., 2017). Online engagement can alleviate this uncertainty with a variety of citizenship behaviors including:

1. Helping new members (Chen, M.J., et al., 2010; Hsu et al., 2017)
2. Deterring inappropriate behavior (Chen, M.J., et al., 2010)
3. Sharing of information and knowledge (Chen, M.J., et al., 2010; Jinyang, 2015; Shiau & Luo, 2012)

In organizations, employees consider their affiliation with an employer to be an exchange that results from a balance between benefits and outcomes for the two parties (Teh et al., 2015). Teh et al. (2015) found that when employees perceive their work contribution as valued and reciprocated, they will respond with prosocial behaviors such as increased work performance and compliance with organizational policies, including information security requirements; however, if employees feel a negative social exchange relationship, they will often exhibit noncompliance with organizational policies. Clinton (2011) carries this cybersecurity compliance behavior to the corporate level, examining potential public policy approaches to security compliance behaviors from private companies with respect to cybersecurity investments in critical infrastructure, suggesting that it is impractical for the government to attempt to seize control of the cybersecurity public – private partnership and force compliance with regulatory requirements. Instead, he proposes that “the government should compensate private entities for making investments that align with the government’s perspective, such as the social contract, rather than mandating that the shareholders subsidize the government function of providing for the common defense” (Clinton, 2011, p. 97).

Theory Testing:

Test 1: The bilateral physical – informational interaction test

Do the theories in this category seek to illuminate firm interactions between physical devices, the networks that connect the devices, and the data, software, and information that travels through the network of devices?

The social exchange theory literature does not explore this bilateral interaction.

Test 2: The bilateral cognitive – informational interaction test

Do the theories in this category seek to clarify the interactions between a firm's decision makers, stakeholders, and rivals, and the consumption of data and information as it relates to decision-making and human action?

Benoit et al. (2016) and Liu et al. (2016) analyze the exchanges of information in social media communities, such as LinkedIn, Facebook, and Twitter, where information is exchanged among members and with the provider of the social media platform. In terms of social exchange, the willingness of members in a virtual community to share valuable information with one another is the foundation of maintaining trust within the community (Jinyang, 2015). Liu et al. (2016) found that greater self-disclosure indicated trust in the service provider and the other members of the online community based on the perception that one's personal information would not be misused and that information disclosure would be reciprocated.

Studies of internet dating found that people's demographic variables, such as socio-economic status, education (Shtatfeld & Barak, 2009), and race (Robnett & Feliciano, 2011), as well as other physical appearance characteristics as self-reported using a range of data elements contributed to the decision to initiate dating communications (Shtatfeld & Barak, 2009; Robnett & Feliciano, 2011).

In each of these examples, social exchange theory is being used to explore the cognitive – informational interaction.

Test 3: The bilateral cognitive – physical interaction test

Do the theories in this category seek to explain the interactions between a firm's decision makers, stakeholders, and rivals, and the use of technological devices to communicate and automate processes?

The social exchange theory literature does not explore this bilateral interaction.

Test 4: The multilateral physical – informational – cognitive interaction test

Do the theories in this category seek to explain the dynamic, multilateral interactions between a firm's decision makers, stakeholders, and rivals, and the use of informational capabilities and technological devices to communicate, automate processes, and consume data and information as it relates to decision making and human action?

The social exchange theory literature does not explore this multilateral interaction.

B6.5 Summary of Category 5 Theory

Table B5. Four Tests of Category 5: Organizational Behavior Theories

Theory	Test 1 P – I	Test 2 I – C	Test 3 P – C	Test 4 P – I – C
Organizational Structures	X	✓	✓	X
Agency Theory	✓	✓	X	X
Power/Resistance	X	✓	✓	X
Social Exchange Theory	X	✓	X	X

B7. Summary of Findings

B7.1 Discussion of Results

The findings of the above tests are summarized in Table B6, and visually represented in Figure B6. A theory either fails or passes each test, with a failure indicated as a cross ('X') and a pass as a checkmark (✓).

Table B6. Summary of Findings

Theory	Test 1 P – I	Test 2 I – C	Test 3 P – C	Test 4 P – I – C
Category 1: Technology Growth				
Sociomateriality (Critical Realism)	X	✓	✓	X
Sociomateriality (Agential Realism)	X	X	X	X
Moore's Law	✓	X	X	X
Taxonomies	✓	X	X	X
Category 2: Decision Making				
Totalitarianism/Quasitotalitarianism	X	✓	X	X
Game Theory	X	✓	X	X
Salience	X	✓	X	X
Category 3: Information & Physical Assets				
Knowledge Management & Knowledge Based View (KBV)	✓	✓	✓	X
Resource Based View (RBV)	X	X	✓	X
Information Security	✓	✓	✓	X
Information Theory	✓	✓	X	X
Resilience	✓	✓	✓	X
Category 4: Online Behavior				
Anonymity	✓	✓	X	X
Bourdieu's Field Theory	X	✓	✓	X
Routine Activity Theory	X	✓	X	X
Vigilantism	X	✓	X	X
Social Engineering	X	✓	✓	X
Category 5: Organization Theory				
Organizational Structures	X	✓	✓	X
Agency Theory	X	✓	X	X
Power/Resistance	X	✓	✓	X
Social Exchange Theory	X	✓	X	X

B7.2 The Bilateral Physical – Informational Interaction Test

To pass this test, a theory had to demonstrate that the object of study was the interactions taking place between elements of the physical and informational dimensions of cyberspace. For example, Burmester et al. (2012) describes cyber-physical systems as entities in the physical environment that are monitored and controlled by integrating them into a distributed computing environment. The preponderance of literature investigating

this bilateral physical – informational interaction fell into *Category 1: Technology Growth* and *Category 3: Information & Physical Assets*. One particular avenue of research in the Anonymity literature, the identity management studies, which explore machine-to-machine information exchanges (Al-Muhtadi et al., 2018; Jardine, 2016; Li et al., 2018; Qui et al., 2017), also examines this interaction.

Choo (2011) explored the use of various smart devices as launching points for malicious software in a study applying Routine Activity Theory to cybercrime, but his was the only study within this literature strain to examine this interaction, while Workman et al. (2008) proposed the use of Agency theory to develop security ontologies in mobile ad hoc networks. Although these specific individual studies examine the bilateral physical – informational interaction, as a general rule, neither Routine Activity Theory nor Agency Theory are used as theoretical tools for the study of this interaction, thus despite these specific studies, these theories do not pass the physical – informational interaction test.

Category 1 includes Sociomateriality, Moore's Law, and a large number of Taxonomies. Sociomateriality is divided between camps: the critical realist perspective and the agential realist perspective. The critical realists are led by Leonardi (2007, 2010, 2011, 2013) and Leonardi and Barley (2008), while Orlikowski (2006, 2007, 2010), Orlikowski and Scott (2008, 2015), and Scott & Orlikowski (2007, 2009, 2013) as the recognized as the principals for the agential realists. Regardless of which perspective is applied, sociomateriality explores the interaction between IT artifacts and people, thus it did not pass this test.

Moore's law is an empirical observation related to the processing capacity of circuit

boards. There are a number of studies that extrapolate Moore's Law to include the exponential growth rate of other physical devices that are used for data storage (Ceruzzi, 2005) software (Hemsath, 2014) and networking technologies such as fiberoptic cables used to send data (Ceruzzi, 2005), making it seem as if it explores the physical – informational bilateral interaction. However, Moore's law is the observation of an empirical phenomenon, which disqualifies it as a theoretical tool for the study of this interaction.

A number of academic articles developed taxonomies for cybersecurity, the vast majority of which explore the cyberattack phenomenon, seeking to classify the different types of attacks (Iqbal et al, 2016; Hernandez-Ardiet, 2013; Fitzpatrick & Dilulio, 2015; Aleroud & Karabatis, 2017; Uzunov & Fernandez, 2014; Somani et al, 2017; Howard & Longstaff, 1998; Kim et al, 2010). Although each of these taxonomies satisfied the test criteria by investigating the interactions between elements of the physical and informational domains, “taxonomies” are not a theory, but rather a classification scheme. The physical – informational interaction test can be applied to a *specific* cyber taxonomy, but when applying this test to taxonomies in general, it provides a null result.

Because sociomateriality fails this test, and both Moore's Law and Taxonomies are disqualified from the study, Category 1: Technology Growth fails to satisfy the physical – informational bilateral interaction test.

Category 3 includes Knowledge Management, the Knowledge-Based View (KBV), the Resource Based View (RBV), Informational Security, Information Theory, and Resilience. With the exception of the RBV, which explores the value of the IT artifact (Melville et al., 2004), each of the theories in this category pass the physical –

informational interaction test. The Knowledge Management literature explores the use of information technology as it relates to the creation, capture, and dissemination of information within the firm (Zhang & Venkatesh, 2017; Zhang, 2017; Sabherwal & Sabherwal, 2005; Wang et al., 2013), while the KBV literature examines how this knowledge can be leveraged as a strategic asset (Hult, 2003). Information science theorists differentiate between the containers of information, such as books, newspapers, and records and the data or information contained within them (Yuxiao, 1988; Pemberton, 1993; McGinn, 1994), and use Information theory to develop algorithms for anomaly detection (Ahmed et al., 2016; Behal & Kumar, 2017; Hong & Chen, 2014; Majda & Gershgorin, 2011) or natural language programming (Bannard et al., 2017; Hillebrandt & Barclay, 2017; Mahowald et al., 2013; Yuxiao, 1988). Information Security and Resilience researchers explore systems architectures to separate informational elements across multiple physical devices in order to build resilience (Danzi et al., 2018), and other systems engineering frameworks to secure cyber-physical system (DiMase, 2015).

Only Category 3 theories and Anonymity technologies passed this test, providing evidence that only the computer science and information systems communities are exploring the physical – informational interaction.

B7.3 Test 2: Bilateral Cognitive – Informational Interaction Test

The criterion to pass this test requires that the theory being tested demonstrates that the object of study was the interactions taking place between elements of the cognitive and informational dimensions of cyberspace. Theorists have been exploring this bilateral interaction for decades, and probably longer, although this study did not examine

literature prior to 1960. Almost every theory examined for the purposes of this study explored the bilateral interaction between the cognitive and informational dimensions.

Category 1 had only one theory examine this interaction – the sociomateriality critical realist perspective. Leonardi and Barley (2008) explore the routine interaction of individuals and organizations with information technologies, explaining that “most information technologies are software rather than solid physical objects. Although software lacks physical properties, it is not conceptual because it limits how it is used in much the same way physical artifacts do (Leonardi & Barley, 2008). However, the critical realist perspective conflates the informational and physical dimensions of cyberspace by bundling the hardware (physical elements) with the software and data (informational elements) into “technological artifacts,” which goes beyond the specific bilateral interaction being examined with this test. If one ignores the merger of two cyber dimensions into the IT artifact, sociomateriality from a critical realist perspective can somewhat pass this test.

Category 2 includes Totalitarianism/Quasitotalitarianism, Game Theory, and Salience. Each of these theories is used to examine how information is processed cognitively for the purpose of decision making, passing this test. As a tool of totalitarianism, propaganda and disinformation in the age of the Internet has “become magnified by an increasing number of information streams, resulting in a reality distortion effect both within the targeted area and beyond” (Fitzgerald & Brantly, 2017) because of the link between information manipulation and its power to skew cognitive biases, affecting how humans make decisions. Game theory models how firms share knowledge (Wu et al., 2015; Ezhei & Ladani, 2017; Gal-Or & Ghose, 2005; Gladstein &

Reilly, 1985; Gordon et al., 2015) or how rival hackers share information (Hausken, 2017) in order to make better decisions, as well as how strategic rivals leverage information in competition with one another. Lastly, the Salience literature explores how information is processed cognitively in the perception of risk based on the framing of questions (Tversky & Kahneman, 1981; Rosoff et al., 2013; van Schie & van der Pligt, 1995), the presentation of risk information (Stone et al., 2003), cultural background (Gelekanycz, 1997), or individual perceptions of risk (Kahneman & Tversky, 1979; Taylor & Thompson, 1982).

With the exception of the RBV, all theories in Category 3 passed this bilateral cognitive – informational test. The Knowledge Management literature considers human beings to be repositories of information (Argote & Fahrenkopf, 2016), with the KBV taking it a step further by exploring how humans have the ability to exploit information for strategic advantage (Hsu & Sabherwal, 2012). Within the information security literature, behavioral information security seeks to understand what inspires end-user conformance to organizational information security policies in order to improve organizational information security (Belanger et al., 2017; Cuganesan et al., 2018), while information security economics attempts to understand and inform how organizations make information security investment decisions (Dor & Elovici, 2016; Huang & Behara, 2013; Mayadunne & Park, 2016; Angst et al., 2017; Chen et al., 2011). Information scientists describe information as a uniquely human phenomenon (Yuxiao, 1988) in which the right information enables the reduction of uncertainty to support optimal decision making (Pemberton, 1993). To close, the Resilience literature explores human behavior as an element of cyber resilience, finding that for most people the objective is to

complete their mission, rather than to be secure, resulting in noncompliance with cybersecurity policies when the rules inhibit job completion (Gisladottir et al., 2017).

Anonymity, Bourdieu's Field Theory, Routine Activity Theory, Vigilantism, and Social Engineering literature make up Category 4. These theories examine online social behavior, including how people build virtual identities, interact with one another, form communities, and commit crimes, and each of these theories passed this test for the bilateral cognitive – informational interaction. Identity is of particular interest in the Anonymity literature because there is a perception that online environments can conceal identity; however, as organizations retain more and more data, the internet is being transformed “from a context of relative obscurity to one of greater transparency,” making it easier to link individuals with the data they generate (Cherner, 2017; Crump, 2003). Bourdieu's Field Theory defines cultural capital as “accumulated knowledge” (Stevenson, 2016) linking traditional and social media in a causal relationship with people's beliefs and political opinions (Handley & Rutigliano, 2012; Couldry, 2003). The use of information sharing for the purpose of victimization is the subject of Routine Activity Theory studies, finding evidence of a link between online information sharing behaviors such as banking, shopping, and communicating with being victimized by cyberbullies and cybercriminals (Kalia & Aleem, 2017; Reyns, 2013; Chen et al., 2017). Vigilantism also explored information sharing, although in this stream of literature, personal information was used to “name and shame” corrupt officials (Ong, 2012; Cheong & Gong, 2010) or cyberaggressors (Jane, 2016; Arvanitidis, 2016) through online publication of their perceived crimes. As a final point, the Social Engineering literature examines humans as the most vulnerable element of an information system.

Because humans tend to trust one another and will share information upon request (Junger et al., 2017), social media is a common source of information used by social engineers to target and gain access to secure systems (Edwards et al., 2017; Junger et al., 2017; Tayouri, 2015).

Category 5 contains theories of organizations, including Organizational Structures and Weberian Theory, Agency Theory, Power and Resistance Theory and Social Exchange Theory, all of which meet this criterion. Despite a lack of formal governance, Organizational Theories find that people will still form and govern virtual communities within cyberspace, conferring governance power based on technical skill and knowledge contributions (Kostakis, 2012; Harknett, 2003; de Laat, 2012; O’Neil, 2014; Holt, 2013). Agency perspectives find that the ability to share information in virtual communities can increase agency in marginalized populations (Gwynne, 2013; Ebeling, 2003), while the asymmetry of information in the online environment impacts the principal – agent relationship in ecommerce (Pavlou, 2007; Lou & Donthu, 2007; Izquierdo-Yusta & Martinez-Ruiz, 2011), requiring cyber-intermediaries to mitigate uncertainty (Lou & Donthu, 2007). From a Foucaultian perspective, knowledge and power are connected and mutually reshaping, and examples of this power – knowledge effect abound on the internet (Beresford, 2003). Further, balance of power in cyberspace is a tension between competing discourses (Denegri-Knott, 2006; Jorgensen, 2016; Liu, 2013; Rohle, 2005) where the Internet causes ‘reality’ and ‘illusion’ to become indistinguishable (Beresford, 2003). Finally, Social Exchange Theory is applied to explore online dating communications as they relate to self-reported socioeconomic (Shtatfeld & Barak, 2009) and racial (Robnett & Feliciano, 2011) data descriptors. The SET studies also examine

social exchanges as they relate to information sharing on social media platforms (Benoit et al., 2016; Liu et al., 2016; Jinyang, 2015).

The way humans use information is a well-researched phenomenon, and every theory except the Resource-Based View and the agential realist perspective of sociomateriality passed this test.

B7.4 Test 3: Bilateral Cognitive – Physical Interaction Test

In order to pass this test, the theory being tested must demonstrate that the focus of the study was the interactions taking place between elements of the cognitive and physical dimensions of cyberspace. Of the twenty-one theories examined in this study, only nine theories passed this test, and only three of these nine theories, all of which fell into Category 3, passed the first two tests: Knowledge Management, Information Security, and Resilience.

From Category 1, the sociomateriality critical realist perspective examines “sociomaterial imbrications” (Leonardi, 2013), merging the tangible and the intangible into a single material entity that interacts with the human or social entity. Category 4 offers Bordieu’s Field Theory, which explores the impact of the sociomateriality phenomenon of people using IT artifacts in order to communicate with one another (Walshaw, 2015; Fuchs et al., 2009) or to acquire and disseminate information (Barnard, 2016; Jansson, 2016; Handley & Rutigliano, 2012) and Social Engineering Theory, which identifies the use of physical methods such as dumpster diving (sorting through organizational trash to find information) or theft of credentials (e.g. identification badges) (Krombholz, 2015; Tetri & Vuorinen, 2013) to collect information, and socio-technical approaches, such as lending a USB drive to human targets (Krombholz, 2015) with the

expectation that these devices will be connected into secure systems. Both Organizational Structures, which have been impacted by the introduction of physical devices such as laptop computers and smart phones (Contreras et al., 2012), and the Power/Resistance literature, which explores the power of companies which own the Internet's points of control (Zajko, 2016), are captured in Category 5, and both theories pass this test. While each of these theories passed test 2, none of these theories passed test 1, removing them as potential theoretical contenders.

Within Category 3, Knowledge Management and the KBV, the RBV, Information Security, and Resilience theories pass this third test. The Knowledge Management literature suggests that knowledge management systems are only valuable when employees use them (Wang et al., 2013). The RBV literature suggests that IT resources generate the greatest amount of capability when used in conjunction with human resources (Ravichandran et al., 2014; Bharadwaj, 2000; Ray et al., 2004; Lioukas et al., 2016). Appropriate access between an object of security, or physical device, and an agent or stakeholder, both humans, is defined in the Information Security Literature. The resilience literature examines cyber-physical & human systems, such as the integration of technology and people through such things as neural prosthetics and computer – brain interfaces (Netto & Spurgeon, 2017; Vanderhaegen, 2017; Herrington & Aldrich, 2013). Each of these lines of inquiry satisfy this test for a bilateral interaction between the cognitive and physical dimensions of cyberspace. Thus, three theories have passed all the bilateral interaction tests: Knowledge Management, Information Security, and Resilience.

B7.5 Test 4: Multilateral Physical – Informational – Cognitive Interaction Test

Although the Knowledge Management, Information Security, and Resilience literature explore all three dimensions of cyberspace, the avenues of investigation are only bilateral in nature. One can infer that the multilateral physical – informational – cognitive interaction exists, but none of these theories is designed to explore this multidimensional interactive phenomenon. Individual studies within each stream of literature will focus on one set of interactions, for example, the preponderance of the Knowledge Management literature falls into one of two disciplines, strategy and organizational theory, both of which focus on the cognitive – informational interaction.

Organizational theorists gravitate toward the investigation of intraorganizational knowledge sharing (Argote & Fahrenkopf, 2016; Chen et al., 2010; Hsu & Sabherwal, 2012; Lewis et al., 2007; McIver et al., 2013; Oldroyd & Morris, 2012; Sanchez & Mahoney, 1996; Sears & Hoetker, 2014; Sung & Choi, 2012; van Ginkel & van Knippenberg, 2008), while the strategists explore leveraging knowledge as it relates to resources and capabilities (Turner & Makhija, 2006; Howard et al., 2013; Forbes, 2007; Hult, 2003), innovation (Alexy et al., 2013; Chatterji & Fabrizio, 2012; Ranganathan & Rosenkopf, 2014), and strategic interorganizational alliances (Alexy et al., 2013; Chatterji & Fabrizio, 2012; Ranganathan & Rosenkopf, 2014; Alnuaimi & George 2016; Howard et al., 2013; Schillebeeckx et al., 2016). There is a third stream of knowledge management literature – knowledge management systems – which focuses on the use of information technology to provide a platform for “knowledge articulation, codification, and communication” (Wang et al., 2013). Although all three bilateral interactions are

investigated, the investigations are conducted with respect to only one of these bilateral interactions. Thus, knowledge management theory fails this fourth and final test.

The Information Security literature follows a similar pattern, dividing along three avenues. The first, technical information security, investigates the physical – informational interaction (Burmester et al., 2012; Cavusoglu et al., 2009; Chen et al., 2015; Johnston & Warkentin, 2010). The second, behavioral information security, investigates the cognitive – physical interaction or the cognitive – informational interaction ((Belanger et al., 2017; Bulgurcu et al., 2010; Crossler et al., 2013; Cuganesan et al., 2017; Lee et al., 2016; McCormac et al., 2017; Posey et al., 2013; Safa & Von Solms, 2016; Safa et al., 2016; Siponen et al., 2014). Last, information security economics, investigates the cognitive – informational interaction (Angst et al., 2017; Chen et al., 2011; Dor & Elovici, 2016; Gordon et al., 2002; Hovav & D'Arcy, 2003; Huang & Behara, 2013; Love et al., 2011; Mayadunne & Park, 2016). There is no existing stream of research with the Information Security literature where all three interactions are examined simultaneously, and it too fails the multilateral interaction test.

Only the Resilience literature directly referenced the multidimensionality of cyberspace. DiMase et al. (2015) identify a future need for a framework that integrates an “approach across physical, information, cognitive and social domains to ensure resilience” (p. 291). In the absence of such an integrated framework, they proposed the use of a multi-scale systems engineering framework that addressed only the physical – informational bilateral interaction. In fact, this particular study suggests that there is a specific need for the Cyber-Based View framework to address the complexity of cyber-physical & human systems. Although the Resilience literature identifies a need for the

Cyber-Based View framework, the resilience theory investigations themselves do not pass this fourth and final test.

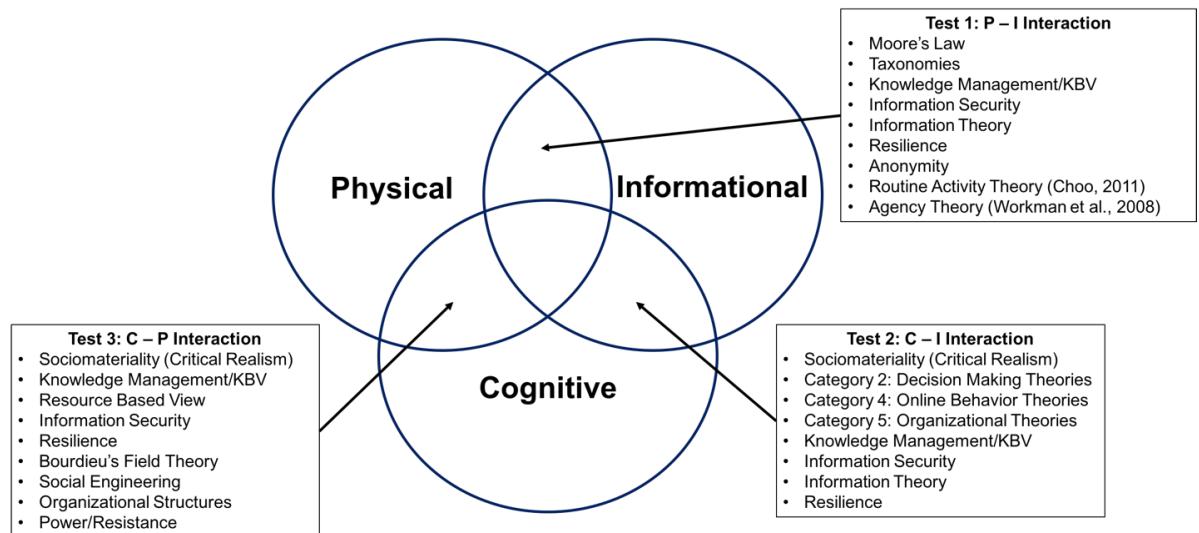


Figure B1. Summary of Findings

B8. Data Sources for Meta-Analysis

- Abdella, M. and Kemer, E. (2014). Eliciting Prospect Theory When Consequences Are Measured in Time Units: "Time is Not Money." *Management Science*, 60(7), 1844-1859.
- Adinolfi, G. (2012). The Institutionalization of Propaganda in the Fascist Era: The Cases of Germany, Portugal, and Italy. *The European Legacy*, 17(5), 607-621.
- Ahmed, M., Mahmood, A., and Hu, J. (2015). A Survey of Network Anomaly Detection Techniques. *Journal of Network and Computer Applications*, 60, 19-31.
- Aleroud, A. and Karabatis, G. (2017). Contextual Information Fusion for Intrusion Detection: A Survey and Taxonomy. *Knowledge Information Systems*, 52, 563-619.
- Alexy, O., George, G., and Salter, A. (2013). Cui Bono? The Selective Revealing of Knowledge and Its Implications for Innovative Activity. *Academy of Management Review*, 38(2), 270-291.
- Alfano, G. (2011). Adapting Bureaucracy to the Internet. The Case of Venice Local Government. *Information Policy*, 16, 5-22.

- Al-Muhtadi, J. (2017). Misty Clouds – A Layered Cloud Platform for Online User Anonymity in Social Internet of Things. *Future Generation Computer Systems*, 40, 1-9.
- Alnuaimi, T. and George, G. (2016). Appropriability and the Retrieval of Knowledge After Spillovers. *Strategic Management Journal*, 37, 1263-1279
- Amaya, H. (2017). The Cultures of Anonymity and Violence in the Mexican Blogosphere. *International Journal of Communication*, 11, 3815-3831.
- Ambs, K. et al. (2000). Optimizing Restoration Capacity in the AT&T Network. *Interfaces*, 30(1), 26-44.
- Amin, S.M. (2015). Power and Energy Infrastructure: Cyber Security, Defense, and Resilience. *Georgetown Journal of International Affairs*, Fall 2015, 70-82.
- Angst, C.M., Block, E.S., D'Arcy, J., and Kelley, K. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly*, 41(3), 893-916.
- Anonymous. (2015). More from Moore. *Nature*, 520(7548), 408.
- Aragon-Correa, J. and Sharma, S. (2003). A Contingent Resource Based View of Proactive Corporate Environmental Strategy. *Academy of Management Review*, 28 (1), 71-88.
- Argote, L. and Fahrenkopf, E. (2016). Knowledge Transfer in Organizations: The Roles of Members, Tasks, Tools, and Networks. *Organizational Behavior and Human Decision Processes*, 136, 146-159.
- Argyres, N. and Mostafa, R. (2016). Knowledge Inheritance, Vertical Integration, and Entrant Survival in the Early U.S. Auto Industry. *Academy of Management Journal*, 59(4), 1474-1492.
- Arvanitidis, T. (2016). Publication Bans in a Facebook Age: How Internet Vigilantes Have Challenged the Youth Criminal Justice Act's "Secrecy Laws" Following the 2011 Vancouver Stanley Cup Riot. *Canadian Graduate Journal of Sociology and Criminology*, 5(1), 18-32.
- Assange, Julian, et al. (2012). *Cypherpunks*. US: OR Books, p. 1.
- Baehr, P. (2014). Totalitarianism in America? Robert Nisbet on the "Wilson War State" and Beyond. *American Society*, 45, 84-102.

- Baham, C., Hirschheim, R., Calderon, A.A., and Kisekka, V. (2017). An Agile Methodology for the Disaster Recovery of Information Systems Under Catastrophic Scenarios. *Journal of Management Information Systems*, 34(3), 633-663.
- Balogun, J., Jacobs, C., Jarzabkowski, P., Mantere, S., and Vaara, E. Placing Strategy Discourse in Context: Sociomateriality, Sensemaking, and Power. *Journal of Management Studies*, 51(2), 175-201.
- Bannard, C., Rosner, M., and Matthews, D. (2017). What's Worth Talking About? Information Theory Reveals How Children Balance Informativeness and Ease of Production. *Psychological Science*, 28(7), 954-966.
- Barad, K. (1998). Getting Real: Technoscientific Practices and the Materialization of Reality. *A Journal of Feminist Cultural Studies*, 10(2), 87-90.
- Barnard, S. (2016). 'Tweet or Be Sacked': Twitter and the New Elements of Journalistic Practice. *Journalism*, 17(2), 190-207.
- Bassett, C. (2007). Forms of Reconciliation: On Contemporary Surveillance. *Cultural Studies*, 21(1), 82-94.
- Behal, S. and Kumar, K. (2017). Detection of DDoS Attacks and Flash Events Using Novel Information Theory Metrics. *Computer Networks*, 116, 96-110.
- Belanger, F., Collignon, S., Enget, K., and Negangard, E. (2017). Determinants of Early Conformance with Information Security Policies. *Information & Management*, 54, 887-901.
- Benoit, S., Bilstein, N., Hogreve, J., and Sichtmann, C. (2016). Explaining Social Exchanges in Information-Based Online Communities (IBOCs). *Journal of Service Management*, 27(4), 460-480.
- Beresford, A. (2003). Fouault's Theory of Governance and the Deterrence of Internet Fraud. *Administration & Society*, 35(1), 82-103.
- Bharadwaj, A. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly*, 24(1), 169-196.
- Bordalo, P., Gennaioli, N. and Shleifer, A. (2012). Salience Theory of Choice Under Risk. *Quarterly Journal of Economics*, 127 (3), 1243-1285.
- Bouman, M. (2003). The Machine Speaks the World's Thoughts. *Parachute*, 112, 108-125.

- Boyd, R. and Field, L. (2016). Blind Injustice: Theorizing Anonymity and Accountability in Modern Democracies. *Polity*, 48(3), 332-358.
- Brickell, C. (2012). Sexuality, Power, and the Sociology of the Internet. *Current Sociology*, 60(1), 28-44.
- Bronco, M. and Rodrigues, L. (2006). Corporate Social Responsibility and Resource Based Perspectives. *Journal of Business Ethics*, 69, 111-132.
- Brown, J.S. and Duguid, P. (1998). Organizing Knowledge. *California Management Review*, 40(3), 90-111.
- Buchholz, L. (2016). What is a Global Field? Theorizing Fields Beyond the Nation-State. *The Sociological Review Monographs*, 64(2), 31-60.
- Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: an Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34 (3), 523-548.
- Burmester, M., Magkos, E., and Chrissikopoulos, V. (2012). Modeling Security in Cyber-Physical Systems. *International Journal of Critical Infrastructure Protection*, 5, 118-126.
- Caralli, R. A., Allen, J. H., Curtis, P. D., and Young., L. R. (2010). *CERT® Resilience Management Model, Version 1.0: Improving Operational Resilience Processes*, CERT Program, Carnegie Mellon University.
- Cassinelli, C.W. (1960). Totalitarianism, Ideology, and Propaganda. *The Journal of Politics*, 22(1), 68-95.
- Cavusoglu, H., Raghunathan, S. and Yue, W. (2008). Decision-Theoretic and Game Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, 25 (2), 281-304.
- Cavusoglu, H., Raghunathan, S., Cavusoglu, H. (2009). Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. *Information Systems Research*, 20(2), 198-217.
- Cebula, J.J. and Young, L.R. (2010). A Taxonomy of Operational Cyber Security Risks. *CMU/SEI-2010-TN-028*, 1-48.
- Cecez-Kecmanovic, D. et al. (2014). The Sociomateriality of Information Systems: Current Status, Future Directions. *MIS Quarterly*, 38 (3), 809-830.
- Cerullo, V. and Cerullo, M. (2006). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management*, 21(3), 70-78.

- Ceruzzi, P. (2005). Moore's Law and Technological Determinism: Reflections on the History of Technology. *Technology and Culture*, 46(3), 584-593.
- Chae, B.K., Olson, D., and Sheu, C. (2014). The Impact of Supply Chain Analytics on Operational Performance: A Resource-Based View. *International Journal of Production Research*, 52(16), 4695-4710.
- Chang, L.Y.C. (2018). Citizen Co-Production of Cyber Security: Self-Help, Vigilantes, and Cybercrime. *Regulation & Governance*, 12, 101-114.
- Chartier, C.R. and Abele, S. (2017). Groups Outperform Individuals in Tacit Coordination by Using Consensual and Disjunctive Salience. *Organizational Behavior and Human Decision Processes*, 141, 74-81.
- Chatterji, A. and Fabrizio, K. (2012). How Do Product Users Influence Corporate Invention? *Organization Science*, 23(4), 971-987.
- Chen, A., Hwang, Y., and Raghu, T. (2010). Knowledge Life Cycle, Knowledge Inventory, and Knowledge Acquisition Strategies. *Decision Sciences*, 41(1), 21-47.
- Chen, M.J., Chen, C.D., and Farn, C.K. (2010). Exploring Determinants of Citizenship Behavior on Virtual Communities of Consumption: The Perspective of Social Exchange Theory. *International Journal of Electronic Business Management*, 8(3), 195-205.
- Chen, H., Beaudoin, C., and Hong, T. (2017). Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors. *Computers in Human Behavior*, 70, 291-302.
- Chen, P.S., Yen, D.C., and Lin, S.C. (2015). The Classification of Information Assets and Risk Assessment: An Exploratory Study Using the Case of C-Bank. *Journal of Global Information Management*, 23(4), 26-54.
- Chen, P., Kataria, G., and Krishnan, R. (2011). Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quarterly*, 35(2), 397-422.
- Cheong, P. and Gong, J. (2010). Cyber Vigilantism, Transmedia Collective Intelligence, and Civic Participation. *Chinese Journal of Communication*, 3(4), 471-487.
- Cherner, L. (2017). None of Your Business: Protecting the Right to Write Anonymous Business Reviews Online. *Columbia Journal of Law & the Arts*, 40, 471-501.
- Choi, K. and Lee, J. (2017). Theoretical Analysis of Cyber-Interpersonal Violence Victimization and Offending Using Cyber-Routine Activities Theory. *Computers in Human Behavior*, 73, 394-402.

- Choo, K. (2011). The Cyber Threat Landscape: Challenges and Future Research Directions. *Computers and Security*, 30, 719-731.
- Clinton, L. (2011). A Relationship on the Rocks: Industry – Government Partnership for Cyber Defense. *Journal of Strategic Security*, 4(2), 97-112.
- Coates, B.E. (2002). “Smart” Government *Online*, Not *Inline*. *The Public Manager*, Winter 2001-02, 37-40.
- Contreras, F., Oliveira, F., and Muller, E. (2012). Internet: Monitored Freedom. *Journal of Information Systems and Technology Management*, 9(3), 459-472.
- Couldry, N. (2003). Media Meta-Capital: Extending the Range of Bourdieu’s Field Theory. *Theory and Society*, 32(5/6), 653-677.
- Crossler, R. et al. (2012). Future Directions for Behavioral Information Security Research. *Computers & Security*, 32, 90-101.
- Crump, C. (2003). Data Retention: Privacy, Anonymity, and Accountability Online. *Stanford Law Review*, 56, 191-229.
- Cuganesan, S., Steele, C., and Hart, A. (2018). How Senior Management and Workplace Norms Influence Information Security Attitudes and Self Efficacy. *Behaviour & Information Technology*, 37(1), 50-65.
- Cusumano, M.A. and Yoffie, D.B. (2016). Technology Strategy and Management Extrapolating from Moore’s Law: Behind and Beyond Microsoft, Intel, and Apple. *Communications of the ACM*, 59(1), 33-35.
- D’Ariano, G.M. and Perinotti, P. (2016). Quantum Theory is an Information Theory: The Operational Framework and the Axioms. *Found Physics*, 46, 269-281.
- Danzi, P., Angjelichinoski, M., Stefanovic, C, Dragicevic, T, and Popovski, P. (2018). Software-Defined Microgrid Control for Resilience Against Cyber Attacks. *IEEE Transactions on Smart Grid*, 2018, 1-9.
- Darke, P.R. and Freedman, J.L. (1993). Deciding Whether to Seek a Bargain: Effects of Both Amount and Percentage Off. *Journal of Applied Psychology*, 78(6), 960-965.
- Davis, A. (2015). Building Cyber-Resilience Into Supply Chains. *Technology Innovation Management Review*, 5(4), 19-27.
- de Laat, P. (2012). Coercion or Empowerment? Moderation of Content in Wikipedia as ‘Essentially Contested’ Bureaucratic Rules. *Ethics of Information Technology*, 14, 123-135.

- Deibert, R. (2015). The Geopolitics of Cyberspace After Snowden. *Current History*, 114(768), 9-15.
- Denegri-Knott, J. (2006). Consumers Behaving Badly: Deviation or Innovation? Power Struggles on the Web. *Journal of Consumer Behavior*, 5, 82-94.
- Denning, P.J. and Lewis, T.G. (2017). Exponential Laws of Computing Growth. *Communications of the ACM*, 60(1), 54-85.
- Devenandham, H. and Ramirez-Marquez, J. (2016). On the Impacts of Power Outages During Hurricane Sandy—A Resilience-Based Analysis. *Systems Engineering*, 19 (1), 59-75.
- DiMase, D., Collier, Z.A., Heffner, K., and Linkov, I. (2015). Systems Engineering Framework for Cyber Physical Security and Resilience. *Environmental Systems Decisions*, 35, 291-300.
- Dinh, L et al. (2011). Resilience Engineering of Industrial Processes: Principles and Contributing Factors. *Journal of Loss Prevention in the Process Industries*, 25, 233-241.
- Do, C., Tran, N., Hong, C., Kamhoua, C.A., Kwiat, K.A., Blasch, E., Ren, S., Pissinou, N., and Iyengar, S.S. (2017). Game Theory for Cyber Security and Privacy. *ACM Computing Surveys*, 50(2), Article 30, 1-37.
- Doolin, B. and Mcleod, L. (2012). Sociomateriality and Boundary Objects in Information Systems Development. *European Journal of Information Systems*, 21(5), 570-586.
- Dor, D. and Elovici, Y. (2016). A Model of the Information Security Investment Decision-Making Process. *Computers & Security*, 63, 1-13.
- Drissel, D. (2007). Internet Governance in a Multipolar World: Challenging American Hegemony. *Cambridge Review of International Affairs*, 19(1), 105-120.
- Dysart, J. (2011). The Hacktivists: Web Vigilantes Net Attention, Outrage, and Access to Your Data. *ABA Journal*, 97(12), 40+.
- Ebeling, M. (2003). The New Dawn: Black Agency in Cyberspace. *Radical History Review*, 87, 96-108.
- Edwards, M., Larson, R., Green, B., Rashid, A., and Baron, A. (2017). Panning for Gold: Automatically Analysing Online Social Engineering Attack Surfaces. *Computers & Security*, 69, 18-34.

- Ezhei, M. and Ladani, B. (2017). Information Sharing vs. Privacy: A Game Theoretic Analysis. *Expert Systems with Applications*, 88, 327-337.
- Farrell, G. (2013). Five Tests for a Theory of the Crime Drop. *Crime Science*, 2 (5), 1-8.
- Fielder, A. et al. (2016). Decision Support Approaches for Cyber Security Investment. *Decision Support Systems*, 86, 13-23.
- Fisher, L.M. (2017). Turing Laureates Celebrate Award's 50th Anniversary. *Communications of the ACM*, 60(9), 20-23.
- Fitzgerald, C. and Brantly, A. Subverting Reality: The Role of Propaganda in 21st Century Intelligence. *International Journal of Intelligence and Counterintelligence*, 30(2), 215-240.
- Fitzpatrick, W. and Dilullo, S. (2015). Cyber Espionage and the S.P.I.E.S. Taxonomy. *Competition Forum*, 13(2), 307-336.
- Flood, C. (2006). Propaganda, Totalitarianism and Film. *Totalitarian Movements and Political Religions*, 7(4), 515-522.
- Flores, W. and Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, 59, 26-44.
- Forbes, D.P. (2007). Reconsidering the Strategic Implications of Decision Comprehensiveness. *Academy of Management Review*, 32(2), 361-376.
- Fuchs, C., Bichler, R., and Raffl, C. (2009). Cyberethics and Co-operation in the Information Society. *Science Engineering Ethics*, 15, 447-466.
- Gal-Or, E., and Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research*, 16(2), 186-208.
- Gardner, H.K., Gino, F., and Staats, B.R. (2012). Dynamically Integrating Knowledge in Teams: Transforming Resources into Performance. *Academy of Management Journal*, 55(4), 998-1022.
- Gaskin, J. et al. (2014). Toward Generalizable Sociomaterial Inquiry: A Computational Approach for Zooming In and Out of Sociomaterial Routines. *MIS Quarterly*, 38 (3), 849-871.
- Geletkanycz, M. (1997). The Salience of 'Culture's Consequences': The Effects of Cultural Values on Top Executive Commitment to the Status Quo. *Strategic Management Journal*, 18(8), 615-634.

- Gelms, J. (2012). High-Tech Harassment: Employer Liability Under Title VII for Employee Social Media Misconduct. *Washington Law Review*, 87, 249-279.
- Gisladottir, V., Ganin, A.A., Keisler, J.M., Kepner, J., and Linkov, I. (2016). Resilience of Cyber Systems with Over- and Under-regulation. *Risk Analysis*, 37(9), 1644-1651.
- Gladstein, D. and Reilly, N. (1985). Group Decision Making Under Threat: The Tycoon Game. *Academy of Management Journal*, 28(3), 613-627.
- Goodman, M. and Khanna, P. (2013). The Power of Moore's Law in a World of Geotechnology. *The National Interest*, Jan/Feb 2013, 64-73.
- Gordon, L., Loeb, M.P., and Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, 34 (3), 567-594.
- Gordon, L., Loeb, M.P., Lucyshyn, W., and Zhou, L. (2015). The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective. *Journal of Accounting Public Policy*, 34, 509-519.
- Gwynne, J. (2013). "The Lighter that Fuels a Blaze of Change": Agency and (Cyber)spatial (Dis)embodiment in *Girls of Riyadh*. *Women's Studies International Forum*, 37, 46-52.
- Hamacher, K. (2012). Resilience to Leaking – Dynamic Systems Modeling of Information Security. *PLOS One*, 7(12), e49804.
- Handley, R. and Rutigliano, L. (2012). Journalistic Field Wars: Defending and Attacking the National Narrative in a Diversifying Journalistic Field. *Media, Culture & Society*, 34(6), 744-760.
- Harknett, R. (2003). Integrated Security: A Strategic Response to Anonymity and the Problem of the Few. *Contemporary Security Policy*, 24(1), 13-45.
- Harris, M.A. and Patten, K.P. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum. *Journal of Information Systems Education*, 26(3), 219-234.
- Hatfield, J. (2018). Social Engineering in Cybersecurity: The Evolution of a Concept. *Computers & Security*, 73, 102-113.
- Haughey, H., Epiphaniou, G., and Al-Khateeb, H. (2016). Anonymity Networks and the Fragile Cyber Ecosystem. *Network Security*, March 2016, 10-18.
- Hausken, K. (2015). A Strategic Analysis of Information Sharing Among Cyber Hackers. *Journal of Information Systems and Technology Management*, 12(2), 245-270.

- Hausken, K. and Bier, V.M. (2011). Defending Against Multiple Different Attackers. *European Journal of Operational Research*, 211, 370-384.
- He, X.D. and Zhou, X.Y. (2011). Portfolio Choice Under Cumulative Prospect Theory: An Analytical Treatment. *Management Science*, 57(2), 315-331.
- Helsper, E.J. (2012). A Corresponding Fields Model for the Links Between Social and Digital Exclusion. *Communication Theory*, 22, 403-426.
- Hemsath, D. (2014). Efficient Code to Counter Dying Moore's Law. *Communications of the ACM*, 57(6), 9.
- Henry, D. and Ramirez-Marquez, J.E. (2016). On the Impacts of Power Outages During Hurricane Sandy—A Resilience-Based Analysis. *Systems Engineering*, 19(1), 59-75.
- Hernandez-Ardieta, J., et al. (2013). A Taxonomy and Survey of Attacks on Digital Signatures. *Computers & Security*, 34, 67-112.
- Herrera, L. (2015). Citizenship under Surveillance: Dealing with the Digital Age. *International Journal of Middle East Studies*, 47(2), 354-356.
- Herrington, L. and Aldrich, R. (2013). The Future of Cyber-Resilience in an Age of Global Complexity. *Politics*, 33(4), 299-310.
- Herzenstein, M., Posavac, S., and Brakus, J. (2007). Adoption of New and Really New Products: The Effects of Self-Regulation Systems and Risk Salience. *Journal of Marketing Research*, 44 (2), 251-260.
- Hidayanto, A.N., Ovirza, M., Anggia, P., Budi, N.F.A., and Phusavat, K. (2017). The Roles of Electronic Word of Mouth and Information Searching in the Promotion of a New E-Commerce Strategy: A Case of Online Group Buying in Indonesia. *Journal of Theoretical and Applied Electronic Commerce Research*, 12(3), 69-85.
- Hillebrandt, A. and Barclay, L. (2017). Comparing Integral and Incidental Emotions: Testing Insights from Emotions as Social Information Theory and Attribution Theory. *Journal of Applied Psychology*, 102(5), 732-752.
- Holt, T. (2013). Exploring the Social Organisation and Structure of Stolen Data Markets. *Global Crime*, 14(2-3), 155-174.
- Hong, L. and Chen, W. (2014). Information Theory and Cryptography Based Secured Communication Scheme for Cooperative MIMO Communication in Wireless Sensor Networks. *Ad Hoc Networks*, 14, 95-105.

- Hovav A. and D'Arcy J. (2003). The Impact of Denial-of-Service Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, vol 6(2), 97-121.
- Howard, J. and Longstaff, T. (1998). A Common Language for Computer Security Incidents. Pittsburgh, PA, CERT Coordination Center at Carnegie Mellon University: 1-33.
- Howard, M., Withers, M., and Tihanyi, L. (2013). Knowledge Dependence and the Formation of Director Interlocks. *Academy of Management Journal*, 60(5), 1986-2013.
- Hsu, C.W., Yin, C.P., and Huang, L.T. (2017). Understanding Exchangers' Attitudes and Intentions to Engage in Internet Bartering Based on Social Exchange Theory (SET) and the Theory of Reasoned Action (TRA). *International Journal of Business and Information*, 12(2), 149-182.
- Hsu, I. and Sabherwal, R. (2012). Relationship Between Intellectual Capital and Knowledge Management: An Empirical Investigation. *Decision Sciences*, 43(3), 489-524.
- Huang, C.D. and Behara, R.S. (2013). Economics of Information Security Investment in the Case of Concurrent Heterogeneous Attacks with Budget Constraints. *International Journal of Production Economics*, 141, 255-268.
- Hucanu, R. and Georgescu, M. (2016). Small Steps or Big Changes in Actual Society: The Impact of Internet of Things. *Journal of Public Administration, Finance and Law*, 10, 132-141.
- Hult, G. (2003). An Integration of Thoughts on Knowledge Management. *Decision Sciences*, 34(2), 189-195.
- Introna, L.D. and Hayes, N. (2011). On Sociomaterial Imbrications: What Plagiarism Detection Systems Reveal and Why It Matters. *Information and Organization*, 21, 107-122.
- Iqbal, S., et al. (2016). On Cloud Security: A Taxonomy and Intrusion Detection and Prevention as a Service. *Journal of Network & Computer Applications*, 74, 98-120.
- Izquierdo-Yusta, A. and Martinez-Ruiz, M. (2011). Assessing the Consumer's Choice of Purchase Channel in the Tourism Sector. *EuroMed Journal of Business*, 6(1), 77-99.
- Jane, E. (2016). Online Misogyny and Feminist Digital Activism. *Continuum: Journal of Media and Cultural Studies*, 30(3), 284-297.

- Jansson, A. (2016). How to Become an 'Elite Cosmopolitan': The Mediatized Trajectories of United Nations Expatriates. *European Journal of Cultural Studies*, 19(5), 465-480.
- Jardine, E. (2018). Tor, What is it Good for? Political Repression and the Use of Online Anonymity-Granting Technologies. *New Media & Society*, 20(2), 435-452.
- Jensen, L. (2015). Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review*, 5(4), 35-39.
- Jinyang, L. (2015). Knowledge Sharing in Virtual Communities: A Social Exchange Theory Perspective. *Journal of Industrial Engineering and Management*, 8(1), 170-183.
- Johnston, A. and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3), 549-566.
- Joiner, K.F. (2017). How Australia Can Catch Up to U.S. Cyber Resilience by Understanding that Cyber Survivability Test and Evaluation Drives Defense Investment. *Information Security Journal: A Global Perspective*, 26(2), 74-84.
- Jones, C.W. (2018). New Approaches to Citizen-Building: Shifting Needs, Goals, and Outcomes. *Comparative Political Studies*, 51(2), 165-196.
- Jones, M. (2014). A Matter of Life and Death: Exploring Conceptualizations of Sociomateriality in the Context of Critical Care. *MIS Quarterly*, 38(3), 895-925.
- Jordan, T. and Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review*, 46(4), 757-780.
- Jorgensen, A. (2016). Competing Visions of eDemocracy in Greenland: Negotiations of Power in Online Political Participation. *Policy and Internet*, 9(2), 210 – 231.
- Juliano, S. (2012). Superheroes, Bandits, and Cyber-nerds: Exploring the History and Contemporary Development of the Vigilante. *Journal of International Commercial Law and Technology*, 7(1), 44-64.
- Junger, M., Montoya, L., and Overink, F.J. (2017). Priming and Warnings are not Effective to Prevent Social Engineering Attacks. *Computers in Human Behavior*, 66, 75-87.
- Kahneman, D. and Tversky, A. (1979). Prospect Theory: An Analysis of Decision Under Risk. *Econometrica*, 47, 263-292.

- Kalia, D. and Aleem, S. (2017). Cyber Victimization Among Adolescents: Examining the Role of Routine Activity Theory. *Journal of Psychological Research*, 12(1), 223-232.
- Kannan, K., Rahman, M.S., and Tawarmalani, M. (2016). Economic and Policy Implications of Restricted Patch Distribution. *Management Science*, 62(11), 3161-3182.
- Karanja, E. (2017). The Role of the Chief Information Security Officer in the Management of IT Security. *Information & Computer Security*, 25(3), 240-258.
- Karatzogianni A. and Gak, M. (2015). Hack or Be Hacked: The Quasi-Totalitarianism of Global Trusted Networks. *New Formations*, 84/85, 130-147.
- Kautz, K. and Jensen, T.B. (2012). Sociomateriality – More Than Jargon Monoxide? Questions from the Jester to the Sovereigns. *ECIS 2012 Proceedings, Paper 54*, 1-13.
- Kautz, K. and Jensen, T.B. (2013). Sociomateriality at the Royal Court of IS A Jester's Monologue. *Information and Organization*, 23(1), 15-27.
- Keil, M., Tan, B.C.Y., Kwok-Kee, W., Saarinen, T., et al. (2000). A Cross-Cultural Study on Escalation of Commitment Behavior in Software Projects. *MIS Quarterly*, 24(2), 299-325.
- Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, 30(4), 470-486.
- Kim, W., Jeong, O.R., Kim, C., and So, J. (2011). The Dark Side of the Internet: Attacks, Costs, and Responses. *Information Systems*, 36, 675-705.
- Kleemans, E., Soudijn, M., and Weenink, A. (2012). Organized Crime, Situational Crime Prevention and Routine Activity Theory. *Trends in Organized Crime*, 15, 87-92.
- Klein, A.G. (2015). Vigilante Media: Unveiling Anonymous and the Hacktivist Persona in the Global Press. *Communication Monographs*, 82(3), 379-401.
- Knapp, K.J. and Ferrante, C.J. (2014). Information Security Program Effectiveness in Organizations: The Moderating Role of Task Interdependence. *Journal of Organizational and End User Computing*, 26(1), 27-46.
- Koomey, J.G. (2010). Outperforming Moore's Law. *IEEE Spectrum*, 47(3), 68.
- Kosseff, J. (2016). The Hazards of Cyber-Vigilantism. *Computer Law & Security Review*, 32, 642-649.

- Kostakis, V. (2012). The Political Economy of Information Production in the Social Web: Chances for Reflection on Our Institutional Design. *Contemporary Social Science*, 7(3), 305-319.
- Krombholz, K., Hobel, H., Huber, M., and Weippl, E. (2015). Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, 22, 113-122.
- Laszka, A. and Felegyhazi, M. (2014). A Survey of Interdependent Information Security Games. *ACM Computer Surveys*, 47(2), Article 23, 1-38.
- Lee, C., Lee, C., and Kim, S. (2016). Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity. *Computers & Security*, 59, 60-70.
- Leonardi, P. (2007). Activating the Informational Capabilities of Information Technology for Organizational Change. *Organization Science*, 18(5), 813-831.
- Leonardi, P. (2010). Digital Materiality? How Artifacts Without Matter, Matter. *First Monday*, 15(6-7), 1-22.
- Leonardi, P. (2011). When Flexible Routines Meet Flexible Technologies: Affordance, Constraint, and the Imbrication of Human and Material Agencies. *MIS Quarterly*, 35(1), 147-167.
- Leonardi, P. (2013). Theoretical Foundations for the Study of Sociomateriality. *Information and Organization*, 23, 59-76.
- Leonardi, P. and Barley, S. (2008). Materiality and Change: Challenges to Building Better Theory About Technology and Organizing. *Information and Organization*, 18, 159-176.
- Leukfeldt, E. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking*, 17(8), 551-555.
- Leukfeldt, E. and Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 37(3), 263-280.
- Lewis, K., Belliveau, M., Herndon, B., and Keller, J. (2007). Group Cognition, Membership Change, and Performance: Investigating the Benefits and Detriments of Collective Knowledge. *Organizational Behavior and Human Decision Processes*, 103, 159-178.
- Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A.K., and Choo, K.K.R. (2017). A Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in

- Internet of Things Environments. *Journal of Network and Computer Applications*, 103, 194-204.
- Lin, L., Geng, X., and Whinston, A. (2005). A Sender-Receiver Framework for Knowledge Transfer. *MIS Quarterly*, 29(2), 197-219.
- Lioukas, C., Reuer, J., and Zollo, M. (2016). Effects of Information Technology Capabilities on Strategic Alliances: Implications for the Resource-Based View. *Journal of Management Studies*, 53(2), 161-183.
- Liu, J.H., Yamagishi, T., Wang, F., Schug, J., Lin, Y., Yu, S., Takahashi, C., and Huang, L.L. (2011). Unbalanced Triangle in the Social Dilemma of Trust: Internet Studies of Real-Time, Real Money Social Exchange Between China, Japan, and Taiwan. *Asian Journal of Social Psychology*, 14, 246-257.
- Liu, S.D. (2013). The Cyberpolitics of the Governed. *Inter-Asia Cultural Studies*, 14(2), 252-271.
- Liu, X., Zhang, J., and Zhu, P. (2017). Modeling Cyber-Physical Attacks Based on Probabilistic Colored Petri Nets and Mixed-Strategy Game Theory. *International Journal of Critical Infrastructure Protection*, 16, 13-25.
- Liu, Z., Min, Q., Zhai, Q., and Smyth, R. (2016). Self-Disclosure in Chinese Micro-Blogging: A Social Exchange Theory Perspective. *Information and Management*, 53, 53-63.
- Lockett, A., Moon, J. and Visser, W. (2006). Corporate Social Responsibility in Management Research: Focus, Nature, Salience and Sources of Influence. *Journal of Management Studies*, 43 (1), 115-136.
- Lott, J.R. (1999). Public Schooling, Indoctrination, and Totalitarianism. *Journal of Political Economy*, 107(S6), S127-S157
- Lopes, A.M., Machado, J.A.T., and Galhano, A.M. (2016). Empirical Laws and Foreseeing the Future of Technological Progress. *Entropy*, 18(217), 1-11.
- Louis, M.R. and Sutton, R.I. (1991). Switching Cognitive Gears: From Habits of Mind to Active Thinking. *Human Relations*, 44(1), 55-76.
- Love, V.D. (2011). IT Security Strategy: Is Your Health Care Organization Doing Everything It Can to Protect Patient Information? *Journal of Health Care Compliance*, 13(6), 21-28.
- Lundgren, B. and Moller, N. (2017). Defining Information Security. *Science and Engineering Ethics*, Nov 2017, 1-23.

- Luo, X. (2002). Trust Production and Privacy Concerns on the Internet: A Framework Based on Relationship Marketing and Social Exchange Theory. *Industrial Marketing Management*, 31, 111-118.
- Luo, X. and Donthu, N. (2007). The Role of Cyber-Intermediaries: a Framework Based on Transaction Cost Analysis, Agency, Relationship Marketing, and Social Exchange Theories. *Journal of Business & Industrial Marketing*, 19(6), 452-458.
- Madsen, P.M. and Rodgers, Z.J. Looking Good by Doing Good: The Antecedents and Consequences of Stakeholder Attention to Corporate Disaster Relief. *Strategic Management Journal*, 36, 776-794.
- Mahowald, K., Fedorenko, E., Piantadosi, S.T., and Gibson, E. (2013). Info/Information Theory: Speakers Choose Shorter Words in Predictive Contexts. *Cognition*, 126, 313-318.
- Majda, A. and Gershgorin, B. (2011). Improving Model Fidelity and Sensitivity for Complex Systems Through Empirical Information Theory. *Proceedings of the National Academy of Sciences of the United States of America*, 108(25), 10044-10049.
- Malone, E.V. (2013). Finding the Solution in WEC Carolina Energy Solutions: The Computer Fraud and Abuse Act in the Workplace. *Catholic University Law Review*, 63, 249-270.
- Marcum, C., Ricketts, M., and Higgins, G. (2010). Assessing Sex Experiences of Online Victimization: An Examination of Adolescent Online Behaviors Using Routine Activity Theory. *Criminal Justice Review*, 35(4), 4112-437.
- Matania, E., Yoffe, L., and Mashkautsan, M. (2016). A Three-Layer Framework for a Comprehensive National Cyber-security Strategy. *Georgetown Journal of International Affairs*, 17(3), 77-84.
- Mayadunne, S. and Park, S. (2016). An Economic Model to Evaluate Information Security Investment of Risk-Taking Small and Medium Enterprises. *International Journal of Production Economics*, 182, 519-530.
- Mazmanian, M., Cohn, M., and Dourish, P. (2014). Dynamic Reconfiguration in Planetary Exploration: A Sociomaterial Ethnography. *MIS Quarterly*, 38(3), 831-848.
- Mazmanian, M., Orlikowski, W., and Yates, J. (2013). The Autonomy Paradox: The Implications of Mobile Email Devices for Knowledge Professionals. *Organizational Science*, 24(5), 1337-1357.
- McGinn, H. (1994). Information Assets. *The Bottom Line*, 7(2), 40-41.

- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017). Individual Differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151-156.
- McIver, D., Lengnick-Hall, C.A., Lengnick-Hall, M.L., and Ramachandran, I. (2013). Understanding Work and Knowledge Management from a Knowledge-in-Practice Perspective. *Academy of Management Review*, 38(4), 597-620.
- Meeks, B.N. (2002). True Blue and Vigilante, Too. *Communications of the ACM*, 45(7), 13-15.
- Melville, N., Kraemer, K., and Gurbaxani, V. (2004). Review: Information Technology and Organizational Performance: An Integrative Model of IT Business Value. *MIS Quarterly*, 28(2), 283-322.
- Mihailidis, P. and Viotti, S. (2017). Spreadable Spectacle in Digital Culture: Civic Expression, Fake News, and the Role of Media Literacies in “Post-Fact” Society. *American Behavioral Scientist*, 61(4), 441-454.
- Misoch, S. (2015). Stranger on the Internet: Online Self-Disclosure and the Role of Visual Anonymity. *Computers in Human Behavior*, 48, 535-541.
- Mitchell, R., Agle, B. and Wood, D. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *The Academy of Management Review*, 22(4), 853-886.
- Moore, G.E. (1965). Cramming More Components Onto Integrated Circuits. *Electronics*, 38(8), 56-59.
- Mortenson, W., Sixsmith, A., and Woolrych, R. (2015). The Power(s) of Observation: Theoretical Perspectives on Surveillance Technologies and Older People. *Aging and Society*, 35, 512-530.
- Mouton, F., Malan, M., and Venter, H. (2012). Development of Cognitive Functioning Psychological Measures for the SEADM. *Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance*, 40-51.
- Mouton, F., Malan, M.M., Leenen, L., and Venter, H.S. (2014). Social Engineering Attack Framework. *IEEE 2014 Information Security for South Africa Conference*, 1-9.
- Mouton, F., Leenen, L., and Venter, H. (2016). Social Engineering Attack Examples, Templates and Scenarios. *Computers and Security*, 59, 186-209.

- Mutch, A. (2013). Sociomateriality – Taking the Wrong Turning? *Information and Organization*, 23, 28-40.
- Nagarajan, M. and Shechter, S. (2014). Prospect Theory and the Newsvendor Problem. *Management Science*, 60(4), 1057-1062.
- Nasi, M., Oksanen, A., Keipi, T., and Rasanen, P. (2015). Cybercrime Victimization Among Young People: A Multi-Nation Study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 16(2), 203-210.
- Nasi, M., Rasanen, P., Kaakinen, M., Keipi, T, and Oksanen, A. (2017). Do Routine Activities Help Predict Young Adults' Online Harassment: A Multi-Nation Study. *Criminology & Criminal Justice*, 17(4), 418-432.
- Netto, M. and Spurgeon, S. (2017). Special Section on Cyber-Physical & Human Systems (CPHS). *Annual Reviews in Control*, 44, 249-251.
- Nevo, S. and Wade, M.R. (2010). The Formation and Value of IT-Enabled Resources: Antecedents and Consequences of Synergistic Relationships. *MIS Quarterly*, 34(1), 163-183.
- Njilla, L.Y., Pissinou, N., and Makki, K. (2016). Game Theoretic Modeling of Security and Trust Relationship in Cyberspace. *International Journal of Communication Systems*, 29, 1500-1512.
- Nuyen, A.T. (2001). The World Wide Web and the Web of Life. *International Journal of Applied Philosophy*, 15(1), 47-57.
- Nycyk, M. (2016). The New Computer Hacker's Quest and Contest with the Experienced Hackers: A Qualitative Study Applying Pierre Bourdieu's Field Theory. *International Journal of Cyber Criminology*, 10(2), 92-109.
- Okediji, R.L. (2003). Trading Posts in Cyberspace: Information Markets and the Construction of Proprietary Rights. *Boston College Law Review*, 44(2), 545-575.
- Oldroyd, J. and Morris, S. (2012). Catching Falling Stars: A Human Resource Response to Social Capital's Detrimental Effect of Information Overload on Star Employees. *Academy of Management Review*, 37(3), 396-418.
- Ong, R. (2012). Online Vigilante Justice Chinese Style and Privacy in China. *Information & Communications Technology Law*, 21(2), 127-145.
- O'Neil, M. (2014). Hacking Weber: Legitimacy, Critique, and Trust in Peer Production. *Information, Communication & Society*, 17(7), 872-888.

- Orlikowski, W. (2006). Material Knowing: The Scaffolding of Human Knowledgeability. *European Journal of Information Systems*, 15(5), 460-471.
- Orlikowski, W. (2007). Sociomaterial Practices: Exploring Technology at Work. *Organization Studies*, 28 (9), 1435-1448.
- Orlikowski, W. (2010). The Sociomateriality of Organizational Life: Considering Technology in Management Research," *Cambridge Journal of Economics*, 34(1), 125-141.
- Orlikowski, W. and Iacono, C.S. (2001). Research Commentary: Desperately Seeking the "IT" in IT research – a Call to Theorizing the IT Artifact. *Information Systems Research*, 12(2), 121-134.
- Orlikowski, W. and Scott, S. (2008). Sociomateriality: Challenging the Separation of Technology, Work and Organization. *The Academy of Management Annals*, 2(1), 433-474.
- Orlikowski, W. and Scott, S. (2015). Exploring Material-Discursive Practices. *Journal of Management Studies*, 52(5), 697-705.
- Ortiz-De-Mandojana, N. and Bansal, P. (2016). The Long-Term Benefits of Organizational Resilience Through Sustainable Business Practices. *Strategic Management Journal*, 37, 1615-1631.
- Osterlie, T., Almklov, P.G., and Hepso, V. (2012). Dual Materiality and Knowing in Petroleum Production. *Information and Organization*, 22, 85-105.
- Padayachee, K. (2012). Taxonomy of Compliant Information Security Behavior. *Computers & Security*, 31, 673-680.
- Padmanabhan, S. (2012). Hacking for Lulz: Employing Expert Hackers to Combat Cyber Terrorism. *Vanderbilt Journal of Entertainment and Technology Law*, 15(1), 191-225.
- Paiva, E.L., Roth, A.V., and Fensterseifer, J.E. (2008). Organizational Knowledge and the Manufacturing Strategy Process: A Resource-Based View Analysis. *Journal of Operations Management*, 26, 115-132.
- Park, I., Sharman, R., and Rao, H.R. (2016). Disaster Experience and Hospital Information Systems: An Examination of Perceived Information Assurance Risk, Resilience, and HIS Usefulness. *MIS Quarterly*, 39(2), 317-344.
- Pavlou, P., Liang, H., and Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal – Agent Perspective. *MIS Quarterly*, 31(1), 105-136.

- Pemberton, M. (1993). 'You Manage What?' RIM and the Meaning of Information. *Records Management Quarterly*, 27 (1), 50-53.
- Peper, F. (2017). The End of Moore's Law: Opportunities for Natural Computing? New Generation Computing, 35, 253-269.
- Perakslis, E.D. (2014). Cybersecurity in Health Care. *The New England Journal of Medicine*, 371(5), 395-397.
- Perea, F. and Puerto, J. (2013). Revisiting a Game Theoretic Framework for the Robust Railway Network Design Against Intentional Attacks. *European Journal of Operational Research*, 226, 286-292.
- Phillips, B.J. (2017). Inequality and the Emergence of Vigilante Organizations: The Case of Mexican Autodefensas. *Comparative Political Studies*, 50(10), 1358-1389.
- Posey, C., Roberts, T.L., Lowry, P.B., Bennett, R.J., and Courtney, J.F. (2013). Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors. *MIS Quarterly*, 37 (4), 1189-1210.
- Pratt, T., Holtfreter, K., and Reisig, M. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, 47(3), 267-296.
- Qui, Y., Ma, M., and Chen, S. (2017). An Anonymous Authentication Scheme for Multi-Domain Machine-to-Machine Communication in Cyber-Physical Systems. *Computer Networks*, 129, 306-318.
- Ramirez, R. and Chourcri, N. (2016). Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review. *IEEE Access*, 4, 2216-2243.
- Ranganathan, R. and Rosenkopf, L. (2014). Do Ties Really Bind? The Effect of Knowledge and Commercialization Networks on Opposition to Standards. *Academy of Management Journal*, 57(2), 515-540.
- Rao, M.B., Jongerden, J., Lemmens, P., Ruivenkamp, G. (2015). Technological Mediation and Power: Postphenomenology, Critical Theory, and Autonomist Marxism. *Philosophy & Technology*, 28(3), 449-474.
- Rao, N.S.V., Poole, S.W., Ma, C.Y.T., He, F., Zhuang, J., and Yau, D.K.Y. (2016). Defense of Cyber Infrastructure Against Cyber-Physical Attacks Using Game-Theoretic Models. *Risk Analysis*, 36(4), 694-710.

- Ravichandran, T., Lertwongsatien, C., and Lertwongsatien, C. (2014). Effect of Information Systems Resources and Capabilities on Firm Performance: A Resource-Based Perspective. *Journal of Management Information Systems*, 21(4), 237-276.
- Ray, G., Barney, J.B., and Muhanna, W.A. (2004). Capabilities, Business Processes, and Competitive Advantage: Choosing the Dependent Variable in Empirical Tests of the Resource-Based View. *Strategic Management Journal*, 25, 23-37.
- Reiners, G. and Soudan, K. (2010). A Game-Theoretical Approach for Reciprocal Security-Related Prevention Investment Decisions. *Reliability Engineering and System Safety*, 95, 1-9.
- Reyns, B. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, 50(2), 216-238.
- Reyns, B., Henson, B., and Fisher, B. (2016). Guardians of the Cyber Galaxy: An Empirical and Theoretical Analysis of the Guardianship Concept from Routine Activity Theory as It Applies to Online Forms of Victimization. *Journal of Contemporary Criminal Justice*, 32(2), 148-168.
- Rirolli, L. and Savicki, V. (2003). Information System Organizational Resilience. *The International Journal of Management Science*, 31, 227-233.
- Robnett, B. and Feliciano, C. (2011). Patterns of Racial-Ethnic Exclusion by Internet Daters. *Social Forces*, 89(3), 807-828.
- Rohle, T. (2005). Power, Reason, Closure: Critical Perspectives on New Media Theory. *New Media & Society*, 7(3), 403-422.
- Rongbin, H. (2015). Manufacturing Consent in Cyberspace: China's "Fifty-Cent Army." *Journal of Current Chinese Affairs*, 2, 105-134.
- Rosoff, H., Cui, J., and John, R. (2013). Heuristics and Biases in Cyber Security Dilemmas. *Environmental Systems Decisions*, 33, 517-529.
- Rutherford, A. (2017). B.F. Skinner and Technology's Nation: Technocracy, Social Engineering, and the Good Life in 20th Century America. *History of Psychology*, 20(3), 290-312.
- Sabherwal, R. and Sabherwal, S. (2005). Knowledge Management Using Information Technology: Determinants of Short-Term Impact on Firm Value. *Decision Sciences*, 36(4), 531-567.

- Safa, N. and Von Solms, R. (2016). An Information Security Knowledge Sharing Model in Organizations. *Computers in Human Behavior*, 57, 442-451.
- Safa, N., Von Solms, R., and Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers & Security*, 56, 70-82.
- Sahebjamnia, N., Torabi, S., and Mansouri, S. (2015). Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience. *European Journal of Operational Research*, 242, 261-273.
- Sanchez, R. and Mahoney, J. (1996). Modularity, Flexibility, and Knowledge Management in Product and Organization Design. *Strategic Management Journal*, 17, 63-76.
- Schaab, P., Beckers, K., and Pape, S. (2017). Social Engineering Defence Mechanisms and Counteracting Training Strategies. *Information & Computer Security*, 25(2), 206-222.
- Schell, G.P. (2010). IT Value: From Moore's Law to a Flat World. *Computer*, 43(9), 79 – 81.
- Schillebeeckx, S., Chaturvedi, S., George, G., and King, Z. (2016). What Do I Want? The Effects of Individual Aspiration and Relational Capability on Collaboration Preferences. *Strategic Management Journal*, 37, 1493-1506.
- Schmidt, U. (2015). Insurance Demand Under Prospect Theory: A Graphical Analysis. *The Journal of Risk and Insurance*, 83(1), 77-89.
- Schuster, P. (2016). The End of Moore's Law: Living Without an Exponential Increase in Efficiency of Computational Facilities. *Complexity*, 21(SI), 6-6-9.
- Scott, S. and Orlikowski, W. (2007). Entanglements in Practice: Performing Anonymity Through Social Media. *MIS Quarterly*, 38(3), 873-893.
- Scott, S. and Orlikowski, W. (2009). 'Getting the Truth': Exploring the Material Grounds of Institutional Dynamics in Social Media. IDEAS Working Paper Series from RePEc. Retrieved 29 January 2018 from: <https://search.proquest.com/docview/1698351009?accountid=14270>.
- Scott, S. and Orlikowski, W. (2013). Sociomateriality – Taking the Wrong Turning? A Response to Mutch. *Information and Organization*, 23, 77-80.
- Sears, J. and Hoetker, G. (2014). Technological Overlap, Technological Capabilities, and Resource Recombination in Technological Acquisitions. *Strategic Management Journal*, 35, 48-67.

- Senn, S. (2015). All Propaganda is Dangerous, but Some are More Dangerous than Others: George Orwell and the Use of Literature as Propaganda. *Journal of Strategic Security*, 8(3), 149-161.
- Serracino-Inglott, P. (2013). Is it OK to be an Anonymous? *Ethics & Global Politics*, 6(4), 217-244.
- Shalf, J. M. and Leland, R. (2015). "Computing Beyond Moore's Law." *Computer*, 48(12), 14-23.
- Shameli-Sendi, A. and Aghababaei-Barzegar, R. (2016). Taxonomy of Information Security Risk Assessment. *Computers & Security*, 57, 14-30.
- Shepherd, D.A., McMullen, J.S., and Ocasio, W. (2017). Is That an Opportunity? An Attention Model of Top Managers' Opportunity Beliefs for Strategic Action. *Strategic Management Journal*, 38, 626-644.
- Shiau, E.L. and Luo, M.M. (2012). Factors Affecting Online Group Buying Intention and Satisfaction: A Social Exchange Theory Perspective. *Computers in Human Behavior*, 28, 2431-2444.
- Shih, E. (2016). Not in My "Backyard Abolitionism": Vigilante Rescue against American Sex Trafficking. *Sociological Perspectives*, 59(1), 66-90.
- Shtatfeld, R. and Barak, A. (2009). Factors Related to Initiating Interpersonal Contacts on Internet Dating Sites: A View From the Social Exchange Theory. *Interpersona*, 3, 19-37.
- Siponen, M., Mahmood, M., and Pahnila, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. *Information & Management*, 51, 217-224.
- Smith, S., Winchester, D., and Bunker, D. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security "De Jure" Standard in a Government Organization. *MIS Quarterly*, 34(3), 463-486.
- Somani, G., et al. (2017). DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions. *Computer Communications*, 107, 30-48.
- Son, I., Lee, D., Lee, J.N., and Chang, Y.B. (2014). Market Perception on Cloud Computing Initiatives in Organizations: An Extended Resource-Based View. *Information & Management*, 51, 653-669.
- Spyridopoulos, T., Karanikas, G., Tryfonas, T., and Oikonomou, G. (2013). A Game Theoretic Defence Framework Against DoS/DDoS Cyber Attacks. *Computers & Security*, 38, 39-50.

- Steinmetz, K. and Gerber, J. (2015). "It Doesn't Have to Be This Way": Hacker Perspectives on Privacy. *Social Justice*, 41(3), 29-51.
- Stevenson, M. (2016). The Cybercultural Moment and the New Media Field. *New Media & Society*, 18(7), 1088-1102.
- Stone, E., Sieck, W.R., Bull, B.E., Yates, J.F., Parks, S.C., and Rush, C.J. (2003). Foreground:Background Salience: Explaining the Effects of Graphical Displays on Risk Avoidance. *Organizational Behavior and Human Decision Processes*, 90, 19-36.
- Strawn, G. and Strawn C. (2015). Moore's Law at Fifty. *IT Professional*, 17(6), 69-72.
- Sullivan, R.F. (2007). The Impact of Moore's Law on the Total Cost of Computing and How Inefficiencies in the Data Center Increase These Costs. *ASHRAE Transactions*, 113(1), 457-461.
- Sung, S.Y. and Choi, J.N. (2012). Effects of Team Knowledge Management on the Creativity and Financial Performance of Organizational Teams. *Organizational Behavior and Human Decision Processes*, 118, 4-13.
- Surroca, J., Tribo, J. and Waddock, S. (2010). Corporate Responsibility and Financial Performance: The Role of Intangible Resources. *Strategic Management Journal*, 31(5), 463-490.
- Tambo, E. and Adama, K. (2017). Promoting Cybersecurity Awareness and Resilience Approaches, Capabilities, and Actions Plans against Cybercrimes and Frauds in Africa. *International Journal of Cyber-Security and Digital Forensics*, 6(3), 126-138.
- Taylor, S.E. and Thompson, S.C. (1982). Stalking the Elusive Vividness Effect. *Psychological Review*, 89, 155-181.
- Tayouri, D. (2015). The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. *6th International Conference on Applied Human Factors and Ergonomics and the Affiliated Conferences, Procedia Manufacturing*, 3, 1096-1100.
- Teh, P.L., Ahmed, P.K., and D'Arcy, J. (2015). What Drives Information Security Policy Violations among Banking Employees? Insights from Neutralization and Social Exchange Theory. *Journal of Global Information Management*, 23(1), 44-64.
- Tetri, P. and Vuorinen, J. (2013). Dissecting Social Engineering. *Behavior and Information Technology*, 32(10), 1014-1023.

- Thatch, L. and Woodman, R.W. (1994). Organizational Change and Information Technology: Managing on the Edge of Cyberspace. *Organizational Dynamics*, 23(1), 30-46.
- Thompson, S.T.C. (2006). Helping the Hacker? Library Information, Security, and Social Engineering. *Information Technology and Libraries*, Dec 2006, 222-225.
- Thompson, M.A., Ryan, M.J., Slay, J., and McLucas, A.C. (2016). Harmonized Taxonomies for Security and Resilience. *Information Security Journal: A Global Perspective*, 25(1-3), 54-67.
- Tokunaga, R.S. and Aune, K.S. (2017). Cyber-Defense: A Taxonomy of Tactics for Managing Cyberstalking. *Journal of Interpersonal Violence*, 32(10), 1451-1475.
- Tosh, D., Sengupta, S., Kamhoua, C.A., and Kwiat, K.A. (2016). Establishing Evolutionary Game Models for CYBer Security Information Exchange (CYBEX). *Journal of Computer and System Sciences*, 2016, 1-26.
- Tounsi, W. and Rais, H. (2018). A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks. *Computers & Security*, 72, 212-233.
- Track, E., Forbes, N., and Strawn, G. (2017). The End of Moore's Law. *Computing in Science & Engineering*, 19(2), 4-6.
- Tran, H., Campos-Nanez, E., Fomin, P., and Wasek, J. (2016). Cyber Resilience Recovery Model to Combat Zero-Day Malware Attacks. *Computers & Security*, 61, 19-31.
- Tuncalp, D. (2016). Questioning the Ontology of Sociomateriality: A Critical Realist Perspective. *Management Decision*, 54(5), 1073-1087.
- Turner, K. and Makhija, M. (2006). The Role of Organizational Controls in Managing Knowledge. *Academy of Management Review*, 31(1), 197-217.
- Tversky, A. and Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, 211, 453-458.
- Tynes, R. (2007). Nation-Building and the Diaspora on Leonenet: A Case of Sierra Leone in Cyberspace. *New Media & Society*, 9(3), 497-518.
- Unger, C. (2015). 'SHOOT HIM NOW!!!' Anonymity, Accountability, and Online Spectatorship in Wafaa Bilal's *Domestic Tension*. *International Journal of Performance Arts and Digital Media*, 11(2), 202-218.
- Urciuoli, L. (2015). Cyber-Resilience: A Strategic Approach for Supply Chain Management. *Technology Innovation Management Review*, 5(4), 13-18.

- Uzunov, A. and Fernandez, E. (2014). An Extensible Pattern-Based Library and Taxonomy of Security Threats for Distributed Systems. *Computer Standards & Interfaces*, 36, 734-747.
- Vaidyanathan, G., Devaraj, S., and D'Arcy, J. (2012). Does Security Impact E-procurement Performance? Testing a Model of Direct and Moderated Effects. *Decision Sciences*, 43(3), 437-458.
- Vanderhaegen, F. (2017). Towards Increased Systems Resilience: New Challenges Based on Dissonance Control for Human Reliability in Cyber-Physical & Human Systems. *Annual Reviews in Control*, 44, 316-322.
- van der Nagel, E. and Frith, J. (2015). Anonymity, Pseudonymity, and the Agency of Online Identity: Examining the Social Practices of r/Gonewild. *First Monday*, 20(3-2). Accessed online 17 April 2018:
<http://journals.uic.edu/ojs/index.php/fm/rt/printerFriendly/5615/4346>.
- van Ginkel, W.P. and van Knippenberg, D. (2008). Group Information Elaboration and Group Decision Making: The Role of Shared Task Representations. *Organizational Behavior and Human Decision Processes*, 105, 82-97.
- van Schie, E. and van der Pligt, J. Influencing Risk Preference in Decision Making: The Effects of Framing and Salience. *Organizational Behavior and Human Decision Processes*, 63(3), 264-275.
- Vardi, M.Y. (2014). Moore's Law and the Sand-Heap Paradox. *Communications of the ACM*, 57(5), 5.
- Venter, H.S. and Elof, J.H.P. (2003). A Taxonomy for Information Security Technologies. *Computers & Security*, 22(4), 299-307
- Venters, W., Oborn, E., and Barrett, M. (2014). A Trichordal Temporal Approach to Digital Coordination: The Sociomaterial Mangling of the CERN Grid. *MIS Quarterly*, 38(3), 927-949.
- Vos, T.P., Craft, S., and Ashley, S. (2012). New Media, Old Criticism: Bloggers' Press Criticism and the Journalistic Field. *Journalism*, 13(7), 850-868.
- Wade, M.R. and Gravill, J.I. (2003). Diversification and Performance of Japanese IT Subsidiaries: A Resource-Based View. *Information & Management*, 40, 305-316.
- Wade, M. and Hulland, J. (2004). Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research. *MIS Quarterly*, 28(1), 107-142.

- Wagner, A. (2017). Information Theory, Evolutionary Innovations, and Evolvability. *Philosophical Transactions Royal Society B.*, 372, 1-8.
- Walshaw, M. (2015). Confirmations and Contradictions: Investigating the Part that Digital Technologies Play in Students' Everyday and School Lives. *Waikato Journal of Education*, 19(1), 237-247.
- Wang, K., Du, M., Yang, D., Zhu, C., Shen, J., and Zhang, Y. (2016). Game-Theory-Based Active Defense for Intrusion Detection in Cyber-Physical Embedded Systems. *ACM Transactions on Embedded Computing Systems*, 16(1), Article 18, 1-21.
- Wang, Y., Meister, D., and Gray, P. (2013). Social Influence and Knowledge Management Systems Use: Evidence from Panel Data. *MIS Quarterly*, 37(1), 299-313.
- Welp, Y., Urgell, F., and Albar, E. (2007). From Bureaucratic Administration to Network Administration? An Empirical Study on E-Government Focus on Catalonia. *Public Organization Review*, 7(4), 299-316.
- Weyman, A.K. and Clarke, D.D. (2003). Investigating the Influence of Organizational Role on Perceptions of Risk in Deep Coal Mines. *Journal of Applied Psychology*, 88(3), 404-412.
- White, W.D. (1992). Information and the Control of Agents. *Journal of Economic Behavior and Organization* (18), 111-117.
- Willer, R., Flynn, F.J., and Zak, S. (2012). Structure, Identity, and Solidarity: A Comparative Field Study of Generalized and Direct Exchange. *Administrative Science Quarterly*, 57(1), 119-155.
- Winters, C. (2009). Cultivating a Relationship That Works: Cyber-Vigilantism and the Public Versus Private Inquiry of Cyber-Predator Stings. *University of Kansas Law Review*, 57, 427-460.
- Workman, M., Ford, R., and Allen, W. (2008). A Structuration Agency Approach to Security Policy Enforcement in Mobile Ad Hoc Networks. *Information Security Journal: A Global Perspective*, 17, 267-277.
- Wright, M. (2014). Predictors of Anonymous Cyber Aggression: The Role of Adolescents' Beliefs About Anonymity, Aggression, and the Permanency of Digital Content. *Cyberpsychology, Behavior, and Social Networking*, 17(7), 431-438.
- Wu, J., Shen, Y.L., Reinhardt, K., Szu, H., and Dong, B. (2013). A Nanotechnology Enhancement to Moore's Law. *Applied Computational Intelligence and Soft Computing*, 2013, 1-13.

- Wu, S.P.J., Straub, D.W., and Liang, T.P. (2015). How Information Technology Governance Mechanisms and Strategic Alignment Influence Organizational Performance: Insights from a Matched Survey of Business and IT Managers. *MIS Quarterly*, 39(2), 497-518.
- Wu, Y., Feng, G., Wang, N., and Liang, H. (2015). Game of Information Security Investment: Impact of Attack Types and Network Vulnerability. *Expert Systems with Applications*, 42, 6132-6146.
- Yuxiao, Z. (1988). Definitions and Sciences of Information. *Information Processing and Management*, 24 (4), 479-491.
- Zajko, M. (2016). Telecom Responsibilization: Internet Governance, Surveillance, and New Roles for Intermediaries. *Canadian Journal of Communication*, 41(1), 75-93.
- Zhang, X. (2017). Knowledge Management System Use and Job Performance: A Multilevel Contingency Model. *MIS Quarterly*, 41(3), 811-840.
- Zhang, X. and Venkatesh, V. (2017). A Nomological Network of Knowledge Management System Use: Antecedents and Consequences. *MIS Quarterly*, 41(4), 1275-1306.
- Zhu, K. (2014). The Complementarity of Information Technology Infrastructure and E-Commerce Capability: A Resource-Based Assessment of Their Business Value. *Journal of Management Information Systems*, 21(1), 167-202.
- Zhuang, Y. and Lederer, A.L. (2006). A Resource-Based View of Electronic Commerce. *Information & Management*, 43, 251-261.
- Zobel, C. and Khansa, L. (2012). Quantifying Cyberinfrastructure Resilience Against Multi-Event Attacks. *Decision Sciences*, 43 (4), 687-710.

APPENDIX C

A SURVEY OF CYBERATTACKS

A Survey of Cyberattacks

The following list of candidate events was compiled using a broad internet search using the following search terms: biggest hacks of all time, notorious hackers, biggest hacks of 2017, biggest hacks of 2016, biggest hacks of 2015, biggest hacks of 2014, biggest hacks of 2013, biggest hacks of all time 2010, biggest hacks of all time 2005, biggest hacks of all time 2000, innovative hacks, biggest government hacks, cyber breaches federal government, cyber breaches critical infrastructure, cyberattack critical infrastructure, twitter facebook botnets, botnets, social engineering hacks, fake news, DDoS, ransomware, bitcoin hacks. The initial data set included 114 events. The events were categorized by cyber event type, including cyberespionage, cybercrime, disruptive cyber events, and destructive cyber events. The data sample was then further stratified by attacker type including nation state, organized crime, hacktivists, terrorist networks, and individuals. A random data sample was taken from each strata in order to ensure that all types of attacks and attackers are represented in the survey. The purpose of including a breadth of attacks and attackers is to ensure the broadest representation of cyberattack in the data sample.

You have been selected to evaluate these cyberattacks because of your expertise in cyber operations. Your evaluations of these events will be used to select the top 10 cyberattacks from the list. These events will then be explored in depth to develop historical case studies illustrating the interactions between people, data, and technology. **Using a scale of 1-5, where 1 is the lowest possible score and 5 is the highest possible score**, evaluate each event according to the following criteria:

- **Success** of the event: organizational impacts, overcoming security measures, goal achievement

- **Scale** of the event number of countries affected, number of organizations affected, impact to operations within the organization, impact to organizational stakeholders

- **Novelty** of the event: in the context of the time when it occurred, creativity/innovation, exploitation of new vulnerabilities, employment of emerging technologies, use of new tactics & techniques

- **Familiarity** with the event are you familiar enough with the event that you are comfortable applying the above criteria?

A Comments block is available for each attack to capture any specifics you might want to add related to your assessment.

Cyberattack	Year	Description	Novelty	Success	Scale	Evolution
Chinese Hack of Weapons		A confidential report prepared for the Pentagon indicates that Chinese cyber criminals breached design files for over two dozen critical weapons systems, including critical missile defense programs.				
Northeast Blackout	2003	The world's second most widespread blackout in history, it was publicly attributed to a downed power line, rather than a cyber-attack (the U.S. government had decided that the 'public' was not yet prepared to learn about such cyber-attacks). The Northeast (U.S.) blackout that year affected an estimated 10 million people in Ontario and 45 million people in eight U.S. states, caused 11 deaths and an estimated \$6 billion in economic damages, having disrupted power for at least two days.				
AOL	2014	Hackers accessed a trove of personal data including AOL users' email addresses, mailing addresses, contacts, encrypted passwords, encrypted answers to security questions used for resetting passwords, and some employee information. Spammers used that information to send "spoofed" emails -- messages that appear to be from a valid address or trusted contact, but are not actually from those contacts -- from about 2 percent of all AOL Mail accounts.				
IoT Botnets	2017	Following the Mirai attack in 2016, 'IoT_reaper,' first spotted in September 2017 by researchers at firm Qihoo 360, the new malware no longer depends on cracking weak passwords; instead, it exploits vulnerabilities in various IoT devices and enslaves them into a botnet network.				
Shadow Brokers	2016	Claimed to have breached the spy tools of the elite NSA-linked operation known as the Equation Group. The Shadow Brokers offered a sample of alleged stolen NSA data and attempted to auction off a bigger trove, following up with leaks for Halloween and Black Friday in 2016.				
Casino Fish Tank	2017	Smart fish tank (IoT) hacked to exfiltrate Casino data. Sensors in the fish tank were connected to a computer that regulated the temperature, food, and cleanliness of the tank. By gaining access to the computer that regulated the fish tank, the hackers then gained access to the network(s) that machine could access				
Defense Threat Reduction Agency	1999	Florida high school student Jonathan James installed backdoor software into the Defense Threat Reduction Agency and intercepted numerous classified emails, including life support code for the International Space Station.				

Commerce Department	2006	The Commerce Department's Bureau of Industry and Security had to throw away all of its computers in October 2006, paralyzing the bureau for more than a month due to targeted attacks originating from China. BIS is where export licenses for technology items to countries like China are issued.				
NSA - Snowden	2013	Snowden worked for several years as a contract employee for the NSA at one of its facilities in Hawaii and prior to that in Japan. Used his privileged access to classified systems to download detailed information on highly secret NSA domestic and international surveillance programs.				
Petya Ransomware	2017	Though it infected networks in multiple countries—like the US pharmaceutical company Merck, Danish shipping company Maersk, and Russian oil giant Rosneft—researchers suspect that the ransomware actually masked a targeted cyberattack against Ukraine. The ransomware hit Ukrainian infrastructure particularly hard, disrupting utilities like power companies, airports, public transit, and the central bank, just the latest in a series of cyber assaults against the country.				
AP Twitter Feed	2013	Twitter account of the Associated Press sent a tweet to almost 2 million followers that warned, "Breaking: Two Explosions in the White House and Barack Obama is injured." At 1:08, the Dow began a short-lived nosedive. It dropped about 150 points, from 14697.15 to 14548.58, before stabilizing at 1:10 p.m., when news that the tweet had been erroneous began to spread. By 1:13 p.m., the level had returned to 14690. During those three minutes, the "fake tweet erased \$136 billion in equity market value," according to Bloomberg News' Nikolaj Gammeltoft.				
U.K. Energy Sector	2017	A report to <i>Motherboard</i> from the UK's General Communications Headquarters (GCHQ), and more specifically the national Cyber Security Centre (NCSC) stated that hackers are targeting the UK energy sector. At the core of the report it is said that 'industrial control system organizations are likely to have been successfully compromised.' Like in the comparable U.S. incident, no speculation of motivations behind the attacks was included.				
Fake News	2016	CIA and other intelligence agencies concluded with "high confidence" that Russia tried to covertly influence the U.S. presidential election. Russian hackers infiltrated computer systems of both major U.S. political parties.				
Dyn Ddos	2016	Botnet launched massive DDoS attack against Dyn the DNS provider. Millions of websites, included Twitter, GitHub, Netflix went down. Botnet covered about 100,000 household devices (IoT webcams and DVRs) infected with Mirai malware.				
American Business	2005-2012	Over the course of eight years, a hacking group from Russia and Ukraine targeted banks and companies, including Nasdaq, 7-11, JetBlue and JC Penney. The hackers stole 160 million credit and debit card numbers and breached 800,000 bank accounts. It is the largest cyber crime case filed as of 2015.				
IRS	2015	Hackers accessed more than 300,000 taxpayer accounts. The hackers targeted the site's Get Transcript feature, which allows taxpayers to view and download copies of the tax returns they filed with the agency—which include sensitive information such as their Social Security numbers and incomes. Although tax filers have to answer multiple identity verification questions to access their files, the hackers apparently came armed with information they had gathered from other sources to correctly answer questions.				
Mafiaboy vs. Yahoo, CNN, eBay, Dell & Amazon	2000	The first major DDoS attack responsible for crippling some of the internet's most popular websites. "Mafiaboy," a.k.a. 15-year-old Michael Calce, set out to make a name for himself when he launched "Project Rivolta," which took down the website of the #1 search engine at the time—and second-most popular website—Yahoo. Thinking it may have been a fluke, he went on to batter the servers of CNN, eBay, Dell, and Amazon in a wave of highly-publicized attacks.				
Bitumb Bitcoin Exchange	2017	One of the largest bitcoin exchanges in the world was hacked, and 30,000 customers' data was compromised.				

Melissa Virus	1999	The fastest-spreading virus of its day, infecting 20% of the world's computers. Coded by a bored New Jersey programmer named David L. Smith, the software was deceptively simple – disguised as a Microsoft Word document, it would spread through email, automatically sending itself to the first 50 names in an infected computer's address book. The document was first uploaded to the alt.sex newsgroup in 1999 and from there it exploded, being sent out so rapidly that it forced infected companies like Microsoft and Intel to shut down outgoing mail until				
Sony	2014	Cyberattack attributed to North Korea in order to stop Sony Pictures from releasing the movie "The Interview" in which talk show hosts are recruited by the CIA to assassinate Kim Jong Un. Outcomes from this attack included the disclosure of intellectual property & internal emails via the internet and WikiLeaks, and the destruction of IT infrastructure. There were also members of the company who lost their jobs.				
Wikileaks (Manning Disclosure)	2010-2011	WikiLeaks posts more than 90,000 classified documents relating to the Afghanistan war in what has been called the biggest leak since the Pentagon Papers during the Vietnam War. The documents are divided into more than 100 categories and touch on everything from the hunt for Osama bin Laden to Afghan civilian deaths resulting from US military actions. October, WikiLeaks publishes nearly 400,000 classified military documents from the Iraq War, providing a new picture of how many Iraqi civilians have been killed, the role that Iran has played in supporting Iraqi militants and many accounts of abuse by Iraq's army and police. November: WikiLeaks begins publishing approximately 250,000 leaked State Department cables dating back to 1966. The site says the documents will be released "in stages over the next few months."				
Twitterbots	2013-Present	Twitter bots produce spam, provide fake followers for anybody willing to pay, and can manipulate debates and public opinion. The effects of large swarms of Twitter bots—so-called botnets—are largely unknown. As soon as a new technique becomes available to identify these accounts, botmasters modify and upgrade their charges to avoid detection. Botnet of 3 million accounts (built to be undetectable) is responsible for a total of 2.6 billion tweets (including retweets), with a daily activity of 500 million tweets. The botnet is a trend-setter, and it has been working for at least two years. Botnets have changed how political campaigns are run. They're programmed with AI and NLP to manipulate public opinion through social media.				
Global Payments	2012	Global Payments handles credit card transactions for small business vendors. Their systems were breached by hackers, and information on people's credit cards was stolen, leading to fraudulent transaction on the users' credit cards.				
James Kosta		James Kosta and partners hacked big business and military computers, including major banks, General Electric and IBM.				
Spamhaus	2013	This DDOS attack was large enough that it slowed the entire Internet across the planet, and completely shut down parts of the internet for hours. The perpetrators used hundreds of DNS servers to reflect signals, amplifying the flood effect and sending up to 300 gigabits per second of flood data to each server on the network. The target of the attack was Spamhaus, a nonprofit professional protection service that tracks and blacklists spammers and hackers on behalf of web users. The Spamhaus servers, along with dozens of other internet exchange servers, were flooded in this 2013 DDOS attack.				
Dropbox	2012	Email and password data for more than 68 million Dropbox users is for sale in the darknet marketplace. The data set, which is from a 2012 breach, includes users' email addresses as well as obscured passwords. Nearly 5 gigabytes of user credential data were leaked. Its price was reportedly set at two bitcoins, by a data trafficker on the darknet website TheRealDeal.				

The Athens Affair – Vodafone Greece	2004	This event involved the illegal tapping of more than 100 mobile phones on the Vodafone Greece network belonging to members of the Greek government and top-ranking civil servants. The taps began sometime near the beginning of August 2004 and were removed in March 2005 without discovering the identity of the perpetrators. The phones tapped included those of the Prime Minister, the Mayor of Athens, top officers at the Ministry of Defense, the Ministry of Foreign Affairs, the Ministry for Public Order, members of the ruling party, ranking members of the opposition Panhellenic Socialist Movement party (PASOK), the Hellenic Navy General Staff, the previous Minister of Defense and an employee of the American Embassy. Phones of Athens-based Arab businessmen were also tapped.				
DoD	2015	Russian hackers gained access to Department of Defense unclassified files. The department quickly identified the hackers and removed them from the network.				
Census Bureau	2015	The Federal Audit Clearinghouse was infiltrated at the Census Bureau, resulting in the loss of federal employee data and information. The hackers were able to retrieve thousands of users' organization user accounts, census data, and contact methods. Audit information that assesses an organization's qualification for federal assistance funding was also stolen. The four files that were breached were later posted on the Web, available to the public. The hacker group Anonymous claimed responsibility for the breach.				
Ashley Madison	2015	The hacker group Impact Team broke into the Avid Life Media servers and copied the personal data of 37 million Ashley Madison users. The hackers then incrementally released this information through various websites. The hack impacted individual reputations. There are claims that user suicides followed after the hack.				
Olympic Vision Business Email Campaign	2016	The fourth malware targeted 18 companies in the United States, Middle East and Asia. In the case of this newly-discovered campaign, cybercriminals made use of Olympic Vision, a keylogger purchased online for \$25. Feigning legitimacy and urgency, the malware is sent to an employee through an email attachment. Once opened, a backdoor is installed and infects the victim's system and steals vital information.				
Facebook Botnet	2014 & 2017	Greek botnet used Facebook to spread malware and infected 250,000 computers to mine crypto-currencies, steal bitcoins, email passwords and banking details.				
U.S. Army Website	2015	Army.mil was taken offline temporarily after it was found that hackers had gained access to the Web site and were posting personal messages. No critical information was accessed. The Syrian Electronic Army claimed responsibility for the attack on Twitter.				
Gemalto	2010-2011	The attackers targeted the company's huge cache of cryptographic keys, although Gemalto says they were unsuccessful. If the hackers did obtain the keys, the hack has huge implications. Gemalto's SIM cards and cryptographic keys are used to help secure the phone communications of billions of customers of AT&T, T-Mobile, Verizon, Sprint, and more than 400 other wireless carriers in 85 countries. Stealing the crypto keys would have allowed the spy agencies to wiretap and decipher encrypted phone communications between mobile handsets and cell towers.				
Robert Tappan Morris vs. the World	1988	A self-replicating worm with a mission: go out to determine the size of the internet. It backfired, replicating itself beyond control and infecting thousands of computers (a lot at the time!), costing millions of dollars in damage, and inspiring the U.S. government to create a emergency response for computers—CERT. The source code was archived on a black 3.5-inch floppy disk now on display at the Boston Museum of Science.				
Stuxnet	2010	This event involved the hack of "air-gapped" Iranian Centrifuges used to process uranium. It resulted in the physical damage of over 1000 centrifuges. The cyberattack is attributed to Israel and the United States, although neither country has acknowledged responsibility.				

APPENDIX D
IRB APPROVAL

Certification of Approval for a Project Involving Human Subjects

Date: 07-Jun-2018

Protocol Number: 25106

PI: SCHUFF, DAVID

Review Type: EXEMPT

Approved On: 07-Jun-2018

Approved From:

Approved To:

Committee: A1

School/College: BUSINESS SCHOOL (1500)

Department: FSBM:MANAGEMENT INFORMATION SYSTEMS (15280)

Sponsor: NO EXTERNAL SPONSOR

Project Title: The Cyber Based View of the Firm

The IRB approved the protocol 25106.

If the study was approved under expedited or full board review, the approval period can be found above. Otherwise, the study was deemed exempt and does not have an IRB approval period.

If applicable to your study, you can access your IRB-approved, stamped consent document or consent script through ERA. **Open the Attachments tab and open the stamped documents by clicking the Latest link next to each document.** The stamped documents are labeled as such. Copies of the IRB approved stamped consent document or consent script must be used in obtaining consent.

Before an approval period ends, you must submit the Continuing Review form via the ERA module. Please note that though an item is submitted in ERA, it is not received in the IRB office until the principal investigator approves it. Consequently, please submit the Continuing Review form via the ERA module at least 60 days, and preferably 90 days, before the study's expiration date.

Note that all applicable Institutional approvals must also be secured before study implementation. These approvals include, but are not limited to, Medical Radiation Committee ("MRC"); Radiation Safety Committee ("RSC"); Institutional Biosafety Committee ("IBC"); and Temple University Survey Coordinating Committee ("TUSCC"). Please visit these Committees' websites for further information.

Finally, in conducting this research, you are obligated to submit the following:

- **Amendment requests - all changes to the study must be approved by the IRB prior to the implementation of the changes unless necessary to eliminate apparent immediate hazards to subjects**
- **Reportable new information - using the Reportable New Information form, report new information items such**

as those described in the Investigator Guidance: Prompt Reporting Requirements HRP-801 to the IRB **within 5 days**

- **Closure report** - using a closure form, submit when the study is permanently closed to enrollment; all subjects have completed all protocol related interventions and interactions; collection of private identifiable information is complete; and Analysis of private identifiable information is complete.

For the complete list of investigator responsibilities, please see the Policies and Procedures, the Investigator Manual, and other requirements found on the Temple University IRB website: : <http://research.temple.edu/irb-forms-standard-operating-procedures#POLICY>

Please contact the IRB at (215) 707-3390 if you have any questions

APPENDIX E
CYBERATTACK SURVEY RESULTS

Table E1. Ranked Results of Cyberattack Survey

Cyberattack	Year	Description	Ranking
Stuxnet	2010	This event involved the hack of “air-gapped” Iranian Centrifuges used to process uranium. It resulted in the physical damage of over 1000 centrifuges. The cyberattack is attributed to Israel and the United States, although neither country has acknowledged responsibility.	1
Northeast Blackout	2003	The world's second most widespread blackout in history, it was publicly attributed to a downed power line, rather than a cyberattack (the U.S. government had decided that the ‘public’ was not yet prepared to learn about such cyberattacks). The Northeast (U.S.) blackout that year affected an estimated 10 million people in Ontario and 45 million people in eight U.S. states, caused 11 deaths and an estimated \$6 billion in economic damages, having disrupted power for at least two days.	2
IoT Botnets	2017	Following the Mirai attack in 2016, 'IoT_reaper,' first spotted in September 2017 by researchers at firm Qihoo 360, the new malware no longer depends on cracking weak passwords; instead, it exploits vulnerabilities in various IoT devices and enslaves them into a botnet network.	3
Twitterbots	2013-Present	Twitter bots produce spam, provide fake followers for anybody willing to pay, and can manipulate debates and public opinion. The effects of large swarms of Twitter bots—so-called botnets—are largely unknown. As soon as a new technique becomes available to identify these accounts, botmasters modify and upgrade their charges to avoid detection. Botnet of 3 million accounts (built to be undetectable) is responsible for a total of 2.6 billion tweets (including retweets), with a daily activity of 500 million tweets. The botnet is a trend-setter, and it has been working for the at least two years. Botnets have changed how political campaigns are run. They're programmed with AI and NLP to manipulate public opinion through social media.	4

Melissa Virus	1999	The fastest-spreading virus of its day, infecting 20% of the world's computers. Coded by a bored New Jersey programmer named David L. Smith, the software was deceptively simple – disguised as a Microsoft Word document, it would spread through email, automatically sending itself to the first 50 names in an infected computer's address book. The document was first uploaded to the alt.sex newsgroup in 1999 and from there it exploded, being sent out so rapidly that it forced infected companies like Microsoft and Intel to shut down outgoing mail until they got it under control.	5
American Business	2005-2012	Over the course of eight years, a hacking group from Russia and Ukraine targeted banks and companies, including Nasdaq, 7-11, JetBlue and JC Penney. The hackers stole 160 million credit and debit card numbers and breached 800,000 bank accounts. It is the largest cybercrime case filed as of 2015.	6
Petya Ransomware	2017	Though it infected networks in multiple countries—like the US pharmaceutical company Merck, Danish shipping company Maersk, and Russian oil giant Rosnoft—researchers suspect that the ransomware actually masked a targeted cyberattack against Ukraine. The ransomware hit Ukrainian infrastructure particularly hard, disrupting utilities like power companies, airports, public transit, and the central bank, just the latest in a series of cyber assaults against the country.	7
Wikileaks (Manning Disclosure)	2010-2011	WikiLeaks posts more than 90,000 classified documents relating to the Afghanistan war in what has been called the biggest leak since the Pentagon Papers during the Vietnam War. The documents are divided into more than 100 categories and touch on everything from the hunt for Osama bin Laden to Afghan civilian deaths resulting from US military actions. October, WikiLeaks publishes nearly 400,000 classified military documents from the Iraq War, providing a new picture of how many Iraqi civilians have been killed, the role that Iran has played in supporting Iraqi militants and many accounts of abuse by Iraq's army and police. November: WikiLeaks begins publishing approximately 250,000 leaked State Department cables dating back to 1966. The site says the documents will be released "in stages over the next few months."	8

Spamhaus	2013	This DDOS attack was large enough that it slowed the entire Internet across the planet, and completely shut down parts of the internet for hours. The perpetrators used hundreds of DNS servers to reflect signals, amplifying the flood effect and sending up to 300 gigabits per second of flood data to each server on the network. The target of the attack was Spamhaus, a nonprofit professional protection service that tracks and blacklists spammers and hackers on behalf of web users. The Spamhaus servers, along with dozens of other internet exchange servers, were flooded in this 2013 DDOS attack.	9
Dyn DDoS	2016	Botnet launched massive DDoS attack against Dyn the DNS provider. Millions of websites, included Twitter, GitHub, Netflix went down. Botnet covered about 100,000 household devices (IoT webcams and DVRs) infected with Mirai malware.	10
Fake News	2016	CIA and other intelligence agencies concluded with “high confidence” that Russia tried to covertly influence the U.S. presidential election. Russian hackers infiltrated computer systems of both major U.S. political parties.	11
Sony	2014	Cyberattack attributed to North Korea in order to stop Sony Pictures from releasing the movie "The Interview" in which talk show hosts are recruited by the CIA to assassinate Kim Jong Un. Outcomes from this attack included the disclosure of intellectual property & internal emails via the internet and Wikileaks, and the destruction of IT infrastructure. There were also members of the company who lost their jobs.	12
Mafiaboy vs. Yahoo, CNN, eBay, Dell & Amazon	2000	The first major DDoS attack responsible for crippling some of the internet's most popular websites. "Mafiaboy," a.k.a. 15-year-old Michael Calce, set out to make a name for himself when he launched "Project Rivolta," which took down the website of the #1 search engine at the time—and second-most popular website—Yahoo. Thinking it may have been a fluke, he went on to batter the servers of CNN, eBay, Dell, and Amazon in a wave of highly-publicized attacks.	13
IRS	2015	Hackers accessed more than 300,000 taxpayer accounts. The hackers targeted the site's Get Transcript feature, which allows taxpayers to view and download copies of the tax returns they filed with the agency—which include sensitive information such as their Social Security numbers and incomes. Although tax filers have to answer multiple identity verification questions to access their files, the hackers apparently came armed with information they had gathered from other sources to correctly answer questions.	14

NSA - Snowden	2013	Snowden worked for several years as a contract employee for the NSA at one of its facilities in Hawaii and prior to that in Japan. Used his privileged access to classified systems to download detailed information on highly secret NSA domestic and international surveillance programs.	15
Census Bureau	2015	The Federal Audit Clearinghouse was infiltrated at the Census Bureau, resulting in the loss of federal employee data and information. The hackers were able to retrieve thousands of users' organization user accounts, census data, and contact methods. Audit information that assesses an organization's qualification for federal assistance funding was also stolen. The four files that were breached were later posted on the Web, available to the public. The hacker group Anonymous claimed responsibility for the breach.	16
Robert Tappan Morris vs. the World	1988	A self-replicating worm with a mission: go out to determine the size of the internet. It backfired, replicating itself beyond control and infecting thousands of computers (a lot at the time!), costing millions of dollars in damage, and inspiring the U.S. government to create a emergency response for computers—CERT. The source code was archived on a black 3.5-inch floppy disk now on display at the Boston Museum of Science.	17
Chinese Hack of Weapons		A confidential report prepared for the Pentagon indicates that Chinese cyber criminals breached design files for over two dozen critical weapons systems, including critical missile defense programs.	18
Ashley Madison	2015	The hacker group Impact Team broke into the Avid Life Media servers and copied the personal data of 37 million Ashley Madison users. The hackers then incrementally released this information through various websites. The hack impacted individual reputations. There are claims that user suicides followed after the hack.	19
Dropbox	2012	Email and password data for more than 68 million Dropbox users is for sale in the darknet marketplace. The data set, which is from a 2012 breach, includes users' email addresses as well as obscured passwords. Nearly 5 gigabytes of user credential data were leaked. Its price was reportedly set at two bitcoins, by a data trafficker on the darknet website TheRealDeal.	20

Casino Fish Tank	2017	Smart fish tank (IoT) hacked to exfiltrate Casino data. Sensors in the fish tank were connected to a computer that regulated the temperature, food, and cleanliness of the tank. By gaining access to the computer that regulated the fish tank, the hackers then gained access to the network(s) that machine could access	21
AP Twitter Feed	2013	Twitter account of the Associated Press sent a tweet to almost 2 million followers that warned, "Breaking: Two Explosions in the White House and Barack Obama is injured." At 1:08, the Dow began a short-lived nosedive. It dropped about 150 points, from 14697.15 to 14548.58, before stabilizing at 1:10 p.m., when news that the tweet had been erroneous began to spread. By 1:13 p.m., the level had returned to 14690. During those three minutes, the "fake tweet erased \$136 billion in equity market value," according to Bloomberg News' Nikolaj Gammeltoft.	22
Global Payments	2012	Global Payments handles credit card transactions for small business vendors. Their systems were breached by hackers, and information on people's credit cards was stolen, leading to fraudulent transaction on the users' credit cards.	23
Commerce Department	2006	The Commerce Department's Bureau of Industry and Security had to throw away all of its computers in October 2006, paralyzing the bureau for more than a month due to targeted attacks originating from China. BIS is where export licenses for technology items to countries like China are issued.	24
AOL	2014	Hackers accessed a trove of personal data including AOL users' email addresses, mailing addresses, contacts, encrypted passwords, encrypted answers to security questions used for resetting passwords, and some employee information. Spammers used that information to send "spoofed" emails -- messages that appear to be from a valid address or trusted contact, but are not actually from those contacts -- from about 2 percent of all AOL Mail accounts.	25
Shadow Brokers	2016	Claimed to have breached the spy tools of the elite NSA-linked operation known as the Equation Group. The Shadow Brokers offered a sample of alleged stolen NSA data and attempted to auction off a bigger trove, following up with leaks for Halloween and Black Friday in 2016.	26
Facebook Botnet	2014 & 2017	Greek botnet used Facebook to spread malware and infected 250,000 computers to mine crypto-currencies, steal bitcoins, email passwords and banking details.	27

U.K. Energy Sector	2017	A report to <i>Motherboard</i> from the UK's General Communications Headquarters (GCHQ), and more specifically the national Cyber Security Centre (NCSC) stated that hackers are targeting the UK energy sector. At the core of the report it is said that 'industrial control system organizations are likely to have been successfully compromised.' Like in the comparable U.S. incident, no speculation of motivations behind the attacks was included.	28
Bithumb Bitcoin Exchange	2017	One of the largest bitcoin exchanges in the world was hacked, and 30,000 customers' data was compromised.	29
Defense Threat Reduction Agency	1999	Florida high school student Jonathan James installed backdoor software into the Defense Threat Reduction Agency and intercepted numerous classified emails, including life support code for the International Space Station.	30
The Athens Affair – Vodafone Greece	2004	This event involved the illegal tapping of more than 100 mobile phones on the Vodafone Greece network belonging to members of the Greek government and top-ranking civil servants. The taps began sometime near the beginning of August 2004 and were removed in March 2005 without discovering the identity of the perpetrators. The phones tapped included those of the Prime Minister, the Mayor of Athens, top officers at the Ministry of Defense, the Ministry of Foreign Affairs, the Ministry for Public Order, members of the ruling party, ranking members of the opposition Panhellenic Socialist Movement party (PASOK), the Hellenic Navy General Staff, the previous Minister of Defense and an employee of the American Embassy. Phones of Athens-based Arab businessmen were also tapped.	31
Gemalto	2010-2011	The attackers targeted the company's huge cache of cryptographic keys, although Gemalto says they were unsuccessful. If the hackers did obtain the keys, the hack has huge implications. Gemalto's SIM cards and cryptographic keys are used to help secure the phone communications of billions of customers of AT&T, T-Mobile, Verizon, Sprint, and more than 400 other wireless carriers in 85 countries. Stealing the crypto keys would have allowed the spy agencies to wiretap and decipher encrypted phone communications between mobile handsets and cell towers.	32

Olympic Vision Business Email Campaign	2016	The fourth malware targeted 18 companies in the United States, Middle East and Asia. In the case of this newly-discovered campaign, cybercriminals made use of Olympic Vision, a keylogger purchased online for \$25. Feigning legitimacy and urgency, the malware is sent to an employee through an email attachment. Once opened, a backdoor is installed and infects the victim's system and steals vital information.	33
U.S. Army Website	2015	Army.mil was taken offline temporarily after it was found that hackers had gained access to the Web site and were posting personal messages. No critical information was accessed. The Syrian Electronic Army claimed responsibility for the attack on Twitter.	34
James Kosta		James Kosta and partners hacked big business and military computers, including major banks, General Electric and IBM.	35
DoD	2015	Russian hackers gained access to Department of Defense unclassified files. The department quickly identified the hackers and removed them from the network.	36

APPENDIX F
RESULTS TABLES: EMPIRICAL PATTERNS

Table F1. Empirical Patterns from Nine Case Studies: Cognitive Dimension

P1: Cyberattacks will include a cognitive dimension.		
Case Study	Examples	References
Stuxnet	<p><i>Nation state governments (Iran, United States and Israel):</i> People who make decisions to benefit the security and prosperity of their country, in this case, Iran, the United States and Israel.</p> <p><i>Engineers at Natanz nuclear facility:</i> People using their knowledge and skills to make operational decisions related to the enrichment of uranium.</p> <p><i>Iranian engineering firms specializing in Industrial Control Systems (ICS):</i> People working for one or more of these engineering firms provided ICS maintenance services to the Natanz facility.</p> <p><i>Trusted software providers (Realtek Semiconductor, Micron Technology):</i> People who were recognized as developers of trustworthy software.</p> <p><i>Hackers/Attackers (possibly Sandworm or Fancy Bear):</i> People who apply their knowledge and skills to gain unauthorized access to computing environments.</p>	<p>Paganini, 2016; Broad et al., 2011; Nakashima & Warrick, 2012; Kushner, 2013; Sanger, 2012; Arthur, 2013; Rogers, 2015</p> <p>Sanger, 2012; Nakashima & Warrick, 2012; Langner, 2011</p> <p>Zetter, 2014</p> <p>Chen & Abu-Nimeh, 2011; Zetter, 2011; Lindsay, 2013</p> <p>BBC, 2017; Greenberg, 2017; Park et al., 2017; Polityuk et al., 2017; Sullivan & Kamensky, 2017; Detsch, 2016; Smith, 2018; Zetter, 2017; Lee et al., 2016; Harrell, 2017; Toecker, 2016; Osborne, 2018</p> <p>Park et al., 2017; Sullivan & Kamensky, 2017; Toecker, 2016; Detsch, 2016; Smith, 2017; Harrell, 2017; Greenberg, 2017; Osborne, 2018</p> <p>Zetter, 2017; Lee et al., 2016; Sullivan & Kamensky, 2017</p>
	<p><i>Electric Power Operations Personnel:</i> People who monitor, manage, and make decisions related to the transmission and distribution of electric power.</p> <p><i>Customers:</i> People who were concerned when they lost power in the cold winter temperatures.</p>	<p>Park et al., 2017; Sullivan & Kamensky, 2017; Toecker, 2016; Detsch, 2016; Smith, 2017; Harrell, 2017; Greenberg, 2017; Osborne, 2018</p> <p>Zetter, 2017; Lee et al., 2016; Sullivan & Kamensky, 2017</p>
	<p><i>Russian Government:</i> People who make decisions to benefit the security and prosperity of the Russian Nation State.</p>	<p>Greenberg, 2017; Polityuk et al., 2017; Park et al., 2017; Sullivan & Kamensky, 2017; Smith, 2018; Adamczyk, 2017; Harrell, 2017</p>
	<p><i>"Paras Jha, an undergraduate at Rutgers, became interested in how DDoS attacks could be used for profit."</i> The person who created the Mirai malware.</p>	<p>Fruhlinger, 2018</p>
	<p><i>Dyn:</i> An Internet Service Provider company. People at Dyn use their skills and knowledge to defend their organization against cyberattack.</p>	<p>Mansfield-Devine, 2016; Liu, 2017; Perirot, 2016; Sanger & Perirot,</p>
	<p>Internet of Things (IoT)</p>	

		2016; <i>Trendmicro</i> , 2017; Greenberg, 2017; Leyden, 2017; Fruhlinger, 2018 Kolijs et al., 2017; Leyden, 2017
<i>Botmaster</i> : A person who uses their knowledge and skills to build, maintain, and operate a botnet.		
<i>IoT device vendors</i> : People who make decisions related to security capabilities built into devices that can be connected to the Internet.		Kolijs et al., 2017; Leyden, 2017; Moriuchi & Chohan, 2018
<i>Bot makers</i> : People who use their creativity to make bots.		Hirsch, 2017; Confessore et al., 2018; Dubbins, 2013; Guilbeault & Woolley, 2016
<i>Trolls</i> : People who deliberately say things to make others angry.		Rosenberg, 2017; Farrell, 2018; Hirsch, 2017; Curran, 2017; Economist, 2017; Timberg & Dwoskin, 2018
Twitterbots	<i>Voters & Public Sentiment</i> : People who make decisions and share opinions about complex issues such as national leadership or alliances. <i>Political groups, religious groups, nation states</i> : Groups of people who have strong opinions and want to influence others to share those opinions.	Woolley & Shout, 2016; Timberg & Dwoskin, 2018; Baranik, 2018 Farrell, 2018; Rosenberg, 2017; Timberg & Dwoskin, 2018; Gu et al., 2017; Guilbeault & Woolley, 2016; Baranik, 2018; Hirsch, 2017; Curran, 2017; Economist, 2017 Techspirited, 2019; Gostev, 2005; Taylor et al., 1999; Raney, 1999; Peterson, 1999; CERT, 1999 <i>WSJ</i> , 1999; <i>NYT</i> , Dec 1999; Smothers, 1999; Taylor et al., 1999; Pearce, 2002; Strickland, 2008; Panda Security, 2013; McNamara, 2014; Cluley, 2009; Mills, 2009; Raney, 1999 <i>Federal Bureau of Investigation (FBI)</i> : People who investigated the crime of disseminating malicious software.
Melissa Virus	<i>Victim organizations and users</i> : Groups of people whose abilities to do their jobs were impacted.	Taylor et al., 1999; Panda Security, 2013; Cluley, 2009; Mills, 2009; Gostev, 2005 Peterson, 1999; McNamara, 2014; CERT, 1999; <i>NYT</i> , Apr 1999; Redmond, 1999; Panda Security, 2013; McNamara, 2014; Mills, 2009 Hudson, 2013; Bray, 2013; Bray & Yadron, 2013; Fox, 2013; Reuters, 2013; Sullivan, 2013; Jones & Finkle, 2013
Hack of American Business 2007-2012	<i>Vladimir Drinkman</i> : A person who was a member of the cybercrime gang.	

		2013; Wood, 2018; Schwartz, 2015; DoJ, 2015, 2018; Armental, 2015
<i>Roman Kotov:</i> A person who was a member of the cybercrime gang.		Hudson, 2013; Bray, 2013; Bray & Yadron, 2013; Fox, 2013; Reuters, 2013; Sullivan, 2013; Jones & Finkle, 2013; Schwartz, 2015; DoJ, 2015, 2018; Armental, 2015
<i>Dmitriy Smiljanets:</i> A person who was a member of the cybercrime gang.		Hudson, 2013; Bray, 2013; Bray & Yadron, 2013; Fox, 2013; Reuters, 2013; Sullivan, 2013; Jones & Finkle, 2013; Wood, 2018; Schwartz, 2015; DoJ, 2015, 2018; Armental, 2015
<i>Cashers:</i> People who were customers of the cybercrime gang.		Hudson, 2013; Reuters, 2013; Sullivan, 2013; Jones & Finkle, 2013; Beekman, 2013; DoJ, 2015, 2018
<i>Russian Government:</i> People who make decisions to benefit the security and prosperity of the Russian Nation State.		Greenberg, 2018; Hackett, 2017; Palmer, 2017; Reilly, 2017; Tung, 2018; USCERT, 2017; Woo, 2018; Doctorow, 2018; Cimpanu, 2018; Fruhlinger, 2017
<i>Shadow Brokers:</i> The malicious people who stole cyberweapons from the NSA and shared them through WikiLeaks in April 2017.		Palmer-2, 2017; Tung, 2018; Collings, 2017;
(Not)Petya Ransomware		Ryan, 2017; Tung, 2017, 2018; Cimpanu, 2018; Collins, 2017; Daneshkhlu et al., 2017; Chopping, 2017; Greenberg, 2018; Hackett, 2017; Matthews, 2017; Olenick, 2018; Osborne, 2018; Ryan, 2017
<i>National Security Agency:</i> The people who developed the exploits used in the ransomware cyberattacks that took place in May and June 2017.		Fruhlinger, 2017; Greenberg, 2018; Hackett, 2017; Nelson et al., 2017; Osborne, 2018; Tung, 2017
<i>Private Manning:</i> The person who served as an intelligence analyst, who made the decision to steal classified data and release it to the public domain.		Sangarasivam, 2013; Nita, 2014; Berghel, 2012; Jones, 2013; Garnett & Huges, 2019; Somashekhar, 2017; Cadwalladr, 2018; Zavis, 2017; Booth et al., 2010; McGreal, 2010; Tate, 2013; Zetter & Poulsen, 2010; Peralta, 2013; Bumiller, 2010; Thompson, 2010; Chan, 2017; Nicks et al., 2011
WikiLeaks & the Manning Disclosure		

	<i>Julian Assange</i> : The person who founded WikiLeaks to provide an outlet for whistleblowers in order to create greater transparency in the world. <i>Adrian Lamo</i> : The person who made the decision to turn in Private Manning to the U.S. Government.	Nita, 2014; Berghel, 2012; Tate, 2013
	<i>U.S. Government</i> : People who make decisions to benefit the security and prosperity of the United States Nation State. <i>“Impact Team”</i> : The people who exposed the Ashley Madison clientele and business model.	Nita, 2014; Berghel, 2012; Garnett & Hughes, 2019; Tate, 2013; McGreal, 2010; Zetter & Poulsen, 2010 <i>Economist</i> , 2015; Rogers, 2015; Tuttle, 2015; Gauthier, 2017; CNNMoney, 2015; Wright, 2015; Dewey, 2015; <i>ICTMW</i> , 2015; Hackett, 2015; <i>Panda</i> , 2017; Solomon, 2017; Chirgwin, 2016; Ragan, 2015; Cox, 2015; Schwartz, 2015; <i>PIPEDA Report</i> , 2016; Basu, 2015
	<i>Avid Life Media</i> : The people who made decisions for the parent company which owned and operated the Ashley Madison website.	George-Cosh, 2015; Tuttle, 2015; Gauthier, 2017; CNNMoney, 2015; Murdock, 2015; Hackett, 2015; Solomon, 2017; <i>PIPEDA Report</i> , 2016
Ashley Madison	<i>Ashley Madison Users</i> : The people who were using the Ashley Madison services to have an extramarital affair because they believed their activities would be secret.	<i>Economist</i> , 2015; George-Cosh, 2015; CNNMoney, 2015; Michelisen, 2015; Hackett, 2015; <i>Panda</i> , 2017; Cox, 2015; Basu, 2015
	<i>Cynosure Prime</i> : People who experimented with different methods to crack the passwords to the Ashley Madison website.	CynoSure Prime, 2015; CNNMoney, 2015

Table F2. Empirical Patterns from Nine Case Studies: Physical Dimension

P2: Cyberattacks will include a physical dimension.		
Case Study	Examples	References
Stuxnet	<p><i>Natanz centrifuges:</i> The tangible devices used to refine uranium to weapons grade.</p> <p><i>USB thumb drives:</i> Tangible devices used to transfer and store data.</p> <p><i>Siemens S7-400 Programmable Logic Controllers:</i> Tangible devices that control the operation of the centrifuges.</p> <p><i>Networked printers:</i> Tangible office equipment connected to the Internet, present in most organizations.</p>	<p>Chen & Abu-Nimeh, 2011; Zetter, 2011; Weinberger, 2011; Rosenbaum, 2012; Lindsay, 2013</p> <p>Farwell & Rohozinski, 2011; Lindsay, 2013; Zetter, 2011; Arthur, 2013</p> <p>Chen & Abu-Nimeh, 2011; Zetter, 2011; Kushner, 2013</p> <p>Chen & Abu-Nimeh, 2011</p>
	<p><i>Supervisory Control and Data Acquisition (SCADA) Systems:</i> Tangible computer systems that operate industrial controls within the electric power infrastructure.</p>	<p>Polityuk et al., 2017; Park et al., 2017; Huang et al., 2018; Detsch, 2016; Smith, 2017; Lee et al., 2016; Harrell, 2017; Osborne, 2018</p>
	<p><i>Siemens Siprotec digital relay:</i> Tangible device used for used for line protection of high and medium voltage electric power networks.</p>	<p>Osborne, 2018; Greenberg, 2017</p>
	<p><i>Remote Terminal Unit:</i> Tangible microprocessor-controlled electronic device that interfaces objects in the physical world to a SCADA system.</p>	<p>Park et al., 2017; Lee et al., 2016; Toecker, 2016; Zetter, 2017; Harrell, 2017</p>
Ukrainian Blackouts	<p><i>Power outage:</i> The absence of electric power resulting in the tangible loss of heat and light.</p>	<p>Osborne, 2018; BBC, 2017; Greenberg, 2017; Polityuk et al., 2017; Park et al., 2017; Sullivan & Kamensky, 2017; Detsch, 2016; Smith, 2018; Adamczyk, 2017; Huang et al., 2018; Zetter, 2017; Lee et al., 2016; Harrell, 2017</p>
	<p><i>IoT Devices (webcams, routers, baby monitors, etc.):</i> Tangible devices that are connected to the Internet.</p>	<p>Kolias et al., 2017; Greenberg, 2017;</p>
	<p><i>Report Server and Command & Control Server:</i> The tangible computer server that contains information about the various devices in the IoT botnet, and the tangible terminal from which commands can be issued to control the IoT botnet.</p>	<p>Kolias et al., 2017; Greenberg, 2017; Moriuchi & Chohan, 2018; Fruhlinger, 2018;</p>
	<p><i>Domain Name Service (DNS) Servers:</i> Tangible computer equipment that translates web addresses such as www.temple.edu into numerical addresses that can be read by machines.</p>	<p>Greenberg, 2017; Moriuchi & Chohan, 2018; Liu, 2017; Periroth, 2016; Trendmicro, 2018; Sanger & Periroth,</p>

		2016; Mansfield-Devine, 2016; Leyden, 2017; Fruhlinger, 2018
<i>Loader:</i> The tangible computer server where IoT devices wait in line to be assimilated into the botnet.		Koliast et al., 2017; Greenberg, 2017; <i>NetLab</i> , 2017
<i>Bot hosting site, cloud servers:</i> Tangible computing tools where bots are stored.		Graham, 2017; Dubbin, 2013
<i>Twitter:</i> Twitter is a website, the tangible computer servers that host the social media content.		Woolley & Shout, 2016; Wojcik, 2018; Graham, 2017; Timberg & Dwoskin, 2018; Guilbeault & Woolley, 2016; Rosenberg, 2017; Spence et al., 2018; Dubbin, 2013; Edwards et al., 2016
Twitterbots	<i>Elections (for example presidential elections, Brexit referendum):</i> The Brexit vote had a tangible impact on the UK/European Union legal and economic relationship. Presidential elections change the direction of government policy and the people involved in the government.	Timberg & Dwoskin, 2018; Baraniuk, 2018; Confessore et al., 2018; Hirsch, 2017; Curran, 2017; Metz, 2018; Woolley & Shout, 2016; Gu et al., 2017; Guilbeault & Woolley, 2016
	<i>Devices:</i> Tangible computing tools such as smartphones, computers, iPads, etc. that people use to interact with Twitter and twitterbots.	Wojcik, 2018; Farrell, 2018; Spence et al., 2018; Woolley & Shout, 2016; Dubbin, 2013; Graham, 2017; Edwards et al., 2014; Baraniuk, 2018; Economist, 2017
	<i>Computers:</i> Tangible devices.	Redmond, 1999; CERT, 1999; Pearce, 2002; Raney, 1999; <i>NYT</i> , Apr 1999; We Live Security, 2016; Strickland, 2008; McNamara, 2014; Mills, 2009; Gostev, 2005; Peterson, 1999; <i>WSJ</i> , 1999; <i>NYT</i> , May 2002; Smothers, 1999
Melissa Virus	<i>Mail servers:</i> Tangible computer servers that manage electronic mail systems.	Redmond, 1999; We Live Security, 2016; McNamara, 2014; Mills, 2009; Raney, 1999; Cheng, 1999
	<i>Pornography websites:</i> Tangible servers that host pornographic content.	Mills, 2009; Taylor et al., 1999; McNamara, 2014; Cluley, 2009
	<i>Telephone:</i> Tangible device used to dial into the Internet.	Mills, 2009; Taylor et al., 1999;
	<i>Payment Processing Systems:</i> Tangible machines and servers to exchange banking details between a point of sale and financial institutions.	Bray, 2013; Bray & Yadron, 2013; Sullivan, 2013; Dol, 2015, 2018
Hack of American Business 2007-2012	<i>Anonymous Web Hosting:</i> Tangible computer servers positioned all over the world.	Armental, 2015; Beekman, 2013; Hudson, 2013; Dol, 2015, 2018; Fox,

	<i>Magnetic Strips on Blank Plastic Cards:</i> Tangible object used to interface with payment processing systems and banking machines.	2013; Reuters, 2013; Jones & Finkle, 2013; Schwartz, 2015
	<i>Automated Teller Machines and Cash:</i> Tangible machine which distributes money in a tangible form – bank notes (cash).	Hudson, 2013; Wood, 2018; DoJ, 2015, 2018
	<i>M.E. Doc's Update Server:</i> The tangible computer server used to push software updates to users over the Internet.	Hudson, 2013; Wood, 2018; DoJ, 2015, 2018; Beekman, 2013
	<i>Desktop Computers and Network Servers:</i> The tangible devices within organizations and homes that were susceptible to the ransomware cyberattack.	Tung, 2017, 2018; Fruhlinger, 2017; Greenberg, 2018; Nott, 2017; Sayer, 2017; Chirgwin, 2018; Cimpanu, 2018; Frenkel et al., 2017; Olenick, 2018
	(Not)Petya Ransomware	Doctorow, 2018; Chirgwin, 2018; Cimpanu, 2018; Collins, 2017; Chopping, 2017; Frenkel et al., 2017; Fruhlinger, 2017; Goldsborough, 2017; Greenberg, 2018; Hackett, 2017; Matthews, 2017; Nelson et al., 2017; Nott, 2017; Olenick, 2018; Osborne, 2018; Palmer, 2017, 2018; Reilly, 2017; Ryan, 2017; Sayer, 2017; Schilling, 2017; Tung, 2017; USCERT, 2017; Woo, 2018
	<i>Security gates at Maersk shipping ports:</i> The tangible physical boundaries that were unable to be operated once the computer systems were corrupted.	Greenberg, 2018; Tung, 2017; <i>Asia News Monitor</i> , 2017; Daneshkhlu et al., 2017; Chopping, 2017; Frenkel et al., 2017; Olenick, 2018
	<i>Maersk Domain Controller located in Ghana:</i> The one tangible computer hard drive that survived the attack and still contained the detailed map and rules for Maersk's global networks.	Doctorow, 2018; Greenberg, 2018
	<i>CD-RW:</i> The tangible object used by Manning to move data from one location to another.	Sangarasivam, 2013; Garnett & Hughes, 2019; Zetter & Poulsen, 2010
	<i>WikiLeaks Website:</i> The tangible servers which host the content shared via WikiLeaks.	Sangarasivam, 2013; Nita, 2014; Berghel, 2012; Jones, 2013; Garnett & Huges, 2019; Somashekhar, 2017; Cadwalladr, 2018; Booth et al., 2010; McGreal, 2010; Tate, 2013; Zetter & Poulsen, 2010; Peralta, 2013; Bumiller, 2010; Thompson, 2010; Chan, 2017; Nicks et al., 2011

	<p><i>Apache Helicopter:</i> The tangible weapon system which fired weapons in Iraq.</p> <p><i>SIPRnet:</i> The tangible computer servers and networks that are used by the U.S. Intelligence community to share and store classified data.</p>	<p>Sangarasivam, 2013; Nita, 2014; Zavis, 2017; Booth et al., 2010; Tate, 2013; Zetter & Poulsen, 2010</p> <p>Berghei, 2012; Zetter & Poulsen, 2010; Booth et al., 2010; Sangarasivam, 2013; Zavis, 2017; Nicks et al., 2011</p>
	<p><i>Ashley Madison Website:</i> The tangible servers which support the Ashley Madison Website.</p>	<p><i>Economist</i>, 2015; Rogers, 2015; Tuttle, 2015; Gauthier, 2017; CNNMoney, 2015; Wright, 2015; Dewey, 2015; ICTMW, 2015; Hackett, 2015; Cox, 2015; Schwartz, 2015; PIPEDA Report, 2016; Basu, 2015; George-Cosh, 2015; Michelsen, 2015; Murdock, 2015; Koller, 2010; Englander, 2015</p>
Ashley Madison	<p><i>Divorce proceedings, job loss, suicides:</i> Tangible events that occurred following the Ashley Madison hack.</p> <p><i>Avid Life Media data servers:</i> Tangible servers that belong to the parent company, Avid Life Media on which the company's core knowledge assets are stored.</p> <p><i>\$19 fee:</i> The tangible fee for service customers paid to remove their data, and any record of their use of the website from the Ashley Madison servers.</p>	<p>George-Cosh, 2015; Rogers, 2015; CNNMoney, 2015</p> <p>Chirgwin, 2016; Ragan, 2015; Cox, 2015; PIPEDA Report, 2016; Basu, 2015; Englander, 2015</p> <p>Gauthier, 2017; Hackett, 2015; Ragan, 2015; Schwartz, 2015</p>

Table F3. Empirical Patterns from Nine Case Studies: Cognitive – Physical Interaction

P3: Cyberattacks will include an element of the cognitive dimension (hacker or human target) interacting with an element of the physical dimension (e.g. a device of some kind, including sensors, computers, telephones, security badges, etc.)		
Case Study	Examples	References
Stuxnet	<p><i>"Iranians were apparently caught off guard and surprised by the degree to which their defences could be penetrated, even against highly protected air-gap systems."</i></p> <p>People from Iran had designed the defense strategy to include (c) a tangible “air gap” between the tangible devices in the Natanz facility and the global Internet. (p)</p> <p><i>"So all it would take was one operator unknowingly plugging an infected memory stick into a control-system computer..."</i></p> <p>A person could make the decision to connect (c) a tangible USB device to the tangible computer systems within the Natanz facility. (p)</p>	<p>Farwell & Rohozinski, 2011</p>
	<p><i>"Whether the "bad guy" was the United States or one of its allies, the attack was causing collateral damage to thousands of systems..."</i></p> <p>People from a nation state, possibly the United States attacked (c) the Natanz uranium enrichment facility but thousands of other machines outside that facility were collateral damage. (p)</p>	<p>Weinberger, 2011</p> <p>Zetter, 2011</p>
Ukrainian Blackouts	<p><i>"United Arab Emirates blocked the transfer of the Siemens computers across the Strait of Hormuz to Bandar Abbas, a major Iranian port."</i></p> <p>People from the UAE stopped other people from delivering (c) tangible computer systems across a tangible body of water (the Strait of Hormuz) to the tangible port of Bandar Abbas in Iran. (p)</p> <p><i>"In December 2015, a first-of-its-kind cyberattack cut the lights to 225,000 people in western Ukraine, with hackers also sabotaging power distribution equipment, complicating attempts to restore power."</i></p> <p>People used their intellect and skills to gain unauthorized access to and sabotage (c) tangible electric power distribution equipment which supplied electricity to western Ukraine, causing a power outage and the tangible loss of heat and light (p) for 225,000 people who experienced discomfort. (c)</p>	<p>Broad et al., 2011</p> <p>Polityuk et al., 2017</p>
	<p><i>"As the attackers utilized the operator HMI's, they operated numerous sites under the control of the dispatcher."</i></p> <p>People with unauthorized access took control from authorized people, and used their access to control (c) tangible electric power distribution equipment with the tangible human-machine-interface equipment. (p)</p> <p><i>"Taking control of the facilities' SCADA systems, malicious actors opened breakers at some 30 distribution substations..."</i></p>	<p>Lee et al., 2016, p. 17</p> <p>Park et al., 2017</p>

	<p>Malicious people used their skills to gain unauthorized access (c) to tangible industrial control systems and electric power breakers (p).</p> <p><i>“The Ukrainian distribution control centers had been completely blinded and were relying on voice radio and cellphones for communication, using pen and paper to manage their local distribution grids.”</i></p> <p>People were managing the distribution of (c) tangible electric power with radios, cellphones, pen and paper because tangible industrial control systems were not functioning. (p)</p>	<p>Toecker, 2016</p>
	<p><i>“...4% of Deutsche Telekom customers – those using specific Speedport models – unable to connect to the Internet...”</i></p> <p>People who were customers of the company Deutsche Telekom were unable to use their (c) tangible Internet-connected Speedport model routers. (p)</p> <p><i>“IoT devices have become the ‘new favorite’ for DDoS hackers because a very large percentage of administrators and users of IoT devices think of them as plug-and-play solutions and, as a result, do not take even the most basic steps to protect these devices from malicious hacking...”</i></p> <p>Malicious people understand that most people do not decide to secure (c) IoT devices. (p)</p>	<p>Mansfield-Devine, 2016</p>
Internet of Things (IoT) Botnet	<p><i>“FBI believes that this attack was ultimately targeting Microsoft game servers.”</i></p> <p>People from the FBI who were investigating the attack concluded that the target was (c) tangible computer game servers. (p)</p> <p><i>“Every organization with a presence on the internet must have a set of authoritative DNS servers...”</i></p> <p>In order to create a virtual presence, people who run organizations must have (c) tangible DNS computer servers.</p>	<p>Vlajic & Zhou, 2018</p>
	<p><i>“...public sentiment on contentious issues including gun control and the 2016 U.S. presidential election.”</i></p> <p>People have strong opinions (c) about the tangible impacts of gun regulations and other government policies (p).</p> <p><i>“...gunman who stormed into Washington, D.C.’s Comet Ping Pong pizzeria...”</i></p> <p>A person decided (c) to carry a tangible gun (p) into a tangible building (p).</p> <p><i>“...social interaction online.”</i></p> <p>People interact with one another using (c) the Internet, a tangible global computer network (p).</p>	<p>Fruhlinger, 2018</p>
Twitterbots	<p><i>“...humans interact with computers similarly to how they would interact with other human beings.”</i></p> <p>People interact with other people (c), and people interact (c) with tangible computer devices (p).</p>	<p>Liu, 2017</p>
Melissa Virus	<p><i>“...he will be prohibited from logging onto a computer network without specific permission from the court.”</i></p>	<p>Baranuk, 2018</p> <p>Farrell, 2018, p. 26</p> <p>Guilbeault & Woolley, 2016</p> <p>Spence et al., 2018, p. 2</p> <p>NYT, 2 May 2002</p>

	<p>People from the court punished [David Smith] by prohibiting him (c) from using tangible computer networks. (p)</p> <p>“...Mr. Smith had caused at least \$80M in disruption, lost commerce, and computer downtime...”</p> <p>David Smith, a person caused organizations to incur (c) tangible financial losses of \$80 million because of the tangible loss of computer connectivity. (p)</p> <p>“Eventually,” says deputy attorney general Christopher Babb, ‘we were able to trace it back to the specific telephone that was being used...’</p> <p>People investigating the cyber disruption were able to identify (c) the specific tangible telephone that connected to the Internet. (p)</p> <p>“Compaq, had to stop Internet connectivity...”</p> <p>The people who worked for Compaq had to make the decision to turn off (c) tangible computer equipment connected to the Internet. (p)</p>	<p>Smothers, 1999</p>
Hack of American Business 2007-2012	<p>“...identified Drinkman and Kalinin as “sophisticated” hackers who specialized in penetrating the computer networks of multinational corporations, financial institutions and payment processors.”</p> <p>Two people, Drinkman & Kalinin who were part of the cybercrime gang were highly skilled at using their knowledge to gain illegal access to (c) tangible computer networks. (p)</p> <p>“...members of the conspiracy scouted potential victims, including visiting retail stores in 2007 and in 2008, to identify their payment-processing systems.”</p> <p>People working with the cybercrime gang conducted surveillance to learn (c) which tangible payment processing systems were functioning at tangible retail locations. (p)</p> <p>“The hackers used anonymous web-hosting services provided by Mikhail Rytikov to hide their identities.”</p> <p>The people who were members of the cybercrime gang worked with a man named Rytikov to hide their identities by using (c) tangible servers hidden all over the world. (p)</p>	<p>Hudson, 2013</p> <p>Bray, 2013</p> <p>Bray & Yadon, 2013</p>
	<p>“Those who have the expertise and the inclination to break into our computer networks threaten our economic well-being, our privacy and our national security.”</p> <p>People feel insecure and threatened by other people with the expertise and motivation to break into (c) tangible computer networks. (p)</p> <p>“M.E.Doc acknowledged that its servers had been affected...”</p> <p>The people from the Ukrainian company M.E. Docs made the decision to acknowledge that they had been compromised (c) and that their tangible update computer servers were affected (p).</p>	<p>Sullivan, 2013; Jones & Finkle, 2013;</p> <p>Fox, 2013; Reuters, 2013</p>
(Not)Petya Ransomware		<p>Frenkel et al., 2017</p>

	<p><i>"At Copenhagen-based shipping giant A.P. Moller-Maersk, computer outages at the company's APM Terminals in several locations meant cargo loading and unloading had to be tracked manually..."</i></p> <p>In order for people who worked at Maersk to make decisions related to the loading and unloading (c) of tangible cargo from ships using pens, paper, and clipboards. (p)</p>	Ryan, 2017	
	<p><i>"One staffer from the Ghana office flew to Nigeria to meet another Maersk employee in the airport to hand off the very precious hard drive."</i></p> <p>People from Maersk's leadership made the decision to have two people, one from Ghana and another from Nigeria, hand-carry (c) the tangible hard drive that functioned as the domain controller for Maersk's entire global operation. (p)</p> <p><i>"By all accounts, this is a monumental effort from Maersk's IT staff, equivalent to installing a new infrastructure from the ground up."</i></p> <p>People who worked for Maersk on the IT team used their skills, knowledge, and resourcefulness to rebuild (c) the entire tangible computer infrastructure. (p)</p>	Greenberg, 2018; Doctorow, 2018	
	<p><i>"Assange actually might be the useful idiot for foreign intelligence services: WikiLeaks might be an instrument of information warfare rather than the purveyor of blown whistles."</i></p> <p>Wikileaks is a website hosted on tangible servers that has become a useful location (p) that the people of nation states can use to manipulate what people think. (c)</p>	Berghel, 2012	
	<p><i>"Manning had access to two classified networks from two separate secured laptops: SIPRNET, the Secret-level network used by the Department of Defense and the State Department, and the Joint Worldwide Intelligence Communications System..."</i></p> <p>People from the U.S. Government made the decision to provide Manning with access (c) to two tangible classified computer networks that were only accessible (p) to people who had been determined to be good decision makers worthy of the public trust. (c)</p>	Zetter & Poulsen, 2010	
Wikileaks & the Manning Disclosure		<p><i>"...the only safe place I seem to have (c) is this satellite internet connection."</i></p> <p>In this person's – Manning's – own words, the only time she experienced a sense of safety was when communicating with other people (c) via the tangible equipment comprising the satellite connection to the Internet.</p> <p><i>"...in the internet chat-rooms in cyberspace where Pvt. Manning disclosed his intentions and actions to Adrian Lamo (who consequently reported him to the FBI)."</i></p> <p>Two people, Private Manning and Adrian Lamo had conversations (c) using Internet "chat-rooms" hosted on tangible computer servers (p), during which Manning talked about her intentions and the decisions she'd been making with</p>	Cadwalladr, 2018 Sangarasivam, 2013

	Lamo, who then made the decision to notify the FBI about Manning's behavior. (c)	
	" <i>Ashley Madison is a website that arranges extramarital liaisons.</i> " The tangible servers that comprise the Ashley Madison website are a location (p) where users can go when they make the decision to engage in an extramarital affair. (c)	<i>Economist</i> , 2015
	" <i>We have hacked them completely, taking over their entire office and production domains and thousands of systems ...</i> " The people responsible for the hack spoke to a reporter, declaring that with their knowledge and skills, they had taken control of (c) the tangible equipment comprising the Website infrastructure. (p)	Ragan, 2015
	" <i>When the employees opened their laptops...</i> " People who worked for AvidLife Media began to use (c) the tangible computers. (p)	Rogers, 2015
	" <i>ALM took immediate steps to attempt to terminate the attacker's access to its systems.</i> " The people who worked for Avid Life Media made the decision to take specific actions to block the hackers' unauthorized access (c) to their tangible computer systems. (p)	<i>PIPEDA Report</i> , 2016

Table F4. Empirical Patterns from Nine Case Studies: Informational Dimension

P4: Cyberattacks will include an informational dimension.		
Case Study	Examples	References
Stuxnet	<p><i>Stuxnet malware:</i> Set of malicious information rules tailored to communicate with Industrial Control Systems.</p> <p><i>Digital certificates from Realtek Semiconductor and JMicron Technology:</i> Information that indicated software comes from a trustworthy source.</p> <p><i>Siemens WinCC/Step7 software:</i> Set of information rules used to program Siemens Simatic Programmable Logic Controllers.</p> <p><i>Expiration date, 24 June 2012:</i> Information within the Stuxnet malware indicating when the software should stop functioning.</p> <p><i>Email & Email attachments:</i> Information delivered in electronic mail form with attached Microsoft Word or Microsoft Excel documents.</p>	Lindsay, 2013; Nakashima & Warrick, 2012; Shapiro, 2016; Sanger, 2012; Rosenbaum, 2012; Paganini, 2016; Rogers, 2015; Broad et al., 2011; Arthur, 2013; Zetter, 2011, 2014; Kushner, 2013; Chen & Abu-Nimeh, 2011; Gjelten, 2010; Farwell & Rohozinski, 2011 Gjelten, 2010; Weinberger, 2011; Zetter, 2011 Chen & Abu-Nimeh, 2011; Zetter, 2011; Kushner, 2013
Ukrainian Blackouts	<p><i>Malware (BlackEnergy3, KillDisk & Crash Override):</i> Information rules of that subvert the proper system information rules allowing unauthorized access and actions.</p> <p><i>Credentials:</i> Information that grants specific kinds of access.</p> <p><i>Protocols:</i> Information rules within the SCADA systems that direct the operation of the industrial control systems.</p> <p><i>Mirai & Reaper Malware:</i> Information rules that orchestrate a botnet.</p>	BBC, 2017; Greenberg, 2017; Polityuk et al., 2017; Park et al., 2017; Detsch, 2016; Smith, 2018; Zetter, 2017; Lee et al., 2016; Harrell, 2017 Greenberg, 2017; Park et al., 2017; Toecker, 2016; Detsch, 2016; Smith, 2018; Zetter, 2017; Lee et al., 2016; Harrell, 2017 BBC, 2017; Greenberg, 2017; Polityuk et al., 2017; Park et al., 2017; Huang et al., 2018; Sullivan & Kamensky, 2017; Toecker, 2016; Smith, 2018; Smith, 2017; Zetter, 2017; Lee et al., 2016; Harrell, 2017; Osborne, 2018 Park et al., 2017; Toecker, 2017; Zetter, 2017; Lee et al., 2016; Harrell, 2017 Park et al., 2017; Osborne, 2018; Greenberg, 2017 Mansfield-Devine, 2016; Vlajic & Zhou, 2018; Trendmicro, 2017, 2018; Greenberg, 2017; Leyden, 2017; Moriuchi & Chohan, 2018; NetLab,
Internet of Things (IoT) Botnet		

		2017; Fruhlinger, 2018; Liu, 2017; Perlroth, 2016; Koliass et al., 2017
<i>Internet traffic:</i> Information sent through networks in the form of data packets.		Vlajic & Zhou, 2018; <i>Trendmicro</i> , 2017; Greenberg, 2017; Moriuchi & Chohan, 2018; Fruhlinger, 2018; Liu, 2017; Perlroth, 2016; Sanger & Perlroth, 2016; Koliass et al., 2017
<i>Firmware:</i> Information rules for the operating system that controls an IoT device.		Koliass et al., 2017; Leyden, 2017; Fruhlinger, 2018; <i>Trendmicro</i> , 2017
<i>Username/password combinations:</i> Information used to connect to an IoT device.		Koliass et al., 2017; Greenberg, 2017; Moriuchi & Chohan, 2018; <i>NetLab</i> , 2017; Fruhlinger, 2018; Sanger & Perlroth, 2016
<i>Tweets:</i> Information statements of 140 characters or less posted or shared through Twitter.		Woolley & Shout, 2016; Wojcik, 2018; Timberg & Dwoskin, 2018; Gu et al., 2017; Guilbeault & Woolley, 2016; Baraniuk, 2018; Hirsch, 2017; Confessore et al., 2018; Edwards et al., 2016
<i>Propaganda & disinformation:</i> Information that is not objective, and is sometimes false, which is used to influence an audience.		Woolley & Shout, 2016; Guilbeault & Woolley, 2016; Baraniuk, 2018; Hirsch, 2017; <i>Economist</i> , 2017; Timberg & Dwoskin, 2018; Curran, 2017; Gu et al., 2017
Twitterbots		Woolley & Shout, 2016; Wojcik, 2018; Graham, 2017; Timberg & Dwoskin, 2018; Edwards et al., 2014; Gu et al., 2017; Guilbeault & Woolley, 2016; Baraniuk, 2018; Farrell, 2018; Hirsch, 2017; Spence et al., 2018; Confessore et al., 2018; Dubbin, 2013; Edwards et al., 2016; Krishna, 2014; Metz, 2018
<i>Algorithms:</i> Information rules or computer programs to be followed by a computer, used to automate Twitterbot accounts.		Timberg & Dwoskin, 2018; Farrell, 2018; Edwards et al., 2016; Metz, 2018; Woolley & Shout, 2016; Dubbin, 2013; Baraniuk, 2018
<i>Melissa Computer Virus:</i> Information rules contained in macros within a Word document.	Melissa Virus	Taylor et al., 1999; Redmond, 1999; CERT, 1999; Cheng, 1999; Pearce, 2002; Raney, 1999; <i>NYT</i> , Apr 1999;

	<i>Virus detector/Antivirus software:</i> Information rules in the form of software that detects malicious information rules.	Strickland, 2008; Peterson, 1999; <i>WSJ</i> , 1999; Smothers, 1999
	<i>Word document with a list of passwords to pornography websites:</i> Information in the form of passwords.	Taylor et al., 1999; Redmond, 1999; Raney, 1999; <i>Techspirited</i> , 2019; Gostev, 2005
	<i>Visual Basic Macros:</i> Programming language used to define information rules.	McNamara, 2014; Cluley, 2009; Mills, 2009; <i>Techspirited</i> , 2019; Taylor et al., 1999
	<i>Credit Card Numbers:</i> Information that ties to financial accounts.	Redmond, 1999; <i>We Live Security</i> , 2016; CERT, 1999; Strickland, 2008; <i>Panda Security</i> , 2013; McNamara, 2014; Cluley, 2009; Mills, 2009; Gostev, 2005
	<i>Google Alerts:</i> Information triggers using words like “data breach,” “credit card fraud,” or “hackers” were set up to query emerging news stories.	Hudson, 2013; Bray, 2013; Bray & Yadron, 2013; Fox, 2013; Reuters, 2013; Sullivan, 2013; Jones & Finkle, 2013; Wood, 2018; Schwartz, 2015; DoJ, 2015, 2018; Armental, 2015; Beekman, 2013
Hack of American Business 2007-2012	<i>Chat Transcripts:</i> The information record of conversations that took place between the members of the cybercrime gang over instant message applications.	Sullivan, 2013; Beekman, 2013; Hudson, 2013; Bray, 2013; Bray & Yadron, 2013
	<i>Structured Query Language & SQL Injection:</i> Information in the form of a programming language designed to manage data held in specific kinds of databases. SQL injection is bad information that gets input into the databases.	Fox, 2013; Sullivan, 2013; DoJ, 2015, 2018
	<i>M.E. Docs software:</i> Information rules in the form of tax and accounting software used by Ukrainian businesses.	DoJ, 2015, 2018; Sullivan, 2013; Wood, 2018; Schwartz, 2015
	<i>Ransomware (Petya, NotPetya, WannaCry):</i> (Not)Petya Ransomware	Tung, 2017, 2018; Fruhlinger, 2017; Greenberg, 2018; Nott, 2017; Sayer, 2017; Chirgwin, 2018; Cimpanu, 2018; Frenkel et al., 2017; Olenick, 2018
		Doctorow, 2018; Chirgwin, 2018; Cimpanu, 2018; Collins, 2017; Chopping, 2017; Frenkel et al., 2017; Goldsborough, 2017; Fruhlinger, 2017; Hackett, 2017; Greenberg, 2018; Matthews, 2017; Nelson et al., 2017; Nott, 2017; Olenick, 2018; Osborne,

		2018; Palmer, 2017, 2018; Reilly, 2017; Ryan, 2017; Sayer, 2017; Schilling, 2017; Tung, 2017; USCERT, 2017; Woo, 2018
	<i>EternalBlue & EternalRomance Exploits:</i> Vulnerabilities within the information rules of the Microsoft Windows Operating System.	Tung, 2018; USCERT, 2017; Fruhlinger, 2017; Greenberg, 2018; Hackett, 2017; Osborne, 2018; Palmer, 2017, 2018
	<i>Network credentials:</i> Information that is shared between different parts of a network to grant one machine access to another.	Fruhlinger, 2017; Schilling, 2017; Greenberg, 2018
	<i>"Collateral Murder" Video:</i> Information stored in the form of full motion video of an airstrike that took place in Iraq.	Sangarasivam, 2013; Nita, 2014; Berghel, 2012; Somashekhar, 2017; Cadwalladr, 2018; Zavis, 2017; Booth et al., 2010; McGreal, 2010; Tate, 2013; Zetter & Poulsen, 2010
	<i>Diplomatic cables:</i> Information in the form of messages related to the diplomatic mission of the U.S. Department of State.	Sangarasivam, 2013; Berghel, 2012; Garnett & Hughes, 2019; Somashekhar, 2017; Cadwalladr, 2018; Zavis, 2017; Booth et al., 2010; McGreal, 2010; Tate, 2013; Zetter & Poulsen, 2010
	<i>Chat Logs:</i> The information record of the conversations between Private Manning and Adrian Lamo.	Nita, 2014; Cadwalladr, 2018; Zetter & Poulsen, 2010
	<i>Afghan and Iraq War Logs:</i> Large collections of information in many formats, including full motion video, documents, diplomatic cables, and other data related to the missions in Afghanistan and Iraq that were shared as content on WikiLeaks.	Berghel, 2012; Garnett & Hughes, 2019; Somashekhar, 2017; Cadwalladr, 2018; Zavis, 2017; Booth et al., 2010; Tate, 2013; Nicks et al., 2011
	<i>Subscriber information:</i> Information about users, such as name, sexual preference, sexual fantasies, physical descriptions, etc.	<i>Economist</i> , 2015; Rogers, 2015; Tuttle, 2015; Gauthier, 2017; CNNMoney, 2015; Wright, 2015; Dewey, 2015; <i>ICTMW</i> , 2015; Hackett, 2015; Cox, 2015; Schwartz, 2015; <i>PIPEDA Report</i> , 2016; Basu, 2015; George-Cosh, 2015; Michelsen, 2015; Koller, 2106; Englander, 2015; <i>Panda</i> , 2017; Solomon, 2017; Ragan, 2015
	<i>Pictures & Conversations:</i>	Dewey, 2015; <i>ICTMW</i> , 2015; Cox, 2015; CNNMoney, 2015; Wright, 2015

Wikileaks & the Manning Disclosure

Ashley Madison

	<p>Information in the form of email exchanges between clientele, photographs of people in various states of dress, and other private exchanges of information.</p> <p><i>Credit card data:</i> Information related to financial accounts of users.</p>	Rogers, 2015; Tuttle, 2015; Gauthier, 2017; George-Cosh, 2015; Dewey, 2015; Murdock, 2015; <i>ICTMW</i> , 2015; Hackett, 2015; <i>Panda</i> , 2017; Ragan, 2015; Cox, 2015; Schwartz, 2015; Englander, 2015
	<p><i>Fembots:</i> Information rules attached to fake Ashley Madison female accounts that generated sexy, enticing digital interactions with male clients.</p>	Dewey, 2015; Tuttle, 2015

Table F5. Empirical Patterns from Nine Case Studies: Cognitive – Informational Interaction

P5: Cyberattacks will include an element of the cognitive dimension (hacker, organization, human target, etc.) interacting with an element of the informational dimension (data, software, knowledge, etc.).		
Case Study	Examples	References
Stuxnet	<p>“The US government has never officially acknowledged that Stuxnet was created and launched by the NSA, allegedly with help from Israeli government hackers...”</p> <p>People from the NSA (the U.S.) have never publicly acknowledged working with people from Israel to create and launch (c) the set of information rules comprising the Stuxnet malware. (i)</p> <p>“But another Stuxnet driver was found using a second certificate, this one stolen from Micron Technology, a circuit maker in Taiwan that was — coincidentally or not — headquartered in the same business park as RealTek.”</p> <p>Malicious people made the decision to steal (c) information in the form of validation certificates indicating software was legitimate (i) from two Taiwanese technology companies (groups of people). (c)</p> <p>“Stuxnet injects its own code...in a manner undetectable by the PC operator.”</p> <p>Operations personnel did not observe (c) the information rules from Stuxnet propagating themselves. (i)</p> <p>“...when it [Stuxnet] attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally.”</p> <p>Operations personnel made decisions based on receiving (c) information indicating that everything was within normal parameters (i).</p> <p>“Phishing emails with infected attachments were sent to the companies’ offices. When the attachments were opened, macros enabled hackers to gain remote access.”</p> <p>People made the decision to open (c) information that arrived in the form of an electronic mail attachment with information rules in the form of macros (i) created by people to gain unauthorized access. (c)</p>	<p>Franceschi-Bicchieri, 2017</p> <p>Weinberger, 2011</p> <p>Chen & Abu-Nimeh, 2011</p> <p>Sanger, 2012</p> <p>Park et al., 2017</p>
	<p>“In the first stage, the adversaries ‘weaponized’ Microsoft Office documents (Excel and Word) by embedding malware called BlackEnergy 3.”</p> <p>People created (c) information documents that contained damaging information rules in the form of malware called BlackEnergy3 (i).</p>	Harrell, 2017
	<p>“Four elements of the payload targeted particular communication protocols specified in the standards IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OLE for Process Control Data Access (OPC DA).”</p> <p>People learned about and targeted (c) specific information communication protocols defined in written information standards with four specific information rules called the “payload” (i).</p>	Osborne, 2018
Ukrainian Blackouts		

	<p>“30 percent of the macro code is dedicated to making analysis of the code difficult, and 69 percent is focused on features designed to obfuscate the maliciousness of the code.”</p> <p>People deliberately crafted confusing and misleading (c) information rules (i).</p> <p>“...custom-made botnets, but also to botnets-for-hire...”</p> <p>Entrepreneurial people will use their knowledge and skills to market their services to operate or create customized (c) information rules in the form of botnet software, such as Mirai or Reaper malware. (i)</p>	Zetter, 2017
	<p>“Mirai, whose source code was leaked last September ...”</p> <p>“‘Anna-Senpai’ posted the code of the Mirai botnet”</p> <p>A person made the decision to share (c) the information rules comprising the Mirai malware. (i)</p>	Vlajic & Zhou, 2018
Internet of Things (IoT) Botnet	<p>“...Reaper is likely intended for use as a booter/stresser service primarily serving the ‘intra-China DDoS-for-hire market.’”</p> <p>People with knowledge and skills are probably marketing their services in China to build and operate (c) botnet information rules such as the Reaper malware. (i)</p> <p>“If the attacker has a bigger fire hose of data than the defender has,’ he [Bruce Schneier, internet security expert] wrote, ‘the attacker wins.’”</p> <p>In a Distributed Denial of Service attack (i), both the people attacking and the people defending “shoot” (c) streams of information in the form of data packets. (i)</p>	Leyden, 2017
	<p>“...politicians, government agencies, and advocacy groups have used bots to engage voters and spread messages.”</p> <p>Individuals and groups of people interact with other people by sending (c) information with Twitterbots (i).</p> <p>“...you set up the pattern for phrases that your bot will respond to.”</p> <p>A person creates (c) data triggers for the Twitterbot (i).</p>	Woolley & Shout, 2016
Twitterbots	<p>“Andriy Gazin, who works for a Ukrainian non-governmental organization Texty, has identified more than 20,000 Russian bot accounts systematically pumping out pro-Kremlin propaganda.”</p> <p>A person identified (c) Twitterbots automatically spreading propaganda (i).</p> <p>“...people report similar levels of information seeking, cognitive elaboration, affective learning, and motivation behaviors when receiving information from a Twitterbot when compared to a human agent.”</p> <p>People learn, form associations with their existing understanding based on, and are motivated to seek (c) information from Twitterbots (i).</p> <p>“...whether perpetrator of the virus meant to cause harm.”</p> <p>People wondered whether David Smith meant to cause harm when he created (c) the information rules that comprised the Melissa virus. (i)</p> <p>“...his goal had simply been to circulate ‘a harmless, joke message.’”</p>	Hirsch, 2017
Melissa Virus		Edwards et al., 2016, p. 669
		WSJ, 1999
		Smothers, 1999

	<p>David Smith created what he believed to be (c) harmless information rules in an electronic mail attachment (i) intended as a prank. (c)</p> <p><i>"In Stockholm, computer-science grad Fredrik Björck suggested that Melissa's code bore a strong resemblance to the work of a virus writer called VicodinES."</i></p> <p>A person, Fredrik Björck, examined (c) the information rules in the Melissa virus (i) and he thought he recognized the work of a person calling himself VicodinES (c).</p>	Taylor et al., 1999
	<p><i>"The Melissa virus lures people to open the document by including the text "Here's the important document you asked for... don't show it to anyone else, -."</i></p> <p>People decided to open (c) the document attached to an email because of information in the subject line. (i)</p>	Redmond, 1999
	<p><i>"Drinkman and Smiljanets not only stole over 160 million credit card numbers from credit card processors, banks, retailers, and other corporate victims, they also used their bounty to fuel a robust underground market for hacked information..."</i></p> <p>Two people from the cybercrime gang, Drinkman and Smiljanets used their knowledge and skills to steal and sell (c) information in the form of over 160 million credit card numbers, (i), and their decisions and actions contribute to the growth of other people making the decisions to participate in the illegal purchase and sale of (c) information. (i)</p>	DoJ, 2018
Hack of American Business 2007-2012	<p><i>"In an instant message chat, Gonzalez advised Kalinin to set up Google alerts for phrases such as 'data breach' and 'hackers' in order to keep track of the news."</i></p> <p>Two people who were members of the cybercrime gang shared information with one another using (c) an information sharing application which preserved a record of (i) one person advising the other to stay informed of other people discovering his actions by setting up (c) an information query with key words that might appear in news stories. (i)</p>	Beekman, 2013
	<p><i>"Dmitry Smiljanets, 32, of Russia would then sell the information..."</i></p> <p>Dmitry Smiljanets, a person would make the decisions related to selling (c) the information, specifically the credit card numbers and account information. (i)</p> <p><i>"When the hackers first gained access in August 2007, they talked about how overwhelming the data haul was."</i></p> <p>The people who were using their knowledge and skills to commit theft experienced the sense of being overwhelmed by (c) the enormity of the amount of information. (i)</p>	Armental, 2015
(Not)Petya Ransomware	<p><i>"an attack designed by and for a state (Ukraine was the target: the malware was put in a malicious update to MeDoc, the country's most popular accounting software.)"</i></p>	Chirgwin, 2018

	<p>People from Ukraine have concluded that the attack was part of hybrid warfare, and that people from Russia corrupted (c) the information rules for the M.E. Does software with the information rules that comprise the NotPetya malware. (i)</p> <p><i>"NotPetya ransomware – released by hackers in April – attacks a vulnerability of the Windows Server Message Block that is believed to have been first developed and exploited by the National Security Agency."</i></p> <p>People from the NSA developed an exploit that took advantage (c) of a vulnerability in the information rules contained in part of the Microsoft Windows Operating System, (i) which people from the nation state launching the attack then integrated into (c) the information rules for the NotPetya malware. (i)</p>	Nelson et al., 2017
	<p><i>"Still, despite the fact that that the widely publicized WannaCry outbreak, which occurred just weeks before NotPetya hit and exploited the same hole, brought widespread attention to the MS17-010's importance"</i></p> <p>People in organizations who were responsible for cybersecurity demonstrated knowledge seeking behaviors and went looking for (c) the information rules that could patch the vulnerability in the Microsoft Windows Operating System – the MS17-010 software patch, because of the WannaCry malicious information rules. (i)</p>	Fruhlinger, 2017
	<p><i>"The ransomware ruse was simply a way for those behind the attack to 'control the media narrative' according to Comae, 'to attract the attention on some mysterious hacker group rather than a national/state attacker.'</i></p> <p>The information rules that comprised the NotPetya malware did not function like the information rules for ransomware, (i) but instead were a ruse by the people who launched the attack in order to divert the attention of victims from hybrid warfare and change (c) the information within the global media narrative. (i)</p>	Nott, 2017
Wikileaks & the Manning Disclosure	<p><i>"Private Bradley Manning, who had a top-secret security clearance, has been held in military custody in Kuwait since his arrest in Iraq in May over the video, which caused great embarrassment to the US military establishment."</i></p> <p>The people of the U.S. military law enforcement community decided to arrest Private Manning because he had made the decision to release (c) the classified information contained in the Collateral Murder full motion video (i) which made the people of the U.S. Government feel embarrassed. (c)</p> <p><i>"...delusions of grandeur — may have led him to disclose the largest trove of government secrets since the Pentagon Papers."</i></p> <p>Manning imagined that other people would view her as honorable and heroic which led her to make the decision to disclose (c) information in the form of highly classified national secrets. (i)</p> <p><i>"He read a statement from Manning in which she reiterated his reasons for leaking classified material, saying he had "started to question the morality" of U.S. policy."</i></p>	McGreal, 2010 Thompson, 2010 Thompson, 2010 Tate, 2013

	Manning's attorney (a person) explained Manning's reasoning to the public by reading (c) information in the form of a written statement that described (i) why Manning made the choice to leak (c) information in the form of national secrets. (i) <i>"The reaction to the video gave me immense hope..."</i> Information recorded in the chat logs captured (i) Manning telling Adrian Lamo about her emotional state, and feeling hopeful about people's reactions to (c) the information released in the full motion video "Collateral Murder."	Booth et al., 2010
	 (i) <i>"The algorithm the company used to do so [store user passwords], bcrypt, was one of the strongest methods available..."</i> The people who worked for Avid Life Media made the decision to use secure storage methods (c) specifically information rules in the form of an algorithm called "bcrypt" to transform user passwords into hashmarks. (i) <i>"11 million Ashley Madison passwords were uncovered by a password-cracking squad known as CynoSure Prime, after they discovered half of customers' login information was not properly secured."</i> A group of people with specialized computer skills – Cynosure Prime – experimented with (c) the Ashley Madison data, specifically the username/password information. (i)	Tuttle, 2015
Ashley Madison	 (i) <i>"We will release all customer records, profiles with all the customers' secret sexual fantasies, nude pictures, and conversations and matching credit card transactions, real names, addresses, and employee documents and emails."</i> The hackers – people responsible – stated that they planned to release (c) the information included in the customer records, such as fantasies, emails, names, address, photographs, and email communications. (i) <i>"ALM confirmed that the 'trusted security award' trust-mark on their home page was simply their own fabrication rather than a validated designation by any third party,' it notes."</i> People made the decision to trust the people of Avid Life Media with (c) their personal information because of a fake "trusted security award" seal (i) that was fabricated by Avid Life Media to fool users. (c)	CNN Money Staff, 2015 ICT Monitor Worldwide, 2015 Chirgwin, 2016

Table F6. Empirical Patterns from Nine Case Studies: Informational – Physical Interaction

P6: Cyberattacks will include an element of the informational dimensions (e.g. malware or data) interacting with an element of the physical dimension (e.g. computer, network, sensor, etc.).			
Case Study	Examples	References	
Stuxnet	<p>“First Stuxnet hunted down frequency-converter drives made by Fararo Paya in Iran and Vacon in Finland.”</p> <p>The information rules in the Stuxnet malware looked for (i) specific tangible devices – frequency-converter drives. (p)</p> <p>“A powerful new computer worm apparently is capable of causing power plants or pipelines to blow up.”</p> <p>A set of information rules – a computer worm – can send instructions to (i) tangible devices such as power plants or pipelines. (p)</p>	Farwell & Rohozinski, 2011 Gjelten, 2010	
	<p>“Once Stuxnet infects a SIMATIC machine, it verifies the presence of a particular type of programmable logic controller (PLC) connected to a particular type of frequency converter running at 807–1,210 Hz.”</p> <p>The information rules in the Stuxnet malware infect (i) specific tangible devices called programmable logic controllers which connect to the frequency converters that make the tangible centrifuge spin. (p)</p> <p>“Stuxnet seized the controls of the machine running the centrifuges and in a delicate, invisible operation, desynchronized the speeds at which the centrifuges spun, causing nearly a thousand of them to seize up, crash and otherwise self-destruct.”</p> <p>The information rules in the Stuxnet malware sent instructions to (i) the tangible centrifuges, which spun at incorrect speeds, causing them to break. (p)</p> <p>“...it [Crash Override] automatically maps out control systems and locates target equipment.”</p> <p>Information rules in Crash Override malware created maps (i) of tangible industrial control systems and specific tangible equipment. (p)</p> <p>“Malware also wiped out essential system files, causing computers to crash.”</p> <p>Information rules in malware deleted information files causing failure (i) of tangible computer systems.</p>	Lindsay, 2013 Rosembaum, 2012 Greenberg, 2017	
Ukrainian Blackouts	<p>“I percent of the macro performs the actual function of delivering the remote access code to a victim’s system.”</p> <p>Only a fraction of the information rules in the form of a macro created the “backdoor” information code (i) within the tangible computer hardware. (p)</p> <p>“Commands were then sent to the circuit breakers and protection relays which only opened circuit breaker switches...”</p> <p>Information triggers in the form of commands operated (i) tangible grid equipment such as circuit breaker switches and protection relays. (p)</p>	Zetter, 2017 Osborne, 2018	

	<i>IoT Botnet:</i> Tangible devices connected to the Internet that are connected to one another (p) through a set of information rules. (i)	Greenberg, 2017; Mansfield-Devine, 2016; Vlajic & Zhou, 2018; <i>Trendmicro</i> , 2017, 2018; Leyden, 2017; Moriuchi & Chohan, 2018; <i>NetLab</i> , 2017; Fruhlinger, 2018; Liu, 2017; Koliass et al., 2017 Vlajic & Zhou, 2018
Internet of Things (IoT) Botnet	<p>“<i>Shodan and Censys perform periodic, distributed, and horizontal scans of devices in the Internet (that is, scans of IPv4 address space).</i>”</p> <p>Tangible servers supporting the Shodan and Censys websites connect to the tangible devices connected to the Internet (p) communicating via a set of information rules and recording specific information – IPv4 addresses. (i)</p> <p>“<i>The report server maintains a database with details about all devices in the botnet.</i>”</p> <p>The tangible IoT devices and a computer server (p) connect via a set of information rules (the botnet) and share specific details which are stored in an information database (i).</p> <p>“<i>...millions of devices are ‘queued’ in the hackers’ code, waiting for a piece of automatic ‘loader’ software to add them to the botnet.</i>”</p> <p>A tangible computer server (the loader) connects to IoT devices (p) via a set of information rules and downloads the botnet malware. (i)</p>	Greenberg, 2017 Greenberg, 2017
Twitterbots	<p>“<i>...nearly half of the Tweets, some 500,000 messages, were generated by just 1 per cent of the 300,000 sampled accounts, clearly suggesting these were automated. In the last 48 hours before the referendum, these comments leaned heavily in favor of Leave...</i>”</p> <p>500,000 information messages generated by automated accounts (i) in the 2 days prior to a tangible event – the Brexit referendum (p).</p> <p>“<i>An important aspect of Twitter’s interface is that it does not require a human agent to transmit information. In recent years, automated programs that act in place of human agents are increasingly used on Twitter.</i>”</p> <p>The tangible servers of the Twitter website (p) interface with the Twitterbot algorithms (information rules) (i).</p> <p>“<i>...bot hosting site ‘Cheap Bots Done Quick (http://cheapbotsdonequick.com/)’</i>”</p> <p>Twitterbot information rules (i) are stored on the tangible computer servers of the bot hosting website (p).</p>	Hirsch, 2017 Edwards et al., 2014, p. 372 Graham, 2017 Dubbin, 2013
Melissa Virus	“ <i>...the virus made its way through 1.2 million computers...</i> ”	Smothers, 1999

	<p>Information rules comprising the Melissa virus propagated itself (i) through 1.2 million tangible computer systems. (p)</p> <p><i>“...the virus backed up and at times incapacitated computer networks...”</i></p> <p>Information rules comprising the Melissa virus transmitted so much information (i) that tangible computer networks broke down. (p)</p> <p><i>“Any mail handling system could experience performance problems or a denial of service as a result of the propagation of this macro virus.”</i></p> <p>Tangible computer servers comprising the electronic mail system could stop functioning (p) due to the self-propagating information rules comprising Melissa. (i)</p> <p><i>“...one infected computer had the potential to infect 50 additional computers for each address list in every address book it found.”</i></p> <p>The information rules in Melissa accessed the information in the electronic mail address book and mailed itself to the first 50 email addresses, traveling (i) from one tangible computer to at least 50 more tangible computers.</p> <p><i>“...\$50 for European cards, which are more expensive because they have computer chips...”</i></p> <p>European credit card numbers (i) had a tangible value of \$50 because they included a tangible computer chip (p)</p>	<p>NYT, Apr 1999</p> <p>CERT, 1999</p> <p>We Live Security, 2016</p> <p>Reuters, 2013</p>
	<p>Hack of American Business 2007-2012</p>	
	<p><i>“One [way] ransomware enters an IT environment] entails...navigating the inner workings of a network to obtain administrator credentials to databases and datastores.”</i></p> <p>The information rules within a ransomware seek out the information contained in network credentials or use a “backdoor” contained within existing information rules to gain access to and transit (i) the tangible networks, computer servers, and desktop/laptop computers within the infrastructure. (p)</p> <p><i>“if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable.”</i></p> <p>The information rules contained in the Petya/NotPetya malware gain the information credentials to enter and encrypt the master boot record (i) of the tangible computer corrupting the device so it cannot operate. (p)</p> <p><i>“...[a key piece of data was wiped out on seven mirrored servers and only survived on a system in Ghana due to a freak blackout that shut down the data-center so that the system was knocked offline before it could be infected.]”</i></p> <p>The tangible data center in Ghana was shut down by the tangible loss of power, so it was not connected to the tangible Maersk networks, which protected it from (p) being corrupted by the information rules of the NotPetya malware and</p>	<p>Schilling, 2017, p. 7</p> <p>USCERT, 2017, 2018</p> <p>Doctorow, 2018</p>

	<p>preserved the critical data and information rules (i) the tangible computer server contained. (p)</p> <p><i>“The attack, which security experts dubbed Petya and appeared to stem in part from an obscure Ukrainian tax software product, exposed fresh weakness in the computer systems that run modern-day societies as the virus rapidly spread unimpeded across Ukraine, Russia, Europe and the U.S.”</i></p> <p>The information rules comprising Petya malware, commingled with the information rules of the M.E. Docs tax and accounting software, highlighted (i) tangible weaknesses in computer systems supporting modern societies. (p)</p>	Chopping, 2017
	<p><i>“The Swedish server in turn redirected traffic to a French host, which assigned an IP address that was part of a 16-address server cluster located in France but registered in Melbourne, Australia.”</i></p> <p>The tangible computer server in Sweden communicated with the tangible computer server cluster in France sending (p) information in the form of data traffic to 16 IP addresses. (i)</p>	Berghel, 2012
Wikileaks & the Manning Disclosure	<p><i>“The video showed a deadly 2007 U.S. helicopter air strike in Baghdad...”</i></p> <p>The tangible Apache helicopter was equipped with a video camera to record tangible missions, such as an airstrike in Iraq (p) in the form of full motion video information. (i)</p> <p><i>“...the classified spaces and places of intelligence information and diplomatic cables...”</i></p> <p>Information in the form of national secrets “intelligence” and messages between the U.S. Government and other Nation State governments (i) resides within tangible servers and computer networks. (p)</p> <p><i>“...a single classified diplomatic cable has appeared on the site:...”</i></p> <p>The tangible servers of the WikiLeaks website contained (p) content information in the form of a diplomatic communication. (i)</p>	Zetter & Poulsen, 2010 Sangarasivam, 2013
Ashley Madison	<p><i>“One of the leaked documents is an infrastructure overview of ALM, including a technical map of the network, and a detailed breakdown of the apps and services used on the company’s front- rail and back-rail servers.”</i></p> <p>Information was contained in a document that captured details about the applications and information services mapped to (i) the tangible computer server infrastructure. (p)</p> <p><i>“...detection and monitoring systems, but those were focused on detecting performance issues.”</i></p> <p>Information rules were designed to detect and monitor (i) the tangible operations within the servers and networks. (p)</p> <p><i>“...Ashley Madison is its most visited website, hosting approximately 36 million user profiles...”</i></p>	Ragan, 2015 Koller, 2016 PIPEDA Report, 2016

	The tangible servers of the Ashley Madison website host (p) the information contained in approximately 36 million account profiles. (i) “... <i>threatening message</i> ” on their computer screens...” Information in the form of a threatening message (i) appeared on the tangible computer screens. (p)	George-Cosh, 2015
--	---	-------------------

Table F7. Empirical Patterns from Nine Case Studies: Cognitive – Physical – Informational Interaction

P7: Cyberattacks will include multilateral interactions between the cognitive, physical, and informational dimensions.			
Case Study	Examples	References	
	<p><i>“The US, in a joint effort with Israeli cyber units, has developed the Stuxnet malware to compromise control systems at the Iranian Natanz enrichment facility.”</i></p> <p>Control systems in an Iranian nuclear enrichment facility were damaged (p) when people from the U.S. and Israel worked together to create (c) a set of information rules called Stuxnet malware. (i)</p> <p><i>“...SIMATIC software runs on the Microsoft Windows operating systems and provides human interfaces to monitor and control the peripheral devices that drive equipment such as centrifuge rotors.”</i></p> <p>People monitor and make decisions related to the control of (c) tangible devices that drive the centrifuge rotors with computers (p) running the information rules contained in the Microsoft Windows operating systems and Siemens SIMATIC software. (i)</p>	Paganini, 2016	
Stuxnet	<p><i>“To get Stuxnet to its target machines, the attackers first infect computers belonging to five outside companies that are believed to be connected in some way to the nuclear program.”</i></p> <p>The tangible computers operating the Natanz equipment had a tangible “air gap” from the Internet (p), so the people who developed the strategy started their attack at organizations of people who worked with the Natanz personnel by injecting (c) the information rules within the Stuxnet malware (i) into tangible computers (p) at five outside companies (organized groups of people). (c)</p> <p><i>“If a worker stuck a USB thumb drive into an infected machine, Stuxnet could, well, worm its way onto it, then spread onto the next machine that read that USB drive.”</i></p> <p>When a person made the decision to connect (c) a tangible device – the USB thumb drive – to other tangible machines, including those in the Natanz facility, (p) the information rules within Stuxnet propagated themselves from (i) one tangible device to another (p).</p>	Zetter, 2014	
Ukrainian Blackouts	<p><i>“...one or more malwares were deliberately developed to attack industrial facilities, with power systems as one of the major targets.”</i></p> <p>Malicious people used their knowledge and skills to develop (c) information rules in the form of malware (i) which they used to attack (c) tangible industrial facilities, specifically electric power systems. (p)</p> <p><i>“...hackers probably used phishing e-mails designed to trick power operators into clicking on malicious documents, thus allowing them access to the network.”</i></p>	Huang et al., 2018	
	Detsch, 2016		

	<p>Unauthorized people gained access by confusing operations personnel into opening carefully crafted (c) information in the form of electronic mail with attached documents that included information rules allowing unauthorized access (i) to tangible computer networks. (p)</p> <p><i>“...hackers are thought to have hidden in Ukrenergo’s IT network undetected for six months, acquiring privileges to access systems and figure out their workings, before taking methodical steps to take the power offline.”</i></p> <p>Information related to access privileges (i) was acquired by unauthorized people who hid themselves for six months and explored (c) the tangible Ukrenergo computer networks (p), to learn how to operate (c) tangible electric power equipment. (p)</p> <p><i>“...includes swappable, plug-in components that could allow it to be adapted to different electric utilities, easily reused, or even launched simultaneously across multiple targets.”</i></p> <p>Information rules (i) were created by people to enable them to change and tailor their attack tactics and techniques (c) to different tangible electric utility equipment environments. (p)</p>	Polityuk et al., 2017
	<p><i>“...in a nutshell, a botnet is a collection of internet-connected computers — the ‘bots’ — that are under remote control from some outside party.”</i></p> <p>Tangible Internet-connected computers (p) are controlled by a person using (c) a set of information rules called a botnet. (i)</p> <p><i>“The Mirai source code was released in a cybercrime forum recently; since when it has been used to build large botnets created from compromised Internet of Things (IoT) devices such as digital video recorders, CCTV systems and so on.”</i></p> <p>A person made the decision to post (c) to a cybercrime information-sharing forum a set of information rules called Mirai, a type of malware that connects (i) tangible Internet connected devices such as video recorders or CCTV systems. (p)</p>	Fruhlinger, 2018
Internet of Things (IoT) Botnet	<p><i>“the attack appears to have relied on hundreds of thousands of internet-connected devices like cameras, baby monitors and home routers that have been infected — without their owners’ knowledge — with software that allows hackers to command them to flood a target with overwhelming traffic.”</i></p> <p>Malicious people used their knowledge and skills to inject (c) a set of information rules comprising a botnet (i) into tangible devices such as baby monitors or cameras (p) owned by people who were unaware of the bad actors’ activities (c). These malicious people were then able to launch a targeted attack against (c) tangible servers using the tangible devices (p) to “shoot” information in the form of data packets. (i)</p>	Perlroth, 2016

	<p>“So far, Hajime hasn’t evidenced malicious behavior; in fact, it actually closes potential sources of vulnerabilities in IoT devices that Mirai-like botnets exploit, causing some researchers to speculate that it was created by a whitehat.”</p> <p>A set of information rules comprising the Hajime botnet closes software vulnerabilities (i) within tangible IoT devices (p), leading some people to conclude that a whitehat (hacker with heroic intentions – a person) was the author. (c)</p>	Koliast et al., 2017
	<p>“The deluded gunman who stormed into Washington, D.C.’s Comet Ping Pong pizzeria had been convinced by online conspiracy sites that it was the coordinating center for Hillary Clinton’s child–sex trafficking ring.”</p> <p>Disinformation (i) read by a person influenced him to decide (c) to carry a tangible gun (p) into a tangible building (p).</p>	Farrell, 2018, p. 26
	<p>“Two-thirds (66%) of all tweeted links were shared by suspected bots... This estimate suggests that automated accounts are more prolific than human users in sharing links on Twitter.”</p> <p>People share (c) links to information (i) using the tangible Twitter platform (p) less often than Twitterbot information algorithms share information (i) on the tangible Twitter platform (p)</p>	Wojcik, 2018
Twitterbots	<p>“...shares in the American ultra-low-cost carrier (ULCC) Spirit Airlines fell 5% the day after videos of passenger fist fights due to cancelled flights made the rounds on social media...fake news could be used to influence stock prices.”</p> <p>Information and disinformation (i) can influence people’s decisions related to trading behavior (c) affecting tangible stock prices.</p> <p>“...Russia-backed bots programmed to automatically tweet animosity-stoking messages in the U.S. gun control debate following last month’s school shooting in Parkland, Fla.”</p> <p>After the tangible school shooting in Parkland, FL (p), people from Russia wrote (c) information rules (computer programs) for Twitterbots to automatically tweet information (i) designed to make American people angry in order to influence their decision making behaviors (c) related to tangible legal controls relating to tangible guns (p).</p>	Gu et al., 2017
Melissa Virus	<p>“Although Mr. [Richard] Smith usually spends his time designing software tools and operating systems, over the weekend he used programmers’ tools to peer inside the document carrying the virus known as Melissa, which has wildly spread through the Internet in recent days.”</p> <p>A person named Richard Smith decided to examine (c) the information rules comprising Melissa and infecting the MS Word document propagating itself (i) through the tangible networked machines comprising the Internet. (p)</p>	McNamara, 2014

	<p><i>"Melissa was one of the first successful email-aware viruses, forcing some large companies to shut down their email gateways because of the colossal amount of email the malware was generating."</i></p> <p>The information rules comprising Melissa generated so much data traffic (i) that people working at large companies decided to turn off (c) their tangible electronic mail servers and gateways. (p)</p>	Cluley, 2009
	<p><i>"Gryaznov: It was just a macro virus and we were well equipped to provide detection and removal for people's computers even then."</i></p> <p>A person named Gryaznov was a security specialist who knew how to detect and remove (c) malicious information rules – malware – (i) from tangible computers (p).</p>	Mills, 2009
	<p><i>"While none of the three companies would divulge its post-Melissa sales figures, they all reported fourfold to fivefold increases in traffic to their Web sites."</i></p> <p>The people at three antivirus companies would not disclose (c) sales information, but the data traffic increased substantially (i) on the tangible servers comprising their Websites (p) because people were trying to protect or repair (c) their tangible computers (p) from the malicious information rules in the Melissa virus.(i)</p>	Raney, 1999
Hack of American Business 2007-2012	<p><i>"The cashers would encode the information onto the magnetic strips of blank plastic cards and cash out the value, by either withdrawing money from ATMs in the case of debit cards, or running up charges and purchasing goods in the case of credit cards."</i></p> <p>People made the decision to purchase (c) information in the form of credit and debit card numbers (i) which the people, "cashers," would then use their knowledge and expertise to encode (c) onto the tangible magnetic strips of the blank plastic cards, which interfaced with the tangible ATMs which would disburse tangible bank notes. (p)</p> <p><i>"Roman Kotov, 33, of Moscow, allegedly specialized in mining the networks Drinkman and Kalinin promised to steal valuable data."</i></p> <p>Each person in the cybercrime gang had a specific set of skills and knowledge: Drinkman and Kalinin would gain access to (c) the tangible computer networks, (p) while Kotov would explore and mine (c) the tangible networks (p) for valuable information and data. (i)</p>	Hudson, 2013 Schwartz, 2015; DoJ, 2015, 2018
	<p><i>"For example, [in an SQL injection attack], a long string of unexpected characters entered into a blank form used to enter an email address can confuse a misconfigured server and dupe it into giving the user privileged access."</i></p> <p>The tangible, networked servers (p) were accessed when the people used their skills and knowledge to provide (c) incompatible information cues in the form of long strings of unexpected characters (i) in a tangible online website form that connected to a tangible server and confused it (p) with bad information rules. (i)</p>	Sullivan, 2013

	<p><i>To protect against detection by the victim companies, the defendants allegedly altered the settings on victim company networks to disable security mechanisms from logging their actions.</i></p> <p>The people in the cybercrime gang used their knowledge and skills to remain undiscovered by changing (c) the security software information settings and information rules that recorded activity taking place (i) within the tangible networks and computer servers. (p)</p>	DoJ 2015, 2018
	<p><i>Even though Microsoft released a patch to address this security vulnerability in March, a computer system that wasn't updated could be vulnerable to this ransomware variant.</i></p> <p>In March, the people at Microsoft developed, released, and advised customers to install (c) a set of information rules that closed the EternalBlue vulnerability so that (i) their tangible computer systems could be secure. (p)</p>	Nelson et al., 2017
	<p><i>...one single infection would become particularlyateful for Maersk: In an office in Odessa, a port city on Ukraine's Black Sea coast, a finance executive for Maersk's Ukraine operation had asked IT administrators to install the accounting software M.E.Doc on a single computer.</i></p> <p>One person who worked for Maersk's Ukrainian operations as a finance executive made the decision to request that the people from the IT staff install (c) the information rules comprising the M.E. Docs tax and accounting software (i) in his tangible computer which exposed the rest of the tangible infrastructure (p) to the malicious information rules contained in NotPetya. (i)</p>	Greenberg, 2018
(Not)Petya Ransomware	<p><i>All computer equipment used by Maersk from before NotPetya's outbreak had been confiscated, for fear that it might infect new systems, and signs were posted threatening disciplinary action against anyone who used it.</i></p> <p>The people who led Maersk were so afraid of further damage that they made the decision to confiscate (c) all tangible computer and network equipment in operation prior to the (p) infection with the information rules contained in NotPetya, (i) and they threatened all the people who worked for Maersk with disciplinary action to ensure that no one decided to use (c) the tangible devices that might possibly contain (p) the malicious information rules. (i)</p>	Greenberg, 2018

	<p><i>“Manning was the source of the largest number of classified documents ever leaked to the public – including the footage used in ‘Collateral Murder’ – and we learn about Manning mostly through his online chats with journalist Adrian Lamo.”</i></p> <p>Information in the form of chat logs captured by (i) tangible computer servers and computers (p) reveals that a person, Private Manning made the decision to share with people in the public at large (c) information in the form of classified documents, including the full motion video “Collateral Murder.” (i)</p> <p><i>“Manning’s release of confidential information to WikiLeaks is taken as fact, opinion is divided as to the moral nature of his actions.”</i></p> <p>People have different opinions of Manning’s moral decision making related to the sharing of (c) information in the form of national secrets (i) using the tangible servers of WikiLeaks. (p)</p>	Nita, 2014
WikiLeaks & the Manning Disclosure	<p><i>“I would come in with music on a CD-RW labeled with something like ‘Lady Gaga,’ erase the music then write a compressed split file...”</i></p> <p>In Manning’s own words, he devised a strategy that involved misdirection and specific knowledge and skills to write (c) specific information rules that captured data on (i) tangible rewritable CDs (p) that he could carry with him. (c)</p> <p><i>“...a Manning user account is created on a FOB Hammer supply room NIPRnet computer that Manning used.”</i></p> <p>In a tangible supply room at Forward Operating Base Hammer in Iraq was a tangible computer which (p) Manning used to explore and communicate by entering (c) information in a user account . (i)</p>	Zetter & Poulsen, 2010
Ashley Madison	<p><i>“...users pay \$19 for the privilege of deleting all their data from the site...”</i></p> <p>People made the decision to pay (c) a tangible \$19 fee (p) in exchange for the people at Avid Life Media to delete (c) information related to their personal details and communications (i) from the tangible Avid Life Media servers. (p)</p> <p><i>“Even if you think you’ve left Dating Site X, your name and messages and mortifying pictures could very well survive on their (apparently hackable) servers.”</i></p> <p>When a person makes the decision to stop using the services provided through (c) the tangible servers that support a dating website, those servers continue to maintain (p) the information content such as messages and photographs attached to a username. (i)</p>	Hackett, 2015
	<p><i>“...the company stored its VPN password on Google Drive, making it easy to obtain for anyone who accessed any employee’s machine.”</i></p> <p>The people who worked for Avid Life Media made the decision to store (c) information in the form of a password (i) for the tangible Virtual Private Network on the tangible servers of Google Drive (p), which created opportunities</p>	Chirgwin, 2016

	<p>for other people to gain unauthorized access (c) to any tangible computer in the networked infrastructure. (p)</p> <p><i>“You could use Pass1234 from the internet to VPN to root on all servers.”</i></p> <p>In an interview with a person who was a reporter, the people (hackers) who called themselves “Impact Team” said that used (c) default password information “Pass1234” which provided access (i) to the tangible servers via the Virtual Private Network. (p)</p>	Cox, 2015
--	---	-----------