Duquesne University
Duquesne Scholarship Collection

Electronic Theses and Dissertations

Spring 5-10-2019

The Dialectics of Cyberspace: Communication Ethics as First Response to Cyber Attacks

Matthew P. Mancino
Duquesne University

THE DIALECTICS OF CYBERSPACE:

COMMUNICATION ETHICS AS FIRST RESPONSE TO CYBER ATTACKS

A Dissertation

Submitted to the McAnulty College and Graduate School of Liberal Arts

Duquesne University

In partial fulfillment of the requirements for

the degree of Doctor of Philosophy

By

Matthew P. Mancino

May 2019

THE DIALECTICS OF CYBERSPACE:

COMMUNICATION ETHICS AS FIRST RESPONSE TO CYBER ATTACKS

By

Matthew P. Mancino

Approved February 22, 2019

Janie Harden Fritz, Ph.D.
Professor of Communication & Rhetorical Studies
(Committee Chair)

Ronald C. Arnett, Ph.D.
Professor of Communication & Rhetorical Studies
(Committee Member)

Craig T. Maier
Associate Professor of Communication & Rhetorical Studies
(Committee Member)

James Swindal, Ph.D.
Dean, McAnulty College and Graduate School of Liberal Arts
Professor of Philosophy

Ronald C. Arnett, Ph.D.
Chair, Department of Communication & Rhetorical Studies
Professor of Communication & Rhetorical Studies

ABSTRACT

THE DIALECTICS OF CYBERSPACE:
COMMUNICATION ETHICS AS FIRST RESPONSE TO CYBER ATTACKS

By

Matthew P. Mancino

May 2019

Dissertation supervised by Janie Harden Fritz, Ph.D.

This project recognizes the need to re-conceptualize cyberspace according to its characteristic dialectical tensions in order to offer lasting, adequate responses to cyber attacks. Scholars across multiple disciplines recognize the ineffectiveness of perimeter defense strategies, or the raising of defensive walls to protect sensitive information as the primary response to cyber attacks (Denning, 2001; Jang-Jaccard & Nepal, 2014; MacKinnon, Bacon, Gan, Loukas, Chadwick, Frangiskatos, 2013). Thus, this project suggests that in addition to a literacy in coding, corporations and policy makers must attend to what Ronald C. Arnett, Janie Harden Fritz, and Leeanne M. Bell McManus (2009/2018) term "communication ethics literacy" to illuminate the goods at stake in cyber attacks. Communication ethics literacy and its emphasis on learning from difference will encourage an examination of the background issues influencing foreground attacks (Arnett, McManus, & McKendree, 2013). The goods that shape cyberspace manifest in the dialectics of cyberspace. After reviewing historic and philosophic approaches to dialectic, this project employs a dialectical framework derived from the work of both Kenneth Burke (1941; 1945/1969) and David Gunkel (2007); Burke recognizes that dialectical terms do not reach a synthesis but rather remain in tension (Tell, 2004), and Gunkel announces the poststructuralist recognition that after their collision, neither term is the same and must be thought of as wholly and radically other. This project examines the dialectics of public/private, anonymity/identity, and national/global and their corresponding attacks of cyberbullying, cyber theft, and cyber terrorism and cyber war. The project concludes with an examination of the goods of public/private, anonymity/identity, and national/global to announce the importance of the maintenance of each pole of the dialectic while engaging cyberspace. This attentiveness yields implications for the continued application of communication ethicists, philosophers of communication, phenomenologists, and philosophers of technology to position communication ethics as a first response to cyber attacks.

DEDICATION

UXŌRĪ ET PUERŌ

ACKNOWLEDGEMENT

I start with the wonderful faculty in the Department of Communication & Rhetorical Studies who I have had the opportunity to study under and work with at Duquesne University and in the Communication Department at Roberts Wesleyan College where Dr. Mrs. Berry and Dr. Paul Stewart first introduced me to concepts in rhetoric and media ecology. From Duquesne, I must in particular thank my committee members. I am thankful of and appreciative to Dr. Maier, whose insightful comments drove the work to a more nuanced and sophisticated level. Dr. Arnett's encouragement cultivated the impetus of this project and contributed to its background and foreground implications. Most of all, I am incredibly grateful and fortunate that Dr. Fritz served as the advisor for this project; she has been a wonderful mentor inside and outside the classroom.

I next acknowledge my professional colleagues and friends. I am thankful to have studied, taught, and served alongside Aurora Pinto, James Begley, Basak Guven, Sarah DeIuliis, Lane Grafton, and Justin Bonanno at Duquesne University. Likewise, I extend thanks to friends who have supported me inside and outside of a professional academic context: Tyler and Hannah Sass, Brent and Rachel Rathke, Dan Celiberti, Kendra Zaffuto, Matt Dearstyne, Steven and Robin Zwier, and, most significantly, Matt and Chelsea Metzger. Additionally, the encouragement and support of Pani Eva Tumiel-Kozak has been fundamental to my education.

Finally, I extend gratitude to my family: my parents, Chuck and Kim Mancino; my brother, Chaz Mancino; my wife's parents, Janet and Larry Carr; grandma, Ann

Hollis; and brothers-in-law, Patrick (and Jen, Audrey, and Ezra) and Michael Carr, who have all been incredibly supportive throughout this entire process. I cannot end this paragraph without also thanking my wife, Susan Mancino, for her unending support.

TABLE OF CONTENTS

Page

Abstract iv

Dedication vi

Acknowledgement vii

Chapter 1 – The Dialectics of Cyberspace:

Communication Ethics as First Response to Cyber Attacks……………………….1

Introduction…………………………………………………………………………..1

Landscaping Cyber Threats……………………………………………………… 4

Cyber Terrorism: The Culmination of Cyber Threats……………………………14

Communication Literature Review………………………………………………25

Cyber Attacks as a Wicked Crisis………………………………………………..33

Project Overview…………………………………………………………………39

Chapter 2 – Cyberspace as Dialectical………………………………………………...44

Introduction…………………………………………………………………………44

History of Dialectic…………………………………………………………………45

The Dialectical Nature of Cyberspace…………………………………………... 59

The Dialectics of Cyberspace………………………………………………………73

Chapter 3 – The Public/Private Dialectic of Cyberspace:

Cyberbullying as a First-Tier Attack…………………………………………...77

Introduction……………………………………………………………………………77

Situating Cyberspace within a Public/Private Dialectic…………………………79

A Communication Perspective on Cyberbullying………………………………..95

Extensions from Hannah Arendt…………………………………………………..102

Communication Ethics Implications……………………………………………113

Chapter 4 – The Anonymity/Identity Dialectic of Cyberspace:

Cyber Theft as a Second-Tier Attack……………………………………………117

Introduction……………………………………………………………………..117

Situating Cyberspace with the Anonymity/Identity Dialectic…………………. 119

Identity/Data Theft as a Second-Tier Cyber Attack……………………………134

Extensions from Ulrich Beck…………………………………………………...147

Communication Ethics Implications……………………………………………158

Chapter 5 – The National/Global Dialectic of Cyberspace:

Cyber Terrorism and Cyber War as Third-Tier Attacks………………………163

Introduction……………………………………………………………………..163

Changing National/Global Borders within Cyberspace………………………...165

Cyber Terrorism and Cyber War as Third-Tier Attacks………………………..178

Ulrich Beck: Individualization and Cosmopolitan Outlook…………………… 188

Communication Ethics Implications……………………………………………198

Chapter 6 – "This is Not That":

Re-Conceptualizing the Dialectics of Cyberspace………………………………203

Introduction……………………………………………………………………..203

Cyber Attacks as Wicked Crises………………………………………………..205

Communication Ethics: Examining the Dialectics of Cyberspace……………...215

Concluding Implications………………………………………………………..232

Chapter 1

The Dialectics of Cyberspace: Communication Ethics as First Response to Cyber Attacks

Introduction

This project recognizes that cyberspace has become a confused concept first because it is conflated with the Internet and the World Wide Web and second because there is ambiguity surrounding the role that cyberspace plays in society. Thus, paying attention to the dialectical nature of cyberspace illuminate communication ethics goods that can become a first response to cyber attacks. I use the term cyber attacks broadly to encompass everything from bullying to identity theft to cyber terrorism.

This proposed project contends that we can better respond to cyber attacks by first understanding the dialectical nature of cyberspace. As cyberspace, the Internet, and the World Wide Web (WWW) increasingly pervade human experience and social interaction, the terms have become conflated in vernacular use. Cyberspace distinctly centers on the emergent human experience derived from interactions with computers and other digital technologies (Strate, 1999). The Internet is a network that connects a vast array of computer networks which can then disseminate information contained therein between and among connected devices; the World Wide Web is an Internet service that mediates users' online experience through hypermedia, which eliminated one's need to use and learn the complex operating systems that were the exclusive way to access online content (Ainscough, T. L. & Luckett, M. G., 1996; Pallen, 1995). As lists of documented cyber attacks increase in number,[1] a focus on the competing goods in tension that are

[1] For an alarming list of cyber attacks in 2016 alone, see Riley Walters (2016).

constitutive of and protected and promoted by various groups present within cyberspace can facilitate adequate responses to cyber threats.

As early as 1999, cyberspace was recognized as “vague” and “drained of meaning” due to the expansive and exponential use of the term (Strate, 1999, p. 383; see also: Zhang & Jacob, 2012, p. 91). Lance Strate (1999) considers the “fundamental issue” of cyberspace as “definition and delimitation” (p. 382). Since the mid-nineties, various metaphors have described cyberspace,[2] including an information superhighway (C-SPAN, 1994), an information marketplace (NRC, 1994), a New World (Gunkel & Gunkel, 1997), the Wild West (Biegel, 2001), a feudal society (Yen, 2002), the *Maat* of the Ancient Egyptian Moral Code (Mancini, 2002), a rainbow (Georgiadou, Puri, & Sahay, 2006), a page (O’Reilly, 2007), a platform (O’Reilly, 2007), and a place (Olson, 2005; Zhang & Jacob, 2012). Stephanie Vie (2008), in *Review of Communication*, describes benchmarks in the development of cyberspace, from the launch as ARPANET in 1969 with the intent to “move information” to the Internet service providers (ISPs) of the 1980s to the World Wide Web (WWW), introduced by Tim Berners-Lee (p. 131). Berners-Lee envisioned the WWW as a reflection of the physical world that was connected by a series of hypertexts (Vie, 2008, p. 131).

Today, these hypertexts have spread beyond the computer screen to connect humans and computers like never before, contributing to what has been referred to as “the Internet of things” (Irwin, 2016; Gálik, 2015; MacKinnon et al., 2013; Thomas, 2006); in such a moment of interconnectivity, cyberspace becomes the locus for much of our daily activities, work, and well-being (Carr, 2016; Hawisher, Selfe, Guo, & Liu,

[2] Donald Fishman (2004) has also recognized the many metaphors applied to understand cyberspace (p. 34).

2006; Kellerman, 2010; Ollier-Malaterre, Rothbard, & Berg, 2013; Turkle, 2011). Thus, we are affected by the state of cyberspace, making it increasingly vulnerable to bullying (Tanrikulu, Kinay, & Aricak, 2015), theft (Manao, Rahim, & Taji, 2015), crime (Brenner, 2007; Bucci, 2012), intimidation (Pittaro, 2007), shame (Webb, 2015), war (McGraw, 2013), and terrorism (Weimann, 2015). This project considers how cyber attacks, a term I use generally to encompass the threats listed here, have become a wicked crisis that requires communication scholars to re-examine ways of speaking and thinking about cyberspace as a starting point for consideration and response.

This project situates the issue of cyber attacks within the field of human communication, providing an historical overview, identifying key points of dialectical tension, and analyzing goods and practices that represent communication ethics. The chapter proceeds in four sections. The first section surveys the historical landscape of cyberspace. The second section discusses the theoretical and social components of cyber terrorism as the culmination of cyber threats. The third section reviews the work of communication scholars related to cyber threats/attacks.[3] The fourth section develops this issue as a wicked crisis in need of communication ethics analysis. Finally, the chapter concludes with a chapter overview and a summary of the significance, methodology, and limitations of the project. Together, these sections aim to situate this project within the field of communication and articulate the scope of the inquiry.

This project asks, "How can we re-consider cyberspace, via its characteristic dialectical tensions, as a means to texture thoughtful responses to cyber attacks?" We live

[3] Throughout this project, I refer to cyber threats as unactualized danger to persons, reputations, and finances. Conversely, I refer to cyber attacks as actualized threats. For instance, a cyber threat would encompass the potential for computer hackers to take control of a smart car to damage people/property whereas a cyber attack would emerge after the hack has occurred.

in an era where the primary mode of defense to cyber attacks is bolstered cyber security via a “perimeter defense strategy” (Jang-Jaccard & Nepal, 2014, p. 974), or a raising of security walls to safeguard the coveted materials or information inside (Denning, 2001; Jang-Jaccard & Nepal, 2014; MacKinnon, Bacon, Gan, Loukas, Chadwick, Frangiskatos, 2013); however, this project contends that this pattern of response does not yield constructive resolution because it does not attend to the multiple, competing goods present within the various contexts of cyberspace. I argue that in addition to literacy in coding, corporations and policy makers must attend to what Ronald C. Arnett, Janie Harden Fritz, and Leeanne M. Bell McManus (2009/2018) have termed “communication ethics literacy.” Communication ethics literacy and its emphasis on learning from difference will encourage an examination of the background issues influencing foreground attacks (Arnett, McManus, & McKendree, 2013). This chapter summarizes the historical and contemporary landscape of cyberspace, situates it within the field of communication, and recognizes cyber attacks as a wicked problem in need of communication ethics analysis to recognize goods made meaningful within the context of dialectical tensions.

Landscaping Cyber Threats

In order to landscape cyber threats, the chapter first offers an explication of cyberspace from the field of communication. Strate (1999) offers a thorough definition of cyberspace and addresses what this project refers to as cyber threats. The section will first situate cyberspace and threats in Strate’s work before addressing a brief history of cyberspace and acts of cyber terrorism. History is addressed in this landscaping because historical awareness will generate insight on particular Internet policies and how these policies will shape the future of the Internet and our engagement with it (Haigh, Russell, & Dutton, 2015, pp. 146–147).

Strate (1999) defines cyberspace as "the diverse experiences of space associated with computing and related technologies" (p. 383). Strate characterizes experiences of cyberspace into a three-level taxonomy (zero, first, and second-order cyberspaces) with referents to an "ontology," "building blocks," and "*cybermediaspace*," a "synthesis" of zero and first order cyberspaces. Strate first establishes zero-order cyberspace as the ontology that involves coordinates of space and time as "*paraspace or nonspace*" and "*cyberspacetime.*" Cyber events occur in the paraspace of cyberspace (what is distinctly not a part of the "*real world*") and through "*cybertime*" (time rooted in objective reality that passes during our interactions with technologies) (pp. 387, 389). Zero-order cyberspace is ontologically established in space and time.

First-order cyberspace holds the physical, conceptual, and perceptual building blocks of our experiences with computer technologies (Strate, 1999, p. 390). The assemblage of these blocks provides cyber events. Without the physical, material computer components, cyber events could not occur. Without the conceptual, there would be no logical or metaphorical understanding of the cyber event in the mind of the user. Without the perceptual, cyberspace would not generate the illusion of the event occurring in space to the senses of the user (pp. 391–396). First-order cyberspace permits the user to experience cyber events.

Finally, Strate (1999) defines second-order cyberspace, or cybermediaspace, as the "*sense of space generated through the user's communication with and through computers and related technologies*" (pp. 399–400). Cybermediaspace includes components of aesthetic space, dataspace, and relational space. The aesthetic emphasizes perceptual cyberspace by accentuating form, the dataspace by stressing content, and the relational by highlighting the two-way nature of cybermediaspace as either between the user and other users, "*social*," or the computer and the user, "*personal*" (pp. 400–403). Second-order cyberspace frames the user's experience of communication with other users and the computer.

In addition to characterizing cyberspace, Strate (1999) also describes cyber threats. These cyber threats occur in the personal relational space of second-order cyberspace, where Strate describes the potential emergence and formation of an "*intimate cyberspace*" or surfacing between the user and computer (p. 403). Strate explains that cyber threats of hacking, email spying, webservers using cookies, and computer viruses are intrusions upon intimate cyberspace (pp. 403–404). Strate labels these cyber threats as "upsetting" without offering strategies for prevention (p. 403).

Strate's article is helpful for describing the user experience in cyberspace as a result of interactions with computing and related technologies. However, this project recognizes experiences of cyberspace as half the question to providing adequate responses to cyber threats. A brief history of the computing and related technologies advances a dialectical understanding of cyberspace that ought to be considered when facilitating adequate responses to cyber threats.

Roy Rosenzweig (1998)[4] adds helpful coordinates to the history of the Internet by situating its development in the 1960s out of the interplay between the Cold War "'closed

[4] Roy Rosenzweig (1998) is the CAS Distinguished Scholar in History and the director of the Center for History and New Media at George Mason University. Rosenzweig has taught at George Mason since 1981 (p. 1552). Thomas Haigh, Andrew L. Russell, and William H. Dutton (2015) credit Roy Rosenzweig (1998) as providing a foundational "historiographic template" on the history of the Internet (p. 148).

[and centralized] world'" and the counterculture "open and decentralized world" (p. 1531). Rosenzweig believes these "dual origins" undergird the present day Internet and the ensuing emergent world (p. 1531). Rosenzweig describes the Internet as the product of the contributed efforts from wizards, bureaucrats, warriors, and hackers. An understanding of these groups and what they protected and promoted yields insight into the development of present-day cyberspace.

First, Rosenzweig (1998) discusses the wizards, or computer whizzes, in *Where Wizards Stay Up Late: The Origins of the Internet*, by Katie Hafner and Matthew Lyon (1996). According to Rosenzweig (1998), Hafner and Lyon provide a "biographical" account (p. 1534), or "great man approach" (p. 1531), that emphasizes the "'young computer whizzes'" (p. 1531) who built the Internet out of "technical curiosity" rather than an "ideological system" or desire for "self-advancement or economic enrichment" (p. 1534). Their story begins with the emergence of ARPANET, from the collaboration of the Advanced Research Projects Agency (ARPA)[5] and the computer-consulting agency Bolt Beranek and Newman (BBN). Initially, ARPANET connected three computer terminals to a mainframe, thus synchronizing their computer system, program language, and operating system (p. 1532). Instrumental computer whizzes that contributed to ARPANET were Larry Roberts, a computer scientist who designed and built the network, Wes Clark, the inventor of Interface Message Processors (IMPs) that enable network function via the insertion of sub-networks between host computers and main-networks, Frank Heart, an employee of BBN who would affordably construct the network, and Bob Taylor, the head of the Information Processing Techniques Office at ARPA. Taylor

[5] Rosenzweig (1998) details that ARPA was established in 1957 in response to the "post-Sputnik panic" over advanced Soviet technologies (p. 1531). ARPA was positioned as a Defense Department that researched technology with a focus on ballistic missile defense systems (p. 1531).

named the problem of connecting computers that formerly spoke incommensurable programming languages and instigated the ARPANET solution (p. 1532).

Rosenzweig (1998) also references Bruce Sterling's influential essay, "Brief History of the Internet" (p. 1532). Sterling places the roots of the Internet in 1964 at the RAND Corporation prior to the establishment of ARPANET. The RAND Corporation was the leading US Cold War "think-tank" tasked with solving how government officials could communicate following a nuclear crisis (Rosenzweig, 1998, p. 1532). Sterling details the involvement of Paul Baran, an engineer at the Rand Corporation, who contributed two "key innovation[s]" to the development of the Internet (Rosenzweig, 1998, p. 1533). The first innovation Baran put forward was a decentralized network that could sustain several hits without collapse and continue to work "through alternative channels" (Rosenzweig, 1998, pp. 1532–1533). The second innovation was "message blocks" that disassembled messages into smaller, individual pieces that were then reassembled by the receiver (Rosenzweig, 1998, p. 1533). Baran's message blocks played an essential role in the development of the packet-switching networks, a "core technology of the Internet," which break data into even smaller pieces that travel across multiple, shared paths (Rosenzweig, 1998, p. 1533). However, Rosenzweig (1998) recognizes that we cannot credit the emergence of the Internet to a "central founding figure" (p. 1534). Instead, he emphasizes the contributions of "bureaucratic teams" that collectively advanced Internet technologies beyond the capabilities of any individual person (p. 1534).

Moving from the whizzes, Rosenzweig (1998) focuses on bureaucrats. As an exemplar of the bureaucratic account, Rosenzweig points to *Transforming Computer*

Technology: Information Processing for the Pentagon, 1962 – 1986, by Arthur L. Norberg and Judy E. O'Neill (1996). Rosenzweig (1998) explains that this work explicated the near proximity between "ARPA computer funding" and "military concerns" (pp. 1534–1535). In fact, they suggest that these "military origins" of ARPANET begat the success of the network (p. 1535). Rosenzweig (1998) stresses contributions that advanced the bureaucratic growth of the Internet introduced by Bob Kahn, an engineer who started at ARPA in 1972 after formerly being employed at BBN[6] (p. 1536). Kahn's first contribution was the "Internetting Project,"[7] which enabled communication across computers on the formerly incommensurable satellite, radio, and ARPANET networks (p. 1536). The second contribution, introduced by Kahn and Vinton Cerf in 1974, was Transmission Control Protocol/Internet Protocol (TCP/IP), which provided a "new and more independent packet-switching protocol" (p. 1536). Military funding was essential to developing TCP/IP, as was the Defense Department, who adopted the protocol in 1980 (p. 1536). The TCP/IP protocol defeated the European standard for "international politics and commerce" and is a direct antecedent of US Internet dominance (pp. 1536–1537).

Rosenzweig (1998) then moves to the "ideological" warrior anecdote, selecting *The Closed World: Computers and the Politics of Discourse in Cold War America*, by Paul Edwards (1997). According to Rosenzweig, Edwards "does not focus specifically on the Internet," yet discusses the emergence of the digital computer as a consequence of and influencer to Cold War politics (Rosenzweig, 1998, pp. 1531, 1537). Edwards

[6] Although Kahn's involvement with the development of the Internet resembles the efforts of a wizard, who works alone and contributed technological innovations out of love for technology rather than profit, Rosenzweig (1998) groups Kahn's involvement amongst the bureaucratic Internet origins.

[7] Rosenzweig (1998) explains that the "Internetting Project" brought both the "concept and the name of the Internet" (p. 1536).

believes the computer was a direct by-product of “closed-world discourse,” or “‘the language, technologies, and practices that together supported the visions of centrally controlled, automated global power at the heart of American Cold War politics’” (Rosenzweig, 1998, p. 1538). Furthermore, the politics of the Cold War were “‘embedded in the machines’” (Rosenzweig, 1998, p. 1538). Rosenzweig (1998) suggests that Edwards’ work focuses on the computer’s contribution to and maintenance of a “centralized command and control” discourse, and contains several exemplars contributing to this discourse (p. 1539).

Before moving to the hacker-social anecdotes, Rosenzweig (1998) differentiates the major difference between the anecdotes of the warriors, the wizards, and the bureaucrats as pertaining to “the depiction of J. C. R. Licklider” (p. 1540). Licklider was a two-time director of IPTO and penned a famous 1960 paper detailing “machine-man symbiosis,” which was instrumental in the shift of “computing from computation to communication” (p. 1540). Rosenzweig describes how Hafner and Lyon and Norberg and O’Neill paint Licklider as “an almost sainted figure” who offered a worldview suggesting that “‘technological progress would save humanity’” (p. 1540). Contrarily, Edwards describes Licklider “as tightly wedded to military goals” (p. 1540). Rosenzweig suggests that, despite the personal views of Licklider, the Defense Department would have declined funding to “projects like ARPANET” unless they could serve a military agenda (p. 1541). Rosenzweig aligned the emergence of computer systems and technologies with “the discourse of the Cold War” by creating the belief these technologies could control closed communication lines (p. 1541).

Finally, Rosenzweig (1998) turns to the social, “hacker” roots of the Internet (p. 1531). Rosenzweig places *Netizens: On the History and Impact of Usenet and the Internet*, by Michael and Ronda Hauben (1997) as representative of the hacker anecdote. This work depicts “Netizens,” or “ordinary users,” who “popularized” the Internet and identified its primary use as for “democratic and interactive communication” (p. 1543). The Haubens root the Internet in the “Usenet”[8] network, a 1979 conception by Tom Truscott and Jim Ellis, which operated as an “international computer newsgroup network” (p. 1543). In addition to explaining the onset of Usenet, the Haubens provide a “more democratic” origin story to ARPANET that centers on Steve Crocker, a UCLA graduate student who took notes during a meeting that established Internet protocols (p. 1544). Crocker’s notes highlight the Requests for Comments (RFCs) that permitted free and collaborative discourse on the Internet (p. 1544). RFCs became an essential component to the development of Internet standards by creating “unprecedented openness” and a “cooperative culture” (p. 1544).

Additionally, *Hackers: Heroes of the Computer Revolution*, by Steve Levy (1985), advances this growth and purpose of the Internet. For Rosenzweig (1998), Levy identifies the “hacker ethic” in the 1960s and 1970s as a “‘philosophy of sharing, openness, decentralization, and getting your hands on machines at any cost—to improve the machines, and to improve the world’” (p. 1545). Levy places the Community Memory project at Berkeley as an exemplar of the hacker ethic. The Community Memory project was a “time-shared mainframe computer” that was open to free public use as a “combined electronic version of a public library, coffeehouse, urban park, game arcade,

[8] Rosenzweig (1998) contends that Usenet lost some users to the WWW, but retained others as of 1998 (p. 1543).

and post office" (p. 1545). Lee Felsenstein, a founder of the Community Memory project, also moderated the "Homebrew Computer Club," where the first PCs were produced (p. 1546).

After detailing the wizard, bureaucrat, warrior, and hacker anecdotes providing Internet origins, Rosenzweig (1998) characterizes "the Internet of the 1990s" as "the perfect synthesis of the anti-hierarchical cultural revolution of the 1960s and the anti-statist political revolution of the 1980s" (p. 1551). However, Rosenzweig considers the Internet still contains "internal tensions and contradictions"—for instance, a view of the Internet as "the home of 'people's capitalism'," that simultaneously appeared "headed down the road to oligopoly" (p. 1551). Rosenzweig attests that the leanings toward "open and closed systems" remain (p. 1551). While a "populist and democratic Internet" can exist and thrive, this conception of the Internet depends upon such influences from the physical world (p. 1552).

The Internet has experienced continual growth since its emergence as ARPANET in 1969. In fact, Thomas Haigh, Andrew L. Russell, and William H. Dutton (2015) describe the Internet as "gigantic and amorphous," too large for a "simple definition" (p. 144). They place the Internet as a growth and extension of inquiry areas in "information technology, computer-based networking, work, and community" (p. 145). Household items, from televisions to cars, and businesses, from bookstores to record labels, exemplify the broad diversity of activities wired to and conducted in, on, and through the Internet (p. 144). The Internet is a tool that connects many broad, formerly disconnected, spheres of existence.

Importantly, Haigh, Russell, and Dutton (2015) point to a distinction between the Internet and the World Wide Web (WWW) (p.151; see also, Vie, 2008, p. 131). The recognition of this distinction is essential to landscaping cyberspace. As discussed already, ARPANET and "Inter-netted" networks (what is now termed the Internet) were intended for sharing information across military and government networks. Conversely, the WWW sought to become a "common information space where multiple individuals could communicate and share ideas" and a "'realistic mirror'" of the work, play, and socialization found in the physical-world (Vie, 2008, p. 131). Since its introduction, the WWW transitioned from Web 1.0 to Web 2.0, a 2004 label from Tim O'Reilly (Thomas, 2006, p. 389). Web 1.0 contained "static" information that relied upon life outside of the computer medium for activating meaningful experience (Zimmerman, 2012, p. 154). Web 2.0, however, attempts to connect all devices through a pattern of participation (O'Reilly, 2005, para. 1); Web 2.0 exceeds Web 1.0 in offering an engaging and dynamic experience through Internet technologies. Web 2.0 permits those not fluent in computer-programming language to generate web content (Zimmerman, 2012, pp. 154–155). The transition to Web 2.0 made the WWW accessible and editable to the everyday user.

As the web continues to grow and extend, Sue Thomas (2006) sketches the "end of cyberspace" with the introduction of the "internet of things," thought to come to fruition in approximately 2036 (p. 390). To explicate the end of cyberspace and the internet of things, Thomas turns to Alex Pang (2006), a Research Director at the Institute for the Future in Silicon Valley, who started the blog "The End of Cyberspace" (p. 389). Pang's blog contends that cyberspace will end as we come to be "'online all the time, everywhere'," thus disintegrating the distinction between cyberspace and the real world (as cited by Thomas, 2006, p. 389). Perhaps, this contention was somewhat prophetic, as the following year attacks occurred through cyberspace that showed the potential of devastating consequences to the physical world, evidencing the blurring of the cyber and the real.

Cyber Terrorism: The Culmination of Cyber Threats

In 2007, the country of Estonia experienced cyber attacks that became a benchmark for global recognition of the destructive potential of cyber terrorist acts. These attacks were distributed denial-of-service (DDoS) launched against the nation's critical networks, and "shut down the websites of all government ministries, two major banks, and several political parities," including the "parliamentary email server" (Herzog, 2011, p. 51). Stephen Herzog[9] (2011) describes the attacks as "a wake-up call to the world," which announced that "potentially autonomous transnational networks" possessed the ability to practically cripple the "critical infrastructure of technically sophisticated nation-states" (p. 56). Herzog stresses that the acts of cyber terrorism against Estonia indicate that the "foreign and security policies of nation-states" must adapt to the digital era because "difficult-to-attribute asymmetric threats stemming from the Internet are likely to harm nation-states in the future" (p. 56). While 2007 was a benchmark year in the history of recognition of the severity of cyber threats, awareness of these risks has continued to increase on a global scale (Aaviksoo, 2010; Czosseck, Ottis, & Talihärm, 2011; Shafqat & Masood, 2016).

Within the United States, politicians across party lines recognize the threat of cyber attacks. For instance, during the 2016 vice presidential debates, current Vice

[9] Stephen Herzog is a Ph.D. candidate in Yale University's Department of Political Science. His research centers on international security, including "nuclear weapons proliferation, arms control, and domestic sources of foreign policy" ("Stephen Herzog," 2018, para. 1).

President of the United States Mike Pence labeled cyber attacks the "new warfare of the asymmetrical enemies that we face in this country" (C-SPAN, 2016). Likewise, 2016 Democratic Party presidential nominee Hillary Clinton (2017) contends: "In the nineteenth century, nations fought two kinds of wars: on land and at sea. In the twentieth century, that expanded to the skies. In the twenty-first century, wars will increasingly be fought in cyberspace" (p. 374). Since the election, conversation continues surrounding Russian interference within the election itself (Ohlin, 2017).

Additionally, in the United Kingdom, Yianna Danidou and Burkhard Schafer describe the growth of cybercrime as a "tier one risk" alongside chemical, biological, radiological, and nuclear threats, military crises, and pandemic outbreaks (pp. 185–186). In a similar manner, Deborah Lupton (2016) refers to the present world as a "Digital Risk Society" (p. 301), and Gabriel Weimann[10] (2008) argues that the Internet facilitates the onset of international terror, the greatest challenge to present security (pp. 74–75). The potential risk of cyber attacks is vast, ranging from threats to nation states to personal identity and data to corporate finances and well-being.

In 2017 alone, numerous corporations suffered as victim to major cyber attacks, including health service networks across England and Scotland, the HBO television network, and Equifax Inc. (BBC News, 2017; Bernard et al., 2017; Kharpal, 2017). In 2016, cyber attacks occurred on the following corporations: Voter records; The Wendy's Company; U.S. Department of Homeland Security, Federal Bureau of Investigation; Verizon Enterprise Solutions; LinkedIn; Myspace; Noodle & Company; Democratic

[10] Gabriel Weimann is a professor of communication at the University of Haifa, Israel and holds the position senior fellow at the United States Institute of Peace. His writings are inclusive of modern terrorism, political campaigns, and the mass media (Weimann, 2004, para. 10). Today, he continues writing on cyber terrorism.

National Committee; Voter Information; CiCi's Pizza; Citibank; Dropbox; Banner Health; Oracle MICROS; Yahoo Inc.; SS&C Technology; Dyn (Twitter, Netflix, and *The New York Times*); U.S. Department of the Treasury, Office of the Comptroller of the Currency (OCC); Friend Finder Networks (Walters, 2016). As contemporary society relies more steadily on computerized technology, the American Power Grid Systems are likewise vulnerable to cyber attacks from hackers (Condliffe, 2017, para. 1). Nations, communities, corporations, and individual persons are at risk to become a victim of the numerous cyber attacks, and this environment of anxiety and peril has produced what has been termed an era of cyber terrorism (Weimann, 2015). Cyber terrorism mirrors the intents of terrorism in the physical world—to instill fear, to coerce, and to recruit (Minei & Matusitz, 2013; Weimann, 2015). The remainder of this section surveys debates about the existence and nature of cyber terrorism as the culmination of cyber threats.

This project resonates with the contention of Maura Conway[11] (2014), who suggests that despite the contentious dispute enveloping whether cyber attacks meet the criteria of cyber terrorist acts, they merit attention and thought (p. 103). Conway turns to definitions of cyber terrorism from Dorothy Denning[12] (2007) and Mark M. Pollitt[13] (1998) to place cyber terrorist acts as premeditated and politically motivated attempts at

[11] Maura Conway is an Irish scholar studying the intersections between terrorism and the Internet. Currently, she holds the position of Professor in International Security in the School of Law and Government at Dublin City University (DCU) in Dublin, Ireland. She is also the coordinator of VOX-Pol, a project funded by the European Union examining the violent implications of participating in online political extremism. Conway has authored over 40 articles and chapters in her area of scholarly inquiry.

[12] Dorothy E. Denning is Emeritus Distinguished Professor of Defense Analysis at the Naval Postgraduate School. She has also held positions at Purdue University and Georgetown University. Her research interests include cyber security and cyber conflict. Denning's expertise on issues of cyber security warranted her inclusion into the inaugural inductees of the National Cyber Security Hall of Fame ("Dorothy Denning," n. d.).

[13] Former military officer and FBI Special Agent Mark Pollitt spent 30 years investigating organized crime, narcotics, stolen property, white collar fraud, and cyber crime. Currently, he teaches at Syracuse University and serves as president of Digital Evidence Professional Services and on the National Institute of Standards and Technology (NIST), Organization of Scientific Area Committees (OSAC), and Digital and Multimedia Sciences Scientific Area Committee ("Pollitt," 2018).

the data destruction of noncombatant targets. Weimann (2008) further acknowledges the dual purpose of the Internet as a platform for terrorists to coordinate and execute plans, as well as launch cyber attacks (pp. 74–75).

Conway argues that there have been no acts of actual cyber terrorism as of 2014 and considers the likelihood of such events low; however, she recognizes the importance of acknowledging the destructive potential of cyber threats and warns that if an act of cyber terrorism were to occur the implications would be devastating. Specifically, Conway identifies four reasons why kinetic attacks to physical matter better fulfill an intent to harm than cyber terrorism: (a) cyber attacks are more expensive and thus impractical; (b) terrorist organizations lack the cyber expertise to carry out such assaults; (c) cyber terrorism is rendered less destructive and rapid; and (d) cyber terrorism is less theatrical (p. 107). She reviews the existing conversation/controversy surrounding cyber attacks focusing on a cyber attacker's intent to harm rather than the technological practices engaged by the hacker.

Conway's work builds upon a conventional understanding of terrorism aimed toward physical matter and two foundational definitions of cyber terrorism. First, she aligns cyber terrorism with conventional kinetic terrorism—characterized by a "political motive" and "violence or the threat of violence" (p. 105). Second, she turns to cyber terrorism as distinct by referencing two leading definitions. The earliest definition referenced by Conway relies on Mark M. Pollitt, who writes in 1998. Pollitt positions terrorism within the realm of cyberspace aimed toward disrupting the functions of computer programs and data. He employs the Section 2656f(d) in Title 22 of the United States Code to understand cyber terrorism, like physical terrorism, as "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents" (Pollitt, 1998, p. 9). Then, Conway considers a later definition, taken from Dorothy E. Denning, in 2007, which Conway recognizes as the "most well-known and respected" (p. 105). Denning understands cyber terrorism as:

> highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act. Rather than committing acts of violence against persons or physical property, the cyberterrorist commits acts of destruction and disruption against digital property….To fall in the domain of cyberterror, a cyber attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism, and it must be conducted for political and social reasons. Critical infrastructures…are likely targets. Attacks against these infrastructures that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or billion dollar banking losses would be examples. (Denning, 2007, p. 124)

Denning's definition articulates the cyber terrorist act as the attempt to destroy or disrupt digital property for the purpose of advancing a political or social objective. Particularly, Denning stressed a reflection of physical terrorism within a virtual context, a political motive, and a threat to physical harm or injury. Denning's reflections on cyber terrorism

(2001; 2007) illuminate the work of Barry Collin,[14] who first addressed cyber terrorism in the 1980s. Denning emphasizes Collin's focus on cyber terrorism as "premeditated," "politically motivated," and "violen[t] against noncombatant targets by subnational groups or clandestine agents" (Denning, 2001, p. 281). Denning's definition is more extensive than that of Pollitt or Collin, but important common denominators include that cyber terrorism involves premeditation and the politically motivated destruction of noncombatant targets.

It is important to note that Denning's 2007 definition builds upon her earlier work that frames cyber terrorism as an extension beyond the movement from activism to hacktivism[15] (Denning, 2001, p. 241). Denning (2001) contends that as activism transforms to hacktivism and then to cyber terrorism, the level of severity and intent to harm increases in intensity and threat. The activist employs a "normal, nondisruptive use of the Internet," advocating to advance a particular belief system or movement (p. 241). The hacktivist emerges in the interplay between "hacking and activism" (p. 241). With hacktivism, Internet use becomes abnormal and disruptive while still maintaining allegiance to support a cause (p. 241). The cyber terrorist melds "cyberspace and terrorism," engaging networks as places for the disruptive actions of attack, recruitment, or the spread of fear (p. 241). The cyber terrorist's actions become increasingly

[14] According to Denning, Collin is "a senior research fellow at the Institute for Security and Intelligence in California" (p. 242).

[15] Denning's contribution is included within the work *Networks and Netwars*, edited by John Arquilla and David Ronfeldt (2001). Arquilla and Ronfeldt describe in the preface that the "fight for the future" has shifted from armies of rival nations confronting one another to the small, nimble operations of terrorist groups, drug cartels, and militant anarchists who can, thanks to computer and information technologies, deploy themselves at anytime from anyplace (p. v). They clarify a distinction between cyberwar, carried out in the military domain, and netwar, activities occurring outside of the military domain that represent an "irregular mode[] of conflict" conducted by terrorists, criminals, and social activists (p. v). While published on October 26, 2001 (following the 9/11 World Trade Center attacks), the impetus of this work emerged from an extension of the netwar concept, introduced by Arquilla and Ronfeldt (1996). Certainly, the online activities contributing to the World Trade Center tragedy increases the need for such examination of online terrorist activity.

destructive, disruptive, and violent; however, Denning argues that the cyber terrorist is actually less likely to advance the cause or foreign policy objectives and instead will most often only lead to bolstered cyber security (p. 242).

Denning (2001) describes both commercial and government systems as equally vulnerable to cyber attacks, and despite efforts to increase cyber security, there is no indication of stronger defense (p. 287). Denning implies that cyber attacks operate within an unending pattern of attack-defense, stronger attack-stronger defense. According to Denning, an act of cyber terrorism does not occur from simply hacking computer software; she reserves this term for an instance where the cyber attack results in the politically-charged violence associated with conventional terrorist acts on physical structures. For instance, if cyber criminals were to hack into the computer software of an airplane, it would not be an act of terrorism unless they were successful in hijacking the plane to harm people and physical structures. Thus, Denning, writing in 2001, believes that there are "no reported incidents" of cyber terrorism, yet the threat had a "significant" influence on strategies for national defense (p. 288).

Susan W. Brenner[16] (2007) contends that the classification system used to determine actions following a kinetic attack should inform the classification system guiding responses during cyber attacks. Brenner understands a cyber attack as the use of computer technology to "undermine[] a society's ability to maintain internal or external order" (p. 381). Her work builds upon the internal-external threat dichotomy used to classify kinetic attacks (p. 381). In response to an internal threat, authorities would follow

[16] Susan W. Brenner is the Samuel A. McCray Chair in Law at the University of Dayton School of Law. Her research specializes in grand jury practice and various contexts of cyber conflict ranging from crime to terrorism ("Susan W. Brenner," n. d.).

the “proscriptive rules” structuring society, and in response to an external threat, authorities would rely upon “military force” or “international agreements” (p. 382).

This internal-external dichotomy also pertains to issues of origin, attribution, and jurisdiction. Specifically, Brenner (2007) considers the “attacker-attribution” and “attack-attribution” (p. 405). The former identifies who is responsible for the attack and the latter who ought to respond to the attack. The attacker-attribution involves locating the attack’s point of origin (i.e., ISP address) and target destination (i.e., government or privately-owned corporations). The “attack-attribution” corresponds with conventional policies for law enforcement jurisdiction (i.e., governed by county, state, and national borders as well as perceived motives) (p. 405). However, identification processes become increasingly difficult as cyberspace “erodes” traditional borders and obscures the well-defined distinction that military personnel respond to acts of war while law enforcement officers respond to criminal activity (p. 438). The difficulty within this identification process emerges from the “mixed-motive scenario” that often characterizes cyber attacks—hackers gain information in cyber crime (to which law enforcement officers would traditionally respond) that fuels cyber war efforts (to which military personnel would traditionally respond) (p. 438). Thus, we are left to navigate the uncharted territory of various forms of cyber attacks, ranging from crime to terrorism.

Brenner (2007), likewise, denies a documented occurrence of cyber terrorism but recognizes the seriousness of the threat of using cyberspace as weapons of mass destruction, distraction, and disruption (pp. 389–398). Brenner considers the use of cyberspace as a weapon of mass destruction unlikely, following the logic that computers cannot physically harm victims. For instance, Brenner argues that a computer triggered nuclear bomb would be perceived and classified as a *nuclear* rather than *computer* disaster (pp. 390–391). The weapon of mass distraction involves a psychological manipulation of a population that undermines civilian faith in the government (p. 391). In such instances, terrorists would use the computer as the primary weapon to wreak havoc and panic by distributing fake messages that are deemed credible as if they were sent from government officials (pp. 391–393). Finally, Brenner categorizes cyber terrorism as a weapon of mass disruption, where terrorists would undermine society's "faith in the stability and reliability of essential infrastructure components" (p. 393). The weapon of mass disruption might attack "mass transit, power supplies, communications, financial institutions, and health care services" (p. 393). These attacks would "demoralize" civilians by causing them to "question the government's ability to keep things working" (p. 394). Ultimately, Brenner considers cyber attacks to appear most often as either a weapon of mass distraction or of mass disruption (p. 398).

For Brenner (2007), these classifications help authorities to understand the nature of the attack and to guide action responses. Appropriate responses require engaging the "distinct and evolving nature of the threats we face," creating appropriate strategies for each new evolving threat (p. 475). Particularly for responding to cyber terrorism, this would involve "integrating," note not "fusing," military and law enforcement personnel (p. 456). For cyber terrorism, in particular, this would involve the military assisting law enforcement officers in confirming that a cyber attack either "has occurred or is in progress; and ascertaining the nature of the attack" (p. 460). Ultimately, she contends that cyber attacks, regardless of their type, should be dealt with as crime rather than war (p. 398).

Similar to Brenner, Steven Bucci[17] (2012) advances the association of cyber terrorism with cyber crime. Bucci problematizes the Western tendency to post everything on the Internet, where the basic research skills of a child on a search engine can bring up information for attacks that would inflict maximal damage to an organization or community (p. 63). Technology is the "Achilles' heel" of the West and specifically new trends of "mobile computing, cloud computing, and the use of smart-grid technology" contribute to increased vulnerability for cyber attacks (pp. 65, 67). The technological reliance of the West creates a large target that becomes increasingly accessible to theft and destruction.

To understand this rising threat better, Bucci (2012) refers to cyber threats as the "new normal" and differentiates them into three tiers—low-level, medium-level, and high-level (p. 57). For Bucci, low-level cyber threats are committed by "individual hackers" and are not connected to any larger organization or infrastructure (p. 58). Medium-level threats include use of the Internet from terrorist organizations, cyber espionage, and organized crime (p. 59). High-level cyber threats are executed by the "full power of nation-states," as exemplified by the 2007 Estonia attacks, and could also accompany kinetic attacks (pp. 59–60). Bucci suggests that the Estonia attacks prompted NATO to recognize "the role cyber plays in national and collective defense" (p. 59). Bucci anticipates that the union of cyber terrorists and cyber criminals committing medium-level attacks will populate the future landscape (p. 60).

[17] Steven Bucci, a former Army Special Forces officer and top Pentagon official, now serves as a visiting fellow in The Heritage Foundation's Allison Center for Foreign Policy Studies. His research interests include cyber security as well as military special operations and defense support to civil authorities ("Steven P. Bucci," 2018).

Within Bucci's (2012) prediction, "limited" knowledge of writing codes will necessitate the cyber terrorist to join the criminal to actualize plans to harm within cyberspace (p. 62). In 2012, Bucci suggests that terrorists utilize cyberspace for "communications, propaganda, financial dealings (fund-raising and fund transfers), recruitment, and intelligence" rather than offensive tactics (p. 62). For instance, programs such as Second Life[18] allow cyber terrorists and cyber criminals to meet online in a hidden, legal platform that can be used to transfer money from account to account (p. 63). Bucci describes Second Life as a "deeply covered and protected" meeting point (p. 63). These online virtual worlds unintentionally create unregulated spaces for transactions and meetings that would be suspect or illegal in physical space. Bucci (2012) also counters and responds to the argument that acts of cyber terror are not as desirable because they lack a theatrical quality by acknowledging the "real fear" that would occur as "bank accounts are zeroed, electricity is absent, or water does not flow" (p. 66). Additionally, the combination of cyber and kinetic attacks could be massively destructive "regardless of one's definition" (p. 66). The psychological damage of cyber attacks can be traumatizing in a different way than kinetic attacks, but traumatic nonetheless.

The literature outside of the field of communication is essential for understanding the rising potential threats of cyber terrorism. This literature confirms the serious threat of cyber terrorism and calls forth our attention (Brenner, 2007; Bucci, 2012; Conway, 2014). As attacks rise in number, the question becomes how can we respond adequately. Although the "perimeter defense strategy" remains a primary response by governments and organizations, the sustainability and long-term success of such defenses is inadequate

[18] Barbara Mitra and Paul Golz (2016) describe Second Life as an Internet-based "3D graphical environment" virtual world that allows users to "construct an avatar and interact through a variety of mechanisms, such as flying, walking, driving, teleporting and chatting" (p. 4).

and only leads to stronger cyber attacks. As early as 2001, Michele Zanini and Sean J. A. Edwards provide four initial methods to adequately respond to cyber terrorist attacks: (1) monitoring terrorist Information Technology use; (2) targeting information flows; (3) engaging better protection services; and (4) using networks to fight networks (pp. 52–54). In 2007, Brenner calls to engage cyber attacks as crime with an integration of law and military enforcement as the cyber attack erases traditional delineations between attack-attribution and attacker-attribution. The urgency of this issue and the lack of clarity in terms of how we talk about and perceive cyber attacks has garnered significant attention from the field of communication. The chapter now turns to the communication literature to understand adequate responses to cyber attacks.

Communication Literature Review

Communication scholars have also addressed the urgency and rising risk of cyber threats and the potential for cyberspace to become a site for terrorist action (Klein, 2015; Minei & Matusitz, 2013; Stahl, 2016; Walker, 2007; Weimann, 2005, 2006, 2008, 2015). This section frames cyber terrorism within the field of communication, focusing on the possibility of and debate surrounding terrorist use of the Internet for acts of violence, theft, recruitment, and identity formation. The nature of cyberspace and our increasing reliance on it for facilitating the smallest and greatest human needs and desires demands attention from the field of communication as the increasing risks related to cyber terrorism continue to threaten social, corporate, and individual realms of human life.

Roger Stahl (2016) describes the rhetorical framing of cyber terrorism as a part of the weaponization of speech within the "information bomb" (pp. 378–379). Stahl identifies the weaponization of language present within the public discourse of numerous presidential administrations—for instance, Lyndon B. Johnson's "War on Poverty," Ronald Reagan's "War on Drugs," and George W. Bush's "War on Terror" (p. 380). For Stahl (2016), this "War on…" metaphor exemplifies the problematic implications of weaponized speech.

Specifically, he locates the Clinton administration as the origin point for the public use of the term "cyberterrorism" as a weaponized form of speech (p. 380). Stahl recounts Clinton's use of the phrase, popularizing it within speeches between 1998 and 1999 (pp. 380–381). He references Carol K. Winkler to express how Clinton's use of cyber terrorism, much like earlier instances of weaponized speech, referred to a broad concept lacking vernacular agreement. Inherent within Clinton's rhetoric was the recognition that cyber terrorism utilized computer technologies to interfere with social structures, but the phrase encompassed a vast spectrum of illicit online activities from hacking to credit card fraud to organized crime to acts of warfare (p. 381). Clinton moved cyber terrorism from passive consideration of a hypothetical "what if" scenario with low likelihood of actualization to a high level concern that urgently demanded political policy and response (p. 381).

Despite Clinton's rhetoric, however, Stahl contends that security experts have yet to deem any cyber attack as an instance of cyber terrorism and have not recognized cyber terrorism as an active strategy for any known terrorist organization (p. 381).[19] Stahl understands cyber terrorism to occur when compromised computer software becomes the means by which someone carries out a terrorist act. For instance, when referencing

[19] Note: Stahl is not recognizing recruit as a strategy for cyber terrorism although other scholar place recruitment within this scope (Minei & Matusitz, 2013; Weimann, 2006).

Ronald Deibert,[20] Stahl writes: “the expertise necessary to ‘bring down the grid’ with a cyberterrorism attack by a nonstate actor is simply not worth the investment when box cutters and gasoline bombs do just as well” (p. 381). Like Conway, Denning, Pollitt, Deibert, and others, Stahl contends that cyber terrorism would only occur when cyberspace would become the means by which to carry out a terrorist attack—cyber terrorism would not emerge until cyberspace becomes the planes that brought down the Twin Towers, the bomb that exploded at the Boston Marathon, or the vehicles used to drive into crowded city streets. Unlike Clinton whose rhetoric of cyber terrorism includes fraud, identity theft, hacking, computer viruses, and threat of much more, these scholars work from a narrowed scope for cyber terrorism. The public discourse expressing a constant and urgent threat of cyber terrorism exemplifies the weaponization of speech, for Stahl, as social anxiety and hype supersede any instance of cyberspace to be used as the means for an act of terror.

Stahl (2016) argues that popular culture, journalism, and media outlets reinforce the weaponized perception of cyber terrorism (p. 381).[21] Together, these sources construct the “rhetorical scaffolding” that supports, upholds, and justifies information as “a rightful object of military control in the War on Terror” (p. 381). Fictional media contributes to a rhetorical situation where citizens increasingly fear the impending threat and possibility of cyber terrorism. For Stahl, cyber terrorism is a rhetorical construct that

[20] Ronald Deibert, Professor of Political Science and Director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto, co-founded and co-funded the OpenNet Initiative (2003–2014) and Information Warfare Monitor (2003–2012) projects. Also, Deibert was former Vice President of global policy and outreach for Psiphon, a leader in opposition to digital censorship (“Ronald Deibert,” n. d.).

[21] For more on the “rhetorical scaffolding” of cyberterrorism in the infosphere, see Michael Stohl (2006). In this article, Stohl examines the relationship between cyber attacks and their portrayal in literature by authors such as Tom Clancy. For Stahl, the writings of Tom Clancy would likewise contribute to the “information bomb” and rhetorically situate the defense of cyberspace under military control in the War on Terror.

arms the information bomb, facilitating the use of communication as a weapon and targeting both citizens and communication professionals. The rhetorical environment of the War on Terror "legitmate[s]" the weaponization of speech within the practices of discourse by U.S. citizens and officials (p. 389). The ways in which we speak, describe, and understand the world creates an environment that frames communication as a weapon. Stahl urges us to "defuse" the information bomb by reflecting on how our public discourse "shap[es] and underwrit[es] certain theoretical trends" (p. 390). The way that we describe and explain the world around us undergirds how one comes to understand it. Stahl contends that careful and critical reflection on cyberspace and terrorist activities will render a clearer understanding of the rhetorical mechanisms propelling the information bomb (p. 390).

Weimann does extensive work on the question of cyber terrorism from the communication perspective. In his early work, Weimann (2005) resonates with Stahl's (2016) contention that there have been no documented, "real" instances of cyber terrorism (p. 130). Weimann writes that although the threat of cyber terrorism may be high for Western societies who often network their "critical infrastructure[s]" through cyberspace, low-level and relatively harmless hacker activities are misnomered as terrorist activity (p. 130). As of 2005, no actual cyber attack was associated with cyber terrorism. However, the threat of cyber terrorism merits a response that distinguishes between the "real significance" of these activities and the fear such a misnomer initiates (p. 146). The potential crippling nature of cyber terrorism must be addressed and responded to without "manipulating" the population about the actual (in)frequency of such acts (p. 146).

In *Terror on the Internet: The New Arena, the New Challenges*, Weimann (2006) writes in response to the “sophisticated terrorist presence on the World Wide Web” that contributed in part to the September 11, 2001 attacks on the World Trade Center (pp. 3–4). Weimann’s research draws from a 1998–2005 “monitoring and archiving” of terrorist web sites and Pew Internet and American Life Project public surveys (p. 4). Weimann describes the Internet as an “ideal arena” for terrorist organizations to communicate (p. 22). A first advantage offered by the Internet and computer-mediated communication is the free and easy transmission of messages (pp. 6–7). A second advantage is the Internet’s mutability; in other words, when a website is taken down, another may readily appear from “other service providers, new URLs, and new formats” (p. 8). Cyberspace acts as an ideal platform for terrorist activity due to the low price, high speed, and ability to construct and reconstruct sites when/as needed.

Weimann (2006) indicates four terrorist uses of cyberspace. First, terrorists employ the Internet for “propaganda” (p. 7). Second, terrorists engage the Internet to disseminate messages (p. 7). The third terrorist use of the Internet is “psychological warfare” (p. 7). Finally, Weimann suggests terrorists employ the Internet for the seven instrumental purposes of: (1) “information gathering”; (2) “hiding instructions, manuals, and directions in coded messages or encrypted files”; (3) “sharing and distribut[ing] information, instructions, manuals, and guidebooks”; (4) “networking terrorists, coordinating attacks, and planning actions”; (5) “to recruit and mobilize supporters”; (6) “to raise funds”; and (7) “as a battlefield between and within terrorist organizations, which use the Net to conduct ideological debates or even personal disputes and internal power struggles” (pp. 9–10). While no act had been labeled cyber terrorism, Weimann recognizes that the threat of cyber terrorism merits attention and response, without inflation or manipulation (p. 10).

In response to this threat, Weimann (2006) documents efforts that counter cyber terrorist use. As of 2006, Weimann describes that counterterrorism efforts were directed at determining where the terrorist networks where located, who were conducting the terrorist attacks, and, if an unwanted transfer of money occurred, determining where and how that money was transferred (p. 11). In the United States, counterterrorism measures specifically involved email monitoring, removing certain websites, and offensive cyber attacks directed toward terrorist web sites (p. 11–12). Weimann recognizes that the offensive cyber attacks were "relatively futile attempts" to limit terrorist influence online (p.12). Weimann then cautions that the "digital war on terrorism" threatens the civil liberties protected by modern democracies (p. 12). This sentiment is echoed in Weimann (2008), where a call is made for information monitoring to respond to cyber terrorism, but a monitoring that does not compromise civilian liberty—a fundamental value upon which West was founded (pp. 82–83).

Weimann (2006) also notes "missed opportunities" resulting from the demonization of the Internet as a "terrorist tool" (p. 12). A first missed opportunity is employing the free, fast, and easily-accessible web to construct nonviolent advances of "policy objectives" and "political grievances" (p. 12). A second missed opportunity is "virtual diplomacy," or employing the Internet to support "good governance" and manage or mitigate "international conflicts and crises effectively and expediently" (p. 12). To help the realization of these objectives, Weimann offers "policy recommendations" (p. 13). The major policy recommendation begins with the realization that terrorism *ipsum* has occurred for centuries and, perhaps, cannot now be completely removed from the Internet. Instead, Weimann encourages users to limit terrorism and protect civil liberties by a search for the "'golden path,' or best compromise" (p. 13). Users can uncover the "golden path" by accepting "some vulnerabilities" of terrorism and "some constraints on civil liberties" (p. 13). Weimann encourages that the "golden path" can be found through: (1) modifications to the USA PATRIOT ACT; (2) the encouragement of "self-policing"; (3) an application of "social responsibility"; (4) the development of "international collaboration"; (5) "building a proactive presence on the Internet"; and (6) "promoting peaceful uses of the Internet" (p. 13).

In *Terrorism in Cyberspace: The Next Generation*, Weimann (2015) continues his work on cyber terrorism and situates cyberspace as one of the most salient means of terrorist communications. This work explores new modes of cyber terrorism, what attacks we might anticipate, and means of countering current and future threats. Weimann turns to the 2013 report *Jihadist Terrorism: A Threat Assessment* from the Bipartisan Policy Center that highlights online self-radicalization as the foremost threat to homeland security in the United States. Additionally, Weimann turns to a Europol report from April 2012 that recognizes that dangers these threats pose to the European Union. Weimann documents acts of lone wolf terrorism in the following countries: Australia, Canada, Denmark, France, Germany, Italy, the Netherlands, Poland, Portugal, Russia, Sweden, the United Kingdom, and the United States. Weimann documents the changes in the cyber landscape and the emergent threats of 2015.

Weimann (2015) echoes his 2006 contention of the Internet's potential for, but current failure to, protect and promote peace. Again resonating with his 2006 search for the “golden path” to lessen terrorism on the Internet, Weimann recognizes that major government agencies worldwide understand the Internet’s potential as a tool and as a weapon. Weimann contends a major challenge in responding to cyber terrorism on the Internet lies in the protection of free speech in the United States and around the world. While counterterrorism measures have legal and practical implications, strategies for response lack a clear path to resolution.

Elizabeth Minei[22] and Jonathan Matusitz[23] (2013) offer a contrary view of cyber terrorism that presupposes its existence and active use. They identify three central practices of cyber terrorism actively engaged today: recruitment, communication, and propaganda (p. 267). Minei and Matusitz recognize cyber terrorism as present prior to any actualized kinetic violence, corruption, or theft. For them, the goal of the cyber terrorist aligns with that of the kinetic terrorist—to instill a sense of fear and anxiety through images and communication that “frighten and coerce” (p. 278). Not only does cyberspace provide a platform for distributing these fear-mongering messages but also it affords an outlet for terrorist organizations to connect, to recruit new members, and to research information legally that informs how attacks (kinetic or via cyberspace) can ensure maximal damage (pp. 275–276). The Internet advances acts of cyber terrorism already in action by offering a platform for message circulation across a wide audience, aimed toward strengthening existing communication channels that have the potential to recruit new members.

[22] Minei is an assistant professor of communication at Baruch College. Her research interests span “leadership, high-reliability organizations, small-group/team communication, entrepreneurial issues, globalization and glocalization, and cyberterrorism” (“Elizabeth Minei,” n. d.).

[23] Matusitz is associate professor in the Nicholson School of Communication and Media at the University of Central Florida. His research addresses “the role of communication in terrorism, symbolism in terrorism, the globalization of culture, and health communication” (“Jonathan Matusitz,” n. d.).

Although no cyber attacks have been labeled acts of cyber terrorism (Stahl, 2016), terrorists can utilize the Internet for purposes of spreading fear, forming identity, recruiting, attacking, or preparing for an attack (Minei & Matusitz, 2013; Weimann, 2006). A gap in the literature lies between the definition of cyber attack versus terrorist use of cyberspace for communication. The increasing reliance of modern society to depend upon the instruments of cyberspace for their slightest need is creating a digital risk society (Lupton, 2016). Scholars in the field of communication do well in raising various areas of concern in relation to the rising levels of cyber attacks. Following Stahl's call to examine the functions at work in the information bomb, the next segment of the chapter examines scholarship that frames the theoretical movement from wicked problems to wicked crises. This investigation creates a textured ground to understand the goods at play in the wicked problem of cyber attacks and facilitates a platform for adequate responses.

Cyber Attacks as a Wicked Crisis

In recent years, "wicked problems" have received scholarly attention from the field of communication (Carcasson & Sprain, 2016; Coombs & Holladay, 2018; Gerding & Vealey, 2018; Grint, 2010; Langellier, 2013; Maier & Crist, 2017; Wickman, 2014; Willis, 2016). This section of the chapter reviews pertinent literature that articulates the theoretical emergence of "wicked problems" (Rittel & Webber, 1973) and their evolution into "wicked crises" (Maier & Crist, 2017). This section draws upon the work of Horst W. J. Rittel and Melvin M. Webber (1973), who first introduced the notion of a "wicked problem," as well as Keith Grint (2010), who considers response strategies for both "wicked" and "tame" problems, and Craig T. Maier and Jonathan Crist (2017), who articulate the move toward wicked crises. This literature attempts to understand social issues that lack apparent or easy solutions, to emphasize the necessity to properly identify a wicked problem, and to open possibilities for addressing these issues at their sources rather than their symptoms.

Rittel and Webber (1973) introduced the idea of a "wicked problem" and contrast it with a "tame problem" (p. 160). They characterize a tame problem as one with known and obtainable objectives that illuminate a path for solution and response. For instance, a tame problem might be represented by the attempt to "accomplish checkmate in five moves" (p. 160) or an electric company's efforts to bring back power after a wind storm; tame problems offer a clearly delineated paths to resolve the issues and are replicable in recurring instances. Wicked problems, however, have no known achievable objectives or "clarifying traits" (p. 160), making solutions to wicked problems shrouded in ambiguity. For example, a wicked problem might be global climate change, bio-hazards, or the widespread addiction to opioids. Wicked problems lack response protocol, precedence, consistency, and clarity of source or response. Furthermore, wicked problems affect a wide audience holding diverse values, making universal response seemingly impossible as solutions that satisfy some will inevitably compromise and displace the needs and values of others (p. 169).

Rittel and Webber (1973) identify ten characteristics that mark wicked problems. First, wicked problems lack a "definitive formulation" (p. 161). That is, one might identify a problem, but its scope, breadth, and connotations cannot be contained. Second, wicked problems lack a "stopping rule" (p. 162), or clearly defined end point. Third, wicked problems require ethical consideration rather than simply practical solutions—

responses to wicked problems exist within the scope of “good-or-bad” rather than in the clearly determined realms of “true-or-false” (p. 162). Fourth, an “ultimate test” of immediacy cannot measure the success of responses to wicked problems (p. 163); the sustainability of long-term implications outweighs short-term fixes. Fifth, wicked problems are serious by nature and offer little room for “trial-and-error” (p. 163)—inappropriate responses could have devastating consequences. Sixth, appropriate responses to wicked problems emerge from a narrow and finite realm of action rather than an infinitely broad scope of possible solutions (p. 164). Seventh, wicked problems are “unique” by nature and thus resist commodification and universally applied responses (p. 164); when responding to wicked problems, one must fight against the temptation to mistake *this* for *that*. Eighth, the origin point of the wicked problem is difficult to ascertain; the roots of wicked problems often run much deeper than our perceived awareness, allowing us to misappropriate symptoms as causes (p. 165). Ninth, the language used to describe wicked problems shapes the social understanding of the issue; thus, inherently within the way we speak about these issues are hints toward response strategies (p. 166). Finally, those tasked with attempting to solve the wicked problem bear significant and serious responsibility and, according to Rittel and Webber (1973), have “no right to be wrong” (p. 166). The definition of the wicked problem, like the wicked problem itself, is multifarious and complex.

Grint (2010) textures Rittel and Webber’s work on wicked and tame problems by offering response strategies, in addition to what Grint terms “critical problems,” or “cris[es]” (pp. 307–308). Grint characterizes critical problems as “self-evident” and often equated beside “authoritarianism,” as there is neither “time for decision-making and action” nor “uncertainty about what needs to be done” (p. 308). Grint emphasizes the association between how we classify an issue and the response strategies engaged. For resolution, tame problems require the “same process” which caused the problem; there is no change in response procedure because the known and desired resolution is obtainable. The tame problem is bound to repeat itself because the problem has not been addressed at the source. The resolution of wicked problems, however, often merits a “delay”; due to the complexity, breadth, and ambiguity of the problem, “consultation and collaboration” are pursued to a point of inactivity. For Grint, critical problems necessitate “decisive commands” for resolution; there is not time for collaboration and the steps to resolution are evident (p. 307). Grint suggests an “addiction” to a particular label can skew public understanding of an issue and limit opportunities for appropriate responses (p. 307). According to Grint, an obsession with classifying problems obscures the ability to recognize their sources and respond with thoughtful strategies.

Grint (2010) contends that if we are to misname a wicked problem as tame or vice versa, then we will undoubtedly employ inadequate response strategies. What is needed to respond to a wicked problem will not solve a tame problem, and likewise, strategies for tame problems will not curtail the wicked problem. Grint explains that “elegant” responses are best suited to the tame and critical problem alike, but are often misapplied to the wicked problem, to which the “clumsy solution,” of Marco Verweij and Michael Thompson (2006), is optimal (pp. 309–310). The “elegant” response is “internally consistent,” proven to have previously worked, and applicable to problems with identifiable objectives (p. 309).

For instance, when attempting a checkmate in five moves, elegant responses would advise positioning the queen piece a knight's move away from the opposing king or the "Blitzkrieg" strategy. The "clumsy solution" has no such clarity for piece positioning or movement and rather develops an "experimental method" from a "wide range of otherwise contradictory policies and cultures" (p. 309). The clumsy solution to a wicked problem recognizes the ambiguity involved in the many connected angles of the problem and explores new ways for piece positioning on the board. Grint suggests that we are addicted to "elegance" in remedying critical, tame, and wicked problems alike (p. 310). However, an elegant response is not always the best solution to a problem—a simple solution to a complex problem will not resolve the problem at its source and may further complicate it. For Grint, world leaders are "addicted to command" with the imposition of elegant responses to all problems and "allergic to leadership" for not identifying and responding to the problem for what it is (p. 310). Grint calls us to remember the importance of problem identification by listening to the problem at hand and determining the appropriate response strategy, setting the stage for Maier and Crist's (2017) "being-in-crisis."

Maier and Crist (2017) introduce the concept of a "*wicked crisis*" within the context of the clergy abuse crisis in American Roman Catholicism (p. 165). Particularly, they use the phenomenology of Jean-Luc Marion and suggest his responsive witness provides a way of "being-in-crisis" to understand ways in which wicked crises may be understood (p. 172). Rather than engage Marion's phenomenology, this project is concerned with how the wicked crisis aligns with the rising threat of cyber terrorism. Maier and Crist define a wicked crisis as being composed of "events so intractable and threatening that they leave even the best leaders speechless and the most prepared organizations grasping for answers" (p. 165). Immediately, this sentiment resonates with cyber terrorism, as definitions and responses are multifarious, ever changing, and shrouded in ambiguity. As such, leaders are not sure how to define and adequately respond to the phenomenon of cyber terrorism.

Maier and Crist (2017) differentiate a wicked problem from a wicked crisis in that problems fall to "strategic planning or leadership" and crises show a problem has created "expectancy gaps" for stakeholders and mobilizes them to unpredictably and dangerously "act publicly against the organization" (p. 170). Again, a wicked problem has "multiple causes and effects" and affects "numerous stakeholder groups with widely divergent interests and grievances" (p. 170). Similarly, a wicked crisis might affect everyone, but in terms of "different and completely incommensurable reasons" (p. 170). The multifarious head of the wicked crisis makes resolution difficult if not impossible. Maier and Crist (2017) characterize the wicked crisis in three ways: they are (1) "unpredictable, ill-defined and swiftly mutating"; (2) only remedied by "clumsy" solutions; and (3) capable of eroding public trust (p. 170). A wicked crisis moves past the wicked problem in complexity, instigating public action against the organization or institution from which the crisis originates.

Cyber terrorism meets each of the three criteria of the wicked crisis. First, cyber terrorism is ambiguously defined and rapidly changing as definitions range from its occurrence to nonoccurrence, intent to harm and intent to recruit. Additionally, cyber terrorism swiftly evolves when the point of attack origin becomes difficult to trace through multiple shattered shards of cyberspace and motivation becomes a key determinant for the nature of the attack. Second, solutions to cyber terrorism are clumsy and temporary. Last, the most viable attack strategies for cyber terrorists aim to disrupt public life, casting doubt on our governments, businesses, institutions, and public services from transportation to health care. Maier and Crist end their article with future research possibilities for study considering wicked crises, asking, "How can they [organizational leaders] allow wicked crisis to 'speak' in all its complexity?" (172). The contention of this project is that communication ethics can add coordinates to "being-in-crisis," allowing crises to speak in all their complexity, and guide a response and understanding to cyber terrorism.

Project Overview

This project contends that an understanding of the goods at stake in cyber terrorism will shape adequate and lasting responses. Communication ethics literacy acts as a methodology to uncovering these goods as they are situated within the complex and dialectical nature of cyberspace. This section provides a brief overview of communication ethics as the methodology of this project, introduces the dialectical tensions that structure the remaining chapters of this dissertation, and ends with a note on significance of this theme.

Arnett, Fritz, and Bell (2009/2018) offer an understanding of communication ethics literacy that hinges upon the protection and promotion of a good in an era of contending goods. Their understanding of communication ethics revolves around coordinates of "difference, learning, and dialogue" (p. xx). Difference is significant to communication ethics because it recognizes the multiplicity of goods that are in contention in this historical moment. What one person protects and promotes, another may disregard, and each good may be a valid way of engaging the world. Learning in communication ethics is a "minimal sense of the good" (pp. xiv–xv). When committed to learning, diversity of perspectives will creatively and constructively clash as one perspective enlightens another. Dialogue, which cannot be demanded, creates the environment necessary for sharing goods; when people seek to listen, rather than tell, the potentiality for understanding emerges.

Arnett, Fritz, and Bell McManus (2009/2018) situate communication ethics as a "pragmatic necessity" to navigate an era of contending goods. Communication ethics, however, requires our attentive reflection. If we fail to reflectively engage practices, we may act in ways that do not protect and promote the goods we aspire to advance. Goods order one's life and provides an understanding of what is proper "to be and do" (p. 3). Arnett, Fritz, and Bell McManus describe that communication ethics does not begin with answers, but rather with the attempt to collaboratively discern "what might work in a given situation" (p. 8). Communication ethics does not tell one answer that is "right" for multiple situations, but attempts to understand and navigate the goods in tension (p. 10).

Arnett, Fritz, and Bell McManus offer a definition of communication ethics influenced by an applied philosophy of communication. Philosophy of communication works from a *praxis* approach that supplies a *why* behind the *how*; communication ethics lies at the juncture of philosophy of communication and applied communication, responding to the questions emerging within historical moments and the corporately agreed upon stories and practices that comprise narrative ground (Arnett, Fritz, & Bell McManus, 2009/2018, p. 41). This project's communication ethics approach seeks to follow the dual emphasis on philosophy of communication and applied communication when responding to cyber threats that culminate in the devastating potential of cyber terrorism.

Communication ethics calls us to learn about the different goods people protect and promote. By engaging learning as a minimal point of agreement, we can understand the *why* behind the *how* of the attacks. From a communication ethics perspective, goods are present from the perspective of cyber terrorists as well as their targets. An effort to learn these goods from a communication ethics perspective becomes a catalyst for re-imaging cyberspace and its influence on the various realms of human existence. Cyber terrorism, as a wicked crisis, is ambiguously defined, constantly evolving, unresolvable, and erodes faith in public institutions. We find difficulty in identifying cyber attack points as well as determining responsible actors. Motivation becomes a key for identifying and labeling cyber attacks and attentiveness to background goods prompt learning that creatively informs response strategies. Thus, by engaging communication ethics as a path to understand cyber terrorism, we can understand the goods at play in the lives of terrorists and civilians alike.

This dissertation pursues this communication ethics analysis in six chapters. Chapter 1 situates the history of cyberspace as a platform for cyber threats, considers the degree to which cyber terrorism exists today, and frames cyber terrorism as a wicked crisis. Chapter 2 positions cyberspace as dialectical, reviews salient schools of thought related to dialectic, and introduces the key dialectics that structures chapters 3 through 5. Chapter 3 examines the tension between understanding cyberspace as a public versus private realm within the context of cyber bullying as a significant form of cyber attack. Chapter 4 engages the dialectic of anonymity and identity as it relates to our use of cyberspace for data storage and its invitation to fraud and identity theft. Chapter 5 explores the way in which cyberspace intersects a dialectic spanning national and global borders, specifically attending to instances of international interference and the potential for cyber terrorism. Finally, Chapter 6 articulates the implications of attending to the dialectics of cyberspace. Without attentive consideration, cyberspace becomes increasingly meaningless as we engage it without thought, thus increasing the vulnerability of society to cyber threats.

This project considers a communication ethics approach to cyberspace might open new possibilities for response to cyber attacks. I contend that new insight will emerge from an exploration of the dialectics of the public/private, anonymity/identity, and national/global realms of cyberspace and their implications for cyber attacks. This interpretative framework offers insight as it manifests from primary and secondary sources addressing communication ethics and the philosophy of technology. This project attempts to understand the evolving nature of cyberspace with a theoretical emphasis on dialectic. The dialectics explored in this inquiry represent existing threats that cyberspace poses to the public domain; however, new dialectics will become apparent as cyberspace continues to evolve. Thus, this inquiry offers a voice to texture the ongoing conversation attempting to understand cyberspace and cyber threats.

The significance of this study emerges as we continue to struggle to respond adequately to the rising problem and number of cyber attacks; the exigency of the project strengthens with the ever-evolving potential of cyber terrorism. By attending to and recognizing the various dialectics at play within cyberspace, the study points toward and critically considers the unacknowledged tensions that contextualize our engagement with cyberspace. The project recognizes the need for their simultaneous acknowledgment to engage cyberspace effectively as a first defense against cyber attacks. Furthermore, this study shows that a historical breadth and depth of philosophical and rhetorical thought contributes to an understanding of current technological engagement. Finally, the present work offers implications that inform personal and professional interactions as well as individual and group endeavors online.

A holistic understanding of the dialectics at play in cyberspace will facilitate a thoughtful and reflective engagement of the network. The present study, thus, adds to communication scholarship by demonstrating that (1) a recognition of the dialectics in cyberspace can facilitate a grounded engagement with the medium, (2) rhetoric and philosophy ought to inform an understanding of cyberspace, (3) a communication ethics analysis will identify divergent goods related to each dialectical tension, and (4) a perspective of cyberspace devoid of careful consideration will contribute to the fragmentation manifested by cyber attacks in the disruption of the user and environment.

Chapter 2

Cyberspace as Dialectical

Introduction

Cyberspace *ipsum* has become conflated in vernacular use with the Internet and the World Wide Web. This confusion between terms contributes to the ongoing opaqueness of cyberspace, which clouds the ability to respond adequately to cyber threats that become manifest in attacks of various degrees—cyber bullying, identity/corporate data theft, and cyber terrorism. This project contends that a recognition of the dialectical nature of cyberspace will illuminate communication ethics goods that can shape lasting and adequate responses to cyber threats.

This chapter makes three major turns. First, the chapter offers an historical and philosophical overview of dialectic from its origins in the ancient world to applications in the twentieth century. This tracing offers a textured ground to understand how dialectic can shed insight on the contradictions inherent within computer and information technologies. The second segment explores scholarship that applies dialectic to cyberspace, recognizing the continued merit of dialectic for illuminating present-day questions. The final section of the paper announces the dialectics pursued in this project—public/private, anonymity/identity, global/national. While these dialectics might be considered reductive of the overall contradictory nature of cyberspace, they are major representative themes for consideration when positioning communication ethics as a first response to cyber attacks.

This chapter attempts to depict cyberspace according to its characteristic dialectical tensions that will open possibilities to respond thoughtfully to cyber attacks, illuminating perspectives of communication ethics goods. Cyber threats fall along a continuum, with motivation being a key determinant in the scope and thus severity of an attack (Brenner, 2006; Bucci, 2012). Working from the acknowledgment that cyberspace is dialectical, this chapter introduces interpersonal (cyber bullying), corporate (cyber theft), and national (cyber terrorism) contexts through which attacks prevail. After introducing these contexts, the project proceeds by analyzing the communication ethics goods that uncover a *why* behind the *how* and that can shape lasting and adequate responses to quell these threats.

History of Dialectic

Dialectic has been an important concept for understanding communication and rhetoric since antiquity (Brownstein, 1965; Desmond, 1985; Gilbert & Lucaites, 2015; Janssens, 1968; Murray, 1988; Ngai & Singh, 2018; O'Hara, 2017; Sporer, & Toller, 2017; Suter & Norwood 2017; Young Lee & Nelson, 2018). Leslie A. Baxter and Barbara Montgomery (1996), in their seminal work *Relating: Dialogues & Dialectics*, clarify the significance of historical and philosophical perspectives of dialectic for interpersonal communication in their theory of relational dialectics. Their work provides an historical tracing of dialectic including the ancient thought of Socrates, Plato, and Aristotle, the progressive notions heralded by Hegel and Marx, and the dialogism of Mikhail Bakhtin. This section follows Baxter and Montgomery's work, reviewing the perspectives offered by each thinker and extending their work to include the insights of 20th century rhetorician Kenneth Burke. Burke's work is particularly helpful as it details the close linkage of dialectic and metaphor, which offers insight to respond to the confusion surrounding the various and conflicting metaphors used to describe cyberspace. This review provides a textured understanding of dialectic attentive to how this concept has changed across historical moments.

Baxter and Montgomery (1996) introduce the notion of dialectic with two basic approaches—dialectic-as-ontological or dialectic-as-epistemological. The ontological versus epistemological debate addresses how dialectics produce new insights from the emergent tensions between the seemingly contrasting viewpoints. As ontological, dialectic begins with the study of being, as represented by Chinese philosopher Lao Tzu and Greek philosopher Heraclitus. Both philosophers lived during the sixth century B.C.E. without any documented knowledge of the other's work (Baxter & Montgomery, 1996, p. 19). Ontological questions address what it means to exist. This school of dialectic grounds much Eastern thought and is apparent through the Yin-Yang symbol. Dialectics from an ontological standpoint considers the opposing forces of light and dark and how these two perspectives always exist in tandem: the seed of the dark being planted in the center of the light and the seed of the light being planted in the dark. Dialectics-as-ontology engage the contradictory tensions that define the meaning of being.

As epistemological, dialectic asks questions about knowledge and how we come to know. Thinkers such as Socrates, Plato, and Aristotle represent this tradition, which characterizes Western thought. The epistemological approach of these philosophers relies upon logical arguments working toward a transcendent truth revealed through discourse. This approach intends to destroy weaker arguments with the logic presented by a stronger argument. Baxter and Montgomery acknowledge that, although predated by Lao Tzu and Heraclitus, Socrates and Plato and their epistemological framing of dialectic are commonly recognized as the origin point for dialectical thought as a philosophical concept (p. 19). Although Socrates never embraced the written word, his work is represented through the Platonic dialogues. As such, this review of dialectic begins with Plato.

Plato lived in a historical moment characterized by Sophistic rhetoric that rejected an objective truth in favor of multiple subjective, relative, and little truths. For the Sophists, truth was a matter of the context; truth was revealed based upon those speaking within it and the audience to whom a rhetor spoke. Plato opposed Sophistry and likewise its view of rhetoric. Specifically, Plato (trans. 1987), in *Gorgias*, offers a critique of Sophistic rhetoric,[24] condemning it as "cookery" (imitations and falsehoods that only give the appearance of healing) as contrasted with the "medicine" offered by the philosopher. However, later in *Phaedrus*, Plato (trans. 1995) comes to believe that a form of rhetoric (quite distinct from the Sophistic portrayal) can reveal truth if it adheres to and is informed by the process of dialectic (Nobles, 1957, p. 208). For Plato, dialectic becomes an essential feature that appropriates the power of rhetoric to reveal truth in the creative clash between opposing forces. Plato's observation had a significant influence on the ongoing understanding of the role of dialectic in rhetoric. For instance, Aristotle (trans. 2018), Plato's student, reveals his teacher's influence as he goes as far to say that "rhetoric is the counterpart to dialectic" (p. 2), and Everett Lee Hunt (1920) suggests Aristotle's *Rhetoric* extends Plato's musings on rhetoric at the end of the *Phaedrus* (p. 39). The dialectic practiced in Ancient Greece is foundational to understanding subsequent schools of dialectic.

[24] Ironically, there is evidence to suggest Plato "coined" rhetoric, the very term for which he held such disdain (Schiappa, 1990, p. 1).

While Baxter and Montgomery (1996) note dialectic in the writings of Saint Augustine, Saint Aquinas, Descartes, Spinoza, Kant, and Rousseau, the next major school of dialectic detailed is from Hegel and Marx. They turn to Microvic (1980) to announce the importance of Hegel and Marx, as their dialectical approaches shaped "a philosophical worldview in the nineteenth century" (as cited by Baxter & Montgomery, 1996, p. 21). Baxter and Montgomery (1996) characterize the Hegelian-Marxian dialectic as ontological due to the influence of Heraclitus on Hegel. Although often considered the same, Hegel's dialectic is distinct from that of Marx (Gunkel, 2007). In fact, Marx (2013) himself clearly distinguishes the two in the first volume of *Capital*, writing that his "dialectical method is not only different from Hegel's, but is its direct opposite" (p. 15). Baxter and Montgomery (1996) help to clarify this distinction by reminding the reader of Hegel's philosophical idealism and Marx's dialectical materialism.

Baxter and Montgomery (1996) place Hegel's *The Science of Logic* and *The Phenomenology of Mind* as the fundamental works detailing the Hegelian dialectic. Furthermore, David Gunkel[25] (2007) offers a helpful explication of Hegelian dialectic from a philosophy of communication perspective. Gunkel (2007) explains Hegel's dialectical process as involving three coordinates: the beginning or initial premise, the negation, and the second negation, sublation, or *Aufhebung* (pp. 23–24). Hegel's beginning is "an abstract universal that is simple, immediate, and thoroughly indeterminate" (p. 23). In *The Science of Logic*, "being" exemplifies the beginning. For

[25] David Gunkel is a Professor in the Department of Communication at Northern University. He research interests are focused on "information and communication technology with a focus on ethics" (David, 2016, para. 1). Apart from *Thinking Otherwise* (Purdue University Press, 2007), he has seven scholarly book publications, including *Hacking Cyberspace* (Westview, 2001), *The Machine Question: Critical Perspectives on AI, Robots and Ethics* (MIT Press, 2012), and *Heidegger and The Media* (Polity Press, 2014). In 2016, he received the Top Single-Authored Book of the Year Award from the National Communication Association Communication Ethics Division for *Of Remixology: Ethics and Aesthetics after Remix* (MIT, 2016).

Hegel, the negation becomes manifest when the beginning recognizes itself as "deficient" and is "endowed with the *urge* to carry itself further" (as cited by Gunkel, 2007, p. 23). "Nothing" illustrates the negation; the second negation relies upon the dual meaning of the word sublation, as both a preservation and cessation (as cited by Gunkel, 2007, p. 24). "Becoming" epitomizes the second negation by maintaining the differences and ending the opposition between "being" and "nothing" (Gunkel, 2007, p. 24). Baxter and Montgomery (1996) explicate that Hegel's philosophy creates an ontology of "Becoming," rather than "Being," that achieves knowledge of the "Idea" as a result of a "higher consciousness of mind" (p. 22). Hegel's project focused solely on the "consciousness of mind"; his student, Karl Marx, would introduce a dialectic with direct social relevance (p. 22).

The Marxian dialectic differs from the Hegelian dialectic by focusing on "people's daily existence" (Baxter & Montgomery, 1996, p. 22). Marxian dialectic proceeds via *thesis*-*antithesis*-*synthesis* (Marx, 2013). For instance, the capitalist creates a *thesis* by fashioning workday hours to maximize his or her own profits (since the cost of materials are fixed and, in fact, due to inflation, likely to rise, the capitalist has learned that one way to increase surplus profit is exploiting the laborer through long workdays). However, the laborer puts forward an *antithesis* by picketing and not working until the hours are decreased. A *synthesis* occurs by the introduction of a law, such as the Labor Act of 1848, that limits the workday to 12 hours. In this way, the synthesis would satisfy laborers and the capitalist—until met by another antithesis from laborer *or* capitalist. This understanding of dialectic focuses its attention on the clash between thesis and antithesis—a contradiction that produces a next step within the framework of historical determinism. Marx's project sought to emancipate the "working class by liberating workers from the constraints of their economic existence" (Baxter & Montgomery, 1996, p. 23). In this framework, each synthesis becomes rendered a thesis that begets an antithesis resulting in yet another synthesis to onset another thesis-antithesis-synthesis toward the culmination of progress.

Next, Baxter and Montgomery (1996) introduce Russian philosopher Mikhail Bakhtin's understanding of dialogism, from *The Dialogic Imagination: Four Essays* and *Speech Genres and Other Late Essays*, to remedy what they perceive as inadequacies with dialectic. Baxter and Montgomery (1996) suggest that Bakhtin's dialogism aids and informs a dialectical approach by asserting a messy and unordered social reality that lacks fixity and boundaries, thus reflecting lived experience better than the closed and ordered terms of the dialectic. Bakhtin disagreed with Hegel and Marx because their theories present neatness and order through univocalism, monologism, and mechanism, which are unreflective of the multivocal, dialogic, and organic lived human experience. For Bakhtin, human experience is dialogic, emerging between at least two interlocutors whose voices possess centripetal forces, or desire for unity and the need to connect with others, and centrifugal forces, or the need for difference and to separate from others. Bakhtin's "chronotope," or "time-space," considers the temporal dimension of dialogue that acts as a constraint and enabler (p. 26). The chronotope determines appropriate language for a specific time, setting, and place. Embedded in chronotopes and within the interplay between the centripetal and centrifugal forces are "utterances," or "link[s] in a chain of dialogue" that are bound by former and latter links in a conversation (p. 27). An utterance carries previous experiences and encounters that give shape to present understandings. Dialogism acknowledges the layers of meanings carried by a given term and the multiple voices present, reflecting the reality of messy and complex lived experiences.

Bakhtin's dialogism informs Baxter and Montegomery's (1996) relational dialectics. Grounded in dialectics-as-ontology, relational dialectics recognizes multivocal contradictions in the context of relationships. Multivocal contradictions expand beyond binary oppositions such as open/closed to include the complicated oppositions among "expressiveness, verbal disclosure, directness, honesty" and "privacy regulation, deception, ambiguity, and [discreetness]" (p. 30). Baxter and Montgomery distinguish relational dialectics with four characteristics. First, building upon the Bakhtinian contention that words are communicative bridges, Baxter and Montgomery suggest that the gap that a word bridges constitutes the relationship. Baxter and Montgomery recognize that there is no true merger between two voices even when they are expressing a similar perspective. Second, dynamics of union (centripetal) and separation (centrifugal) are overlapping and ongoing *ad infinitum* at the root of relationships. Third, the context is a fluid part of the relationship that enables, constraints, and regulates actions. Lastly, Baxter and Montgomery do not discount the contributions of monologic or dualistic approaches to looking at relationships, suggesting that relational dialectics is dependent upon and grows out of this work. Relational dialectics employs dialogism to understand the complex interplays composing interpersonal relationships.

Although not included in the tracing of dialectical thought by Baxter and Montgomery (1996), the field of communication recognizes the serious thought Burke offers to dialectic (Crusius, 1986, 1988; Ercolini, 2003; Crable, 2000a, 2000b, 2003, 2009; Murray, 2002; Zappen, 2009). In fact, James P. Zappen (2009) suggests that Burke's work merges "dialectic and rhetoric with dialogue and poetic myth in a *dialectical-rhetorical transcendence*," which should be regarded as a "major contribution to rhetorical theory" (p. 280). Likewise, Timothy W. Crusius (1986) asserts that Burke offers an "original contribution to dialectic" through his pentad in *A Grammar of Motives* (p. 24). Crusius (1988) also considers Burkean dialectic alongside Aristotelian and Hegelian to uncover the fruitful contributions of Burke's work. This section concludes with consideration of Burke's (1941) work on dialectic that first appeared in *The Kenyon Review* and was later extended in *A Grammar of Motives* (1945/1969).

Burke (1941) provides an initial framing of dialectic in "Four Master Tropes."[26] Here, Burke explains the close relationships[27] between and among what he terms the "master tropes"[28] of irony/dialectic, synecdoche/representation, metonymy/reduction, and metaphor/perspective. The master tropes indicate the rhetorical power of language to "create[] meaning" (Burke, 1941, p. 421). This section moves through a description of each trope, beginning with irony, to ground a Burkean understanding of dialectic.

The trope irony, paired with dialectic, permits the transcendence of terms (Burke, 1941, p. 431). Burke makes this move by equating "dialectic" with "dramatic," for "where ideas are in action, we have drama; where the agents are in ideation, we have dialectic" (p. 431). Burke differentiates his irony-dialectic pairing from relativism by situating relativism as a "fragmentation" or "isolation," where the whole is seen in terms of only one position (pp. 431–432). Conversely, irony attempts to create "a *development*"

[26] This article was later included as an appendix to *A Grammar of Motives*.

[27] Burke (1941) suggests the master tropes "shade into one another" as the complexities in one bring forth the remaining (p. 421).

[28] Burke (1941) gives each master trope a literal term; included here after the slash following each trope.

that employs *all* the terms from multiple positions; dialectic is then the presence of each character as they contribute to the ongoing plot development (p. 432). Burke outlines "true irony" in drama through the acknowledgment of three attributes: "kinship with the enemy"; a hedging of "superiority"; and the necessity of the "most representative character" to be both "adjectival" and "substantial" (pp. 435–437). Kinship with the enemy requires the recognition that the "hero" is indebted to and consubstantial with the enemy (p. 435). Superiority can act as a "foil" to true irony and thus must be hedged (p. 435). A temptation might arise to label particular foolish characters obsolete, but true irony requires the acknowledgement that the fool is a "necessary modifier" to the overall development, for without folly wisdom could not be known (p. 435). The most representative character is required to be adjectival by "embodying" a qualification of the aggregate definition and substantial by likewise embodying the "conclusions of the development of the whole" (p. 437).

Socrates exemplifies the most representative character in the Platonic dialogues. True irony cannot emerge without these qualifiers. Irony works to produce a representative anecdote through an incorporation of all the parts included in the whole. Dialectic, likewise, consists of an amalgamation of the parts belonging to the whole. Synecdoche is ironic because in being representative, all the characters or terms contained may be made present.

Synecdoche concerns valid representations in the interplay of part and whole. As Burke (1941) explains, synecdoche is "part for the whole, whole for the part" (p. 426). The part must function as a two-way "road" that leads down the street from the whole to the part and back up the street from the part to the whole (p. 428). Burke exemplifies the "noblest synecdoche" through "metaphysical doctrines proclaiming the identity of 'microcosm' and 'macrocosm'" (p. 427). In metaphysical doctrines, "either the whole [macrocosm] can represent the part [microcosm] or the part can represent the whole" (p. 427). Burke also exemplifies synecdoche through political, sensory, and artistic representation (p. 427). Burke finds that drama is synecdochic because the beginning and close each contain elements of the other in a consubstantial relation. The importance of synecdoche lies in the stress on "*relationship* or *connectedness*" (p. 428). The part and the whole are consubstantially linked in synecdoche. However, Burke recognizes that while this trope is representative, it is simultaneously a reduction, allowing for an overlap between synecdoche and metonymy[29] (p. 426).

Metonymy is a "special application of synecdoche" (Burke, 1941, p. 428) and functions as a way to relate the incorporeal to the corporeal (p. 424). Where a synecdochal reduction allows one to return to the whole, a metonymical reduction would not. Burke distinguishes between anecdotes based on reduction and representation: "*anecdotes 'scientifically' selected for reductive purposes are not representative*" (p. 430). For Burke, an "informative anecdote" is based on metonymy, while a representative anecdote is based on synecdoche (pp. 430–431). An informative anecdote employed by science does not portray the holistic picture that could be provided by the representative anecdote. Informative anecdotes are one-way roads leading away from the whole to a reduced part that cannot return to a description of the whole. Burke suggests that a science comprised of "representative anecdotes," rather than "informative anecdotes" (misrepresentative, reductive results from experiments), holds the potential for scientific

[29] David Tell explains the overlap in that a synecdoche is a "corrective to metonymical excess" or excessive reduction (Tell, 2004, p. 43).

truth and discovery (p. 431). The representative and informative anecdotes held within the dialectic are made visible through the metaphor or perspective.

The final trope, metaphor, Burke (1941) explains as a lens for viewing "something *in terms of* something else" and a detailing of a character from the perspective of another (p. 421–422). Metaphor provides a way of seeing that brings notions of consubstantiality and identification to a discussion, allowing conversants to understand the topic of conversation. Burke pairs metaphor with perspective, as a way of seeing the world, a "'carrying-over' of a term from one realm into another" (p. 423). Metaphors allow us to see the "thisness of a that" (Burke, 1941, 421). Words themselves are metaphors and can be employed in conversation to relate the corporeal "that" to the incorporeal "this." A physical entity in the world is reduced to a word. When working from a shared perspective or metaphor, a reduction to a microcosm "this" from a macrocosm "that" may function representatively, allowing the topic of conversation to be understood. Metaphor enables one to view the world through the metonymic expression of the incorporeal in terms of the tangible via the representative anecdote, which dialectically transcends the whole through the part and vice versa.

After establishing the strong overlap and interplay between irony, synecdoche, metonymy, and metaphor, Burke (1945/1969) extends his thought on "dialectic in general" in *A Grammar of Motives* (p. 402). Rather than focus on its interplay among other tropes specifically, Burke parses out dialectic as a "transformation of terms" centered around the "three heads" of: (1) merger/division; (2) the major pairs of action-passion, mind-body, being-nothing; and (3) transcendence (p. 402). First, Burke explicates merger/division, offering the scapegoat, which begets "vicarious atonement" or purification through suffering, as a “clear example” of the three principles at work—merger, division, and new merger (p. 406). The inequities of the iniquitous are shared by the scapegoat, forging the merger. However, these inequities are “ritualistically alienated” from the iniquitous, thus creating division (p. 406). Upon sacrifice, a new merger then emerges from the “unification” of the purified whose identity is “defined in dialectical opposition to the sacrificial offering” (p. 406). Childbirth also offers an example of the dialectical paradox of substance: conception as merger, cells splitting and growing as division, and birth itself as the new merger where the consubstantiality of the familial source associates the child with *these* parents rather than *those* (p. 405). The scapegoat mechanism and childbirth illustrate the Burkean dialectical head of merger/division.

Burke (1945/1969) then details the three pairings of mind-body, being-nothing, and action-passion, which he suggests are more specific generalizations of merger and division (pp. 418–419). Burke suggests that the mind-body opposition has an “obvious” ground that offers one of the two as original (mind) and the other as derivate (body) (p. 419). Since the terms “can be taken to represent the other,” idealist or materialist reductions are “readily available,” and the rhetorical shift between a mind/body leaning can either “idealize” a speaker’s cause or “materializ[e]” the opponent’s cause (p. 419). Next, Burke suggests the grouping of being-nothing as “most prevalent” as the pair of essence-existence (p. 419). Burke describes the action-passion pairing as a “particularized logic,” such as peace-war, cooperation-competition, and faith-knowledge (pp. 419–420). The three pairings act as localized examples of merger and division.

Finally, Burke (1945/1969) considers the role of transcendence in dialectic as when the transformation from merger to division indicates a "change of *principle*" with the discovery of a "new motive" (pp. 419–420). The Platonic dialogues offer such a dialectic, where the end transcends the beginning and renders the start of the dialogue visible "in terms of the new motivation encountered en route" (p. 422). Thus, the *Phaedrus* can be read in terms of the Socratic, dialectical method rather than as a depiction of sexual intercourse, the nature of the lover and non-lover, and who it is better to be (p. 424). Burke provides a textured examination of the concept of dialectic and its interrelation to the tropes of metaphor, synecdoche, and metonymy.

Crusius (1986) recognizes Burke's pentad, a *questioning* of motives, as a contribution to dialectic (p. 23). Crusius contends that Burke's dialectic studies "verbal universes" and disinterestedly pursues the implications of a vocabulary (p. 24). Crusius recognizes the centrality of substance, which "places concepts in relation to their opposites," and identification, which creates communities from interest groups, to Burkean dialectic (pp. 26, 29). The Burkean pentad seeks to uncover motivational substances, but this process is paradoxical because for the discussion of a subject involves a discussion of the negative, what the subject is not (p. 28). The contradictions of the substance unveil the "limitations" of a perspective and "justify other viewpoints" (p. 28). Identification depends upon substance, uncovering the varying perspectives and what side one will align with. Burke's pentad offers contributions to dialectic through his conceptions of substance and identification, which then merit a change in perspective.

Crusius (1988) writes that Burke's dialectic resonates with the Hegelian dialectic[30] due to his hermeneutical approach. Burke's dialectic attempts to revert texts from monologue to dialogue, thereby situating the word as a "human voice in time" (p. 123). Crusius suggests that Burke's integration of dialectic with dialogue allows dialectic to stand "back on its feet" (p. 126). Crusius suggests that Burke's dialogically informed dialectic takes us beyond the text and offers a "revival of orality *for literacy*" (p. 128). Burke's dialectic offers the conceptual tools to examine the many voices carried by a word and their organization into sentences and paragraphs in order to uncover the motivation behind an action.

According to Zappen (2009), Burke's whole contribution to dialectic can be uncovered from a reading of *A Grammar of Motives* alongside *A Rhetoric of Motives*. Zappen (2009) explains Burke's dialectic in the *Grammar* as "a merger of opposing ideas" at varying, generalized levels via "linguistic abstraction and transformation" that respects diversity while seeking transcendence (pp. 280–281). Likewise, in the *Rhetoric*, Burke offers dialectic to allow interlocutors to reach "higher level generalizations represented in mythic images through the power of the poetic imagination" (p. 281) through dialogue. The significance of the dialectical-rhetorical transcendence across the *Grammar* and the *Rhetoric* lies in its challenge to rhetoric to consider the relation between individual discourses that create enlarged communities, transcending "individual

[30] While Burke and Hegel both suggest dialectic proceeds by antithesis, recognize the limitations of human nature, and view the tensions in language as a "source of insight into ourselves," Crusius considers that Burke does not have an ontological leaning (p. 116). The debate surrounding Burke's project as ontological or epistemological is hotly contested among Burkean scholars; see Crable (2000a) and Thames (2018), who suggest that dramatism (and therefore Burke's dialectic) *is* ontological and literal, thus aligning Burke with the Hegelian dialectics-as-ontology. While not identifying Burke's approach as ontological, Crusius (1988) differentiates the Burkean dialectic from the epistemic Platonic, which seeks to uncover truth dialectically through verbal analysis, and Aristotelian approaches, which associate dialectic with training in argument (p. 116).

and group ideologies and interests" (Zappen, 2009, p. 281). Zappen points to the significance of Burke's dialectic in the recognition and reconciling of differences between individuals and groups, creating an expanded community.

The various perspectives on dialectic offer a textured understanding of how dialectics change historically. First, schools of dialectical thought can be grouped into dialectics as ontological (the study of existence) and dialectics as epistemological (the study of knowledge). Eastern schools of thought are typically tied to the ontological approach, with the Yin and Yang as an exemplar of the way that light and dark exist together. Western schools of thought are more likely to be rooted in an epistemological approach, discovering truth through methods of argumentation. Second, Baxter and Montgomery (1996) bring Bakhtin's dialogism into conversation with dialectics to inform their approach. A dialogic approach to dialectics recognizes the mutlivocality and complexity of the terms in opposition. Finally, Burke's conception of dialectic likewise recognizes dialogue and attempts to restore layers of interpretation, understanding, and meaning to words once thought monologic. Additionally, Burke illuminates the close relation of dialectic and metaphor. The metaphor by which we approach a given topic contains the possible interpretive possibilities and sets parameters for understanding. The next section of the chapter reviews the work of scholars who consider the contradictions in tension, or dialectics, in cyberspace.

The Dialectical Nature of Cyberspace

Dialectic recognizes the tensions at play in a given substance. Lance Strate (1999), Michael Heim (1999), Martin Dodge and Rob Kitchin (2001), and Gunkel (2007) recognize the contradictions that are colliding in information and computer technologies and cyberspace. Strate (1999) focuses on what he terms the initial distinctions of public/private, sacred/profane, and permanent/transitional. Heim (1999) recounts the dialectical user base of cyberspace, grouping consumers of technology into “naïve realists,” who withhold from computerized devices at all costs, and “technological idealists,” who whole-heartedly and unquestioningly accept and use technologies at face value. Heim suggests the middle path of “virtual realism” as a balance between these extremes. Dodge and Kitchin (2001) offer eight dialectics that ground their attempt to “map” cyberspace and demonstrate the benefits of this approach. Gunkel (2007) reviews resolutions to the logic of binary opposition and offers ways to “think otherwise” about these dialectics. Together, these scholars offer new means to understand cyberspace and establish the importance of dialectic for responding to this new domain of human experience.

Strate (1999) describes the dialectical nature of cyberspace through his discussion of key “distinctions” that produced tension and collision during the time of Web 1.0 (1989–2006) (p. 405). A first distinction is the differentiation of “*public and private space*” (p. 405). Whereas public cyberspace is “generally accessible to all,” such as the results uncovered by Google searches, private cyberspace has no such accessibility and is limited to individual users connected through “individual computers and intranets, private channels or chat rooms, and closed discussion lists” (pp. 405–406). While anyone can access the webpages in public cyberspace, private cyberspace requires users to sign in, adjust settings, or be granted special access through particular intranet providers. However, Strate recognizes the difficulty, if not impossibility, of genuinely public or private online spaces. Private cyberspace allows for “surveillance and control” that fundamentally denies our traditional assumptions of privacy (p. 406). Likewise, the "fluid and often impersonal" nature of public cyberspace challenges our normal conceptions surrounding the public sphere, wherein known individuals can put forward a distinct voice that shapes the public domain (p. 406). Cyberspace is a meeting, clashing, or "merging" of public and private spaces (p. 406).

Strate (1999) recognizes the second distinction as spanning the "*sacred and profane*" (p. 406). Strate describes the profane as emerging in sites of "work or entertainment" and the sacred in the allocation of designated religious and commemorative spaces (p. 406). Users engage cyberspace for work by researching projects and communicating with other co-workers as well as for entertainment activities such as listening to music, watching videos, or playing games. In contrast, online sacred spaces can be found among the home pages affiliated with "religious organizations," web memorials for deceased individuals, or in the "nonphysical (and therefore potentially spiritual) properties of cyberspace taken as a whole" (p. 406). Cyberspace is a collision of spaces that are both sacred and profane.

Strate (1999) observes the third distinction as between "*permanent and transitional space*" (p. 406). A permanent space is "regularly occupied" and receives consistent care, i.e., a home or place of employment (p. 406). Conversely, a transitional space is an unoccupied "interzone," i.e., a bus stop or airport (p. 406). Strate (1999) describes that portions of the cyber landscape are permanent, or "owned, controlled, and stable," while others are transitional, or un-owned, uncontrolled, and unstable (p. 406). Permanent cyberspace lends into traditional conceptions of property ownership in the physical world. Much like how people care for their homes, swimming pools, or cars, they tend to and update their web pages and profiles. Transitional cyberspace breathes life into the Wild West metaphor that suggests “anything goes” online from the creation of false identities that differ from reality in lifestyle, appearance, or gender/sex to online harassment through “flaming and spamming” (p. 406). Strate observes distinctions of public/private, sacred/profane, and permanent/transitional within cyberspace that are a clashing of opposing tendencies. Michael Heim[31] (1999) likewise acknowledges the contradictions inherent in cyberspace and names these distinctions dialectic proper.

Heim (1999) acknowledges the dialectical nature of cyberspace with a particular emphasis on the divided user base, what he sorts between “naïve realist[s]” and “technological idealist[s]” [32] (p. 33). According to the naïve realist, computers and similar technologies unnecessarily complicate and distract from real life; therefore, naïve realists choose to opt out of technological use whenever possible. Conversely, the technological idealist enthusiastically embraces and actualizes the potentialities offered by and contained within computer technologies without pause, hesitation, or question. In order to resolve the opposition between realist and idealist, Heim works from a Platonic sense of dialectic, as opposed to a Hegelian or Marxian model, to offer a path of “virtual realism” (pp. 39, 41). The virtual realist is the middle road between the naïve realist and the technological idealist, recognizing the necessity of embracing technology alongside the importance of reflecting on the environment that technologies create and change. The virtual realist practices “techalysis,” a process of “criticism, practice, and conscious

[31] According to a 2012 interview with Laurean Ralón in Figure/Ground, Heim is referred to as “the philosopher of cyberspace.” His scholarly works include *Electric Language: A Philosophical Study of Word Processing* (Yale University Press, 1986), *The Metaphysics of Virtual Reality* (Oxford University Press, 1993), and *Virtual Realism* (Oxford University Press, 1998). These scholarly books have Chinese, Japanese, and Korean translations (Ralón, para. 1).

[32] Heim (1999) also suggests the existence of a third group of “skeptics” who believe that attempts to understand cyberspace are “pointless,” as were the writings of early television and film critics who could not foresee future uses of these technologies (p. 38).

communication" that creates a new social awareness (pp. 41, 44). The virtual realist offers a critical reflection that curbs an unbridled enthusiasm and adoption of or resistance to technologies.

Heim's (1999) significance lies in the affirmation of an historical and hypertextual understanding of dialectic to uncover potential resolutions to the cyberspace dialectic. An approach to dialectic from its roots in the Platonic dialogues, which highlight the "oppositions found in dialogue" through a championing of the Socratic question and answer method, offers creative insight to bring forth the virtual realist between the opposing positions of naïve realist and technological idealist (p. 39). Heim applies Platonic dialectic to uncover a way of being and living in conversation between these opposites, detached from both the Hegelian idealistic uncovering of the "social change" that drives human evolution and the Marxian materialistic, concrete tracing of social history, which is completed only with war and revolution (p. 26). Additionally, Heim rejects Hegel and Marx, because "a cyberspace synthesis is not in sight" (p. 39). A turn to Plato "sustains opposition as the polarity that continually sparks the dialogue, and the dialogue is the life of cyberspace" (p. 41). Heim turns to Plato for a cyberspace dialectic through dialogue that recognizes the terms do not reach a synthesis and continue to live amid the give and take in the conversation of adopt or withhold.

Rather than focus on the user base, Dodge[33] and Kitchin[34] (2001) turn to eight dialectics in their attempt to map cyberspace (pp. 13–24). The first dialectic is

[33] Martin Dodge (Ph.D., University College London) is a senior lecturer at the University of Manchester. His research focuses on the "social and spatial enrollment of digital technologies" and "urban historical geography" ("Martin Dodge," 2017). Dodge has curated the web-based Atlas of Cyberspaces (1995–2007) and has co-authored *Mapping Cyberspace* (with Rob Kitchin; Routledge, 2001), *Atlas of Cyberspace* (with Rob Kitchin; Addison-Wesley, 2001), and *Code/Space* (with Rob Kitchin; MIT Press, 2011).

[34] Rob Kitchen (Ph.D., University of Wales Swansea) is professor and ERC Advanced Investigator in the National Institute of Regional and Spatial Analysis at Maynooth University. His research interests include

space/spacelessness. Cyberspace exists in space through the institutions that influence its design and as spaceless in its denial of the constraints of physical geography. The second dialectic is place/placelessness. The poles of this dialectic examine the extent to which cyberspace creates authentic or inauthentic places of interaction. The third dialectic is industrial/post-industrial. Technology and automation restructure industrial organizational life into a post-industrial-based economy exposed to global markets. The fourth dialectic is public/private. This dialectic corresponds with a weakened public sphere as users' online interactions produce a "digital trace" associated with a loss of individual privacy (p. 19). A fifth dialectic is broadcasters/listeners. Cyberspace alters conventional social rules that determine who can talk and who can listen. The sixth dialectic is real/virtual. This dialectic brings forth a conflation between experiences in the physical world and our consumption of mediated content. The seventh dialectic is nature/technology. The lines between nature and technology blur with continual advancements in bioengineering and artificial intelligence that grant humans an increasing capability to control their material circumstances. The final dialectic is fixed/fluid. This dialectic particularly relates to identity as physical embodiment becomes a necessary antecedent to explore cyberspace. Dodge and Kitchin recognize these dialectic as constructive and "transform[ative]" (p. 13) and use them as geographical markers that guide their aim to map cyberspace.

Gunkel (2007) builds upon Heim's distinction between the naïve realist and the technological idealist as he details the binary oppositions that inform human

software, big data, smart cities; the Internet and cyberspace; cartographic theory, mapping and dashboards; data infrastructures and practices; spatial theory and geographic methods; the development of the discipline of geography; and similar concerns. He has authored or edited 28 books and has written over 180 articles and book chapters ("Rob Kitchin," n. d.).

understandings of computer technologies and cyberspace. In *Thinking Otherwise: Philosophy, Communication, Technology*, Gunkel argues that society negotiates the binary oppositions of cyberspace through the following four methods: (1) either/or logic, (2) balance, (3) dialectic, and (4) poststructuralism (p. 3). However, Gunkel advocates for a "thinking otherwise" about, around, and outside of these distinctions as a more insightful and constructive means to understand the dialectics of cyberspace (p. 3). These four methods and their problematic consequences prompt Gunkel to advance a method otherwise to reconcile the binary oppositions that fill information and computer technologies.

Gunkel (2007) depicts either/or logic as ineffective for reconciling the opposing forces clashing within information and computer technologies. According to Gunkel, the either/or logic only serves to preserve the struggle between the two sides, framing one as fundamentally correct and the other as incorrect. While explicating the either/or, Gunkel expands upon Heim's distinction between the technological idealist and the naïve realist and articulates thinkers who contribute to each camp. Foundational to the idealist belief system is the contention that computers enhance entertainment, work, and connectivity, providing a "reengineered" version of the Christian heavenly paradise on earth (p. 14).[35] Contrarily, the naïve realists believe that such earthly techno-paradises are illusions that mistake earthly states for eternal paradise.[36] The realists and idealists live in an eternal struggle as one can only select between yes/no, right/wrong, and black/white. Either/or logic only maintains and advances the struggle between the two opposing sides.

[35] Gunkel places J. C. R. Licklider and Robert Taylor, Nicholas Negroponte, Howard Rheingold, Pierre Lévy, William Mitchell, and Margaret Wertheim among the technological idealists (p. 14).
[36] Gunkel identifies Ted Kaczynski, Neil Postman, Mark Slouka, Hubert Dreyfus, and Plato as among the naïve realists (pp. 14–15).

Likewise, Gunkel (2007) suggests the balance approach is ineffective for resolving technological binary oppositions and only worsens the original conflicts. This balance approach is akin to a juggling act that conserves and maintains the original oppositions, rather than seeking to acknowledge a third term or achieve a synthesis. Rather than choosing a side or reducing the conflict, the balance resolution seeks equilibrium between the terms where neither can "gain the upper hand" (p. 17).[37] However, Gunkel describes this method as internally inconsistent and problematic; practitioners of this approach advocate for neutrality and a middle path, yet they are not neutral and do, in fact, choose a side—the side of taking the balance approach while ignoring and quieting the other methods of opposition-resolution. Thus, balance is not achieved and the practitioners do not align their words with their deeds.

Next, Gunkel (2007) uncovers three primary applications of dialectic applied to resolve the binary oppositions impregnating information and computer technologies. Those seeking to define "hybrid concepts" are especially predisposed to select a dialectical approach (p. 25). The primary dialectical methods applied to computer and information technologies are from Hegel's process of beginning, negation, and *Aufheben*, sublation, or second negation or from Marx's process of thesis-antithesis-synthesis (p. 25). First, dialectic appears from those attempting to resolve the distinction between the virtual and the real as "virtual reality" (p. 26).[38] Second, a dialectical perspective emerges from the cyborg convergence between humans and machines.[39] Third, dialectic is

[37] In the balance camp, Gunkel places Heim, Andrew Calcutt, Andrew Shapiro, and Marshall and Eric McLuhan (pp. 18–19).

[38] Scholars doing work with the virtual include Pierre Lévy, Peter Horsfield, Mark Poster, Woolley, Heim, and Stanovsky (Gunkel, 2007, pp. 25–26).

[39] Scholars doing work on the cyborg include Manifred Clynes and Nathine Kline, Chris Hables Gray, and Anne Balsamo (Gunkel, 2007, pp. 26–27).

manifest in the notion of remediation, as either the result of the collision between immediacy (singular representation) and hypermediacy (multiple representations) or the co-presence of media in other media (elements of the book and television in the Internet or vice versa).[40] Scholars apply dialectic to negotiate the opposing tendencies of cyberspace, particularly when concerned with virtual reality, cyborgs, and remediation. Dialectic offers a way to synthesize a third term out of the contradictory, binary terms in information and computer technologies (i.e., virtual reality, cyborg) or to sublate the terms in remediation.

Gunkel describes two consequences that result from a dialectical resolution of opposing tendencies in information and computer mediated technologies. First, one cannot easily avoid the Hegelian dialectic as oppositions are readily framed through this lens (p. 29). Second, negations/antitheses are perceived as "derivative, contradictory, and deficient" (p. 30). In other words, in each of these three applications of dialectic there is a "bias" toward or privileging of the real over the virtual, the human over the machine, and toward immediacy rather than hypermediacy (p. 31). For Gunkel, these consequences render dialectic inadequate to resolve the contradictions within cyberspace. As a way to remedy these inadequacies, Gunkel turns to poststructuralism.

Poststructuralism offers a wholly different way to re-think binary oppositions as well as the ability to step outside the Hegelian dialectical system. Gunkel (2007) lists Gilles Deleuze, Félix Guattari, Jacques Derrida, Emmanuel Levinas, and Michel Foucault as contributing to his understanding of poststructuralism (pp. 32–33). Gunkel identifies Mark Taylor and Donna Harraway as scholars who contribute to a poststructuralist

[40] The primary scholars doing work on remediation are Jay David Bolter and Richard Grusin (Gunkel, 2007, p. 27).

resolution to the binary oppositions in information and computer technologies (p. 33). According to Gunkel, both Taylor and Harraway contribute helpful coordinates to thinking otherwise about binary oppositions with the consistent contention that all the opposed terms are affected, or “contaminated,” by what the dialectical approach might label the third term (p. 35). For instance, in an academic department at an institution of higher education that champions a “scholar/teacher” approach to the classroom, the terms “scholar” and “teacher” are at opposition and resolved by their combination in “scholar/teacher.” For the poststructuralist, the new term “scholar/teacher” is affected by the connotative and denotative definitions associated with both of the prior, separate terms. Scholar/teachers are neither just scholars nor just teachers; scholarship plays an integral role in their teaching and teaching influences their scholarship—both terms are contaminated as they collide, bleed into one another, and shape a wholly new and radically other understanding of “scholar/teacher.” Within academia, a person’s roles as a scholar and a teacher collide to reorder identity in ways that make the labels “scholar” and “teacher” inadequate representations of who this person is and what this person does. Poststructuralism provides an exit to the binary opposition and offers a wholly and radically other approach to understanding the terms.

Gunkel understands Taylor’s work on virtual reality to offer two implications. First, both technological idealists and naïve realists assume that the problems of virtual reality are “exclusively a matter of technology” (p. 34). Second, this first contention preserves the “traditional metaphysical distinctions” between mind/body, natural/artificial, human/machine (p. 34). However, understanding the problems of virtual reality as solely related to technology does not lend into adequate understanding of virtual reality, for it is “entirely otherwise” and thus irreconcilable by the either/or logic, attempt to achieve a balance, or a dialectical synthesis or sublation (pp. 34–35). Likewise, Harraway contends that everything in the opposition is contaminated, calling for a reconsideration of the traditional distinctions between humans/animals, organic/mechanic, and physical/non-physical (p. 35). Poststructuralist thought applied to information and computer technologies offers the tools to think otherwise.

Gunkel (2007) recognizes three consequences in poststructuralist thought. First, while poststructuralists struggle to name a third term out of the opposition, *neologism* (or the introduction of a completely new term) or Derrida’s *paleonomy* (or the repurposing of an old word endowed with different connotations) offer two possibilities (p. 36). Second, these new or newly purposed terms “risk becoming reappropriated into the existing binary oppositions” which they seek to work against (p. 37). Finally, there is no “finality,” or end, to the task of poststructuralism (p. 38). Since the newly created or defined term is at “risk” to fall into the existing or formerly existing binary opposition, the task of applying poststructuralist thought to information and computer technologies is endless as new hierarchies emerge and exert hegemony (p. 38). In summation, poststructuralist thought is at risk for becoming increasingly abstracted from the “real questions and issues that matter” (p. 39). While poststructuralism offers a way to think otherwise about information and computer technologies, there are a number of elements that demand attention to avoid a relapse into the binary opposition.

After reviewing the either/or, balance, dialectical, and poststructural methods of reconciling binary opposites, Gunkel (2007) articulates his method “otherwise” epistemologically, metaphysically, and ethically (pp. 41–43). Epistemologically, the binary approach suggests that any given phenomenon is thought reducible to *x* or *not-x*. However, such a categorization is reductive, non-representative, and unreflective of a phenomenon's true complexity. Metaphysically, Gunkel traces the normative questions, understandings, and expectations of present day technology as emergent from the attitudes of Theuth and Thamus toward writing (a then new technology) that were detailed by Socrates in Plato's *Phaedrus*. Theuth presumes writing will benefit society through strengthening or extending the human capacity for memory while Thamus considers writing will be a detriment to society through weakening or numbing the human capacity for memory. The attitudes of Theuth and Thamus shape the "well-established conceptual opposition" and metaphysical paradigm that purports the traditional, dualistic hegemony and conventional understandings of technology (p. 42). Ethically, the binary oppositions "are never neutral" (p. 42). Every conceptual opposition features a derivate, and therefore inferior, term. Gunkel calls for a thinking otherwise for epistemological, metaphysical, and ethical reasons.

Gunkel (2007) concludes with four "summary statements" that can guide the "endlessly self-reflective practice and interminable analysis" that is thinking otherwise (p. 152). First, Gunkel suggests that "[b]inary opposition is not optional" (p. 152). In other words, binary oppositions structure human patterns of thought beyond their manifestation and application to information and computer technologies. Second, binary oppositions are biased. That is, one term in the opposition is always privileged and imposes a hierarchy that "make[s] exclusive and prejudicial decisions about others" (p. 153). Third, binary oppositions cannot be escaped; resisting the system is acting within the system, for resistance supplies the secondary, contradictory term that fuels the system. Thus, rather than a contradictory term, Gunkel calls for an “alternative transaction” that deliberately and disruptively reprograms the device or operating system to function otherwise and exposes alternative function paths as necessary (p. 154). This alternative transaction occurs from residing and learning how to function within the binary opposition. Fourth, Gunkel suggests that “there is no finality” (p. 154). In other words, there is no synthesized third term, but, as poststructuralism suggests, “it [thinking otherwise] can only take place as a kind of ‘interminable methodological movement’ that must continually submit its own results and innovations to further scrutiny” (p. 155). While there is no single method of thinking otherwise, these four summary steps can offer coordinates to those attempting the practice.

Gunkel (2007) illustrates the process of thinking otherwise through a fictitious, alternative beginning to the film *The Matrix.* This film exemplifies a binary opposition through the clash between the virtual and the real. At the start of the movie, Neo, the film’s protagonist, is confronted by a binary choice between selecting either a red pill or a blue pill that represent the opposing sides of the dominant opposition shaping Western thought since the time of Plato. If Neo should select the blue pill, he will continue to live in an illusion, numb and ignorant to the truth of the world around him. A selection of the red pill will cause Neo to emerge from the illusory world presented to him by the matrix and awaken him to the real world. Unsurprisingly, Neo selects the red pill—a choice necessitated by the hegemonic dominance of Western philosophy and the storyline of the movie. However, Gunkel imagines a third choice for Neo—one that represents a “thinking otherwise.” Rather than selecting between the binary opposition posed to him in the form of a red pill or a blue pill, Gunkel envisions Neo getting up and walking away—to live within the matrix with the knowledge that it is a false world. Walking away from the pills would be a radical thinking otherwise, an alternative transaction that steps outside the binary logic upheld by dominant Western philosophy.

In summary, this section has introduced the contradictions and binary oppositions that are present in information and computer technologies and the applications of dialectic to understand the nature of cyberspace. Strate (1999) identifies what he terms the “distinctions” of public/private, sacred/profane, and permanent/transitional. Heim (1999) advances a Platonic sense of dialectic regarding how the technological idealist and naïve realist negotiate their differences in conversation. Heim suggests that the ground beneath the virtual realist offers a middle path of balance between the enthusiasm of the idealist and the reservation of the realist. Heim encourages a practice of technalysis to critically engage and analyze the technologies that society uses. Dodge and Kitchin (2001) announce eight dialectics that represent the nature of cyberspace itself and aid in a virtual re-mapping of this digital platform. Finally, Gunkel (2007) offers an extensive depiction of the many contradictions and oppositions that are inherent within computer and information technologies and the ways society attempts to resolve them (either/or, balance, dialectic, poststructuralism). Gunkel’s ultimate advocation, however, is for thinking otherwise and having alternative transactions that allow us to step outside the dominant binary oppositions structuring technologies. Technology is wholly other and, as such, requires creative engagement. The next section of the chapter introduces the three dialectics of cyberspace that become the focus of chapters three, four, and five of this project.

The Dialectics of Cyberspace

With full recognition that cyberspace is composed of multiple and contrasting dialectical tensions, this section establishes the three dialectics pursued in the proceeding chapters of this project: a public/private dialectic, an anonymity/identity dialectic, and a national/global dialectic. Inherent within each of these dialectics is a collision of contradictory terms that meet, only to break apart existing conceptions about the material consequences of each term and subsequently to re-order cyberspace as something radically and wholly other—cyberspace thus is not a alternative reality to the physical 'real' world. Instead, cyberspace influences the 'real' world with physical as well as virtual consequences. These consequences emerge in direct response to colliding dialectical binary oppositions. These dialectics act as contemporary extensions and representations of the contradictions announced in the previous section. While many dialectics characterize cyberspace, these three become salient in the contemporary moment of Web 2.0 and make vulnerable individual well being, corporate data, and national security, which become threatened by cyber attacks.

The public/private dialectic attends to the clash of what information we show and that which we conceal in various contexts, as well as contextualizing the reflexive interaction between cyberspace used as a private tool and for public actions. Strate (1999) acknowledges the public/private dialectic and characterizes public spaces as accessible, fluid, and impersonal, conversely, the private spaces are limited-access, observed, and controlled. Strate acknowledges the impossibility of obtaining a truly public or private space online as we have in the physical world, pointing toward Gunkel's (2007) poststructuralist reconciliation of the binary oppositions inherent within information and computer technologies—the space online that emerges from the collision of public and private is wholly and radically other. This collision of public and private spaces runs the risk of turning into Hannah Arendt's (1958) conception of the social, a space that emerges between public and private spheres where information from the private sphere is inappropriately brought within the public sphere and vice versa. The information posted in an online context can affect our online identity and our offline identity. The social element of cyberspace creates a fertile ground for cyberbullying—a first tier of cyber attack this dissertation examines.

The anonymity/identity dialectic likewise contributes to cyberbullying and creates opportunities for cyber theft. Anonymity allows users to hide their physical world identities behind a screen name; this screen name also ties them to an identity. Actions of cyber theft typically occur under a screen name, such as the "Kind Mr. Smith" who stole content from the HBO television network in July/August 2017 (Rindner, 2017). The potential for theft is increasingly putting society at risk, leading into Ulrich Beck's risk society. Beck (1992) recognizes that the neoliberal society creates the simultaneous potential for unlimited economic growth *and* nuclear, chemical, genetic, and ecological risks. Beck (2013) extends this project to consider digital risk. Deborah Lupton (2016) builds upon Beck to suggest the advent of a digital risk society. The work of Ulrich Beck on risk can inform the digital realm, addressing questions of cyber theft—the second tier of attack this project considers.

The national/global dialectic acknowledges the ways in which the Internet is altering our physical sense of boundaries between countries in the real world. For instance, the concept of neutrality between warring nations must be re-examined when attacks pass through the neutral nation's wires, airwaves, or data cloud (Kelsey, 2008). Here, again, the work of Beck (2006) can inform a sense of boundaries and borders in what he terms an era of "reflexive modernity," characterized by its "boundarylessness" (pp. 2–3). Beck offers the "cosmopolitan outlook" as a way to navigate the boundaryless space (p. 3). The cosmopolitan outlook is a substitution of the either/or binary logic for a "both/and logic of inclusive differentiation" (pp. 4–5). Beck notes the presence of dialectical tensions when trying to navigate the changing national/global borders that cyberspace is carving and re-carving. Borders become an essential question when considering cyber terrorism for locating the point of attack origin and who is accountable (Brenner, 2007). Beck offers a voice that adds texture to the changing national borders in the digital age across which acts of cyber terrorism occur—the final tier of cyber threat the dissertation examines.

The dialectical method pursued in this project is itself a both/and. The primary understanding of dialectic pursued in this dissertation is the Burkean model. The Burkean model gives a robust and holistic understanding of dialectic that details its close relationship to metaphor and considers the three major heads of: (1) merger/division; (2) the three major pairings of mind-body, being-nothing, and action passion; and (3) transcendence. Additionally, Burke's understanding of dialectic is hermeneutical and, similar to Bakhtin's dialogism, attempts to restore mulitvocality to univocality. Burke's dialectic is essential for this project because he recognizes that there is no synthesis or end for the dialectics that society lives within.[41] However, Burke's dialectic must be

[41] As David Tell (2004) explains, Burke binds dialectic (irony) with the representative anecdote (synecdoche) in the human linguistic search for the "most representative anecdote," that is "conspicuously…partial, [] incomplete…[and] rhetorical" (p. 47). Thus, Burke's dialectic has no synthesis,

informed by Gunkel's poststructuralist approach to thinking otherwise. Burke's new merger and Gunkel's new term have a point of commonality in that each must be treated and understood as radically other. Cyberspace and information and computer technologies fundamentally change the opposing terms that are in contention that make up the network. Burke helps us to see and understand the terms that are in contention; Gunkel reminds us that the new merger is radically and wholly other. The next three chapters will address each of these dialectics and their corresponding attacks in detail. The next chapter begins by looking at cyberbullying amid the public/private dialectic of cyberspace.

but rather unites dialectic and rhetoric to function as a changing of perspectives that brings new epistemological insight upon the terms under discussion.

Chapter 3

The Public/Private Dialectic of Cyberspace:

Cyberbullying as a First-Tier Attack

Introduction

This chapter explores how cyberspace, the World Wide Web, and the Internet reconfigure human interpersonal communication within online public and private spheres. Following the insights from communication literature addressing the effects of cyber-mediated communication and the philosophical distinction between the public, private, and social spheres of human existence offered by Hannah Arendt (1958/1998), this chapter suggests that the maintenance of an appropriate balance between private and public life in an online context is crucial to assuage the potential for users to engage cyberspace as a platform for cyberbullying. Scholars recognize cyberbullying as an "emerging social problem" (Felt, 2017) rife with social and psychological harm (Toma, 2013; Reinecke et al., 2017). This project contends that attentiveness to the public/private dialectic can uncover communication ethics goods at stake within cyberbullying as a first-tier cyber attack.

The first section of this chapter situates conceptions of cyberspace within a public /private dialectic. Overviewing how computer-, electronic-, digital-, and cyber-mediated communication change interpersonal communication practices assists our understanding of how cyberspace transforms conventional notions of public/private spaces, opening possibilities for the potentially devastating consequences of cyberbullying. The second segment of the chapter identifies themes within the field of communication calling forth three response strategies: corporate/institutional cyber discourse, regulatory mechanisms, and bystander intervention. The third section turns to the philosophical work of Hannah Arendt, whose theoretical distinctions of the *vita contemplativa* (thinking, willing, and judging) and the *vita activa* (labor, work, and action) point toward meaningful insight on the public/private dialectic; Arendt urges us to protect and promote boundaries between these two spheres (public and private life) of human existence and articulates the intersections between contemplative reflection and active engagement with others. This portion also considers extensions of and responses to Arendt's work offered by Ronald C. Arnett[42] (2013), Deborah Eicher-Catt[43] (2013), and Judith Butler[44] (2015). The chapter concludes with implications and a transition to the anonymity/identity dialectic.

The significance of this chapter lies in the call for understanding the public/private dialectic of cyberspace that frames user engagement. Scholars recognize that online communication can serve two contending purposes: (a) to bring users closer together by opening paths for communication across physical, geographic, and ideological boundaries, or (b) to isolate users by severing genuine human connections and instead facilitating echo chambers and opportunities for bullying and harassment (Colleoni, Rozza, & Arvidsson, 2014; Turkle, 2011). Importantly, scholars contend that

[42] Arnett is an internationally known scholar on dialogue and communication ethics, a 2017 Distinguished Scholar of the National Communication Association, The Patricia Doherty Yoder and Ronald Wolfe Endowed Chair in Communication Ethics, and the Henry Koren, C.S.Sp., Endowed Chair for Scholarly Excellence (2010–2015). He is the author/co-author of eleven scholarly books, 92 scholarly articles, and 38 book chapters. His work on Arendt brings her into the field of communication and identifies communication ethics implications stemming from her scholarly corpus ("Ronald C. Arnett," 2018).

[43] Eicher-Catt is a seminal voice in the field of communicology, philosophy of communication, and semiotics. She is the author over 35 scholarly publications and co-edited *Communicology: The New Science of Embodied Discourse* ("Deborah Eicher-Catt," 2018). Specifically, she (2013) offers insights on civility from a semiotic phenomenological perspective that relies upon Arendt's distinctions between public/private/social; she contends that civility is more than a standard social code and instead requires cultural reflection on "the good of the common" (p. 3).

[44] Butler holds the Hannah Arendt Chair at the European Graduate School (EGS) and serves as an important voice in the contemporary application of Arendtian scholarship. Butler's work on existential and economic precarity as well as her performative theories of gender and assembly build upon and extend Arendt ("Judith Butler," 2018).

the ultimate byproduct of communication technologies, whether to join or to isolate, emerges in response to the means of user engagement (Colleoni, Rozza, & Arvidsson, 2014; Flaxman, Goel, & Rao, 2016; Walther, 1996); the standard practices of technological use determine the ensuing environment. A reflective engagement with cyberspace that recognizes the different spheres at play prompts users to be more knowledgeable about the effects of their communication on the surrounding world and offers a first response to cyberbullying as a first-tier cyber attack.

Situating Cyberspace within a Public/Private Dialectic

Communication scholars demonstrate how computer-, electronic-, digital-, and cyber-mediated communication alters human understandings of interpersonal interaction in public and private contexts (Anderson, 1994; Carpio, 2018; Cathcart & Gumpert, 1994; Meyrowitz, 1985, 1994; Putnam, 2000; Walther, 1992, 1993, 1996, 2017; Walther, Anderson, & Park, 1994; White, 2015). This corpus of literature points toward the contradictory byproducts of cyber-mediated communication that both enhance and constrain the qualities of and possibilities for interpersonal connections. For instance, while some commend improved connectivity across growing geographic distances (Walther, 1993) and celebrate new possibilities for free speech, civic engagement, and public participation (Rahimi, 2011; White, 2015), others lament diminishing face-to-face interpersonal skills (Turkle, 2011) and warn against limitations on public action (Putnam, 2000) through the emergence of fake news (Stefanita, Corbu, & Buturio, 2018) and echo chambers (Colleoni, Rozza, & Arvidsson, 2014). Since the 1980s, communication scholars have continued to consider how cyber-mediated technologies alter human conceptions of physical places and communication between and among people. This section surveys this literature, focusing on the ways that cyberspace has come to change interpersonal communication by opening and limiting possibilities for engagement in public and private life.

Before the advent of the World Wide Web brought a surge of interconnectivity and hyperlinks that made the Internet a powerful communication tool for all users regardless of their knowledge of programming or coding, Joshua Meyrowitz, writing in 1985, addressed the changes that electronic media introduced. In the newly emerging mass mediated society, Meyrowitz responded to a "lack of boundaries" that created a culture he termed "essentially placeless" (pp. 315, 317). Meyrowitz combines the theoretical work of Erving Goffman and Marshall McLuhan to bring new understanding to the effects of electronic media on social behavior (pp. 2–3). Although Meyrowitz (1985) focuses on how technologies alter physical and social places, he describes the changing distinctions between public and private spaces as the "most significant" implication of his work (p. 328).

Meyrowitz (1985) offers insight on the general ways that electronic media alter public and private spaces by transforming "social forums" and connecting people in ways never conceived of before (p. 5). Where society once existed in a "situational geography," organized by pre-existing standards and classifications, electronic media brought forth an overlap of the formerly distinct public and private spheres (pp. 5–6). For example, the television disregards existing situational geography by exposing its content to all viewers regardless of age appropriateness. Electronic media usher in "architectural" changes that undermine conventional relationships "between physical setting and social situation" and thus disregard the public or private context (pp. 6–7). Electronic media reconfigure behavior by setting new norms and behavioral patterns.

Meyrowitz (1985) overviews consistencies and novelties in the behavioral patterns surrounding electronic media. Social behavior, in physical as well as electronically-mediated spaces, centers on "projecting certain impressions and concealing others," depending on the context (p. 320). However, as electronic media blur contexts with abstruse boundaries between public and private life, social behavior deviates from traditional practices in physical spaces (p. 320). Electronic communication totalizes information access and sharing regardless of another's role-related right to know, which violates normative conceptions of authority (p. 322). Such horizontal information sharing restructures social behavior in response to ambiguously blurred public and private spheres.

Meyrowitz (1994) extends his considerations on electronic media and place in an essay appearing in Rob Anderson, Kenneth Cissna, and Ronald C. Arnett's *The Reach of Dialogue*. In this work, Meyrowitz contends that electronic media "play with place" and violate boundaries (p. 152). While electronic media can alter one's sense of place in public and private contexts in infinite ways, they maintain connections to physical places—a cell phone, television, or computer physically exists in one place but simultaneously "merge[s] many formerly distinct" behaviors from different contexts within user interaction with the medium (p. 152). Meyrowitz exemplifies this principle by comparing a book and television. Whereas the book results in total immersion in the text, a television alters definitions of place in an "unstable and inconsistent manner" (p. 152). In other words, a television, like a book, may hold a viewer's attention or be ignored, but it also offers a third and distinct option—that of half attention; the realm of half attention made manifest by electronic media alters patterns of human communication by dividing user's concentration between physical space and mediated content. Meyrowitz understands electronic media as creating a situation that governs communicative rules. His early account of the effects of electronically-mediated technologies situates the public/private dialectic as fundamental to understanding not only the technology but also the resulting communication behaviors.

Contributing to this same edited volume on dialogue, Rob Anderson (1994) argues for computer-mediated communication's ability to open new possibilities for interpersonal interaction. Anderson (1994) writes that electronic devices, and by extension digital devices, offer "increased presence and rejuvenated possibilities for dialogue" (p. 106). For Anderson, theoretical insights from Walter Ong (1967), Mikhail Bakhtin, and Vincent Crapanzano (1990) allow for dialogue to occur through an electronically-mediated device. Anderson (1994) works from a particular school of dialogic thought[45] characterized by "*unanticipated consequences*" and the "*recognition of strange otherness*" (p. 93). For Anderson, neither partner knows what the other will say, which begets a sense of the unknown. In facing the unknown, communicators work together in a "*collaborative orientation*" that manages the "*vulnerability*" each partner reveals through conversation (p. 93). The language in a dialogue mutually implicates the communicators to share in a "*temporal flow*," or certain timeframe that constrains and guides the focus of the discussion (pp. 93–94). Finally, for Anderson,

[45] Anderson is working from a particular understanding of dialogue articulated by Cissna and Anderson (1994). This understanding is not representative of the phenomenological perspective of dialogue articulated by Arnett (1981). For further clarity about these schools of dialogical thought, see Anderson (1982) and Arnett (1982).

"*genuineness/authenticity*" characterizes dialogue (p. 94). Communicators draw from and upon lived experiences that bring forth new insight and understanding between one another, and Anderson suggests that electronic media can mediate the process of dialogue.

Anderson's work opposes Peter L. Berger, Brigitte Berger, and Hansfried Kellner's (1974) *The Homeless Mind*, which challenges the potential for electronic media to facilitate a dialogue (as cited by Anderson, 1994). Berger et al. contend that technology distances people from one another and creates an unproductive sense of "anonymity" (as cited by Anderson, 1994, pp. 96–97). Anderson counters this position, arguing that anonymity "remove[s] the very ground for dialogue" only in a physical sense, turning to theoretical conceptions of mediated presence offered by Ong, Bakhtin, and Crapanzano.

Anderson begins with Ong (1967), who situates presence as relational rather than physical. For Anderson, Ong's understanding of presence as the "call of one interior through an exterior to another interior" (as cited by Anderson, 1994, p. 99) permits facilitation through mediated technologies and does not necessarily rely upon physical contexts. From this perspective, a phone as an exterior mediated device transmits the interior thoughts of one communicator to the interior thoughts of another communicator. Bakhtin, likewise, challenges traditional notions of presence in dialogue when engaging a text—where physical presence is, again, unnecessary (Anderson, 1994, pp. 101, 104). Anderson highlights that Bakhtin offers opportunities for a reader to have a dialogue with a text as new insights emerge between the two. Finally, Crapanzano challenges traditional notions of presence through his understanding of "'shadow' dialogue," or a secondary dialogue within the head of an interviewee during an interview (Anderson, 1994, p. 104). This interior conversation within two-way communication allows the interviewee to generate new insight.

Together, Ong, Bakhtin, and Crapanzano, for Anderson, separate the notion of physicality from presence. Ong notes the importance of the communication of interiority through external means, Bakhtin recognizes text as a communicator of interiority, and Crapanzano suggests that an interiority can communicate with itself. Anderson (1994) combines the notion of Bakhtin's "absent presence" with Crapanzano's "shadow dialogue" to assert that mediated systems enhance the dialogic self (p. 105). Anderson observes that society intertwines technology and media with the self and furthermore defines the self according to media. In combining the theories of Ong, Bakhtin, and Crapanzano, Anderson (1994) emphasizes the role that mediated environments play in creating dialogue. From this perspective, meditated communication devices open opportunities for dialogue even when no one is on the other end in real-time due to the technology's ability to bring unanticipated, unexpected interaction between the conversants in public and private contexts.

Also appearing alongside Meyrowitz and Anderson, Cathcart and Gumpert (1994) acknowledge that often communication requires mediation. In mediated communication, the medium shapes "behaviors and attitudes" while simultaneously mirroring pre-existing "interpersonal behaviors," thus converging individual self-development with "media-development" (p. 159). Their work presents a social construction model that offers a reflexive portrayal of user engagement and mediated environments; users engage mediated devices that shape the social environment simultaneous with the social environment shaping the users' modes of engagement with the device.

Cathcart and Gumpert (1994) identify four types of mediated interpersonal communication that construct public and private life in significant ways. This typology is inclusive of and extends beyond electronic- or computer-mediated channels. The first contains devices that mediate interpersonal communication across physical distances such as telephones, Morse code, or letters (p. 161). By opening paths for connection and communication, private and public information travels across physical space. For instance, events occurring in Los Angeles, Tokyo, and Cairo become accessible around the world, transforming what falls within the realm of public communication.

The second simulates or imitates interpersonal communication practices in face-to-face settings via mediated platforms such as "para-social interactions" or "broadcast-teleparticipatory communication" (p. 161). This type feigns intimacy with celebrities via television and exclusive interviews where public and private communication converge (p. 163). For instance, viewers may feel like they truly know Fred Rogers and are part of his neighborhood but overlook the mediated nature of the encounter that renders this relationship one-sided. The viewer may only come to recognize the public nature of the mediated interaction (which simulates private communication) when appearing as a stranger to Fred Rogers in a face-to-face encounter.

The third relies upon a computer that functions as a distinct "interpersonal prox[y]" (p. 161). While often simulating face-to-face behaviors like the second type, person-computer communication primarily involves software such as Microsoft Word or Adobe Photoshop. In this form, the computer software itself mimics patterns of human communication. Although not in existence when Cathcart and Gumpert published their essay, Siri's voice commands exemplify person-computer communication. Using "Hey Siri" as the voice command to activate this program mimics the language patterns used to engage another human interlocutor in face-to-face settings. As a result, we begin to refer to this program as a person—granting gender identities and often thanking "her" for the information provided. Our interactions with Siri take on an element of private communication, which becomes increasingly complicated with the recognition that Apple, through this app, always listens to us, waits for the words "Hey Siri," and stores our requests.

The final type, which they term "*unicommunication*," acknowledges the communicative power of nonhuman artifacts (p. 161). For Cathcart and Gumpert, unicommunication includes "objects of clothing, adornment, and personal possession" (p. 166). They contend that these items communicate for us in social and cultural settings, thus altering public life. For instance, students delivering a presentation to a class dressed in sweatpants, t-shirts, and tennis shoes with earphones strung over their shoulders communicate a significantly different message to their instructor and peers than those wearing a suit, dress, or tie. The manner of dress produces distinctly different environments for the presentation and the class; their choice of attire mediates a public message, which contextualizes interactions with others.

As technologies mediate communication, the social construction of public and private communication fundamentally changes the interaction. For Cathcart and Gumpert, mediation is necessary for communication to occur; communication is always mediated by some sort of technology (both electronic and non-electronic). Their typology of mediated communication offers insight into the changing nature of communication between and among human and nonhuman agents that can transform public and private spaces in both constructive and problematic ways. Cathcart and Gumpert stress the importance of the co-creation of social realities in the production of new ways to consider public and private boundaries.

Unlike Meyrowitz (1985; 1994) and Cathcart and Gumpert (1994), Joseph B. Walther (Walther, 1992, 1993, 1996, 2017; Walther, Anderson, & Park, 1994) frames computer-mediated communication (CMC) as a context of interpersonal interaction that can either strengthen or weaken interpersonal relationships dependent on the manner of use. Walther (1992) contends that CMC does not eliminate the nonverbal codes that provide highly meaningful insights to face-to-face communication; instead, he finds these nonverbal cues implemented in new and equally significant ways. Writing during an era of email and computer conferencing, Walther (1993) examines the effects of CMC on human impression formation and finds that, with an appropriate amount of time and message reception, impressions form “despite never meeting face-to-face” (p. 393). In fact, Walther, alongside Jeffrey F. Anderson and David W. Park, (1994), suggests that “extended interaction” in a mediated context can be just as productive as face-to-face encounters (p. 477). Walther (1996) offers interpersonal communication strategies that can enhance relational intimacy through CMC and likewise those that can intentionally obscure identity for impersonal engagement (p. 4); CMC can be used to isolate interlocutors or to draw them closer together. Recently, Walther (2017) has contended that interpersonal metaconstructs emerging in CMC contexts require examination from communication scholars to grasp a broader and more representative understanding of interpersonal communication generally as it exists in a highly mediated and technological milieu. Throughout his corpus, Walther has offered a consistent voice advocating that CMC opens up new avenues for interpersonal communication that contribute to existing perceptions of public and private life.

Contrary to Walther, Robert Putnam (2000) argues that electronically-mediated communication has contributed to a steady decline in American civic engagement.[46] For Putnam (2000), a lack of civic engagement corresponds with diminished "social capital,"[47] which generally serves as a detriment to public and private life (pp. 18–21). Civic engagement with institutions allows members to collaborate in fostering public goods, such as "rais[ing] scholarships or fight[ing] disease," and private goods, such as building "friendships and business connections" (p. 20). Specifically, Putnam examines increased involvement with technology and mass media as a contributor to decreasing civic engagement.

Putnam (2000) identifies two major ways that electronic media limit civic engagement—by "individualiz[ing]" news and entertainment and by "privat[izing]" consumption (pp. 216–217). Although he focuses primarily on television, he extends his analysis to television's "electric cousins" such as computers, portable CD players, and camcorders (p. 246). While these devices can create a civic "gathering place" that strengthens bonds and communication, they are "not sociologically compelling" enough to "lead[] to action" (pp. 243–244). As these mediated devices increasingly emphasize

[46] Putnam (2000) exemplifies the decline in civic involvement through the closure of the following organizations due to a lack of revitalization from "freshsets of new members": (1) the Bridge Club of Glenn Valley, Pennsylvania; (2) the chapter of the National Association for the Advancement of Colored people in Roanoke, Virginia; (3) and The Charity League of Dallas (pp. 15–16).

[47] For the intellectual development of social capital, Putnam (2000) points to the work of twentieth century scholars such as L. J. Hanifan, Jane Jacobs, Glenn Loury, Pierre Bourdieu, Ekkehart Schlicht, and James S. Coleman (pp. 19–20).

entertainment, they result in more time spent at home, more time spent with devices than communities, less energy and passion, less conversation among family members and friends, and diminished opportunities to enhance interpersonal relationships (pp. 223–238). Putnam's observations can undoubtedly extend to contemporary digital devices connected through cyberspace and their effects on public and private life.

Sharing Putnam's concerns, Sherry Turkle (2011) notes the effects of electronic media on interpersonal communication, with a specific focus on the Internet and computer technologies. In *Alone Together: Why We Expect More from Technology and Less from Each Other*, Turkle (2011) addresses the interpersonal face-to-face consequences of viewing technology as a "substitute" for human interaction in a physical realm (p. 11). Importantly, she suggests that people attempt to have intimate relationships through computers and with robots that are ultimately unsatisfying. She recognizes that, while computer technologies may be able to simulate relationships and streamline communication, they create "half-li[t]" communities and can render us "feel[ing] ultimately alone" (p. 12). Turkle makes the important observation that online connections, despite being "deeply felt," are reductive in that people "only need to deal with the part of the person" portrayed in that particular online community (p. 293). As such, online communities fail to represent the holistic person, which ultimately produces misconceptions that influence physical communities as well; participants simply "lose the inclination" to see a person beyond their perceived needs or wants (p. 293). Turkle suggests that connections formed and maintained through computer technologies produce ultimately unsatisfying relationships in both public and private contexts.

Offering an alternative perspective, Babak Rahimi (2011) suggests that cyberspace can become a site of civic engagement and political dissent. Directly countering Putnam's claim that mediated technologies limit civic engagement, Rahimi suggests that the very means through which the Internet is "operated, developed, and creatively transformed" requires engagement from users that could be understood as civic action (p. 161). Rahimi textures this perspective with Downey and Fenton's (2003) observations, who suggest that cyberspace is a "virtual public" that forms new opinions through "discourses, activities, and, moreover, interventions of older media" (as cited by Rahimi, 2011, p. 161). That is, the Internet yields a place for dissent that invigorates public discourse. According to Rahimi, cyberspace offers a site for political activism and civic engagement by providing a platform for citizens to voice public opinion and engage those who feel differently.

Donata Marletta (2010), likewise, advances the perspective that successful communication formation mediated through Internet technologies merges with the physical public sphere. Marletta (2010) argues that face-to-face and online communication "exist in a kind of symbiosis, nourishing and complementing each other" (p. 85)—for example, she finds that online communities have a "clear need" for meetings in physical space (p. 89). Marletta turns to V. Turner (1982) to understand this new space at the clash of the real and the virtual through "the notion of *liminal* space—Latin for threshold" (Marletta, 2010, p. 91). Liminal space regularly privileges ritual (pp. 91–92). Marletta explains that rituals transition individuals "from one state to another" and liminality is "a state of being between phases" (p. 92). Thus, "virtual and non-virtual realities merge together" in liminal space (p. 92). Marletta frames a fluid sphere actualized through the mutual reliance of interactions in and between real and virtual spaces that build communities and advance public life.

Contrarily, Maggie Jackson (2009) considers how computer and information technologies minimize the human capacity for communication and genuine face-to-face connections. In particular, Jackson observes the Internet's emphasis on multitasking as a standard practice for digital technology use; she contends that multitasking ultimately prevents the user from maintaining sustained concentration and attention even in offline contexts, rendering the users' capacity to "comprehend what's relevant and permanent" more difficult (p. 14). Jackson describes human attention capabilities as composed of three "networks"—awareness, focus, and planning (p. 23). Awareness is an "alerting" to "incoming stimuli" (p. 23). Focus is an "orienting" toward incoming stimuli that are selected and deemed pertinent from the millions of incoming sensations (p. 23). Planning is an "executive network" that negotiates between "complex cognitive and emotional operations" to determine engagement with incoming stimuli (p. 23). Jackson warns that society is approaching a dark age as the increasing prevalence of digital technologies weaken awareness, focus, and planning, ultimately limiting possibilities for human advancement in public and private contexts.

Nicholas Carr (2010) also outlines consequences of Internet technologies on brain functionality in his book, *The Shallows: What the Internet Is Doing to Our Brains*; like Jackson, Carr contends that the Internet minimizes sustained "concentration and contemplation" (p. 6). Societal adoptation and use of the Internet represents a "transition" between thinking with an "undistracted," "linear mind" to a mind that processes information distractedly and circuitously in "short, disjointed, often overlapping bursts"

(p. 10). The format and structure of web page content has re-ordered brain functioning toward a “Jet Ski” skimming over the words where serious readers once engaged deep, sustained thought (p. 7). Carr argues that the Internet fundamentally alters the make-up of the human brain through the concept of “neuro-plasticity,” or the ability for the brain to “reorganize[]” the patterns of neuron firing (p. 25). Although the brain’s plasticity weakens with age, it never completely ceases. Carr’s fear is that “as we come to rely on computers to mediate our understanding of the world, it is our own intelligence that flattens into artificial intelligence” (p. 224). Carr finds that a reliance on the Internet and computer technologies eradicates human intelligence, critical thinking, and reflective engagement with the world around us.

Carr (2014) continues this project in *The Glass Cage: How Our Computers Are Changing Us.* Where *The Shallows* offers a holistic, generalized effect of the Internet on the human brain, *The Glass Cage* supplies a more specific and particular account of these changes. Carr (2014) describes how a task completed with only the “aid” of computers leads to the “cognitive ailments” of “*automation complacency*” and “*automation bias*” (p. 67). Carr describes automation complacency as a “false sense of security” derived from computer technologies and automation bias as people giving “undue weight to the information coming through their monitors” (p. 69). For instance, Carr explains that pilots who rely on autopilot can no longer manually land planes and younger generations of Inuit/Igloolik hunters, who could once navigate snow covered terrain, lost this ability after reliance on GPS navigation systems. Technologies put the capacity of the human brain to think freely, independently, and accurately at risk. People place more trust and confidence in the information delivered from algorithms than from human knowledge emerging from conversation and exploration.

The influence of algorithms on constructing social reality and shaping human perception has been well documented in the communication literature (Andersen, 2018; Just & Latzer, 2017; Totaro & Ninno, 2014, 2016; Van den Bulck & Moe, 2018). For instance, Paolo Totaro and Domenico Ninno (2014) note the seminal role algorithms play in "regulat[ing] our daily lives," as well as "manufacturing processes" and citizen/customer services (p. 30). Natascha Just and Michael Latzer (2017) extend this sentiment, recognizing the "self-learning" and "relatively autonomous" functions that minimize predictability and control as algorithms can adjust their functioning in ways unanticipated by the creator (p. 254). Jack Andersen (2018) describes the powerful influence of algorithms in shaping patterns of human communication that reflect the device's functions for "searching, archiving, ordering, and filtering" (p. 1136), and furthermore Martin Hilbert, Saifuddin Ahmed, Jaeho Cho, Billy Liu, and Jonathan Luu (2018) describe how algorithms influence human attitudes. Through an analysis of YouTube activity during the 2016 US presidential election, Hilbert et al. contend that algorithms determine human emotion and perception via search inquires that contribute to the production of echo chambers. Algorithms drastically influence and potentially limit opportunities for public communication, discourse, and deliberation by offering pre-determined results that often reflect pre-existing attitudes.

Communication scholars also recognize the emergence of echo chambers through social media platforms (Colleoni, Rozza, & Arvidsson, 2014; Flaxman, S., Goel, S., & Rao, 2016; Hayat & Samuel-Azran, 2017; Usher, Holcomb, & Littman, 2018). Elanor

Colleoni, Alessandro Rozza, and Adam Arvidsson (2014) respond to scholarly conversation about social media's role in affirming or disaffirming the potential for "political homophily," or the polarization of political beliefs (p. 319). They overview literature suggesting that the Internet fosters a public sphere[48] in addition to contentions that it results in the emergence of echo chambers.[49] They find that the byproduct is reflective of the user mode of engagement. In a 2009 analysis of Twitter, they found that users who engaged the platform as a "social medium" were more likely to produce echo chambers than those who approached it as a "news medium" where diverse ideas clashed in a virtual public sphere (p. 328). Seth Flaxman, Sharad Goel, and Justin M. Rao (2016) affirm this finding, suggesting that individuals can choose content consistent with their individual beliefs as in an echo chamber scenario or that they can "reduce[s] ideological segregation" and expand the public sphere (p. 299). The responsibility falls upon users of technology, who must deliberately seek diversity and difference in content and perspective rather than passively and unreflectively accepting echo chambers manufactured by social media. As social media echoes back only what we express into the platform, the virtual space represented diverges from the diverse and contentious nature of the public domain. While social media holds the potential to expand the public sphere, it requires a deliberate and thoughtful engagement from users.

The public/private dialectic has shaped the communication literature considering the effects of cyber-mediated communication for decades. This conversation spans from those who contend that cyber-mediated communication enables or enhances

[48] See: Brundidge, 2010; Holt, 2004; Wojcieszak & Mutz, 2009 (as cited by Colleoni, Rozza, & Arvidsson, 2014, p. 318).

[49] See: Bimber & Davis, 2003; Davis, 1999; Galston, 2003; Mutz & Martin, 2001; Noveck, 2000; Sunstein, 2001; Wilhelm, 1998 (as cited by Colleoni, Rozza, & Arvidsson, 2014, p. 318).

communication in public and private contexts (Anderson, 1994; Cathcart & Gumpert, 1994; Rhaimi, 2011; Walther, 1992, 1993, 1996; White, 2015) to those who suggest that it minimizes interpersonal communication to the detriment of the human condition (Carr, 2010, 2014; Jackson, 2009; Turkle, 2011; Putnam, 2000). Electronic media, digital technologies, and the Internet completely change conceptions of public and private life in unknown and potentially unstable ways (Marletta, 2010; Meyrowitz, 1985, 1994); these changes require our attention and consideration. The use of cyberspace as a platform for public discussion and dialogue becomes a conscious choice (Colleoni, Rozza, & Arvidsson, 2014; Flaxman, Goel, & Rao, 2016). In this environment, people turn to the Internet as a source for information, human connection, and identity formation in ways that make them vulnerable to cyberbullying and harassment especially as virtual and physical identities continue to merge. The next section considers cyberbullying from a communication perspective to understand how this phenomenon emerges in response to blurred conceptions of public and private life.

A Communicative Perspective on Cyberbullying

Cyberbullying as a distinct social phenomenon has become increasingly problematic throughout the past decade (Felt, 2017). News media, scholars, and public research services alike announce the negative social consequences of cyberbullying, presenting alarming findings. A 2018 Pew Research Center study found that 59% of American teenagers have experienced bullying, harassment, or abuse online (Anderson, 2018, para. 1), ranging from offensive name-calling, false rumors, unwanted sharing of explicit images, stalking, and physical threats. Significant public conversation and research links cyberbullying to increased rates of suicide (Lenhart, 2013; Ollve, 2016;

Young, Subramanian, Miles, Hinnant, & Andsager, 2017, p. 1082). In fact, Michael Ollove (2016), writing for the PEW Charitable Trusts, attributes cyberbullying to a spike in teen suicide from 2.18 to 2.75 per 100,000 people between 2006 and 2014 (paras. 5–6). The devastating consequences of cyberbullying surpass those of screen addiction (Tynes, 2016) with significant consequences for mental health and well-being (Greenfield, 2018). This section of the chapter reviews the literature within the field of communication to situate the communicative act of cyberbullying as the manifestation of cyber attacks stemming from the eclipse of public and private distinctions.

While cyberbullying can occur across online platforms, social media networking sites remain a central location for this problematic behavior (BBC News, 2019). Several scholars associate diminished self esteem with social media use, regardless of whether one experiences cyberbullying (Reinecke, Aufenanger, Buetel, Dreier, Quiring, Stark, Wölfling, & Müller, 2017; Stefanita, Udrea, Durach, & Corbu, 2018; Toma, 2013), but the popularity, design, and purpose of social media sites bring forth strong associations with cyberbullying due to the platform's characteristic emphasis on self-presentation and self-evaluation (Toma, 2013, p. 215). Self-presentation (posting content that contributes to one's self perception and sense of identity) coupled with self-evaluation (measuring popularity, self worth, or success by number of likes, comments, or retweets) makes social media users vulnerable to cyberbullying as users' profiles become easily accessible outlets for attack.[50] In light of such a reality, *The Guardian*'s Patrick Greenfield (2018)

[50] Debates about social media use and self-esteem stand behind these correlations. For instance, Reinecke et al. (2017) contend that social media propels "burnout and depression/anxiety" as well as "decreased levels of psychological well-being" as users feel the need to constantly manage self presentation on the site (p. 106). Likewise, self evaluation occurs as social media users quantify their relationships via network connections and their ability to attract attention immediately from their peers, which actively contributes to "information overload" and the "stress and strain" of maintaining an always accessible media presence (pp. 91, 106); diminished self esteem could be the result of feeling overlooked when a post does not garner the

reports accusations that social media giants such as Facebook, Snapchat, and Twitter do not do enough to prevent cyberbullying practices from occurring on their platforms (para. 1). However, before we can expect social media corporations to offer regulatory mechanisms, society must reach a clear understanding of what behaviors constitute cyberbullying.

In 2010, Anthony J. Roberto and Jen Eden provided a summary of the emerging phenomenon of cyberbullying as a form of digital communication based upon previously identified definitional coordinates. Their work, alongside a 2014 study in collaboration with Matthew W. Savage, Leslie Ramos-Salazer, and Douglas M. Deiss, summarizes characteristic themes of cyberbullying as the "*deliberate*" and "*repeated*" employment of communication technology by single or multiple users to "*threaten or harm*" others in the network (Roberto et al., 2014, p. 98). Their investigation found that over one-third of college freshman admitted to cyberbullying a peer and identified three predictive behaviors: verbal aggression, risky behaviors, and cyberbullying victimization (p. 106). Roberto et al. (2014) believe that communication professionals are "particularly well suited" to offer preventative measures to potential cyberbullies (p. 111). Their work calls for greater awareness about the nature and contexts of cyberbullying as a starting point for shared understanding, prevention, and response.

public response expected by a social media user. However, Drew P. Cingel and Megan K. Olson (2018) reject assumptions that social media participation necessarily lowers self esteem. They note that not all uses of social media network connections are alike, and uses vary in regard to the level of active/passive engagement and in the use of visual versus text-based participation—not all activities diminish self esteem or open possibilities for cyberbullying. Srividya Ramasubramanian, Marissa Joanna Doshi, and Muniba Saleem (2017) explain how social media participation can open paths for connection between diverse users and simultaneously form online systems of support. These support systems could allow for individuals to stand together against cyberbullying attacks and provide networks for enhancing the potential for self-esteem.

Consistent with the definition offered by Roberto and Eden (2010), Alvin J. Primack and Kevin A. Johnson (2017) describe cyberbullying as a "repeated and willful enactment of aggressive communication behavior via digital technologies to inflict intentional harm on others" (p. 30). Their work, however, frames cyberbullying as "extensions of school relationships" that move from the physical schoolyard to virtual spaces where personal profiles intimately intertwine physical and virtual identities (p. 30); what occurs in virtual interactions has a direct effect on physical relationships and perceptions of identity. Thus, personal profiles in virtual spaces make the targets of cyberbullying available for attack in a 24-7 setting that extends well beyond the scope of the school day or academic year. To regulate cyberbullying, Primack and Johnson offer the "digital schoolhouse gate" that recognizes fluid boundaries between virtual and physical spaces (p. 31)—someone can act as a representative of the school outside of the schoolyard context and after school hours. This metaphor of a "digital schoolhouse gate" determines which activities fall under the jurisdiction of school officials based upon "audience, school language, effect, and First Amendment precedent" (p. 31). These criteria enable school administrators to determine if bullies and targets (whether fellow students, instructors, or administrators) act as representatives of the school regardless of their physical location during the time of attack (p. 42). Primack and Johnson note the way in which cyberbullies "encroach upon targets' private lives" and impede upon the target's ability to interact with others in public life, which they understand to be "a precondition for a healthy democracy" (p. 43). Cyberbullying traverses the lines of public and private spaces, threatening democratic society and re-conceptualizing the boundaries between physical and virtual spaces.

Sally Vogl-Bauer (2014) extends this discussion with a specific focus on the responsibility of faculty members at institutions of higher education in the prevention of cyberbullying. Vogl-Bauer considers the various contexts in which policies of prevention can become institutionalized practices. She identifies three levels for cyberbullying prevention: micro-levels (prevention tactics in student-faculty interactions), meso-levels (collaborative faculty-faculty prevention efforts), and macro-levels (institutional participation in societal prevention campaigns). Examination of the micro-level yields insight and strategies to assist faculty members with the identification of triggers and behaviors characteristic of students who act as cyberbullies. On the meso-level, teachers can work collaboratively with one another to understand how cyberbullying shapes the instructional environment and how they can respond to this issue in concert—such as by reviewing existing policies or providing further guidelines about appropriate behavior and response. The macro-level addresses how the institution can participate in larger social efforts to prevent cyberbullying, to implement appropriate response mechanisms, and to recognize how deliberate actions effect public perceptions of the institution. Cyberbullying not only threatens the well being of students and their ability to succeed in the pursuit of higher education but it also influences institutional retention and recruitment. Therefore, faculty members have a responsibility to implement prevention strategies into their interactions with students, fellow faculty, and the institution.

Michael Arntfield (2015) resonates with the need to implement institutional regulations for cyberbullying prevention. He positions cyberbullying at the forefront of "technological, social, and policy debate[s]" within North America (p. 371) and calls forth "enforcement agencies" to criminalize acts of cyberbullying (p. 384). Arntfield urges society to recognize the “paradigm shift” in the human conceptualizations of place and digital environments brought forth by online bullying (p. 384). He finds the anonymous nature of cyberbullying particularly threatening as it eliminates the obligation for publicly accepting responsibility for the consequences of one’s actions. For Arntfield, public enforcement agencies would have the capability and jurisdiction to remove this mask of anonymity and apprehend perpetrators with appropriate communication and disciplinary action.

Also calling for institutional regulatory policies, Tijana Milosevic (2016) places responsibility on the social media companies themselves, charging these corporations with accountability for the actions and communication occurring on their platforms. Just as corporations in physical space become liable for what occurs on their physical property, Milosevic contends that social media companies must accept responsibility for what occurs on their virtual property. In an era without legal parameters for mandatory anti-cyberbullying mechanisms, Milosevic urges for stricter corporate policies to address the issue (p. 5165). Milosevic observes that, rather than accepting this responsibility, companies engage in a pattern of blaming cyberbullying on individual user behaviors (p. 5175). For Milosevic, the “increasingly privatized” nature of the “digital public sphere” advances this issue (p. 5177) without recognizing virtual corporate responsibility despite comparable precedent in physical spaces.

Broadening the scope of individual responsibility, Nicholas Brody and Anita L. Vangelisti (2016) investigate the role of bystander intervention in cyberbullying prevention. While they acknowledge the value of institutional policies and educational programs in cyberbullying prevention (p. 115), their focus is to urge bystanders to act in response to cyberbullies and in support of targets (p. 95). According to Brody and Vangelisti, bystanders play a crucial role in curtailing bullying by “act[ing] immediately” and offering “social support” (p. 112). In particular, they task “close friends” with significant responsibility because these relationships most often extend between the online-offline boundaries (pp. 114, 116). For Brody and Vangelisti, individuals should not accept instances of cyberbullying and should act in deliberate opposition in the midst of these practices.

Likewise, Andrew C. High and Rachel Young (2018) advocate for “bystander intervention” as a “highly effective” tool in minimizing instances of online harassment and violence (p. 29). Focusing on “practical recommendations,” High and Young identify “distinct types of messages” that are representative and typical of cyberbullying encounters (p. 41). Rather than calling for regulatory oversight, High and Young call for campaigns that empower bystanders in the prevention of cyberbullying and train them in support strategies (p. 44). Successful campaigns should (1) build effective support systems around targets of cyberbullying, (2) equip bystanders with tested language content for intervention and peer counsel, and (3) identify relationships that can best provide support systems. High and Young contend that institutional resources are best used when educating individuals on practical response strategies that prevent, intervene in, and positively respond to the negative consequences of cyberbullying that affect psychosocial well-being, which include increasing rates of suicide, depression, and anxiety as well as diminishing self esteem.

These scholars agree on the devastating effects of cyberbullying and consistently call for attentive response from communication scholars and practitioners. Three response trends emerge from this literature: (1) definitional inquires that shape social and institutional discourses about cyberbullying (Primack & Johnson, 2017; Roberto et al., 2014; Vogl-Bauer, 2014); (2) requests for corporate/organizational regulatory measures (Arntfield, 2015; Milosevic, 2016); and (3) training programs that empower bystander intervention (Brody & Vangelisti, 2016; High & Young, 2018). Through each of these response strategies, communication scholars identify the need to protect users from harassing online activity and grant individuals and institutions the responsibility to intervene. With the recognition that online activity influences face-to-face encounters in physical spaces, cyberbullying practices and response tactics call forth thoughtful and reflective consideration about communication in public and private contexts. This emphasis on the public/private dialectic that contextualizes the nature of cyberspace and permits the powerful effects of cyberbullying creates an entrance for the work of Hannah Arendt. Arendt urges society to consider the necessary distinctions within this dialectic in order to uphold a healthy public domain. The next section reviews her work, pointing toward communication ethics analysis and implications.

Extensions from Hannah Arendt

Hannah Arendt has claimed significant attention from international scholarly audiences, sparking ongoing conversation and controversy throughout her career and to the present day (Rabinbach, 2004). Communication scholars exemplify the value of Arendt's work for theoretical and applied contexts (Allers, 2010; Arnett, 2012, 2013, 2016, 2018; Bell, 2005; Arnett, Bell, & Fritz, 2010; Eicher-Catt, 2013; Frost, 2016; Hammer, 2000; Kaposi, 2009; Lechte, 2018; Maier, 2016; Tamboukou, 2013). This section reviews Arendt's call for deliberate distinctions between public and private spheres within the human condition and argues that her emphasis on thinking, willing, and judging (*vita contemplativa*) is essential for labor, work, and action (*vita activa*) in the public domain. The section then turns to three scholars who extend Arendt's work on the public/private distinction: (1) Ronald C. Arnett (2013), who brings Arendt into the field of communication, historically texturing labor, work, and action, and announcing communication ethics implications; (2) Deborah Eicher-Catt (2013), who approaches Arendt's public/private distinction from a semiotic phenomenological perspective that emphasizes the social and cultural influences that frame communication and civil public discourse; and (3) Judith Butler (2015), who extends Arendt's project with application to performative engagements in the public sphere motivated by the private domain

In 1958, following a worldwide perception of the Russian launch of Sputnik as affirmation of the human ability to leave Earth, Arendt emphasized that the global community must pragmatically and necessarily attend to the human condition. In her fifth book, aptly named *The Human Condition*, Arendt (1958) provides theoretical distinctions between the *vita activa* and *vita contemplativa* as an origin point for considering human activity in public and private life. While the *vita contemplativa* (composed of thinking, willing, and judging) is a reflective contemplation of the world, the *vita activa* is "devoted to public-political matters" (p. 12). The activities conducted in the *vita activa* are: (1) labor, or the "biological process of the human body," (2) work, or the "unnaturalness of human existence" in the production of an "'artificial' world of things" that exist beyond the human life span, and (3) action, or that which "corresponds to the human condition of plurality…political life" (p. 7). Labor emerges in the energy we exert to sustain life itself (e.g., eating, sleeping, childbirth). Work occurs in the production of nonhuman entities separate from human life itself (e.g., manufacturing tools, clothing, or automobiles). Action manifests in meaning making in the public domain (e.g., identity formation, activism, storytelling) Action allows humans to congregate in the political sphere and shape the world in which they live.

Central to Arendt's (1958) project are the necessary distinctions between public and private life and a warning against their problematic overlap in what she terms the "social" (pp. 28, 38). Arendt describes public life as the concern for the common and private life as care for personal relationships and property. In public life, humans live together in communities tasked with negotiating standards of conduct, whereas in private life, humans live amongst their families and carry out the tasks to sustain life and the home. The social realm emerges when private concerns are brought into the public sphere or when public matters invade private life (p. 68). For Arendt, this becomes problematic as the social blurs the conceptual *foci* of the realms of public and private, which were formerly distinct. These distinctions become a starting point for scholarly consideration that continues in a contemporary moment.

Arnett (2013)[51] overviews Arendt's thought as it contributes to the field of communication ethics. Beginning with the distinctions that comprise the *vita activa*, Arnett (2013) explains that while labor ensures human existence from one generation to the next via the life process (child rearing and raising), work frames the human as a

[51] Globally, Arnett (2013) positions Arendt as a cautionary voice in response to the "artificial light" of modernity, a light coursing through society that generates undue optimism and unrealistic expectations from an unquestioning adherence to the paradigm of progress and an overemphasis on the capabilities of the individual, who attempts to remove the self from a larger social and historical embeddedness (p. 4). Artificial light begets "confusion" between and within spheres of existence, "conviction" regarding ungrounded worldviews, and "banality of routine" that clouds the reflective act of thinking, thus creating a blind adherence to processes and procedures that constrains creative responses (p. 4). According to Arnett, Arendt counters artificial light with the able metaphor "genuine light" that thinks and reflects, distinguishes between realms of existence, identifies the ground on which one stands, and opens new communicative responses (p. 3).

"creator and builder" of goods that are neither natural nor essential to the life process and action as "the human story with and among others" (p. 65). Action renders human work meaningful; it is the affirmation of work and ideas within the public domain. For Arendt, labor, work, and action are constitutive of the human condition, but it is action that distinguishes the human from both beasts and gods (p. 65). Arnett explains that, for Arendt, beasts conduct labor alone in the same way that gods labor and work in isolation—contrarily, action, as the affirmation of deeds in the public sphere by others, is unique to the human condition.

Arnett articulates how the intertwined functions of Arendtian labor, work, and action have historically structured public and private life throughout human existence. Leading toward a contemporary moment of cyber-mediated communication, Arnett reviews public and private life in the Greco-Roman world, the Middle Ages, and Modernity. For the Greeks and Romans, there was a clear delineation between public and private and the activities that occurred in each sphere. The public was the place of action, the affirmation of and striving for immortal deeds worthy of remembrance (p. 65). Conversely, the private was the realm of labor, limited to the household, where one owned property and raised a family.

With the collapse of the Roman Empire and onset of the Middle Ages, public and private realms shifted with the prominence of the Catholic church as a social authority. The Catholic church offered a public space of "freedom, courage, and risk" and the household a private space of "security, necessity, and survival" (p. 66). The Middle Ages emphasized a pursuit "for the eternal" rather than gaining public reputation for accomplishing deeds worth remembering (Arnett, 2013, p. 65), prompting a shifting emphasis from "'good deeds' in the public sphere" to "'good works' in the private human life" (p. 68). The Western Christian world of the Middle Ages charged the private sphere with the action once held in the public, emphasizing the eternal reward from works of charity, service, and giving rather than historical "immortality" from the retelling of publicly affirmed and remembered deeds.

With the transition into the Modern world, Arnett (2013) identifies Arendt's emphasis on the unforeseen emergence of the "social sphere of conformity," which eradicated the boundary between public and private life (pp. 67–68). Arnett (2013) characterizes the Arendtian public sphere in Modernity as a place where individuals reject tradition and substitute an "individualist" impulse to conform and "to stand above human history" (p. 66) for distinctive personhood. The public sphere of Modernity differs from that of the Greco-Romans in its disregard of the struggle involved with the construction of immortal deeds for an attitude that 'I arrived here on my own.' Modernity eliminates the celebration and acknowledgement of human action, the unique element of the human condition, in the public sphere and ushers in the social realm, or a "blurring of public and private," that "makes excellence anonymous" (p. 67). The Modern impulse, likewise, alters the private realm through a shift to the "escape into the intimate," or the pursuit of private property as the "center of one's attention" (p. 68). The social realm makes the recognition of human action and excellence impossible, due to the replacement of the agreed upon story that once bound the community together with the conformist individualistic attitude to stand above history and disregard tradition, thus weakening the human condition.

As Modernity displaced the traditional public domain tasked with uncovering meaning in human struggle and identifying excellence, the social realm found firm ground with an emphasis on “charm” and personality (Arnett, 2013, p. 67). Arnett explains how this shift unintentionally resulted from the Middle Ages’ emphasis on good works in the private sphere. The Modern mindset replaced good works of charity and service with personality, charisma, and individual disposition. Both Arnett and Arendt lament this substitution where charm, personality, and charisma rather than hard work and meaningful action determine merit and produce a sense that everything is worthy of remembrance.

Through his account of *The Human Condition*, Arnett (2013) offers four communication ethics implications. First, Arnett suggests that Arendt contends that the differentiation of labor, work, and action contributes to one’s ability to engage a task of meaningful creation. Second, Arnett privileges the public role of the storyteller that generates public acknowledgement of the value and merits of hard work and meaningful action. Third, Arnett clarifies how public and private life both contribute to the construction of identity. Finally, Arnett emphasizes attentiveness to contemplation “before, during, and after action” (p. 76). Thoughtful reflection reveals whether an activity sustains life (labor), allows life to function (work), or allows life to flourish (action) and carefully distinguishes public and private realms of human interaction. For human flourishing, public and private life cannot submerge into one social realm, but instead must exist in tandem with the recognition that they shape identity together. Arnett’s communication ethics application announces that we are part of an ongoing story and that our contributions to the human condition shape its ongoing development.

Following Arnett's lead, Eicher-Catt (2013) presents a semiotic phenomenological portrayal of the Arendtian public/private divide applied to cultural functions of (in)civility. Eicher-Catt explains that rising instances of incivility in the public domain directly reflect the problematics Arendt warned against with the emergence of the social. Eicher-Catt argues that as divides between public and private life blur into a social realm, boundaries between Self and Other are "ignored, erased, co-opted and/or blurred within sign actions" (p. 15). In response, Eicher-Catt urges us to consider the body as a "sign" and the actions of this "embodied sign" as meaningful to shaping public discourse, pushing us toward reflective consideration of the "'good of the *common*,' not the common *good*" (p. 3). Eicher-Catt's application of Arendt calls us to re-implement distinctions between private and public life that facilitate healthy public discourse (p. 3).

According to Eicher-Catt (2013), the problematic discourse of the social realm overlooks the body as a sign, eliminates possibilities for "real discourse," and erases difference for conformity or extreme individualism based on free speech (pp. 5, 8). In the social, private bodies, rather than shaping the public sphere with the weight of their significations derived from experience, become a sign "overrun by the public codes of intelligibility" (p. 8). The social warps discourse and civility to following "pre-learned social codes of conduct," rather than attending to and questioning the situation at hand (p. 8). In addition to the blind adherence to existing codes, the social might conversely reject the pre-existing codes and fixate on the assumption that "our messages are just as legitimate as another's (free speech)" (pp. 8, 15). The social either adheres blindly to the past with misunderstood perceptions of historical discourse or rejects history entirely for an individualist mindset that privileges and conceptualizes the self beyond all else (p. 8). The problem within the social sphere centers on the misappropriation of public and private discourse.

Through a semiotic phenomenological examination of discourse, Eicher-Catt attempts to reconcile the problematics of incivility and disingenuous civility by acknowledging and respecting boundaries between public and private spheres that maintain the good of the common. Eicher-Catt's articulation of civility guides an understanding of the public as the "human CAPACITY [for phenomenological negotiation of] sign actions that have real consequences to our communal existence" (p. 15). For Eicher-Catt, civility locates the public as an "aesthetic space" that fully "honor[s] the private, ineffable realm of the Other" (p. 15). Semiotic phenomenology offers a way to maintain the distinctions between public and private and uphold the good of the common in a mass mediated moment, where the ascendance of the social threatens the ability to respect, honor, and learn from others.

Butler (2015) also affirms the importance Arendt's notion of action but provides a revisionary application to its relationship with public life. In *Notes Toward a Performative Theory of Assembly*, Butler responds critically to Arendt's public and private distinction. Butler emphasizes the communicative power of performative human action, but understands Arendt's work to limit action to public life alone. Instead, Butler advances a proposal that integrates public and private influences for the engagement of action without falling prey to the problematic realm of the social. Butler seeks to uncover the formation of embodied, concerted action that questions "the inchoate and powerful dimensions of reigning notions of the political" (p. 9). Butler acknowledges that performative embodiment constitutes human action to challenge social imbalances and injustices without limiting such action to the public sphere. Action exists where bodies meet one another, properly supported by public and private influences. For Butler, Arendt’s divide between public and private life threatens the disavowal of “interdependent relations upon which our lives depend” (p. 44). The conditions for action in the public sphere rely upon that which is begotten by the private sphere. For Butler, the private sphere grounds possibilities for people to appear and act in public spaces.

In texturing the Arendtian public/private dialectic, Butler (2015) introduces the important notion of “performativity,” or that through the act of acting itself, individuals or groups embody the power to shape the public sphere (p. 58). Butler’s performativity recognizes that public space lies “between the people,” is not “tied to a location,” and is always and invariably embodied, even when virtual (p. 73). For Butler, Arendt’s notion of “material supports for action” is limited to the private sphere and is not only “part of action,” but also “what is being fought about” (p. 73). The role that the body plays in action clarifies political demonstrations in the public sphere (e.g., Arab Spring, the Occupy Movement, antiprecarity demonstrations). Butler stresses the import of and necessity for the private to create the conditions for action in the public sphere. Her conception of performativity rests on coordinates of the body, appearance, equality, vulnerability, and interdependency.

The body permits the manifestation of communicative action. Butler does not limit performativity or the body to the physical realm; they are also inherent within the virtual (pp. 8, 11). Butler accepts the Arendtian articulation of appearance and equality as imperative for action, yet rejects their limitation to the public sphere. Butler (2015) explains that Arendtian appearance is neither a physical location nor outside the action that "invokes and constitutes it" (p. 77). Actors embody appearance in both public and private communicative relationships. Butler emphasizes that the Arendtian "principle of equality" suggests that freedom happens in the differences that emerge within the relations that exist between us (p. 88) rather than in sameness or commonalities between members of a community. Butler extends this claim by adding equality, which surpasses both speaking and writing as bodies who, through action, "bring the space of appearance into being" (p. 89). The space of appearance derives from action and the maintenance of the relation of equality in order to facilitate discourse.

Furthermore, Butler textures this discussion of appearance and equality with notions of vulnerability and interdependency. Butler frames vulnerability as an "openness" (p. 149) that infrastructures, architectures, and human relations cast weight upon in the constraining and enabling of public discourse. Embodied vulnerability is both "beyond" and "part of" communicative actors (Butler, 2015, p. 149). Interlocutors and their discourse are shaped by existing material conditions. Butler's interdependency suggests that solidarity forms between unknown and undetermined participants in the public sphere; for Butler, our very notion of the self emerges only through our interdependency with others. When entering the public, communicators have no control over "who else is arriving" (p. 151). Thus, Butler recognizes that we must live and interact in a public domain made of others whom we do not choose and, at times, may not know or like; yet, we enter this domain partially formed, open and vulnerable to the influence of these others.

Butler turns to Arendt to warn that any attempt to control which others coexists the world alongside us is an act of genocide (p. 113). Butler relies upon Arendt's critique of Adolf Eichmann to articulate an exemplar who engages such an act. Eichmann was a high-ranking S.S. officer in charge of scheduling transportation to the Nazi death camps. Arendt served as the *New Yorker* reporter at the Eichmann trial in Jerusalem. Her response to Eichmann was to label him as a bureaucrat who embodied the "banality of evil"—extreme commonness coinciding with unreflective thoughtlessness. Eichmann's crimes against humanity had become commonplace as he engaged acts without question. Arendt finds Eichmann guilty of failing to consider the consequences of his actions and their effects on the public sphere. Furthermore, Butler uses this case to demonstrate violations against the fundamental human qualities of appearance, equality, vulnerability, and interdependency.

Arendt invites society to the *vita contemplativa*, or the contemplative life that involves thinking, willing, and judging, as an antecedent to action. Just as in the Eichmann trial, Arendt recognizes that a lack of thoughtful and reflective engagement on one's actions can close possibilities for creative responses to challenge a problematic *status quo* and have detrimental effects on the public sphere. Arnett (2013) recognizes that, for Arendt, the public sphere of Modernity has all but collapsed into the social realm, which ambiguously mixes public and private concerns and exchanges action from the Greco-Roman public recognition of immortal deeds worthy of remembrance for a public acknowledgement of charm, personality, and charisma that believes everything is worth archiving. Among his central implications is the reminder to think before, during, and after action, exemplifying the productive interaction between the *vita contemplativa* and *vita activa.* Likewise, Eicher-Catt (2013) notes that problematic discourse functions—banality ('this is unquestionably the way we handle business') or narrow-mindedness ('my way of doing business is just as good as yours and I do not need to listen to you')—ignore the human capacity for contemplation, deny an invitation for discourse, and eliminate opportunities to learn from difference. Butler (2015) notes that action always carries embodied experience from the private and can occur wherever bodies meet (in either public or private realms). Contemplation must accompany action to ensure the good of both the public and the private spheres. The final section offers communication ethics implications from this study.

Communication Ethics Implications

This chapter contends that cyberbullying emerges from the confusion of ambiguously mixed public and private spaces online; we anachronistically engage cyberspace, confusing it as either a fundamentally public or private space, when in actuality this dialectic transforms it into something wholly other. A review of literature on the dialectic revealed that scholars have recognized the ways cyberspace has changed public and private life since the earliest days of the Internet. Furthermore, communication scholars note how these changes alter interpersonal communication with ongoing discussions about how these alterations either enhance or diminish public and private life in face-to-face relationships and physical spaces. Hannah Arendt's theoretical distinctions of public, private, and social urge necessary attentiveness to reflective contemplation accompanied by meaningful action. As scholars continue to extend Arendt's work, the implications for the ever-evolving public, private, and social spheres manifest insight for uncovering communication ethics implications that can offer a first response to this first-tier cyber attack.

The dialectical method engaged by this project, informed primarily by Kenneth Burke and David Gunkel, facilitates an understanding of the public/private opposition within cyberspace. First, Burke's (1941; 1945/1969) articulation of dialectic names the terms in tension—here, public and private life. These two spaces exist in tandem; the dialectic will not resolve itself, but rather, cyberspace must live amidst the give and take as partially public and partially private. When posting messages within cyberspace, users must recognize that online spaces ambiguously combine public and private life and that each word carries multivocal weight as well as numerous possibilities for diverse interpretations. Gunkel (2007) extends this recognition by calling us to think about cyberspace as something completely otherwise, fundamentally transformed by the dialectic. Cyberspace, as a potential third term emerging from the synthesis of public and private spaces, must be thought of as comprehensively alternative to existing standards. Cyberspace is neither exclusively public nor private but instead wholly and radically different. Users cannot engage cyberspace as a blurred realm between public and private without falling into the problematic realm Arendt termed the social, which yields problematic discourse functions, as Eicher-Catt demonstrated. Cyberbullying, thus, becomes an exemplar of such problematic discourse functions.

This chapter contends that cyberbullying emerges in response to misunderstanding the public/private dialectic of cyberspace. While some scholars contend that technologies and cyberspace enhance communication in public and private contexts (Anderson, 1994; Cathcart & Gumpert, 1994; Rhaimi, 2011; Walther, 1992, 1993, 1996; White, 2015), others argue these reduce the human capacity for communication (Carr, 2010, 2014; Jackson, 2009; Turkle, 2011; Putnam, 2000). Although both may be true, scholars recognize the means of user engagement on cyber platforms determines whether or not cyberspace enhances public and private communication (Colleoni, Rozza, & Arvidsson, 2014; Flaxman, Goel, & Rao, 2016). Likewise, scholars call upon individual users to intervene in ongoing manifestations of cyberbullying (Brody & Vangelisti, 2016; High & Young, 2018). Society must recognize that human actions online implicate human bodies and physical worlds that contextualize what happens as a result of cyber-mediated communication and cyberbullying. This chapter finds four implications:

1. Cyber-mediated communication across cyberspace reconfigures public and private spaces. The Internet, World Wide Web, and cyberspace enter a space and affect public or private content in unpredictable and unstable ways. Particular users, however, makes a conscious choice regarding how to interact with others in cyberspace as either an enlarged public sphere or reduced echo chamber that only confirms their existing beliefs/sentiments.

2. Cyberbullying as a first-tier cyber attack is the manifestation of the confusion of this newly constructed, ambiguous space. Cyberbullies fail to recognize their embeddness in a larger online context that combines various spheres of human interaction beyond the context in which they know particular targets.

3. The consequences of posting private information to an online public setting include a 24-7 exposure to the cyberbully and the blurring of formerly separate support systems. Where in the physical world, the targets of bullying can return home to a space

that the bully cannot access, the virtual world does not permit such distinctions between realms of existence. The entanglement of computer technologies and identity makes users increasingly vulnerable to the relentless attacks on the virtual self in cyberspace.

4. Arendt's *vita contemplativa* can act as an antecedent to the *vita activa*—contemplation and reflection should accompany action to ensure that communication is thoughtful. To prevent cyberbullying, users must embrace the call to think, will, and judge before posting and recognize that their posts traverse a realm that is radically other than traditional conceptions of public and private. Cyberbullying and cyber-mediated communication implicate human bodies in ways fundamentally otherwise than physical public and private realms.

Cyberbullying emerges when users engage cyber-mediated communication thoughtlessly and fail to recognize that cyberspace, while containing both public and private realms, is greater than the sum of these parts. Although communication online is frequently anonymous (Arntfield, 2015), the manner in which users communicate through online platforms affects lives and identities offline in deeply personal ways. The next chapter introduces this dialectic of anonymity and identity as another fundamental tension defining cyberspaces as wholly different than offline spaces. Furthermore, the next chapter extends consideration to individual/corporate cyber theft as a second-tier cyber attack emerging from misconceptions of the highly dialectical nature of cyberspace.

Chapter 4

The Anonymity/Identity Dialectic of Cyberspace:

Cyber theft as a Second-Tier Attack

Introduction

This chapter examines the ways in which cyberspace, the World Wide Web, and the Internet restructure user conceptions of self through online anonymity and identity. By overviewing the communication literature addressing user constructs of anonymity/identity, pursuing scholarship on identity data cyber theft, and turning to the conception of risk society offered by Ulrich Beck[52] (1986/1992), this chapter suggests that reconsidering the anonymity/identity dialectic in an online context is necessary to limit cyber theft. Cyber theft as a second-tier attack includes the nefarious use of cyberspace as a platform for personal and corporate data theft in various cyber contexts. This project contends that cyber theft emerges from confusion and misappropriation of cyberspace due to its dialectical nature in regard to identity and anonymity. Increasing corporate reliance on the Internet accelerates opportunities for identity theft and drastically increases the number of potential victims (Siegel, 2007). As such, corporations' online records become an ideal target for cyber theft, making vulnerable personal data and identity.

The first section of this chapter situates conceptions of cyberspace within a dialectic of anonymity/identity as articulated in the scholarly communication literature.

[52] Ulrich Beck is described as "one of Germany's most prominent public intellectuals" (Smale, 2015, para. 1). He was presented one of the first awards for lifetime achievement bestowed by the International Sociological Association (Smale, 2015, para. 11). *Risk Society*, his most known work, published in 1986, was given "currency" by the Chernobyl nuclear accident that led to the work's translation into 35 languages (para. 4). He is the author of 20 books, including *The Reinvention of Politics: Rethinking Modernity in the Global Social Order* (1997), *World Risk Society* (1998), *What Is Globalization?* (1999), *Individualization: Institutionalized Individualism and its Social and Political Consequences* with Elisabeth Beck-Gernsheim (2001), *Cosmopolitan Vision* (2006), and *German Europe* (2013).

This research explores the various benefits of and detriments to online anonymity and considers how participation in online spaces contributes to identity construction as a selective rhetorical practice. The second section recognizes cyber theft as a phenomenon most often occurring through attacks to corporations and their personal data records and thus explores common corporate responses to attacks of cyber theft. Due to the scant literature in the field of communication addressing cyber theft in the corporate context, this section turns to scholarship in law, management, and information sciences to understand cyber security recommendations for corporate practitioners. The third section turns to the work of sociologist Ulrich Beck (1986/1992; 1992), who offers a theoretical articulation of a "risk society" within what he terms "reflexive modernity" and to later extensions of Beck's risk society into a cyber and digitalized context (Deibert[53] & Rohozinski,[54] 2010; Lupton,[55] 2016). The chapter concludes with implications of this application and a transition to the national/global dialectic.

The significance driving this chapter rests in the call to understand the anonymity/identity dialectic of cyberspace. Scholars recognize that the construction of online identity is a rhetorical practice (Brookey & Cannon, 2009; Brunskill, 2014; Eklund, 2011; Jordan, 2005; Khang & Yang, 2011; Walther, 1996; Zhang, 2008) and

[53] Ronald Deibert is a professor of political science and the director of the Citizen Lab in the Munk School of Global Affairs at the University of Toronto, as well as a co-founder and co-funder the OpenNet Initiative (2003–2014) and Information Warfare Monitor (2003–2012) projects. Previously, Deibert acted as the vice president of global policy and outreach for Psisphon, an organization dedicated to opposing digital censorship ("Ronald Deibert," n. d.).

[54] Rafal Rohozinski is a respected cyber expert and a consulting senior fellow for the Cyber, Space and Future Conflict Programme at the International Institute for Strategic Studies (IISS). Rohozinski is also a co-founder of the SecDev Group, a political risk and intelligence agency. Rohozinski is among *Forbes* magazine's list of top ten cyber experts to watch. Additionally, Rohonzinski has taught at and received fellowships from the Ford Foundation and the Munk School of Global Affairs" ("Rafal Rohozinski," 2019).

[55] Deborah Lupton is Centenary Research Professor in Communication at the University of Canberra, Australia. Lupton has authored or co-authored 16 books and 170 journal articles and book chapters, in addition to having edited or co-edited six books. Within her research interests fall big data cultures, surveillance society, digital technologies, the analysis of wearable technologies, and risk ("Deborah Lupton," 2017).

identify two opposing functions of anonymity: (a) as helpful and contributing to the protection of civilian rights that further democracy (Akendiz, 2002), explore offline identity (Mahfood, Olliges, Astuto, & Suits, 2005), and engage with social movements (Tsui, 2015), or (b) as harmful because it fosters theft (DiMaggio et al., 2001) and/or "hateporn" (Williamson & Pierson, 2003). However, anonymity and identity constructions exist far beyond the control of individual Internet users; regardless of what users deliberately post or store in online platforms, access to their personal data is often far more available due to corporate records and customer profiles. This context frames the background of the anonymity/identity dialectic and a corresponding connection to cyber theft as a second-tier cyber attack.

Situating Cyberspace within the Anonymity/Identity Dialectic

Communication scholars demonstrate how cyberspace has become a dynamic platform that allows users opportunities to express and form identity and to hide behind a mask of anonymity (Brookey & Cannon, 2009; Jordan, 2005; Mahfood, Olliges, Astuto, & Suits, 2005; Lin, 2017; Marciano, 2014; Tsui, 2015). This discussion situates the possibilities for identity and anonymity as a defining dialectic of cyberspace. While some scholars consider the anonymity of cyberspace as helpful (Akdeniz, 2002; Bargh & McKenna, 2004; Mahfood et al., 2005; Tsui, 2015), others contend that it is harmful (DiMaggio et al., 2001; Williamson & Pierson, 2003). Likewise, some scholars contend that cyberspace constructs identity anew (Brookey & Cannon, 2009; Brunskill, 2014; Eklund, 2009; Jordan, 2005; Marciano, 2014), while others consider it a reflection of the physical world (Boler, 2007; Brookey & Cannon, 2009; Eklund, 2009; Mullany, 2004). This section engages this split in the literature and focuses on how online systems provide opportunities for both anonymity and identity that require us to reconsider cyberspace in light of this dialectic.

The earliest discussions of this dialectic emerging in the mid-1990s grant us coordinates for later discussion. As introduced in the previous chapter regarding the public/private dialectic, Rob Anderson (1994) contends that electronic communication provides opportunities for mediated presence and identities as it opens possibilities for public and private dialogue between users, and Joseph B. Walther (1996) recognizes that, similar to his stance of cyber-mediated communication as a tool that can either enhance interpersonal relationships or isolate users, the implications of cyber-mediated communication largely mirror our practices of use. Specifically, Walther recognizes that computer mediated-communication can be incorporated strategically as either personalized (with heightened identity) or depersonalized (with heightened anonymity); the user engagement with the platform determines the end result. As this earlier conversation extends to conceptions of anonymity and identity within cyberspace, this dialectic becomes important to understanding the role of cyber-mediated communication and its implications for identity expression and anonymous action.

A central concern about the implications of anonymous online action is emergent possibilities for hate speech and the expression of extremist ideologies. Paul DiMaggio, Eszter Hargittai, W. Russel Neuman, and John P. Robinson (2001) offer an early characterization of anonymity in the young World Wide Web, articulating fear that this platform for communication obscured by a mask of anonymity “may heighten the level of extremist and hate speech” (p. 321). Their work follows Lawrence Lessig (1999), who hypothesizes about the potential for emergent “institutions of self-regulation” to combat the potentially harmful uses of cyberspace (as cited by DiMaggio et al., 2001, p. 321). DiMaggio et al. offer three proposed regulatory standards. First, they call for "equality in Internet access" to ensure fair opportunities for voicing opinions about political, economic, and social issues (p. 328). Second, they advocate for "meaningful privacy norms" that could protect users from threatening actions by anonymous actors (p. 328). Finally, they suggest "rules governing intellectual property" that protect the creative and original work of civilians, who could then share information in a cyber-mediated context effortlessly without the threat of theft (p. 328). Implicit within the three proposed standards offered by DiMaggio et al. is an assumed association between anonymity and problematic behaviors that potentially pose various threats to society ranging from hate speech to information theft.

Extending from this perceived association between anonymous action and problematic behaviors, Larry Williamson and Eric Pierson (2003) label this proliferation as *hateporn*. Williamson and Pierson define hateporn as "the promulgation through the Internet of the rhetoric of hate" (p. 251). They identify five online spaces/practices where hateporn thrives: (1) the misappropriation or radicalization of religious traditions; (2) interaction with immersive online gaming communities; (3) participation in chat rooms; (4) listening, sharing, and viewing music and music videos; and (5) quasi-educational sites that "pedal hate in the name of 'enlightenment'" (p. 252). Particularly, they find hateporn problematic as it influences, or perhaps indoctrinates, children into the use of and belief in hate messages. As the cyber-environment facilitates "complete-anonymity," it eradicates notions of "accountability" and ethics (p. 261). Thus, Williams and Pierson urge society to "rethink accountability" in "legal ethics" and "conventional critical praxis" given the possibilities of online anonymity (p. 261). Williams and Pierson extend the associations of anonymity and criminal activity by arguing that patterns of hateful rhetoric tear at a healthy and functioning society.

Countering this presupposed connection between anonymity and "criminal activity," Yaman Akdeniz (2002) announces that online anonymity is fundamental to ensuring a democratic cyberspace and becomes a prerequisite for guaranteed "free speech" online (p. 224). Without the possibility for anonymous action online, the Internet, for Akdeniz, ubiquitously becomes a platform for corporations, law enforcement, and government entities to engage in "personal snooping" (p. 223). The Internet invites an un-invited voyeurism, opening possibilities for individuals and institutions to peer into "personal information and correspondence," compromising "confidentiality" and "authentication" (p. 223). For Akdeniz, online anonymity constructively prevents these unwanted intrusions by enhancing the "economic" and "cultural" benefits of the Internet for "individual freedom and collective democracy" (p. 234). Online anonymity provides opportunities for free speech and an enlarged cyber-mediated public sphere.

Likewise, John A. Bargh and Katelyn Y. A. McKenna (2004) advocate for the benefits of online anonymity. In fact, they contend that this anonymous platform offers "transformational qualities" to cyber-mediated communication and enhances the quality of relationships between and among users (p. 586). According to Bargh and McKenna, online anonymity fosters opportunities for "self-expression" that allow users to reveal personal values and beliefs; in these instances of online anonymous self-disclosure, people feel secure enough to express themselves freely and thus build relationships based upon shared perspectives on deeply personal topics (p. 586). In this way, online anonymity advances interpersonal relationships and accelerates the depth of connection between users in a short period of time. Bargh and McKenna find that online anonymity offers opportunities for self-expression and relationship growth often masked in face-to-face physical spaces.

While celebrating the value of anonymity in connecting online users and building relationships between them, Amanda D. Lotz and Sharon Marie Ross (2004) examine the potential to use Internet forums for audience research. Through online platforms of self expression, users disclose information about personal beliefs and attitudes that can meaningfully contribute to academic and corporate research; however, problems of "perceived privacy," "consent," and "balancing anonymity with data accessibility" produce novel ethical questions for researchers when using Internet forums for data collection (p. 502). These problematics render "ethically responsible research methodology" complex and necessitate "reflexivity throughout the research process" (p. 502). Bearing in mind the coordinates of privacy, consent, and anonymity, Lotz and Ross find that there is no "set of universally applied rules for Internet-based audience research" (p. 509). Because of unanswered questions about anonymity, the Internet becomes an unstable source for ethical research as participants are often unaware of how others use their information or the consequences of their disclosure.

A helpful example explicating a similar insight emerges from Louise Mullany (2004), who examines the construction of gender identity and social patterns of power relationships in online advertising. Writing during the era of Web 1.0 when the Internet offered a platform of interconnected hyperlinks but had not yet developed extended possibilities for user-generated content, Mullany describes the mechanism of "email advertising language" (p. 292). She argues that as users reveal gender identities online, corporations begin to interact with them according to conventional assumptions about the "binary oppositions between male-female and masculinity-femininity" (p. 303). According to Mullany, disclosure of gender identity and the consequential advertising practices constrain online representations and self expression. By using the existing perceptions of conventional gender norms, advertisers inherently support and strengthen "existing power relations" and stereotypes (p. 303). Mullany, similar to Lotz and McKenna's (2004) concerns about data collection from online anonymous self-disclosure, emphasizes problematic consequences about online identities, particularly related to how disclosure of gender identity corresponds to the proliferation of advertising practices that further establish offline power relations.

Extending this discussion into an era of Web 2.0, Lokman Tsui (2015) warns of the increasing ease for cyberspace to lead not only to corporate research and advertising but also to government surveillance. Specifically considering anonymous participation in social movements via cyberspace, Tsui emphasizes governmental capabilities "to resist, respond to and counter" social movements mediated through cyber platforms (p. 447). While the anonymous nature of actions on the Internet "complicates" these efforts, governmental agencies are able to adapt to, "anticipate[,] and respond to" evolving technological environments (p. 452); even when users engage anonymous online avatars, governments and corporations find ways to identify and profile specific users. Furthermore, the Internet lies at the intersection between the government and commercial corporations that "decentraliz[e]" the digital milieu and erase possibilities for online autonomy (p. 452). Positioned at this intersection, all Internet users fall under government and corporate surveillance. Without strict laws dictating reasonable and appropriate surveillance, financial resources and research efforts result in rapid advancements in surveillance technology accompanied by little accountability, protection, or transparency from corporations or government entities (p. 452). Despite the anonymous nature of online interactions, constant and pervasive surveillance of specific and identified individuals becomes increasingly commonplace.

Continuing discussion about ethics and the dialectic of anonymity and identity, Sebastian Mahfood, Ralph Olliges, Angela Astuto, and Betsy Suits (2005) offer a "canon" of readings that guide ethical consideration of cyber-mediated communication (p. 11). Specifically, they identify online anonymity as an "ethical issue[]" and describe how anonymous online actions actually partake in identity formation and exploration with consequences for offline self development (p. 4). They explain that anonymous interactions online facilitate participants' efforts to "explore their own identities, reconstruct their own worlds, and engage others in virtual communion" (p. 7). Through this process of anonymous identity exploration, "meaningful" communication constructs communities that contribute to users' conceptions of self in both online and offline contexts (p. 7). Aware of existing practices of identity masking in physical social settings, they contend that the "immediate" anonymity of cyberspace can protect individuals under the threat of persecution and also assist users to "seek truth" when their personal identity might act as a barrier to uncovering a certain kind of knowledge in nonvirtual spaces (p. 7). Anonymity can provide users with opportunities to practice "narrative reasoning" that allows participants to test different solutions to similar problems that they might encounter in the real world without threat to their name or recognition of their face (p. 7). This environment enhances ethical communication and identity formation by releasing "social pressures" that limit actions in offline contexts (p. 17). Mahfood et al. find several benefits to online anonymity in the development of a strong community and announce the interconnected nature of online anonymous action as it reflexively shapes offline identity and conceptions of self.

John W. Jordan (2005) also considers the ambiguous intersections between community and identity formation in cyberspace by pointing toward a case study that reminds us that there is no guarantee that online identity expression corresponds to offline reality. Jordan examines the "strange events" surrounding Kaycee Swenson's blog, documenting the challenges of an American teenager living with and battling leukemia (p. 200). Although the blog recounted Swenson's struggle with leukemia for over two and a half years and drew "many supporters," she never actually existed in the physical world (p. 200). Kaycee Swenson was naught but a "digital dream," an online illusion created by Debbie Swenson. This fictional blog brought outrage from followers and fellow bloggers, prompting questions about the "relationships between computers, community, and communication" (p. 200). Jordan points to two implications from these occurrences. First, the size and diversity of the Internet population denies correlation between network access and identity; identity as portrayed online cannot provide a "great deal" of information about those with whom we communicate via cyberspace (p. 215). Second, society lacks a "common definition of 'community,'" bringing forth multiple motivations for users' participation and identity portrayals online (p. 215). To better understand the implications of identity and anonymity in online communities, Jordan calls for attentive focus on the “contingent circumstances” and “rhetorical language” that cause online communities to emerge and that motivate users to identify and participate with others through cyberspace (p. 215). For Jordan, ambiguity and uncertainty characterize online communities, limiting our ability to understand and even trust identities as portrayed in online spaces.

Following a recognition that online spaces produce ambiguous portrayals of reality that reflect a potentially dark side of the human condition, Brian Simpson (2005) considers appropriate and problematic methods of sheltering children from these encounters. Simpson (2005) contends that for children, online interactions contribute to identity exploration in significant and meaningful ways. This recognition prompts him to reconceptualize notions of “harm” and protection as it relates to both “‘inappropriate’ interactions” and the “right to access” (p. 116). For Simpson, filters that protect children from all potentially inappropriate online content are in fact harmful as they produce a fictional space that fails to represent the dangers of online and offline experiences. These filters become particularly problematic as they encourage unrealistic expectations and perceptions of the world. As an alternative, Simpson calls for a “balance” between blocked content and exposure to potentially “transgressive online activity” (p. 130); just as we cannot filter all pain, anxiety, or fear from children’s experiences of the physical world, we cannot create a disingenuous space online that masks the potential real dangers of online interactions. A balance between blocked content and online transgressions allows children the “right to play” and construct “an informed and creative imagination” (p. 130). For Simpson, children forming their identities should have the right to explore the Internet with a balance between age-appropriate and inappropriate content similar to that which they might confront in the physical world.

Advancing the acknowledgement that online and offline interactions co-inform reflexive notions of identity (despite online possibilities for anonymity), Megan Boler (2007) celebrates the potential for "New Digital Cartesianism" that further divides conceptions of mind and body and laments the reality of unactualized embodied online interactions. Boler advocates for the ability for the Internet to provide a space where users can participate and interact with others despite discriminatory limitations of bodily appearance based on gender, race, (dis)ability, and other features. In this way, a digital divide between mind and body could advance opportunities and empower anonymous individuals to act; however, rather than complete anonymity, Boler (2007) suggests that cyber interactions implement "reductive bodily markers that re-invoke stereotypical notions of racialized, sexualized and gendered bodies" (p. 140). She contends that online communication, despite transcending the corporeal, employs the body to determine reality and truth (p. 140). Boler demonstrates how, even when acting online through an anonymous avatar void of race, gender, religious orientation, and age, for example, users "crave information about traditional markers of the body" in offline settings (p. 140). Despite being anonymous digital avatars, users are unable to escape their physical embodiment in online interactions; even in virtual space, we act through bodies contextualized within existing social and cultural standards.

Consistent with this finding, Lina Eklund (2011) explores the female construction of gender identity and sexuality in the social context of the massive multiplayer online role-playing game *World of Warcraft*. She finds that games like *World of Warcraft* mirror the physical world, meaning that female players carry “offline gender identity and social contexts when they go online” (p. 339). These contexts of identity are present in online identity construction for female players, but these players in the virtual world gain some possibility of expression “depending on their needs and wants” (p. 339). As real world sexualities inform the online construction of gender identity, the virtual identity, although created within the context of physical world identities, offers possibilities for selective portrayals that may be similar or dissimilar from physical world identities.

Also recognizing that online portrayals of identity correspond with selective representations of one’s complete offline personhood, Mei Zhang (2008) announces the rhetorical strategies that contribute to identity portrayal. Zhang examines a Chinese university alumni website to determine the “construction of harmony, memory, and identity online” (p. 86). She provides an analysis of alumni group profiles to understand identity expression in personal, family, and national contexts. Her analysis finds that cyberspace is seminal in allowing users to partake in “a harmonious community, collective memory, and cultural values” (p. 86). Interestingly, she found that users selectively expressed images and messages that portrayed identities privileging harmony as a consistent and “defining theme” across profile messages (p. 88). Zhang emphasizes online identity construction and expression as a distinctive employment of rhetorical strategies that selectively portray the self, aimed toward shared expectations and values.

Also emphasizing possibilities for users to express and explore identity via selective representations of self, Robert Alan Brookey and Kristopher L. Cannon (2009) and Smeeta Mishra and Gaby Semann (2010) celebrate the ability for online anonymity to grant the expression and exploration of identities outside of majority demographics or traditional expectations. Specifically, Brookley and Cannon (2009) consider gender and sexual identity formation in the online gaming community, Second Life (SL). Brookey and Cannon recognize SL as a particularly helpful platform for considering gender and sexuality as it grants users the primary responsibility of content creation as they design avatar representations of self. Brookey and Cannon suggest that SL is “liberat[ing]” as it permits violations of “traditional gender roles and sexual norms” alongside conventional expressions representative of real life identity and contexts (p. 146). Likewise, Smeeta Mishra and Gaby Semann (2010) consider online anonymity within the context of practicing the Islamic faith within the United States by South Asian immigrants. As Gisela Webb (1995) observes, online anonymity becomes important as “mainstream American social life is often at odds with the practice and performance of Islam” (as cited by Mishra & Semann, 2010, p. 87). Despite offline religious prejudice, Mishra and Semann (2010) praise online anonymity for facilitating the comfortable discussion of “personal questions” that pertain to “relationships, diet, clothing, personal grooming, finances, etc.” (p. 99). Anonymous interactions via cyberspace allow individuals to explore alternatives to traditional standards and majority identities.

Addressing these alternative possibilities within transgender communities, Avi Marciano (2014) acknowledges how anonymous online participation permits members to act without the offline threats of persecution or discrimination. Addressing the intersections of online and offline identity construction, Marciano finds three spheres of participation: preliminary, complementary, and alternative. The preliminary sphere allows users opportunities to explore transgender identities virtually and anonymously before embracing these identities in physical world contexts (p. 830). The complementary sphere offers "*another* social arena" for members of transgender communities to express this aspect of their identity online as an accompaniment to identifiable offline contexts (p. 830). The alternative sphere is "especially pertinent" as it facilitates identity expression without the fears and threats associated with "offline limitations" (p. 834). As an alternative sphere, the anonymous quality of cyberspace provides transgender users "meaningful experiences" that may be difficult to find offline (p. 834). Transgender people can enter cyberspace and remove misrepresentative or inadequate portrayals for selective expressions of "chosen identities" that create alternative realities (p. 835). Marciano announces possibilities for selective identity portrayals in cyber-mediated contexts to represent particular groups of people more adequately than identity management strategies used to navigate physical world contexts.

David Brunskill (2014) problematizes practices of selectively framing identity via social media platforms, announcing dangerous implications for the user's psyche. Brunskill (2014) characterizes social media as a "show and tell process" that exhibits only positive and strategically framed content (p. 408). By showcasing only "favourable material" from the lives of individuals, the user of a social media site creates a "positively skewed" avatar with significant divides between online and offline image portrayals (p. 408). In turn, the avatars that users create for themselves place the psyche at risk and can trigger "shifts" that result in perceptions of inconsistent identity emerging from what has been left in anonymity (p. 409); as social media users manage personal profiles and view their peers, they begin to take note of incongruous identity portrayals and appearances in self and other. To reconcile these discrepancies, Brunskill calls for a merging between online and offline identities that offer more representative portrayals of self that result in "one balanced, harmonious whole" (p. 409). Brunskill advocates for users of cyberspace to build more representative portrayals of the self, inclusive of both their assets and faults.

Bo Feng, Siyue Li, and Na Li (2016) address how more representative identity constructions can strengthen support messages in online communities. Feng, Li, and Li explore online support communities that allow users to interact anonymously through self-generated accounts. They find that within these anonymous platforms, "personal identity cues" may contribute to successful online communication by affording "more person-centered and polite support messages" (p. 268). They suggest that identity construction strategies such as profile/account self-identification photos and disclosure of first names may contribute to higher levels of perceived social presence that leads to "more sensitive and socially appropriate support" (p. 268). Despite this contention, they argue that identity cues cannot replace the importance of the actual communication interactions and that identity cues do not guarantee the success of online support messages. Feng, Li, and Li note the potential for identity cues to contribute to stronger support messages despite the possibility for anonymous interaction.

Moving from anonymous person-to-person support sites to community formation, Zhongxuan Lin (2017) examines "'re-imagined communities'" created by online participants in Macau (pp. 229–230). For Lin, re-imagined communities "resist" identity legitimation, "reclaim their resistance identity," and "restructure their project identity" (p. 230). This process of resisting, reclaiming, and restructuring provides coordinates to "re-imagine" the future "beyond national identity" (p. 242). The study suggests that new communities can emerge based upon the "identity politics of the governed" rather than the “identity politics of the governors” (p. 242). Lin offers coordinates to empower citizens (the governed) to compose social identities that counter and divert from the institutionalized messages of societal identity hierarchies distributed by the governors.

Communication and mass media scholars have participated in discussions about the implications of identity construction and anonymous action online since the onset of Web 1.0 in the 1990s; Anderson (1994) and Walther (1996) announce early consideration about how users cultivate identity and obscure themselves in anonymity via computer-mediated communication platforms. Scholars debate the helpful (Akdeniz, 2002; Bargh & McKenna, 2004; Mahfood et al., 2005; Tsui, 2015) and harmful (DiMaggio et al., 2001; Williamson & Pierson, 2003) implications of online anonymity. Likewise, scholars consider how cyberspace introduces novel strategies for identity construction (Brookey & Cannon, 2009; Brunskill, 2014; Eklund, 2009; Jordan, 2005; Marciano, 2014), how participation in online platforms creates an alternative space for identity expression that mirrors or reinforces physical world identities (Boler, 2007; Brookey & Cannon, 2009; Eklund, 2009; Mullany, 2004), and how rhetorical practices strategically frame particular portrayals of offline identities (Brookey & Cannon, 2009; Brunskill, 2014; Eklund, 2011; Jordan, 2005; Khang & Yang, 2011; Zhang, 2008). As users increasingly find ways to construct and form identities online and place personal data in online platforms, their participation opens themselves to attacks on identity, particularly related to identity theft and data mining. The next section considers cyber theft as a second-tier cyber attack and addresses implications for identity theft and corporate responses for protecting customers’ personal information.

Identity/Data Theft as a Second-Tier Cyber Attack

A 2017 Pew Research Center study reports that cyber attacks are a “fact[] of life” for governments, businesses, and individuals in the present day “digitized and networked world” (Smith, 2017a, para. 1). The report found that 64% of the American population has had personal information stolen or compromised by a corporate “data breach” and, as a result, lack “trust in key institutions” (para. 3). A common theme throughout the literature on cyber theft, data theft, and identity theft is the observation that these attacks frequently occur through breaches and vulnerabilities in corporate records of stakeholders’ personal data. As lawyer Kenneth M. Siegel (2007) describes, identity theft “partially” results from “corporations engaging in data sensitive transactions without maintaining adequate security programs” (p. 784). Siegel’s assertion maintains currency over a decade later as corporations continually rely on online platforms for business communication and transactions. Indeed, Nathan Heller (2018), reporting for *The New Yorker*, finds that social media “[u]sers have no way of protecting their data against theft” based upon Facebook’s data policy (para. 3). Examples of cyber theft include fraudulent credit card charges, compromised account numbers, email or social media hacking, compromised social security numbers, and fraudulent tax returns (Smith, 2017a, para. 4).[56] A second Pew Research Center report recognizes that the majority of Internet users are not informed of proper cyber security practices, which only accelerates the ease and

[56] Since 2016, personal information has been compromised in corporate cyber theft aimed at US government agencies and corporations ranging across industries. As of July 2018, Lily Hay Newman reports massive cyber attacks on and through US power companies, more than 300 universities located in the US and abroad, data exposures from companies such as Exactis, Under Armour, and the VPNFilter, which targets routers through companies such as Netgear, TP-Link, Linksys, ASUS, D-Link, and Huawei (Newman, 2018). In 2017, Calyptix Security reported massive cyber attacks on or from Equifax, Uber, WannaCry, Yahoo!, Deep Root Analytics, 60 universities and federal agencies, Taringa, and Verizon. In 2016, Kevin Anderton (2017) reports that major attacks occurred on the US Department Of Justice, LinkedIn, Tumbler, MySpace, the Democratic National Convention, Yahoo!, the World Anti-Doping Agency, Dyn, and AdultFriendFinder.

frequency of cyber theft (Smith, 2017b). This section reviews corporate responses to cyber theft to understand the negative implications for individual users.

Cyber theft and corporate data breaches span legal, social, and ethical considerations about the responsibility and role of corporations in information security. Corporate considerations about customer information management begin with the legal responsibilities of organizational entities—when data is compromised, does the corporation remain liable to the customer for the stolen information, and if so, what does this rectification look like? Early scholarly discussions answering this question and offering organizational response strategies emerge within law journals. Specifically, Peter Lichtenbaum and Melanie Schneck (2002) and Timothy A. Vogel (2002) consider this question and address recommendations for organizational responses.

Lichtenbaum and Schneck (2002) offer an early perspective on how to respond to cyber attacks. Lichtenbaum and Schneck (2002) identify organizational cyber security as a “double-edged sword” that benefits patrons while increasing operational costs for conducting online business and limiting user privacy (p. 40). Lichtenbaum and Schneck provide three suggestions to assist organizations in the full consideration of “cost, loss of privacy, and potential liabilit[ies]” (p. 48). First, across industries corporations should communicate with competitors and similar organizations to share best practices for cyber security (p. 45).[57] Second, corporations can invest in encryption technology that ensures another level of privacy protection (pp. 46–47).[58] Finally, organizations can monitor

[57] However, Lichtenbaum and Schneck note potential problem areas with this strategy related to potential complications related to “antitrust implications,” lose of proprietary information disclosed in the Freedom of Information Act (FOIA), and participation within the Information and Analysis Center (p. 45).
[58] However, companies encrypting their data must both ensure that the encryption codes are legal in other nations and consider future liabilities beyond the “immediate costs” (Lichtenbaum & Schneck, 2002, pp. 46–47).

employees to confirm appropriate uses of personal data and to prevent internal activities that increase organizational vulnerability to various malware.[59]

Furthermore, Vogel (2002) offers early scholarly recommendations for corporate cyber security legal practices. Vogel identifies who the attackers might be, how they might get access to corporate data, and what measures might prevent attacks. When characterizing a profile for potential attackers, Vogel (2002) distinguishes between "hacker[s]" (those who hack for fun), "cracker[s]" (those who hack for profit), "political zealot[s]" (those who hack to make political statements), and "spammer[s]" (those who do not necessarily aim to harm operations but who may "halt" corporate communications) (pp. 36–37). Outside of this typology, attackers might come from foreign governments, competitors, and investors who are "interested in information possessed by American business" (p. 36). Furthermore, disgruntled employees can be a "big source of risk" to the company and could serve as an additional path of cyber vulnerability (p. 37). Vogel offers this list of potential attackers to assist corporations in understanding avenues of risk within the conversation on cyber security.

After identifying a typology, Vogel (2002) attends to differences in intent as cyber attackers pursue access to corporate data and/or systems, in addition to interrupting business flow. Vogel encourages corporations to be self-aware of their own cyber environment. Businesses should have people clearly identified and "responsible for the network security" (Vogel, 2002, p. 43). Another crucial element is to be aware of the vulnerabilities in the network. Following logically, knowledge of the environment, vulnerabilities, and personnel facilitates one to "assess the legal risks" (p. 44).

[59] However, employee monitoring could infringe upon employee privacy rights (Lichtenbaum & Schneck, 2002, p. 47).

Additionally, Vogel (2002) urges corporations to assess “remedial measures” that ensure that companies know and repair vulnerabilities prior to cyber intrusions (p. 44). Once material defects have been repaired, companies should test the upgrades. By securing the physical infrastructure channeling cyberspace, organizations will have stronger cyber-defenses.

Finally, Vogel (2002) recommends addressing “contract and compliance problems” by reviewing the policies of the network to understand the nature of the cyber intrusions better (p. 45). Vogel calls for “networking security provisions” through reviewing and writing “network security into commercial contracts” (p. 45). A review of network security enables the company to determine the best course of action to address problems. Vogel (2002) recommends initiating “[i]ncident response plan[s]” that “anticipate” types of security violations and outline initial response strategies (p. 45). Incident response plans involve “mapping the escalation,” creating “public relations efforts,” and “testing the water” (p. 46). When mapping the escalation, organizations classify security breaches and designate the action to be taken in each area. Public relations efforts include having guidelines in place for notifying affected parties, and “testing the water” allows organizations to evaluate security plans by luring potential hackers toward the upgraded security systems. This strategy allows corporations to understand vulnerabilities and system operations in response to various threats. Through the consolidation of his typology, assessment of intent, and recommendation of response coordinates, Vogel provides organizations and attorneys effective methods to retaliate against illicit cyber activity and garner a “clear[er] understanding [of] the nature of the threat" (p. 46). Vogel's work situates cyber security within the realm of risk management and legal considerations that provide an early guide for corporations.

Extending this discussion, Peter Grabosky (2007) considers how legal prosecutors might construct responses to cyber attacks within a corporate environment. Grabosky (2007) begins with the "principle of *nullum crimen sine lege*"; he explains that this principle indicates that many Western nations privilege legal standards to the point that any action is permissible, no matter how problematic the behavior may be, as long as a law does not prohibit it (p. 208). This notion complicates cyber attacks due to constantly evolving technologies that continually create new possibilities for problematic behavior in an online context that may not technically be illegal under the law because the action is novel and prior to any legal consideration. Thus, Grabosky suggests that an adequate corporate response to cyber attacks depends upon effective "collaboration…with public law enforcement agencies" (p. 221). To facilitate this cooperation, Grabosky urges for law enforcement offices to invest in extended tools to investigate and evaluate cyber crime (p. 222). Furthermore, Grabosky calls for organizations to be transparent about intrusions, despite potentially revealing vulnerability to stakeholders. Grabosky explains that we need to reconsider the responses to problematic behaviors not yet legally prohibited, which requires extensive collaboration between prosecutors, corporations, and law enforcement agencies.

In this vein, Eneken Tikk (2011) calls for an extension of existing laws that allows for cyber crime to fall within valid interpretation rather than developing "new legal frameworks" (p. 3). According to Tikk, reinterpretation becomes necessary with the quick "increase in sophistication" of cyber attacks (p. 1). Tikk offers ten rules to frame cyber security practices that draw upon the “quality and interpretation of existing law” (p. 3). First, Tikk suggests a “Territoriality Rule,” where the cyber domains within a nation are subject to that nation’s sovereignty (p. 4). Second, Tikk offers a “Responsibility Rule,” where a nation state is responsible for attacks attributed to servers within the country’s geographical boundaries (p. 5). Third, Tikk provides the “Cooperation Rule,” where even if an attack did not originate from a server in the nation but simply passes through the nation’s servers, the country maintains an obligation to assist the victim state (p. 6). Fourth, Tikk announces the “Self-defence Rule,” which suggests all states have a “right to self-defence” when falling prey to cyber attacks that justifies counter attacks (p. 7). Fifth, Tikk states the “Data Protection Rule,” where the information retrieved from monitoring is “personal” unless otherwise specified (p. 8). Sixth, Tikk considers the “Duty of Care Rule” that states that nations are responsible for providing “a reasonable level of security in their information infrastructure” (p. 8). Seventh, Tikk provides an “Early Warning Rule,” where personal victims must be notified of “known” and/or “upcoming” cyber threats (p. 9). Eighth, Tikk supplies an “Access to Information Rule,” where the public is informed of threats to “life, security and well-being” (p. 10). Ninth, Tikk outlines “the Criminality Rule” that suggests that “common cyber offences” must be included in “substantive criminal law[s]” (p. 11). Finally, Tikk describes the “Mandate Rule,” which aids in “defining and coordinating international efforts in cyber security” (p. 12). With these rules, Tikk provides opportunities for cyber attacks to fall within valid interpretation of existing law, which aids in the criminalization and prosecution of these actions.

In order to enhance understanding of the intersections of cyber warfare, law, and the corporate environment, Chris Colvin, Daniel B. Garrie, and Siddartha Rao (2013) label cyber attacks as a "back door" breach that exposes corporations and individuals to increasing risk (p. 3). Their work emerges from a study of international corporate response strategies to cyber attacks that spans industries and business areas. Colvin, Garrie, and Rao find three results: (1) the "[b]asic knowledge" of security systems to defend against cyber attacks is "inconsistent and inadequate"; (2) there is a "lack of real incentives" concerning the report of cyber attacks, thereby "encourag[ing] a culture of silence"; and (3) "'Big Data'" and cyber risks are "pervasive across nearly every business sector" (p. 8). They recommend a cyber security model that involves two steps: (1) as businesses learn they are "targeted by cyber hackers," they should report their concerns confidentially to federal agencies for assistance; and (2) corporations should work with federal agencies to ensure that businesses can supply payments to victims of cyber theft and channel liability (p. 21). Colvin, Garrie, and Rao acknowledge holes within the current legal frameworks that open corporations and individuals to vulnerabilities. Based upon the findings from their study, they recommend additional oversight that can confirm safety measures for corporations and individuals.

Nathan Alexander Sales (2013), likewise, calls for stronger legal regulations of cyber security. Sales recognizes that a "large-scale cyber-attack" on America would likely "target privately held critical infrastructures—banks, telecommunications carriers, power companies, and other firms whose compromise would cause widespread harm" (pp. 1505–1506). Sales considers cyber security beyond and as separate from "criminal law" or "armed conflict," calling forth distinctive "regulatory terms" (p. 1503). Sales offers four important steps in cyber security. First, Sales calls for people to monitor and identify “malicious code” (p. 1508). Second, vulnerable organizational targets should have stronger defense systems to “defeat malicious code” (p. 1508). Third, systems should be built in a “resilient” manner that allows function during and fast recovery after cyber attacks (p. 1508). Finally, organizations need to respond after the attack occurs through “hackbacks,” or sending a return hack to the source that sent the initial hack (p. 1564). Sales offers four abstract coordinates before moving into tangible recommendations for organizations as they defend against cyber breaches.

Sales (2013) supplies three practical suggestions positioned to bolster cyber security. First, businesses might use a distributed biosurviellance network to collect and share information about cyber-threats as opposed to using only a single “central regulator to monitor” activity (p. 1567). Second, organizations might be “active” in initiating collaboration with other corporations about setting “industry-wide cyber-security standards” (p. 1568). Finally, corporations should disconnect infected computers from the network. For Sales, these three practical steps assist organizations when combating cyber attacks.

Moving from law to information sciences, Kenneth J. Knapp and William R. Boulton (2006) identify twelve trends[60] that landscape the role of information sciences in corporations and cyberspace. Together, these trends announce patterns of increasing

[60] These are the twelve trends Knapp and Boulton (2006) identify: (1) “Computer-Related Security Incidents Are Widespread”; (2) “Entry Barriers Are Low for Cyber-Attacks”; (3) “Dangerous Forms of Cyber-Weapons Have Emerged”; (4) “Many Nations Have Information Warfare Capabilities”; (5) “Increased Economic Dependency on Information Infrastructures”; (6) “Private Sector Is the Primary Target”; (7) “Cyber-Technology Is Increasingly Used in Perception Management”; (8) “Cyber-Technology Is Increasingly Used in Corporate Espionage”; (9) “Cyber-Technology Is Increasingly Used by Organized Crime”; (10) “Cyber-Technology Is Increasingly Used against Individuals and Small Businesses”; (11) “Growing Demand for Cyber-Insurance”; and (12) “Growing Demand for Information Security Professionals” (pp. 77–83).

government and corporate reliance on cyberspace for information management and an increasing need for security guarantees as cyber weapons become more powerful. Their work identifies the spread of information warfare to civilian and commercial areas and offers two avenues for "effective information security management"—"*architectural*" and "*managerial*" strategies (p. 84). The architectural strategy promotes a defense of multiple security layers that "increase the time and resources necessary for attackers" (p. 84). This approach recommends layered defense walls that protect sensitive information and simply create more work for the cyber attacker. The managerial strategy involves internal preparation for cyber attacks. To implement the managerial strategy, corporations should enact four steps: (1) hiring security officers; (2) training employees; (3) assessing risk; and (4) managing policies that protect the corporation from cyber risk. This strategy assembles a team of employees to identify and respond to cyber risks. By identifying existing trends and recommending response strategies, Knapp and Boulton offer important guidance for professionals in information management, technology, and sciences.

Continuing an information management focus, Mark Fabro and Eric Cornelius (2008) suggest that cyber security measures must be designed to respond to distinct operating systems. Specifically, they contend that strategies for response must be suited to "accommodate for the uniqueness and nuances associated with control systems" (p. 1). They contend that abstracted recommendations about cyber security will not unilaterally work across corporations, industries, or operating systems. They refer to a "flexible framework" of general recommendations that can be applied across a variety of technological systems; this flexible framework lays a foundation for safe cyber security practices that improve or strengthen existing “control systems environments” (p. 1) but does not exhaustively respond to the particularities of each distinct system. Fabro and Cornelius identify the highly complex nature of cyber security across operating systems and warn against assuming that widely generalizable techniques can adequately respond to the specialized contexts across corporations and industries.

Shifting the focus from corporate responses to cyber attacks to volunteer peer collaboration, Andres Schmidt (2012) considers problems of Internet security violations as well as the evolving nature of cyberspace. Schmidt (2012) recognizes the complexity of Internet security as involving “political, technical, and economic dimensions” and contends that potential responses to these varying dimensions could create different Internet security measures (p. 452). For Schmidt, a cyber attack is a human or technological failure that “put[s] at risk what actors have defined as pivotal to their Internet-related interests” (p. 452). To alleviate risks of cyber attacks, Internet security measures represent any “process or activity that assists in the reestablishment of the status quo” (p. 452). In the information technology literature, Schmidt describes the various Internet security strategies that respond to cyber attacks: system monitoring, incident detection and analysis, attacker identification, incorporation of new hardware or software, collection and distribution of information of the attack and new systems, system reconfiguration, patch distribution and development, attacker sanctioning, and network tweaking for optimal response. Schmidt importantly identifies these practices as typical organizational response strategies and acknowledges the breadth of potential solutions. His focus, however, lies within peer production of response strategies found on websites where users share information about security breach protection and recovery.

Schmidt (2012) contends that the open access and peer production capabilities available online require us to reconsider the nature of cyberspace and cyber attacks. First, Schmidt observes that cyber attacks, although serious and worthy of attention, do not necessarily bring life to a "standstill" or cripple the entire infrastructure of a country (p. 460). Second, the introduction of monetary or hierarchical incentives could demotivate users to share knowledge or advice about how to alleviate or recover from the negative implications of attacks; users participating in open access peer production may be more likely to follow "intrinsic motivations" than to participate for monetary rewards (p. 460). Third, limiting correctional authority to law enforcement agencies creates a "monopoly" that prevents community intervention or peer responses (p. 460). Fourth, institutionalizing "social production elements" committed to open access and transparency would advance peer-produced cyber security response efforts and support "ad-hoc incident response activities" (p. 460). Fifth, Internet security is "public good" that must merge merit-based models of cyber security prevention with social commitments for Internet communities to willingly participate in the open access peer production responses to cyber attacks (p. 460). Schmidt points to the important recognition that community involvement as an alternative and complementary platform can function as a strong deterrent to cyber attacks.

Recognizing the interdisciplinary scope and wide reaching implications of cyberspace, Dan Craigen, Naida Diakun-Thibault, and Randy Purse (2014) acknowledge the complexity of defining cyber security and hope to put forward a definition that reaches across disciplinary bounds (p. 14). Craigen et al. review nine definitions of cyber security stemming from "computer science, engineering, political studies, psychology, security studies, management, education, and sociology" (p. 14). They offer a comprehensive definition that represents the distinct dialectical concerns and contexts emerging from the various disciplines reviewed. They define cyber security as "*the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign* de jure *from* de facto *property rights*" (p. 17). Their definition recognizes the dialectics at play across industries and disciplines in the attempt to "influence the approaches of researchers, funding agencies, and organizations" countering the threats of cyber attacks (p. 18). Craigen et al. contend that a shared definition will offer a starting place for professionals across disciplines to collaborate in uncovering a holistic answer to the risks of cyber attacks.

Extending a call for collaboration, Florian Skopki, Giuseppe Settanni, and Roman Fiedler (2016) consider responses to cyber attacks as a "problem halved" when shared across disciplines and corporations (p. 154). They stress that the rising sophistication of cyber intrusions requires "targeted and coordinated countermeasures" (p. 155). For Skopki, Settanni, and Fiedler, online advice for cyber attack response is often "generic, not shaped to particular industries and often lacks in-depth knowledge" (p. 155). With sophisticated and directed attacks and generally generic response strategies, "cyber security centers" are necessary but difficult to build and governmental bodies or companies are poorly equipped to run or utilize them as a resource (p. 155). Skopki et al.'s work explicates the complexity of cyber security by providing a holistic description of cyber security information sharing, a survey of the existing defense practices, and an evaluation of the direction of security for the future. Skopki et al. call for cyber security centers at the national level, which are "informed about the security status of the national critical infrastructure providers" and coordinate cyber attack prevention and protection (p. 174). They contend that information sharing centers are key to collaboration on minimizing, preventing, and recovering from cyber attacks related to identity theft, malware, hacking, and similar practices.

This literature suggests that cyber theft affects both individuals and corporations as a second tier cyber attack. Across disciplines, scholars agree that response strategies must be examined. Three response trends emerge from this literature: (1) adequate responses to cyber attacks are met by a respect for the particularity of the given situation (Farbo & Cornelius, 2008; Schmidt, 2012; Skopki, Settanni, & Fiedler, 2016); (2) responses to cyber attacks require information sharing (Grabosky, 2007; Lichtenbaum & Schneck, 2002), an understanding of the corporate environment (Vogel, 2002), and physical and cyber defense systems (Lichtenbaum & Schneck, 2002; Schmidt, 2012; Skopki, Settanni, & Fiedler, 2016; Vogel, 2002); and (3) preventative measures to cyber attacks include tactics such as a hackback (Sales, 2013; Tikk, 2011), administrative laws (Sales, 2013), or national cyber security centers (Colvin, Garrie, & Rao, 2013; Skopki, Settanni, & Fiedler, 2016). The anonymity/identity dialectic is crucial at both ends of cyber theft—determining the identity of the attacker as well as insuring and protecting private information for individual Internet users and corporations. The potential for theft that lies at the foot of anonymity and identity puts society at risk; the work of Ulrich Beck can assist notions of risk in the social and digital realm.

Extensions from Ulrich Beck

Communication scholars are increasingly finding the work of German sociologist Ulrich Beck (1944–2015) pertinent for theoretical and applied research (Abe, 2015; Constante Martins, 2015; Han, 2016; Heng, 2006; Lash, 2015, 2018; Mythen, 2013; Rantanen, 2015; Wieviorka, 2016). This section reviews both Beck's work on the risk society and secondary literature connecting Beck to risk and cyberspace/digital platforms, explicated in greatest detail by Deborah Lupton (2016). This section applies Beck to issues of cyber security, specifically within the realm of cyber theft, to yield insights relevant to the identity/anonymity dialectic of cyberspace.

The same year as the Chernobyl nuclear accident, Beck (1986/1992) described the growth of what he terms a "risk society" with his book *Risikogesellschaft* [translated into English as *Risk Society: Towards a New Modernity*]. Beck's risk society is the result of "the social production of wealth in advanced modernity" (p. 19). In other words, neoliberal capitalism has created the potential for exponential economic growth as "*genuine material need*[s]" are reduced to mechanisms of "technological productivity," which is likewise increasing (p. 19). For instance, a pen factory before the period of advanced modernity produced pens in response to a specific demand; production satisfied a genuine material social need. However, in the era of advanced modernity imbued with neoliberal capitalism, production expands in excess as the pen factory competitively vies for the reputation of 'best pen.' Neoliberal capitalism prompts production beyond demand and introduces differentiation based upon quality in terms of writing, grip, price, and other defining qualities. Any particular pen model meets one or a combination of these criteria. However, within this neoliberal framework the pen factory creates not only possibilities for exponential growth and profit but also the potential for increasing risk—for instance, what if no one purchases the excess of pens produced, and how can society bear the environmental impact of the disposable plastic used in production? Beck problematizes the unintended consequences of an oversaturation of pen (and other) factories as producing "unknown" rates of "hazards and potential threats" (p. 19). Beck fears that society has traded the security of the planet for neoliberal commitments to production, job security, technological efficiency, and financial profit.

Beck (1986/1992), in response to the emerging risk society, pursues the question, "How can the risks and hazards systematically produced as a part of modernization be prevented, minimized, dramatized, or channeled?" (p. 19). Beck describes this period of advanced modernity as "*reflexive*" in that the technology that once made "nature useful" now overshadows nature in order to reorganize resources to maintain optimal production (p. 19). Prior to a ubiquitous environment of advanced, reflexive modernity, production was responsive—manufacturers produced products in a way that fitted nature to benefit the human condition (i.e., producing pens so humans could extend their memory and thought capabilities). However, within reflexive modernity, production becomes about production, profit about profit, and technological efficiency about technological efficiency. While production may still benefit the human condition at some level, the focus remains on production rather than environmental or societal implications.

Within this reflexive era, the question of how we can optimize and maintain production, profit, and technological efficiency becomes the focus rather than questions of whether we should pursue such goals. For Beck, the risks of reflexive modernity could manifest the "self-destruction of all life on Earth" (p. 21). For instance, market realizations that sustainability and reducing material resources sells have reorganized and redirected market efforts in ways that reflexively advance neoliberal commitments rather than uphold the environmental sentiments motivating these trends. Thus, manufacturers produce in excess clothing, magnets, decorative signs, bumper stickers, posters, and many other products with Kermit the Frog saying "Be Green." In actuality, rather than maintaining commitments to environmental sustainability or green efforts or their associated risks, production remains devoted to neoliberal capitalism.

Beck not only introduces the concept of risk society, but also characterizes the nature of risk itself. Risk identification becomes a crucial question because risks often escape "*perception*" (Beck, 1986/1992, p. 21). Beck defines risk as "*a systematic way of dealing with hazards and insecurities introduced by modernization itself*" (p. 21). However, in reflexive modernity, previous standards for "the calculation of risk" have "*collapse*[d]" (p. 22). Due to the imperceptibility of risks, existing standards of engagement must be redrawn. Beck provides five characteristics of risk in his project. First, risk "evades human perceptive abilities" and "induce[s] systematic and often *irreversible* harm" (pp. 22–23). Second, risk "produce[s] *new international inequalities*" as some people are more affected than others (p. 23). Third, risks are in a "*bottomless barrel*" and, within reflexive modernity, continually emerge (p. 23). Fourth, knowledge takes on a new "political significance" in that risk knowledge must be diffused (pp. 23–24). Finally, risk society is "*catastrophic*" in that risk management "can include a *reorganization of power and authority*" (p. 24). Risk and risk management fundamentally alter existing social hierarchies, standards, and organizations.

According to Beck (1986/1992), risks are "*mediated on principle through argument*" (p. 27). Argument becomes a central coordinate for risk legitimation due to the opacity of causality. Beck writes that "presumptions of causality escape our perception" and are always "imagined" or "implied to be true," remaining "uncertain and tentative" (p. 28). To publicize a risk requires a good and persuasive argument (p. 32). Thus, risk legitimation becomes the task of public relations practitioners, "argumentation craftsmen," and rhetoricians (p. 32). Beck also recognizes the centrality of ethics to risk legitimation and solution as practitioners and society members ask, "*How do we wish to live?*," when contributing to the ensuing world (p. 28). The identification of risks and the determination of their best resolution fall to questions of rhetoric and ethics.

Beck (1992) clarifies his project on risk by identifying four types of risk that emerge from reflexive modernity; these "four pillars" of risk include "nuclear, chemical, genetic and ecological" contexts (pp. 101–102). According to Beck, society has become "*uninsured*" with an inverse relation between security and danger—as risk increases, societal efforts for protection disappear (p. 101). Risk society features risks that could result in "irreparable damage" in the form of nuclear, chemical, genetic, and ecological issues, which broadly threaten society (p. 102).

Furthermore, Beck finds a correlation between the "incalculability of consequences" and a "lack of accountability" (p. 102). Because the devastation caused by nuclear, chemical, genetic, and ecological risks could be so far-reaching, accountability and identifying points of blame become increasingly difficult. For example, it is difficult to trace who specifically is to blame for the extinction of the passenger pigeon. This lack of accountability and responsibility does not create a binary between winners and losers but rather a totalizing amount of losers. Beck notes that “no one is an expert” and “new knowledge can turn normality into hazards overnight” (p. 106). He acknowledges that ambiguity and uncertainty accompany risk even when potential risks go unobserved. New information about an existing context or event can actualize awareness of risk, transforming what was formerly perceived as a state of harmony into chaos as new knowledge replaces existing ambiguities.

Despite the gloom of the risk society, Beck (1992) does not leave us without hope. Rather than condemning humanity to a forsaken residence, he offers a twofold solution with interlocking coordinates: (1) “a division of powers” and (2) “a public sphere” composed of “dissenting voices” (p. 119). Beck contends that difference is the ideal means to remedy the problems inherent within the risk society. Beck urges society away from a monolithic entity and voice that sees and thinks only one way. The only means to understand and respond to the abundant risks in society adequately is through a public composed of individuals who do not see things the same way. Diversity of perspective can assist society as individuals identify different issues and solutions. Following this call for difference, various scholars respond to Beck’s risk society and extend his insights into new and evolving contexts.

A first voice countering Beck’s notion of risk is Mitchell Dean[61] (1998). Dean connects Beck’s notion of risk to Michel Foucault’s understanding of government to put forward the concept of “reflexive government” (p. 27). By reflexive government, Dean

[61] Mitchell Dean is a sociologist specializing in historical and political theory. Since December 2012, he has been a professor of public governance at the Copenhagen Business School. Dean was affiliated with the University of Newcastle as a professor of sociology from 2010–2012 and Macquarie University from 2000–2010. Dean has published nine books, including *State Phobia and Civil Society: The Political Legacy of Michel Foucault* with Kaspar Villadsen (2016), *The Signature of Power: Sovereignty, Governmentality and Biopolitics* (2013), and *Governing Societies: Political Perspectives on Domestic and International Rule* (2007) (“Mitchell Dean,” 2019).

refers to the “shifting of the liberal problematic of security from the security of social and economic processes to the security of governmental mechanisms” (p. 27). Dean contends that the risk sociology of Beck lacks an “analysis of the particular practices, techniques and rationalities through which risk can be constructed as a governable entity” (p. 27). Dean responds to and extends the work of Beck to offer a holistically nuanced conception of risk.

Dean (1998) identifies and counters three components of Beck’s risk that he labels as “mistaken” and “unhelpful” (p. 28). First, while Beck understands risk to be “*totalizing*,” Dean finds that there is “virtue” in an examination of the “specific types of risk rationalities and practices” (p. 28). Second, Dean counters Beck’s contention that risk shares basic characteristics across all contexts by suggesting that risk is “heterogeneous” and responses come from “diverse elements” that can be “put together in different ways” (p. 28). Third, Dean advances a “nominalist position,” suggesting that risk management strategies derive from a wide “range of moral and political programmes and social technologies” in opposition to Beck’s “realist assumption” that the risks faced each day are beyond “calculation and control” (p. 28). Furthermore, Dean counters Beck’s risk society. Dean recognizes “incalcuab[ilty]” as Beck’s defining characteristic of the risk society and suggests that a “post-risk-calculation society” may better represent Beck’s concern (p. 29). Dean contends that the problem with Beck’s risk society is a “double confusion” where, on the one hand, risk is incalculable and, on the other hand, risk relies upon quantitative measures for recognition and identification (p. 29). Dean contributes to a public sphere of dissent about the very nature and function of Beck’s characterization of risk.

To amend what Dean (1998) perceives as the shortcomings of Beck's project, he turns to François Ewald, who offers an alternative to so-called incalculable risks. According to Dean, Ewald departs from Beck in two helpful ways. First, Ewald contends that risks are "a form of rationality" and thus calculable (p. 29). In other words, thinking about risks in a particular way illuminates a specific means to manage them. Second, Ewald encourages an investigation of "*the technical and practical aspect of governing risk*" (p. 30). Thus, Ewald unites risk and "the practices of insurance" and "techniques" that facilitate the navigation of risk (p. 30). Dean contributes to Beck's call for a public sphere of dissenting voices by texturing and extending conceptualizations of the risk society.

In support of Beck's work, Ronald J. Deibert and Rafal Rohozinski (2010) provide parameters for cyber risks "*to* cyberspace" and "*through* cyberspace" (pp. 16–18). Risks *to* cyberspace emerge within "the physical realm of computer[s] and communication technologies" while risks *through* cyberspace occur within virtual realm of information and data housed on cyber platforms (pp. 16–18). Deibert and Rohozinski offer a simple definition of risk as the "possibility of incurring loss," and they note that risk distribution, or who is vulnerable to incur the loss, illuminates who or what a given society values (p. 18). In extending Beck's risk society to cyberspace, Deibert and Rohozinski observe that risk distribution transfers from nations or corporations to "private actors" and contend that this redistribution carries significant consequences (p. 18). Additionally, they extend the "socially constructed" aspect of risk to "technological characteristics" that contextualize how individual users participate with risk online (p. 18). This extension yields "unintended" and "paradoxical" consequences for cyber risk mitigation (p. 18). Similar to the risks of Beck's reflexive modernity, the "mitigation of risk" in cyberspace becomes a "central" concern (p. 18). Deibert and Rohozinski establish strong connections between Beck's risk society and cyber risk.

Deibert and Rohozinski (2010) find three implications in their extension of Beck's risk society to cyberspace. First, combating risks on digital networks facilitates a worldwide communication network that expands "transnational non-state actor activities" (p. 30). Second, cyber security practices shift the "responsibilities and authority" from the state to private actors (p. 30). Third, actions to prevent cybercrime "can be seen as an internationalization of the state" (p. 30). Deibert and Rohozinski expand Beck's risk society to include cyber risk and note the varieties of risks that may occur both *to* and *through* cyberspace.

Sofie Blinkenberg Federspiel and Benedikte Brincker (2010) offer yet another voice to texture Beck's public sphere with a focus on software risks. Federspiel and Brincker suggest that "uncertainty about the severity, the intensity, and the reality of risk" characterizes Beck's risk society (p. 40). Federspiel and Brincker find such risks within software technologies and recognize that the "digitalization of information" simultaneously increases efficiency and vulnerability (p. 39). The efficiencies that result from software include improved connectivity and communications. However, software systems are vulnerable in the sense that physical borders between nation states are transcended and the "risks associated with software" are incalculable (p. 41). Uncertainty is a major coordinate of risk society, and the use of software technology through cyberspace increases civilian uncertainty and vulnerability. A consideration of software risks broadens the scope of the risks facing contemporary society.

Deborah Lupton (2016) does extensive work extending Beck's public sphere with a focus on digital technologies and cyberspace, coining the phrase "digital risk society," the acknowledgement that human intertwinement with digital technologies puts individuals and society at risk (p. 301). Lupton understands digital risk society as emergent from the work of Beck (2013), where he announces that the Internet poses the "global digital freedom risk" or a threat to user "privacy and freedom of speech" as personal digital devices record user private data (as cited in Lupton, 2016, p. 305). Beck responds to the global digital freedom risk with a call for the "protection of personal data" (Lupton, 2016, p. 305). As this call has yet to be answered by corporations, governments, and individuals, Lupton announces the ongoing evolution of a digital risk society.

Lupton (2016) sketches five characteristics of digital risk. First, the changes in digital society are "rapid," allowing for more dangerous threats to emerge continually (p. 302). Technology permits accelerated change and vulnerabilities to spiral out of control rapidly. Second, digital technologies create "power dimensions" as technological companies such as Google, Amazon, and Apple "structure contemporary social life" (p. 302). A third characteristic of digital risk society is identified as "[f]orms of watching (veillance)" (p. 303). Companies and governments are able to obtain much information about civilians without the civilian's knowledge or consent. A fourth coordinate of digital risk is the continuous production of "[m]assive digital datasets," which "creat[e] and recreat[e] digital risk assemblages" (p. 303). Finally, digital risk society creates a reliance on devices that expose society to high levels of risk if a device were to fail or to be “manipulated maliciously” (p. 304). Digital risk threatens society in new and significant ways.

Lupton (2016) announces three kinds of digital risk. First, Lupton (2016) describes “digitising risk,” where digital platforms “mediate and remediate risk” (p. 303). In other words, people turn to digital media for information about events in the physical world. Lupton exemplifies this problematic through the Ebola crisis (2014) and Hurricane Sandy (2012), where many users uploaded (mis)information pertaining to these events to the Internet. The volume of users posting made the “validity” of the information difficult to determine and prompted the spread of “[m]isinformation” (p. 304). The posting of information to online servers contributes to the digital risk society by potentially spreading false information.

Second, Lupton (2016) positions “digital technology use” within the digital risk society (p. 304). The risks associated with digital devices are multiple: (1) online addiction; (2) exposure to pedophiles; (3) cyberbullying; (4) illegal, dark web activities; and (5) underdeveloped social and athletic skills (pp. 304–305). Additionally, the risks of digital technology use include the sale of personal data for “commercial reasons” and “the risk of losing privacy and personal security of one’s data” (p. 305). For instance, users’ addresses, telephone numbers, credit card numbers, and social security numbers become vulnerable to theft even when placed in a then- secure or credible server. The use of digital technologies contributes to the digital risk society by exposing users to the threat of data theft and health risks.

Third, Lupton (2016) identifies “digital social inequality risks,” or the recognition that those without access to technology are disadvantaged in terms of “communication, education, information or better employment opportunities" (p. 306). Such risk can be exemplified by technologies that permit discriminatory "dataveillance" to "exclude individuals from public spaces" or "algorithmic discrimination" that targets "individuals or social groups based on pre-selected characteristics" (p. 306). Digital social inequality risks contribute to the digital risk society by discriminating against those who do not have access to certain technologies or who inhabit social/class standings underappreciated by society.

Lupton (2016) concludes with recommendations for how to navigate the digital risk society. She recognizes that new digital technologies continually emerge and the attempt to understand how they shape the landscape necessitates a sociology of risk that examines the "affordances, uses and politics of digital technologies and the data that they generate and circulate" (p. 307). Importantly, such a framework involves coordinates beyond the traditional theorization of risk that also includes the "sociomaterial contexts" of digital risks and how they interact with "big data, digital sensors, software, platforms and algorithmic authority" (p. 307). Lupton contributes to Beck's public sphere by sketching the digital risk society and noting that risk minimization (or eradication) extends beyond traditional methods of risk analysis.

Beck's renowned *Risk Society* was published the same year as the Chernobyl nuclear accident, which drastically contributed to the exigency of his project; society must thoughtfully engage the risks that imbue this moment of reflexive modernity lest civilization as it is known be destroyed. Beck calls us to recognize that, as a result of neoliberal capitalism, we live in a society that experiences unlimited potential for growth alongside the simultaneous potential for nuclear, chemical, genetic, ecological, and digital risks. Beck (1992) suggests we might manage these risks by dividing powers away from monolithic control toward a public sphere of dissent; difference can illuminate diverse quadrants of risk and drive potential solutions. Extending Beck's work to illuminate present day quandaries, notions of risk reach toward cyberspace and digital technologies (Deibert & Rohozinski, 2010; Federspiel & Brincker, 2010; Lupton, 2016). Explorations of cyber risk bring forth three trends: (1) digital risks are identified as "*risks to*" and "*risks through*" cyberspace (Deibert & Rohozinski, 2010); (2) software contains risk as users transcend physical borders and expose themselves to potentially compromised data (Federspiel & Brincker, 2010); and (3) digitized risk culminates in new potential for the spread of false information, cyber theft, and algorithmic discrimination (Lupton, 2016). Simply put, participation on cyberspace and with digital devices holds risk. Following the call of Lupton (2016), the final section offers communication ethics implications from this study to mitigate digital risk, particularly emerging through cyber theft, outside of traditional risk analysis.

Communication Ethics Implications

This chapter contends that cyber theft emerges from the confusion arising from the ambiguous mix of user identity and anonymity online; we mistakenly engage cyberspace as a site where we believe we have control over what we conceal and reveal pertaining to our identities, when in actuality cyberspace offers government entities and corporations immense power to organize data in the construction of consumer identity profiles. This identity/anonymity dialectic transforms user identities even when users engage cyberspace as an anonymous platform into something wholly other. A review of literature on the identity/anonymity dialectic reveals that scholars have recognized the ways that cyberspace has permitted opportunities to conceal and reveal identity since the time of Web 1.0 and how anonymity can be either an asset or detriment to online activity. However, the cyber security practices of corporations, alongside user behaviors, expose individuals to the threat of cyber theft. Beck's conception of the risk society compels civilians to recognize the effects that their actions have on the surrounding environment, which become increasing apparent in an era of neoliberal capitalism. Scholars who extend Beck's work find present day implications for cyberspace, cyber risk, and digital risk that contribute to the communication ethics implications proposed as a first response to this second-tier cyber attack.

The dialectical method this project pursues, influenced principally by the work of Kenneth Burke and David Gunkel, enables an understanding of the anonymity/identity opposition within cyberspace. Burke's (1941; 1945/1969) consideration of dialectic articulates the clashing terms—anonymity and identity—as in constant and persistent tension. These terms exist beside one another; the dialectic will not reach a synthesis, but generates a separate space between partial anonymity and partial identity. As users create profiles and post messages within cyberspace, they must acknowledge what they create or say is neither exclusively identifiable nor non-identifiable; there are multiple factors contributing to how cyberspace participation contributes to identity construction and anonymous action.

Gunkel's (2007) insights advance this project's understanding of dialectic by announcing the necessity of considering cyberspace radically otherwise than an exclusive place of anonymity or identity. Cyberspace, as a potential third term emerging from the synthesis of user anonymity and identity, must be thought of as comprehensively alternative to existing standards of anonymous and identifiable spaces. Cyberspace produces actions radically different than those completed in the physical world and thus effect identity and anonymity wholly otherwise. When users engage cyberspace without a recognition of the distorted lines between anonymity and identity, they make themselves vulnerable to the dangers Lupton (2016) articulated as inherent in the digital risk society (the spread of misinformation, cyber theft, and digital inequalities).

This chapter contends that cyber theft as a central risk of the digital risk society results from misunderstanding the anonymity/identity dialectic of cyberspace. While some scholars contend that anonymous communication in cyberspace is helpful (Akdeniz, 2002; Bargh & McKenna, 2004; Mahfood et al., 2005; Tsui, 2015), others suggest that it is harmful (DiMaggio et al., 2001; Williamson & Pierson, 2003). Scholars recognize that cyberspace functions in ways that permit the construction of identity anew (Brookey & Cannon, 2009; Brunskill, 2014; Eklund, 2009; Jordan, 2005; Marciano, 2014) or mirror existing expressions of identity in the physical world (Boler, 2007; Brookey & Cannon, 2009; Eklund, 2009; Mullany, 2004), Consistently, however, scholars recognize the framing of the self online as a rhetorical practice (Brookey & Cannon, 2009; Brunskill, 2014; Eklund, 2011; Jordan, 2005; Khang & Yang, 2011; Zhang, 2008); users selectively chose items or aspects they believe will represent themselves best or represent themselves as they wish to be perceived and decide to obscure or hide other aspects of their identities (Walther, 1996). However, as cyber practices collect more and more user data that continually accumulate online, corporations become targets for data theft, and their data security practices become an important issue. Despite efforts to obscure, select, and safeguard identity, humans have little control over their personal information available online or how that data is protected. This chapter finds four implications:

1. Users believe that they are in control of the rhetorical construction of their identities online, selecting what they believe to represent themselves strategically in the light they choose for a given situation or purpose. While this belief may hold true in certain contexts, such as their appearance on social media profiles, users lack control of what information becomes available through other entities (whether by friends and family members, governments, or corporations). Despite user selection of particular aspects for a given context, more personal information than users realize or desire is online and becomes vulnerable to cyber theft through corporate hacks and other forms of attack.

2. Cyber theft as a second-tier cyber attack is the manifestation of the confusion of this newly constructed, ambiguous space. Users fail to recognize their embeddedness in a larger online context that can potentially contribute to their perceived and selected anonymity. Various spheres of human interaction beyond a particular online context find ways to influence identity construction even as one participates anonymously in cyberspace. Even when presenting themselves as anonymous, users act through their given bodies and the identity influences that have contributed to particular understandings of the self.

3. A consequence of posting personal information to the Internet creates user vulnerability, anxiety, and uncertainty as to whether this information is secure. While in the physical world, targets of theft are physical and the absence/presence of the thief is known, in the digital world of cyberspace, targets of theft are virtual, and the absence/presence of the thief can go unknown or unnoticed. The Internet emerged as a

Cold War military technology; it should not be surprising that it continues to maintain potential for Cold War tactics of surveillance, spying, and theft.

4. Beck's risk society points to the fact that the source of the risk is difficult, if not impossible, to trace. What appears to be a solution to the given risk may be a solution only from a certain way of looking at the issue. Thus, the notion of a public sphere of dissent and difference becomes essential for risk management and the potential for resolution. Some people can see and propose solutions for risks and problems that may be invisible to others. Difference and constructive argumentativeness drive the resolution and management of risks. Scholars from communication, law, information sciences, and political theory should continue to consider the identity/anonymity dialectic as it relates to cyber theft in the digital risk society.

One defining element at the root of cyber theft is the confusion between cyberspace as an anonymous space and/or cyberspace as an identifiable space. Cyberspace is beyond rhetorical identity construction and perceived anonymity. The massive amount of user personal data held by corporations make these institutions an ideal target for cyber attacks and data breaches. Another important coordinate for a holistic understanding of cyber attacks is a consideration of the ways in which they transcend traditional borders between nation states (Federspiel & Brincker, 2010). The next chapter introduces and investigates this dialectic between global and national borders as another primary opposition that shapes cyberspace. Additionally, the proceeding chapter places cyber terrorism and cyber warfare as a third-tier cyber attack that results in part from the national/global boundaries transformed by the dialectical nature of cyberspace.

Chapter 5

The National/Global Dialectic of Cyberspace:

Cyber Terrorism and Cyber War as Third-Tier Attacks

Introduction

This chapter addresses how cyberspace, the World Wide Web, and the Internet re-conceptualize borders and boundaries between nation-states. In an era prevalent with social, political, and personal reliance on cyberspace, we must recognize that the Internet changes the path of how information passes through national borders travelling from source to recipient; when an Internet user in the United States accesses information from a German website, the information could pass through several nations between the source and destination. This path violates existing conceptions of national borders in the physical world and makes possible the potential for destructive consequences ranging from cyber crime to cyber terrorism and cyber war. As noted by communication scholar Stephen J. Hartnett (2011), cyber crimes in times of peace are a testing ground for acts of cyber war—the same tactics engaged by cyber criminals may re-emerge in times of cyber war. Furthermore, Roger Stahl (2016) notes that the term cyber terrorism is a weaponized, rhetorical use of language that can persuade the public toward defensive and political acts, perhaps even a mobilization to arms. This literature merits consideration of cyber terrorism alongside cyber war as a timely and worthwhile endeavor. This project contends that an understanding of the global/national dialectic reveals communication ethics goods threatened within cyber terrorism and cyber war as third-tier cyber attacks.

This chapter proceeds in four sections. The first articulates cyberspace within a national/global dialectic. Relying upon the work of communication scholars, this section attends to the implications of the Internet's ability to re-draw borders between nation states. The second section explores the contention that the Internet fundamentally alters conventional understandings of physical geography that in turn offer implications for the international regulation of information across a new frontier of borders governed by the infrastructure of cyberspace. The third section expands connections to the work of sociologist Ulrich Beck. By moving from Beck's first book *Risk Society* to his later work in *Cosmopolitan Vision* and *Individualization*, this project forms a holistic view of his corpus. The chapter concludes with communication ethics implications and offers a segue to the project's concluding chapter. Together, literature from communication scholars addressing how cyberspace alters borders along a national/global dialectic, scholarship from outside of the field communication focusing on how the Internet alters boundaries and opens possibilities for cyber terrorism and war, and the theoretical discussion offered by Beck and Elisabeth Beck-Gernsheim (2002) pertaining to a new national identity composed of individualization and Beck's (2004/2006) globally reflexive cosmopolitan outlook suggest that attentiveness to this dialectic provides insight related to communication ethics as a first response to cyber attacks.

The importance of this chapter resides in understanding how the global/national dialectic of cyberspace defines user engagement within this international communication platform. Discussions pertaining to cyberspace and nation-state borders uncover two conflicting findings: (a) that cyberspace is grounded in geographic locations (Halavais, 2000; Hedley, 2003; Rogers, 2012), and (b) that cyberspace completely denies and redraws geographic borders (Dodge & Kitchin, 2001; Eco, 2006/2007; Gearing, 2014; Jiménez, Orenes, & Puente, 2010; McDonnell, 2009). Importantly, scholars recognize that a variety of entities, ranging from governments to corporations and individual users, compete within the re-conceptualized frontier of cyberspace to gain political and economic power through acquiring bandwidth, public recognition, and access to user data (Dodge & Kitchin, 2001; Eco, 2006/2007)—where previously such power might have been limited to governments, today, corporations such as Google, Amazon, and Apple have the ability to distribute, survey, conceal, and collect both personal and national data. Cyberspace, as a platform blurring domestic and international boundaries, opens this access to non-state actors, cyber criminals, and terrorist groups while also providing a new outlet for attack between warring nations. Communication scholars identify these changing boundaries as a central characteristic of cyberspace and recognize the vulnerability it presents for the proliferation of cyber terrorism and cyber war.

Changing National/Global Borders within Cyberspace

Communication scholars acknowledge that cyberspace alters borders along a national/global dialectic (Davisson, 2011; Dodge & Kitchin, 2001; Gearing, 2014; Halavais, 2000; Hedley, 2003; Jiménez, Orenes, & Puente, 2010; McDonnell, 2009; Rogers, 2012; Weber, 2011). Scholars debate, however, whether users' physical geographic locations govern what they have access to online (Halavais, 2000; Hedley, 2003; Rogers, 2012) or whether cyberspace constitutes a new and unmapped terrain that eradicates existing borders between nation states (Dodge & Kitchin, 2001; Jiménez, Orenes, & Puente, 2010). Furthermore, some scholars note that cyberspace encourages opportunities for improved international communication and interconnectivity (Gearing, 2014; Weber, 2011), while others find opportunities to close discourse across national boundaries (Weber, 2011). This review of literature progresses historically, detailing early deliberations on cyber borders between national and global states from the year 2000 to 2014 and focuses on the extent to which cyberspace exists within a national/global dialectic.

Alexander Halavais (2000) offers early observations of how geographical physical borders between nation states influence online activity. Halavais insists that national borders in the physical world exert a “measureable effect” on the geography of the Internet rather than constituting what some consider an “anarchic” space (p. 8). Halavais, however, acknowledges that the intangible and abstract notion of cyberspace makes determining cyber borders difficult. This difficulty is twofold: first, it has a seemingly infinite domain associated with an inability to recognize “where, exactly, the internet ends”, and second, its interconnected, “distributed network” complicates the process of measuring total data flow (pp. 9–10). To move forward with his analysis, Halavais suggests that we can organize online activity according to “media classes,” or patterns and functions of Internet use (p. 10). Media classes may include functions such as an international marketplace, a correspondence technology, a research tool, or a site for blogging. The organization offered by these media classes assists in the measurement of communication flows, rather than *all* data flows, and provides coordinates for conceptualizing cyber borders (p. 9).

In this study, Halavais (2000) examines a “sample of web pages” with particular focus on the structure provided by their hyperlinks as they direct information within this space (p. 12). According to Halavais, hyperlinks form the infrastructure of online content and “linkage structure[s],” which in turn make them the “best way” to determine the relationship between national borders and the Internet (p. 13). Halavais likens hyperlinks in the virtual world to roads in the physical world; similar to the manner in which roads fill a "social need" and "road map[s]" illuminate geographic patterns, so too do hyperlinks satisfy the needs of Internet users by connecting content between and among webpages (p. 12). By examining these hyperlinks, Halavais hopes to construct a virtual road map of online content that subsequently offers insight into the nature of online borders (p. 12).

Halavais (2000) finds two primary trends from his analysis of hyperlinks. First, he suggests that, despite the internationality of the medium, Internet users are not likely to "cross international borders" through a hyperlink (p. 16). In other words, a user surfing the web in the United States is not likely to be redirected to a Polish webpage through a hyperlink but rather to another US webpage with similar content. The organizing infrastructure of cyberspace generally governs communication flows within the borders of nation states; hyperlinks on French webpages typically lead to content on other French webpages just as hyperlinks on Chinese webpages typically lead to content on other Chinese webpages. Halavais's second observation is that when hyperlinks do connect webpages generated in different countries, users are "far more likely" to find themselves redirected to websites in the United States. Halavais suggests this may be a result of the "imbalance in the number of sites hosted in each country" (p. 16)—more of the content available through cyberspace has been created within the geographic bounds of the United States than other nations, or simply put, the United States hosts more websites than other countries.

From these trends, Halavais (2000) advances the contention that physical borders between countries still "remain significant" even though this virtual space lacks clearly identifiable borders (p. 22). Halavais charges future researchers to enhance understanding of the nature of cyber borders beyond the infrastructure of hyperlinks by investigating the "social and informational structure" of the web (p. 24), specifically within the context of the Internet's lack of "technological, regulatory or economic impediments to transnational interconnections" (p. 22). Without clear regulatory control, cyber borders become even more opaque. Halavais contends that the Internet offers a new balance between virtual and geographic boundaries and that within this balance inherently lies the influence of national borders.

Similar to Halavais, Steve Hedley (2003) attempts to understand the role of national borders in cyber contexts. In an attempt to bridge communication and law, Hedley asks "who governs cyberspace" or who makes the laws and rules that shape this new terrian (p. 215). Hedley questions whether cyberspace is a distinct place situated "within the boundaries of known nations" or a completely new territory that violates existing conceptions of nation states (p. 215). The answer to this question provides insight into the nature of cyber borders between nations. Hedley recognizes that laws are currently "not well enforced in cyberspace," but that the domain still exists within nations and ought to be designated as a part of the nation where the user is located geographically (p. 217). This recognition assumes that nation states are responsible for the cyber activity conducted by users within their geographical borders—thus, if a user in Canada engages in cyber crime, that user is acting within Canadian borders even in the virtual context.

Hedley (2003) suggests that within this structure, nation states engage in "cyber enclosures" that direct users to a specific selection of online content without necessarily prohibiting access to material outside of this portion of cyberspace (p. 217). For instance, when people in the United States search for Google.com, they are automatically directed to the American version of this site that yields American search results but are not prevented from accessing Google.fr (the French version of this site). Contrarily, some countries enact cyber enclosures that not only direct users to a particular subset of online content but also inhibit those users from accessing content beyond this domain. However, the transnational characteristic of cyberspace complicates its governance. For instance, although a certain action might be illegal in one country, the practice might be protected under the laws of another country. Thus, the Internet faces the "paradox of nationalism," or that the enforcement of a nation's laws requires international cooperation and the enforcement of similar laws in legal systems throughout the world (p. 217). The paradox requires both that nations work together and that international standards for online legal activity align. The paradox emerges online as countries try to enforce national rules but find that these distinctive laws must tend toward generality so that they can be successfully enforced in the virtual realm of cyberspace and between its unclear cyber borders.

Hedley (2003) offers three strategies that nations can enact when "attempting to assert [online] national authority" (p. 218). First, countries can attempt to inhibit and outlaw problematic behaviors, such as users' attempts to "break copyright," "steal money," distribute obscene images, and similar actions (pp. 218, 220). Second, countries can provide a group of monitoring officials, "a police presence in cyberspace," to remove or flag any inappropriate or illicit online activities (pp. 218, 221). Third, nations can develop codes of online conduct or policies of cyber "civil law" that define the "rights and duties" for citizens engaged in cyber activities (pp. 218, 222). However, varying legal standards in different nations problematize the establishment of online police forces and announce variations in civil laws within different contexts. Thus, Hedley notes the unlikelihood and potential impossibility for isolated nations to exert "*exclusive* jurisdiction over their own portions of cyberspace" (p. 222). Hedley describes the Internet as in a state of "chaos," stemming from the inability to enforce national laws in a fundamentally international space (p. 222). While recognizing that the paradox of nationalism requires nations to work together and mirror one another's laws to ensure the protection of citizen rights in cyberspace, Hedley believes that an international order will emerge.

Rather than focusing on issues of jurisdiction, Jim McDonnell (2009) examines online communities, social networks, and virtual worlds to highlight their differences from physical spaces. McDonnell suggests that the "enthusiasm" for virtual communities rests in their ability to extend and enhance human connections across the bounds of geographic constraints (p. 4). In fact, the strongest criticism against virtual communities is their lack of "face-to-face interaction" (p. 4). Although lacking this component of human connection, virtual communities facilitate interactions across the ethnic, economic, and generational borders that often divide people in the physical world. Despite the enhanced possibilities to build human connections, administrators and community participants can attempt to place limitations on who can join online communities depending on designated entrance requirements (e.g., gender, interest, religious beliefs, sexual orientation). These imposed borders for inclusion and exclusion tend to reflect the social and political boundaries present in the physical public domain.

For McDonnell (2009), the passage from the physical world of "mundane reality" to a virtual context allows users to redesign themselves with any attributes they choose (p. 5) and opens possibilities that transform existing notions of borders. He extends the conversation about cyber borders from nation states to social and economic boundaries. McDonnell contends that the future borders in the cyber context grant civilians the ability to extend identity structures through online profiles shaped by both the physical and virtual worlds (p. 6). The nature of cyberspace and the opportunities this domain affords are the result of rhetorical deliberations reflective of both online and physical contexts. McDonnell focuses on the borders that cyberspace permits individual users to cross, including geographic and bodily limitations, and demonstrates how those borders relate to and extend beyond physical contexts.

Also contending that physical and virtual spaces co-inform one another, Antonio García Jiménez, Pilar Beltrán Orenes, and Sonia Núñez Puente (2010) suggest that cyber borders and virtual communities exist apart from and are yet a real part of the world. Jiménez, Orenes, and Puente describe that the communication practices utilized through cyberspace offer an alternative to existing geographic-based standards of community formation. This extension occurs by permitting "real-time contact and interchange between members of [physical] communities" (p. 214). While virtual communities have borders, these divides differ from the "traditional boundaries" between nation states (p. 214). For Jiménez, Orenes, and Puente, we must recognize the reality of virtual borders as existing in a context distinct from geographic boundaries.

To clarify distinctions between physical and cyber borders, Jiménez, Orenes, and Puente (2010) offer two coordinates of geographical borders in the empirical world. First, geographic borders align with states and mark distinctions between “geography, politics, economics, and the administrative sphere” (p. 215). Nations determine these borders through histories of conflict and deliberation that demonstrate how geographic boundaries can change throughout history (e.g., comparing a pre-World War II map of Central Europe with a present day map of the same physical space). Second, geographic borders can be symbolic in the demarcation of “social representations” between nation states; that is, national borders can constitute dividing lines between cultures, but cultural boundaries can also exist separate from and regardless of “physical and official barriers” (pp. 215–216). Geographic divisions within physical space and fluid boundaries between cultural spheres combine to form national identities that contribute to the physical unification of a nation state.

Accompanying the coordinates of physical boundaries, Jiménez, Orenes, and Puente (2010) find three characteristics that influence virtual borders. First, the Internet changes notions of space and time in ways that conceptualize them as “simultaneously infinite and infinitesimal” (p. 217). Thereby, the Internet connects users to an infinitely large, limitless space mediated by a device continually made smaller (from the size of an apparatus larger than one room during the onset of the Internet to modern-day devices smaller than the human hand in the time of Web 2.0). Second, the Internet accelerates and decelerates time—accelerating time as information from early antiquity to the present day is brought to users in seconds and decelerating time as users must determine how best to apply this information in the advancement of the public domain (p. 217). Third, the Internet alters human “corporeality” (p. 217). That is, the limits of the human body are “blurred” in its online representations (p. 217). Rather than being tied to geographic, economic, political, and cultural distinctions, the Internet alters notions of borders in “the transmission of data” (p. 217). The Internet simultaneously engages users situated within their given physical circumstances and opens opportunities for them to act beyond the confines of these conditions.

These distinctions guide Jiménez, Orenes, and Puente (2010) to a multivocal, six-themed descriptor of virtual borders (p. 219). First, the “cyber border” separates “what is inside and outside cyberspace” (p. 219). Second, they suggest that a “mixed border” converges real and cyber borders (p. 219). Third, the “virtual social border” has a real referent and connection “to a territory that is not a state” (p. 219). Fourth, a linguistic “community border” emerges from online communities with shared “ideas, values, or interests” (p. 219). Fifth, “community borders with territory” in the physical world are “linked to the material and economic spheres” that result from “territorial relocations,” which provide “financial or managerial benefits” in the virtual world (p. 219). Finally, the “applied virtual border” emerges when technology influences preexisting physical borders between nations and states (p. 219). Jiménez, Orenes, and Puente’s typology of virtual borders characterizes how cyberspace redefines and informs boundaries from physical contexts.

Amber Davisson (2011) advances an understanding of borders by focusing on the interplay between maps in virtual and physical spaces. She contends that these maps of virtual borders can “advance political agendas” (p. 102). Specifically, Davisson examines maps from the 2008 United States presidential election and contrasts the traditional “red-and-blue map” with user-generated maps created from either Google Maps or Google Earth (p. 102); each map reveals particular interpretive options. Davisson suggests that the differentiation between the traditional broadcast maps and user-generated digital maps illuminate a transition from a “philosophy of broadcast media” to a “philosophy of digital media” (pp. 102–103). This shift corresponds with the move from broadcasters displaying one portrayal of the American political environment to users participating in the rhetorical creation of materials that strategically represent this same milieu. The maps created and distributed online during the election cycle have ramifications for the physical world and its ongoing relation to cyberspace. To exemplify this insight, Davisson describes an occurrence in Lakewood Park, Massachusetts, where someone carved a “large ‘W’ with a slash” into the ground as a political message in opposition to then-President George W. Bush (p. 119). The “W” was captured by Google Earth satellites and sent a visible message to those who accessed maps through the program (p. 119).

Davisson (2011) concludes with three implications that describe how digital maps alter borders between physical and virtual spaces. First, digital technologies facilitate the creation of “new maps and new interpretations,” offering different perspectives on the political landscape of the United States (p. 118). Second, online capabilities permit users to construct ideologies “from the bottom up” in the creation and manipulation of data as interpreted in a map of individual voting habits (p. 118). Third, the use of new media allows “nonexpert media producers” to create “rhetorical interpretations” of events that have “far-reaching implications” for “political decisions” (p. 119). Davisson acknowledges how cyberspace changes representations of physical borders and how users have the ability to participate in deliberation about determining these boundaries.

Shifting the focus to governmental capabilities to restrict and block online content, Rolf H. Weber (2011) contends, "Traditional borders do not exist in cyberspace" (p. 1187). Instead, the Internet emerges both as a space for the "timely exchange of opinions and ideas" and as a site that can withhold information for the benefit of strategic government actions (p. 1186). Federal government agencies specifically become Weber's focus when exploring the ability to withhold information within national boundaries. Weber acknowledges that no "international accords" or "specific rules" exist to determine the permissibility of a government's right to conceal or to interfere with the free flow of information online and that government practices of blocking information online could have "cross-border" implications (p. 1187). Practices of restricting access to information online correspond with a lack of international agreement on appropriate standards for information access, which can affect unintended publics in various nations. According to Weber, government efforts to interfere with information access can become a source of international tensions and even lead to conflict. Thus, ambiguous cyber borders point toward governmental responsibility to consider international relations within the framing of their cyber policies.

Weber (2011) suggests that international "shared responsibility" is a guiding principle for determining when it is valid for a country to prevent the free flow of information (pp. 1187). Although no international governance standards exist, Weber draws upon international law[62] tied to the "fair and equitable use of certain common

[62] Weber (2011) draws upon the following international laws: (1) The Declaration on Principles Guiding Relations Between Participating States; (2) The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies; (3) The United Nations Convention on the Law on the Non-navigational Uses of International Watercourses of 1997; (4) The Kyoto Protocol to the United Nations Framework Convention on Climate Change of 1992; (5) The Convention on the Transboundary Effects of Industrial Accidents of 1992; (6) The International Law Commission's Draft Convention "Responsibility of States for Internationally Wrongful Acts"; and (7) The Cybercrime Convention of the Council of Europe of 2001.

resources" to ground the formation of customary law (pp. 1188–1189). Importantly, Weber identifies international legal instruments as exemplars for recommendations[63] on the prevention of "transboundary disruption[s]" within the "stability, robustness, resilience, and openness of the Internet" (p. 1189). Weber's framing of the Internet as a common resource necessitates the coordination of international shared governance to ensure that national subsets within the global community are not marginalized or disenfranchised. Thus, Weber urges the development of "concrete international legal instruments" that establish "clear guidelines" for the sharing of information across virtual borders (p. 1192). Emphasizing the Internet as a shared resource, Weber considers the importance of employing and using the Internet in a way that facilitates cross-border communication while protecting the rights of international citizenships.

Richard Rogers (2012), likewise, builds upon a recognition that physical locations in national geographic boundaries play a significant role in influencing search results and access to online content. He observes this trend as a massive shift in "the politics of web space" since the late 1990s (p. 195). In fact, Rogers describes this practice as the "symbolic end of cyberspace" (p. 193). He identifies a French lawsuit filed against Yahoo! in 2000 as a seminal turning point in the development of this trend. This lawsuit brought forth charges against Yahoo! as a corporation, demanding that the web service employ software that would block Nazi memorabilia web pages (p. 193). This case introduced a new understanding of content management in online services; now, rather

[63] Weber (2011) offers the following legal instruments to lend insight to the prevention of online disruptions: (1) International Law Commission's Draft Articles on Prevention of Transboundary Harm for Hazardous Activities, adopted in 2001; (2) Declaration of the United Nations Conference on Human Environment, Principle 21; (3) The Rio Declaration on Environment and Development of 1992; and (4) various international treaty laws which adopt the principle of prevention (e.g., Article 194 of the United Nations Convention on the Law of the Sea, Article 1 of the Convention on the Prevention of Marine Pollution by Dumping Wastes and Other Matter, Article 2 of the Vienna Convention for the Protection of the Ozone Layer).

than governments supplying the technological know-how to block unwanted content, corporations must accept this responsibility by locating and associating information such as IP addresses with specific national standards. This change fundamentally altered the nature of cyberspace, thus marking its symbolic end for Rogers. After this lawsuit, web software began to collect information on users' geographic location and cipher content accordingly, making cyberspace, which was once conceptualized as "placeless," grounded in and through physical locations (p. 194). Rogers documents a significant historical shift in the architecture of cyberspace that identifies physical location as an essential and necessary component for organizing this information.

Offering an alternative emphasis on cyberspace's ability to transcend national borders and physical locations, Amanda Gearing (2014) reflects on the way that the Internet alters conceptions of boundaries between nation states within the context of journalism. Gearing examines the implications of online network theory for present and future journalistic practices (p. 63). Noting the longstanding important collaborative efforts between reporters and media outlets, she contends that cyberspace offers a new relationship and collaboration between nations for investigative journalism. These collaborative efforts, which she understands as characteristic of a cyber era, offer new possibilities for researching and publishing "complex stories" at a low cost (p. 66). The Internet allows journalists to participate internationally in crafting stories, garnering connections across social media, and gathering a "wide-rang[e]" of information (pp. 72–73). For Gearing, journalists transcend physical borders through cyberspace and gather/share resources with one another for more complete and accurate stories.

Communication scholars have recognized the global/national dialectic as characteristic of the nature of cyberspace since the year 2000. Together, this literature points toward three themes. First, cyber borders are ambiguous, meriting attention and consideration as to whether these boundaries align with or re-conceptualize physical and national spaces (Hedley, 2003; Jiménez, Orenes, & Puente, 2010; Weber, 2011). Second, the organization of content on cyberspace can be categorized through data flows, "media classes" (Halavais, 2000), "cyberspace enclosures" (Hedley, 2003), or physical locations (Rogers, 2012). Third, while this organization reflects associations to physical location, government censorship, and native language, cyberspace simultaneously transcends boundaries as it opens opportunities to communicate across and within geographic spaces (McDonnell, 2009; Davisson, 2011; Gearing, 2014). Although cyberspace reconfigures conventional notions of physical and national borders into new, increasingly global amalgamations, the flow and use of information online might offer coordinates for new policies about communication, access, and civilian rights. The next section considers how a recognition that cyberspace changes conceptual understandings of boundaries leads toward implications for international relations and the problematic potential for third-tier cyber attacks that culminate in cyber terrorism and cyber war.

Cyber Terrorism and Cyber War as Third-Tier Attacks

As explained in the introductory chapter of this project, scholars debate the prevalence and very existence of cyber war and cyber terrorism (Brenner, 2007; Bucci, 2012; Conway, 2014; Denning 2007); however, there is general agreement about the potentially devastating consequences these threats pose. This section reviews and builds upon this material. Beginning with scholars from outside of the field of communication who call for a remapping of cyberspace (Dodge & Kitchin, 2001), this section articulates the link between ambiguous cyber borders and threats toward international relations that could make cyberspace an ideal platform for dispute. Inherent within this possibility is the potential for cyber terrorism and cyber war; therefore, this section culminates with a discussion about how the national/global dialectic leads toward third-tier cyber attacks at the cusp of cyber terrorism and cyber war.

In 2001, computer technician Martin Dodge and scholar of human geography Robert Kitchin offered their work, *Mapping Cyberspace*. In short, this project addresses how cyberspace alters conceptual understandings of boundaries to the point that we must consider how to remap this new frontier of human interaction. They adopt a framework that draws upon social constructivist, political economic, and postmodern frameworks. From the social constructivist position, Dodge and Kitchin announce the influence of mediated culture and the users' participatory role in contributing to how online engagement shapes social reality (p. 27). The political economics perspective announces the influence of "broader social and economic structures of capitalism" (p. 27). The postmodernist framework fosters an important recognition of difference and reconfiguration of modernist understandings of "space, time, reality, [and] nature" (p. 28). The social constructivist and political economic perspectives, in conjunction, recognize that user interactivity as well as social, economic, and political systems play an influential role in constructing cyberspace in a postmodern context. They suggest that this new frontier requires a remapping and, furthermore, that the dialectical tensions that comprise the virtual world of cyberspace assist with this task.[64]

[64] Dodge and Kitchin (2001) recognize the following dialectics that contribute to a mapping of cyberspace: (1) "*Space/spacelessness*"; (2) "*Place/placelessness*"; (3) "*Industrial/postindustrial*"; (4) "*Public/private*";

After framing the scope of their project, Dodge and Kitchin (2001) articulate how maps assist in the human ability to understand geography in physical and virtual spaces. Maps, both physical and virtual, create visualizations that facilitate understandings of the world and aid in identifying who controls, who can access, and who can use particular spaces (Dodge & Kitchin, 2001, p. 69). Specifically when dealing with virtual contexts, the process of "spatialisation" allows humans to understand a spatial structure "where no inherent or obvious one exists" (p. 69). Spatialization assists cyber-cartographers when facing the challenge of using "visual spatial forms" that lack materiality or geographic referents; spatialization helps to group complex, mutable information that is "non-spatial or immaterial" (p. 70). According to Dodge and Kitchin (2001), a cyber map, although resulting from methods significantly distinct from traditional cartography, would facilitate a human understanding of the nature of this space and lend insight into how it re-structures physical spaces.

Therefore, Dodge and Kitchin (2001) call for and offer a "radically new" method of cyber cartography, which they base on three coordinates (p. 71). First, they distinguish the role of geographic referents and spatialization in maps of information and computer technologies (ICTs) as well as maps of cyberspace. Maps of ICTs would include information about where individual devices with unique IP addresses are located within physical space—for instance, a network map used by Verizon locating all cell phones and cell phone towers. Maps of cyberspace, however, lack a "geographic referent" and instead rely upon spatialization as a strategy "to make comprehensible data that would

(5) "*Broadcasters/listeners*"; (6) "*Real/virtual*"; (7) "*Nature/technology*"; and (8) "*Fixed/fluid*" (pp. 13–24). These dialectical tensions were identified in the time of Web 1.0. Although Dodge and Kitchen's framework is still relevant, the current project provides an updated representation of the dialectical nature of cyberspace in an era of Web 2.0.

otherwise be too complex to understand" (p. 71). While maps of ICTs can correspond with physical locations, maps of cyberspace do not. Maps of cyberspace attempt to visualize the user experience of ICTs—while ICT devices are located in physical locations, the abstract notion of experience extends beyond physical contexts into a cyber world.

Second, Dodge and Kitchin (2001) note the way that cyber maps can visualize "immateriality/materiality" (p. 71). When portraying materiality, maps disclose particular functions or representations of physical space—e.g., blue prints of building structures or maps of trails in a national park. When portraying immateriality, maps visualize information such as citizen voting patterns or the virtual layout of a webpage. Extending this discussion to an era of Web 2.0, ICTs could map materiality in terms of reproducing roadways onto virtual platforms—for instance, what appears on Google maps. Cyberspace, however, maps materiality based upon gathering information and patterns of daily movement through physical spaces—for instance, identifying significant locations based upon users' interaction with the Google map software. In terms of immateriality in an era of Web 2.0, ICTs can map user preferences, such as viewing habits on Netflix. Cyberspace could then take this data to make inferences about how to re-organize the information available on the site with viewing recommendations—e.g., by relocating a particular movie from an unseen virtual location to a visual presence on a home page. Both ICTs and cyberspace contain the ability to map immateriality/materiality.

The third and final coordinate of Dodge and Kitchin's (2001) cyber cartography pertains to form (p. 71). Maps can represent data in "static, animated, interactive, [and] dynamic" forms (p. 71). A static map is unchanging, similar to a traditional map in the physical world. The animated map allows viewers to witness a series of static maps that represent change across time (p. 72). The interactive map allows people to use their cursor to participate with the map and to learn more information about a desired topic. The dynamic map updates itself in real time as new information becomes available (p. 72). These cartography forms model representations seen on both ICT and cyberspace maps.

Dodge and Kitchin (2001) recognize the difficulty of determining representations of data in cyberspace and offer considerations for how cyber-cartographers can make this data comprehensible. Acknowledging that cyberspace exists outside or beyond traditional notions of space and place, cyber cartography requires a remapping in response to the changing borders of this virtual platform. Maps will advance our ability to understand and navigate the evolving frontier of cyberspace and its dialectical nature. Their emphasis on cyberspace specifically connects to the interactive and experiential characteristics of human engagement in online activities—activities that simultaneously influence interaction with physical spaces.

Also reflecting on the ways that cyberspace and the Internet restructure the boundaries of the physical world, Italian semiotician, linguist, and philosopher Umberto Eco[65] (2006/2007) articulates how a cyber environment alters conceptions of national borders and international relations. Eco begins by defining and describing the purposes of a border in physical spaces. For Eco, a border or boundary defends the community it

[65] Umberto Eco completed his graduate work at the University of Turin in 1954. He holds 34 honorary PhDs from internationally-known universities in the United States (Brown University; Rutgers University; Loyola University, Chicago; State University of New York; Indiana University) and abroad (e.g., Odense University, Denmark; Royal College of Arts, London; Academy of Fine Arts, Warsaw). His work addresses philosophy, cultural theory, semiotics, linguistics, aesthetics, and morality. Additionally, he authored of seven novels ("Umberto Eco," n. d.).

encircles from the “attack[s]” and “gaze[s]” of outsiders (p. 78). He turns to the Great Wall of China as an exemplar of this contention, which served the dual purpose of “defend[ing] subjects” and “safeguard[ing] the secret of silk production” (p. 78). However, Eco notes the extent to which the Internet alters these traditional notions of borders and questions the very “definition of the nation-state” (p. 78). He extends his discussion by identifying this unintended consequence as a result of cyberspace.

Eco (2006/2007) looks beyond an understanding of the Internet as a site for “international and multilingual chat lines” toward the various unintended consequences that result from the unreflective use of this technology, including diminished national borders and a loss of privacy (p. 78). According to Eco, to perceive the Internet as solely or primarily a communication transmission technology overlooks the social and political functions of this platform on an international scale. Namely, the Internet “collapse[s]…boundaries” as the network sends information between and through nation-states in the physical world, which results in two unforeseen consequences (p. 79). First, no nation “can prevent its citizens from knowing what is happening in other countries,” and second, online technologies permit any source with enough technological know-how to exert surveillance and power “over the activities of citizenry,” thus leading to a loss of privacy (p. 79). The Internet eradicates borders between nation states and re-orders existing power relations. The Internet changes the amount and type of information that citizens can access within and beyond national borders while also altering relationships between power sources.

Eco (2006/2007) articulates how the Internet grants the government and other institutional entities the power to observe the behaviors and actions of private citizens.

Likewise, however, he emphasizes that the Internet also produces a digital "panopticon"[66] where private citizens can monitor the activities of government and corporate officials (p. 79). While the Internet diminishes conceptions of borders that once protected people and nation states from attack and voyeurism, it also creates a new domain of international and social relations. A borderless cyberspace allows citizens from any nation to monitor the actions of international governments and, likewise, international governments gain access to spy on their own citizens as well as foreign nation states and their citizenships. For Eco, we do not yet understand the potential implications of this trend for international relations, privacy management, or the very conception of nation states. Implicit within Eco's work is a concern about potential conflicts between nations that could lead to international dispute.

As boundaries between nations change in a cyber context, so do international relations in the physical world. Thus, cyberspace becomes a valid potential realm to carry out international disputes. These disputes could result in a wide range of cyber attacks and threats that could culminate with cyber terrorism and cyber war. The remainder of this section reviews material on cyber terrorism presented in the introductory chapter of this project and articulates how this phenomenon could extend to instances of cyber war. Ultimately, this project contends that in order to respond adequately to these threats, one must understand cyberspace as existing within a national/global dialectic.

As reviewed in the first chapter of this project, cyber terrorism is a growing threat that, despite disagreement centering on its existence or occurrence, merits attention.

[66] In 1830, Jeremy Bentham introduced the idea of the panopticon as a way to survey prisoners. The panopticon regained currency in the work of Michel Foucault (1978), and this selection is included within a 2014 anthology, *Philosophy of Technology*, edited by Robert C. Scharff and Val Dusek. Umberto Eco (2006/2007) extends the notion of the panopticon to the Internet and a loss of privacy.

Although the majority of scholarly literature denies an actual, documented instance of cyber terrorism, the term has been in circulation since Barry Collin introduced it in the 1980s, with later definitions offered by Mark M. Pollitt (1998) and Dorothy E. Denning (2007). Together, these definitions provide important common themes, which include premeditation and politically motivated *destruction* of noncombatant targets. Importantly, these scholars draw a distinction between cyber hacking (the stealing or compromising of information) and the destruction of noncombatant targets (what would lead to violence toward civilian lives). Thus, cyber attacks aimed at inanimate and intangible entities such as money, identity, and reputation do not constitute cyber terrorism. Cyber terrorism emerges when there is a threat to human life or physical well-being.

The movement toward actualized instances of cyber terrorism, however, remains a consistent concern (Brenner, 2007; Herzog, 2011; Weimann 2005, 2006, 2008, 2015). While Gabriel Weimann (2006) frames the Internet as a preferred platform for terrorist communication, propaganda, psychological warfare, and information, Susan Brenner (2007) extends these threats into a series of risks including the use of cyberspace for weapons of mass destruction, distraction, and disruption. Both Weimann and Brenner recognize that terrorist groups already use the Internet as a communication and recruitment tool and that if they were to advance their coordinated efforts, violent and life-threatening circumstances could occur. For instance, the 2007 cyber attacks targeted toward the country of Estonia globally announced the possibility for interfering with a nation's critical networks (Herzog, 2011). These attacks demonstrated how terrorist groups or nation states could use cyber platforms to incite fear, anxiety, and disruption that could result in violence or destruction. Thus, the cyber attacks we have seen so far are merely a glimpse or precursor of what could be to come in the actualization of cyber terrorist efforts.

In response to cyber attacks and in efforts to minimize the possibility of cyber terrorism, scholars suggest, we must move past the pattern of attack-defense, stronger attack-stronger defense (Argomaniz, 2015; Denning, 2001). Weimann (2006, 2015) contends that we must uncover a "golden path" that allows federal agencies to monitor problematic online behaviors that may be indicative of cyber terrorism while simultaneously protecting individual privacy as a foundational value of Western democracy and society. Alternatively, Brenner (2007) and Steven Bucci (2012) argue that prevention best occurs in response to cyber crime. Brenner (2007) suggests that rather than understanding cyber attacks as acts of war, we should think of them as crime, and thus task law enforcement rather than military personnel with response. Elizabeth Minei and Jonathan Matusitz (2013) suggest the importance of learning languages and understanding cultures to facilitate an understanding of both the language on terrorist websites and the cultural milieu from which these attacks emerge. These scholars suggest that responses to existing cyber attacks frame our ability to prevent occurrences of cyber terrorism and reflect the nature of how we interact with cyberspace as a domain for social and political action.

Communication scholar Roger Stahl (2016) emphasizes the power of rhetorically framing cyber activities. Specifically, he acknowledges that, socially and politically, we use the term cyber terrorism as a rhetorical instance of weaponized language. As explained in chapter 1, Stahl understands weaponized rhetoric as the political practice of waging war on language or some other intangible concept itself (e.g., War on Drugs, War on Poverty, War on Cyber terrorism). Weaponized language creates a particular understanding of the world and persuasively urges the public toward actions that accomplish strategic purposes. In the case of weaponizing language about cyber terrorism, we move toward the potential to turn our rhetoric into physical or virtual acts of war. Thus, the rhetorical use of the term cyber terrorism brings society to the cusp of cyber war.

Antonia Chayes (2015) also announces that society is at the brink of cyber warfare. She notes that cyber attacks are ambiguous and fall along a "grey area between war and peace" (p. 476). We lack clarity on what exactly constitutes cyber war as we question who is responsible and what are appropriate punishments. Chayes suggests that our complete reliance on a platform rife with significant "hardware and software flaws" renders entire nations and populations vulnerable to cyber attacks that exist in a space outside of "traditional concepts about war" (p. 476). Unclear definitions of 'cyber crime,' 'cyber attack,' and 'cyber war' at national and international levels result in confusion about proper response tactics (p. 482). Thus, cyber attacks are difficult to respond to since they exist in an indeterminate space on the brink of cyber war.

Contributing a potential response to cyber attacks between nations, Grant Hodgson (2016) offers the notion of a "cyber treaty" to bolster international defense measures (p. 259). Hodgson's cyber treaty involves three elements: (1) "intrusion detection and networking"; (2) "cyber investigations"; and (3) "data exchanges" between nations (p. 259). When nations agree to engage a cyber treaty, they would work together to share information about data breaches and successful defense strategies that could increase global cyber security. The cyber treaty offers a model for nations to effectively protect themselves against unwanted intrusions (p. 232). A global network of information sharing about cyber attacks would counteract the existing difficulty in determining the "attribution" or the source of the attack (p. 232).

This section traced how ambiguous notions of cyber borders alter existing conceptions of international relations that could result in instances of cyber terrorism and cyber war. Dodge and Kitchin (2001) suggest that cyberspace requires an entirely new mapping system to illuminate insight on how users engage the space in local and international contexts. Eco (2006/2007) recognizes that cyberspace changes notions of boundaries that ultimately alter existing conceptions of nation states. These changing borders exist within the national/global dialectic and open possibilities for cyber terrorism and cyber war. To help re-contextualize understandings of cyber terrorism and cyber war along a global/national dialectic, this project returns to the work of Ulrich Beck and Elisabeth Beck-Gernsheim (2002) and Ulrich Beck (2004/2006) with a focus on his notions of "individualization" and "cosmopolitan outlook." These concepts build upon chapter 4's emphasis on Beck's risk society to provide a more holistic view of Beck's project (Selchow, 2016) and how it relates to cyber terrorism and cyber war as third-tier cyber attacks.

Ulrich Beck: Individualization and Cosmopolitan Outlook

Continuing from the previous chapter, this section expands considerations from the German sociologist Ulrich Beck as they pertain to cyber terrorism and cyber war. The previous chapter applied Beck's risk society to understand the dialectic of anonymity/identity in response to individual and corporate data theft as a second-tier cyber attack. However, Sabine Selchow[67] (2016) argues that Beck's central concern was to offer alternative perspectives to the unceasing risks present in contemporary society; for Selchow, a holistic view of these alternative perspectives requires themes present in his risk society as well as in his notions of the "cosmopolitan outlook" and the "tradition of the national perspective" manifest in individualized society (p. 370). This section contends that insights from Beck and Beck-Gernsheim's (2002) *Individualization* and Beck's (2004/2006) *Cosmopolitan Vision* can inform responses to cyber terrorism and cyber war as third-tier cyber attacks.

To review, Beck's risk society states that we live in a period of reflexive modernity. In other words, as a result of neoliberal capitalism, the competition filling the marketplace introduces nuclear, genetic, chemical, and ecological risks that threaten the destruction of society as we know it (Beck, 1986/1992; 1992). Later, scholars apply Beck's conception of risk to understand cyber risks (Deibert & Rohozinski, 2010) and software risks (Federspiel & Brincker, 2010) and to announce the onset of the "digital risk society" (Lupton, 2016). This section will now further explore Beck's conception of the national perspective through *Individualization* (2002), co-written with his wife Elisabeth Beck-Gernsheim, and conceptualization of the new, cosmopolitan world through his *Cosmopolitan Vision* (2004/2006).

Expanding on the framework he began in *Risk Society*, Beck and Beck-Gernsheim's (2002) work on individualization informs the national pole of the global/national dialectic. Although individualization sounds inequitable with the national,

[67] Sabine Selchow, Ph.D., is affiliated with the University of Sydney, where she is a Research Fellow in the ARC-Laureate Program in International History. Her research interests include global and cyber security, EU security, human security, global civil society, reflexive modernization, and methodological cosmopolitanism. She is the author of one book, the co-editor of three books, and the author or co-author of several book chapters and journal articles ("Sabine Selchow," n. d.).

Beck and Beck-Gernsheim (2002) explain that the present day process of individualization erodes “social-structural conditions for political consensus” that enable the “collective political action” of nation states (p. 29). Thus, Beck and Beck-Gernsheim suggest that the “closed space of national politics no longer exists” (p. 29). In order to understand the structure of nation-states in the present moment, we must engage the process of individualization, or that which empowers individuals to exert influence on and over governments “from below” (p. 29). To contextualize the term “national” in the global/national dialectic of cyberspace, the chapter offers a survey of Beck and Beck-Gernsheim’s notion of individualization.

Beck and Beck-Gernsheim (2002) begin with an overview of the concept of individualization. From an overarching perspective, individualization represents a “disintegration” of former social entities and the “collapse” of “state-sanctioned” norms for biographies, perspectives for understanding, and role models (Beck & Beck-Gernsheim, 2002, p. 2). Individualization eradicates universally-agreed-upon standards of conduct—notions of what is proper to be and to do. Furthermore, individualization is a “compulsion” that drives the creation and management of identities and communities that respond to a world of constant change (p. 4). This creation and management opens the door to choice at increasingly infinitesimal levels. Where previously an agreed-upon framework informed common understandings of traditions and institutions, individualization empowers individuals to choose “[l]ife, death, gender, corporeality, identity, religion, marriage, parenthood, social ties” (p. 5). As a result, Beck and Beck-Gernsheim suggest, “national consciousness” fails to unify nations; instead, national unity can only be found within unification against “challenges present at the centre of [individualized] lives"—identified as "integration through values" or "joint material interests" (p. 18). In other words, individuals do not rally around nation states but instead join together in subsets of a formerly unified nation in the pursuit of material goods or shared interests. For instance, a series of individuals may join forces to oppose corporate data surveillance or may gather in line waiting for the release of the new iPhone. Unification within an era of individualization is no longer connected to a geographic location but rather to individual preferences and interests.

Beck and Beck-Gernsheim (2002) further characterize individualization as holding the "promise" to live "a life of one's own," a *leitmotif* of Western society (p. 22). The so-called 'life of one's own' grounds fifteen principles[68] that holistically characterize individualization; this project reviews representative themes from these characteristics. One theme is the ability to lead a life of one's own. In other words, Beck and Beck-Gernsheim point to a "highly differentiated" society (p. 23) that denies an agreed-upon master narrative resulting in the fragmentation of society and the possibility for individuals to become consumed in their own story—to the disregard of others. Another theme is that these 'own lives' are remarkably similar to others; thus, distinctiveness is a myth of individualization. Instead, reflexive modernity separates individuals under the guise of distinctiveness in highly similar ways. Individuals become "standardized" through the combination of "achievement and justice" in "the interest of the individual and rationalized society" (p. 23). That is, institutions offer coordinates through which

[68] Beck and Beck-Gernsheim (2002) comprehensively characterize individualization with the following fifteen characteristics. These characteristics frame society in reflexive modernity: (1) "highly differentiated"; (2) creating non-"peculiar" or unique lives; (3) depending on institutions; (4) invocating a "do-it-yourself biograph[y]"; (5) celebrating the individual's condemnation to a life of constant activity; (6) associating failure with individuals rather than external circumstances; (7) globalizing individual lives; (8) a de-traditionalizing individual lives; (9) an "experimental life"; (10) a "reflexive life"; (11) a life with "high self esteem"; (12) radical distinguishability; (13) calling for "radicalized democracy"; (14) living for others; and (15) "a depoliticization of national politics" (pp. 23–28).

individuals judge their actions and lives in ways that are similar but “non-identical” (p. 27). All of the choices available to individuals allow them to create for themselves their own lives, traditions, and beliefs that then influence the practices of governments and nations. Beck and Beck-Gernsheim focus on the role that the individual plays in influencing nations and governments from the ground up.

In *Individualization*, Beck and Beck-Gernsheim (2002) offer a helpful commentary on the “national” coordinate of the national/global dialectic of cyberspace. Beck and Beck-Gernsheim invert traditional understandings of national sociology by examining how the individual contributes to the make-up of the nation. This study is significant because it illuminates that the individualized state of individuals renders collective political action increasingly impossible. Thus, nations can no longer be understood as collective unities, but rather as a set of individuals that influence governmental politics from below. In fact, Beck and Beck-Gernsheim suggest that, within the individualized nations, only the collectively acknowledged concerns of the individual in terms of intangible values or tangible materiality might unite a nation’s people. Within an American context, the intangible value of “freedom” might unite civilians, as would a universal distribution of material objects such as “iPhones.” However, this only represents one coordinate of the national/global dialectic. For a full understanding of this dialectic and Beck’s contribution to it, I explore the global outlook outlined in his (2006) *Cosmopolitan Vision*.

In *Cosmopolitan Vision*, Beck (2004/2006) situates the human condition as “cosmopolitan,” or characterized by a “global sense” that emphasizes “boundarylessness” (pp. 2–3). Within the current state of reflexive modernity, cosmopolitanism characterizes society. The cosmopolitan outlook adopts a global mindset and rejects "either/or logic" for an inclusively differentiated "both/and logic" (pp. 4–5). To contextualize understandings of the cosmopolitan outlook, Beck crafts a metaphor of Lego construction. The cosmopolitan civilian selects pieces from a "globally available" Lego box and builds a "progressively inclusive self-image" (p. 5). In other words, the cosmopolitan Lego box is not tied to a particular set; while individual sets of Wild West, Deep Sea, and Outer Space Legos are contained within this collection, creators are not limited to either the Wild West, the Deep Sea, or Outer Space—they have the ability to construct a scuba diving cowboy on Mars! Such are the inclusive possibilities for identity construction available to a civilian with a cosmopolitan outlook. A cosmopolitan outlook reflectively respects difference and multiple traditions and is inclusive rather than exclusive.

Beck (2004/2006) further contextualizes the cosmopolitan outlook with five principles. The first principle is the "*experience of crisis in world society*" (Beck, 2004/2006, p. 7). Here, Beck acknowledges that the risks produced within a risk society are global in scale, extending beyond the boundaries of one solitary nation to interdependent international contexts (e.g., climate change, nuclear war, and scarcity of water produce risks on a global scale). The second principle that Beck suggests is a "*recognition of cosmopolitan differences*" between cultures that often goes unexplored or unactualized, thus resulting in a "*cosmopolitan conflict character*" (p. 7). This conflict emerges when an intentional commitment to difference corresponds with an unwillingness or lack of interest in learning from and about those differences. The third principle pertains to "*empathy*" and "*perspective-taking*" (p. 7). In other words, a cosmopolitan outlook permits one to understand that the perspective one takes in viewing a risk shapes its appearance and manifestation—approaching a conflict as an opportunity is much different than approaching it as a problem. The fourth principle of the cosmopolitan outlook comes with the acknowledgement that we do not understand how to live in a global society without borders, which in turn compels us to "redraw old boundaries and rebuild old walls" (p. 7). The final principle of the cosmopolitan outlook is what Beck terms the "*mélange principle*," or the interpenetration of "local, national, ethnic, religious *and* cosmopolitan cultures and traditions" (p. 7). Here, Beck identifies attitudes of provincialism as a necessary counter to cosmopolitanism and announces coordinates according to which these unifications may occur. The cosmopolitan outlook enables creative insight and new understanding to emerge from the assemblage of an identity based upon a mixed collection of perspectives, identities, and traditions.

Through the five tenets of the cosmopolitan outlook, Beck (2004/2006) articulates the anachronism of the "old differentiations" of either/or logic (p. 14). The notion of cosmopolitanism is now "essential to survival" in an era of unceasing risk (p. 14). To solidify the connection between the risk society and cosmopolitanism, Beck demonstrates the necessity of establishing a cosmopolitan outlook through a substitution of "the currently prevailing ontology and imaginary of the nation-state with" his concept of "methodological cosmopolitanism" (p. 17). For Beck, determining a cosmopolitan outlook is a necessity of the contemporary historical moment, for the "risks of modern society are…transnational," and any attempt to control risk could generate "global conflicts and debates" (p. 18). For Beck, risk is essential to understanding the necessity for the cosmopolitan outlook.

Beck (2004/2006) extends this connection to risk with three insights. The first insight distinguishes between "*cosmopolitanism*" and "*cosmopolitanization*" (p. 19). According to Beck, cosmopolitanization is "*unconscious*," "*passive*," and lacks struggle, choice, and moral authority (pp. 19–21). Conversely, cosmopolitanism partakes in the "great human experiment in civilization" and contributes to "world culture" (p. 21). Beck distinguishes between cosmopolitanization as a "the (forced) mixing of cultures" and the cosmopolitan outlook (or cosmopolitanism) as an "awareness" of the mixing (p. 21). In other words, cosmopolitanized persons are confused about their inability to find an ethnic alternative to Taco Bell's 'Crunchwrap Supreme' in their travels to Mexico. One in possession of the cosmopolitan outlook, however, understands that the Crunchwrap Supreme originated in the United States rather than abroad. Beck announces "*institutionalized cosmopolitanism*" as the practices established by cosmopolitan nations that respond to ecological, economic, and terrorist crises that alter spatial, temporal, and social dimensions of risk (p. 22). Different texturings of the cosmopolitan outlook contribute to a firm understanding of how the concept differs from cosmopolitanization.

Beck's (2004/2006) second insight critiques the national outlook and methodological nationalism. The national outlook is what the common citizen adopts, and methodological nationalism shapes the methodology adopted by the social scientific researcher. Both the national outlook and methodological nationalism are among the "most powerful convictions" of society and politics (p. 24). They attest that "'modern society' and 'modern politics'" exist only as nation states (p. 24). This contention, although historically grounded, is without logical base; therefore, Beck counters this stance with the cosmopolitan outlook. Methodological nationalism is historically grounded in eight faulty principles,[69] perhaps best summarized through the egregious misassumption underlying the “where-are-you-from-originally dialogue” (p. 25). This question creates a jaded understanding of the world that contends that each human has “one native country” and “conforms to the either/or logic of nations and the associated stereotypes” (p. 25). Methodological nationalism makes the misassumption that Americans born in the United States only have ties to the US and ascribe only to characteristics of American culture through which they understand the world in black and white terms.

Beck’s (2004/2006) third insight necessitates the cosmopolitan outlook through a detailing of a descriptive methodology superior to a nationalistic framework. A first component of the cosmopolitan methodology is the recognition of global, interconnected risk. As Beck explicates, risks extend beyond “national and international political agendas” and call for collaboration between even the most “indifferent or hostile parties” (p. 36). A second component of the cosmopolitan methodology is the transition from national to “post-international risk politics” that call “non-state-centered” entities to mitigate and manage risk (p. 36). In other words, risks extend beyond the boundaries of individual nation states and merit collective action. The third component of the cosmopolitan methodology is a measurement of the global inequalities that the national methodology is not equipped to determine. Finally, the fourth component is “*banal*

[69] Beck (2004/2006) lists eight mistaken principles of the methodological nationalism: (1) the belief that the “nation-state defines the national society”; (2) the supposition of a “fundamental” opposition between national and international boundaries; (3) the ethnocentrism emerging from the belief that “[o]ne’s own society” serves as a “model for society in general”; (4) the territorial circumscription of culture that leads to false assumptions of plurality through “universal sameness” or “incommensurability”; (5) an “*essentialist outlook*” that “*separates historically interwoven cultural and political realities*”; (6) understandings through only “either/or categories” that do not adequately understand the cosmopolitan age; (7) distinctions between “*narrower and broader senses of methodological nationalism,*” and (8) distinctions between the “*international and the cosmopolitan*” (pp. 27–32).

cosmopolitanism," or the increasing global-ness of the world that demands a cosmopolitan outlook (p. 40). Although banal cosmopolitanism holds the potential to go unrecognized, it also has the potential to "be understood in terms of a new reflexivity" (p. 41). An everyday thoughtful comparing, contrasting, and combining of materials from various cultures provides citizens with skills to live and thrive in a global context. The cosmopolitan methodology allows civilians and researchers to explore the world with recognition that they are globally connected to their neighbors.

Beck (2004/2006) makes the important recognition in *Cosmopolitan Vision* of the necessity for a cosmopolitan outlook that recognizes plurality and interconnectedness. The cosmopolitan outlook rejects either/or logic for a framework of both/and. Cultures, languages, traditions, and religions are a part of the cosmopolitan world and combine together to mitigate, manage, and respond to the global risks that plague society. Importantly, the cosmopolitan outlook is not a forced, as would be a cosmopolitanized perspective. The cosmopolitan outlook brings understanding to the global community and responds specifically to the global end of the global/national dialectic.

This section reviewed the work of Beck (2004/2006) and Beck and Beck-Gernsheim (2002) to glean insights about the global/national dialectic of cyberspace. Beck's work on risk is extended to concerns of cyberspace through risks that occur to and through cyberspace (Deibert & Rohozinski, 2010), software (Federspiel & Brincker, 2010), and digital technology use/possession (Lupton, 2016). Holistically, Beck's project shows the close interplay between risk, the cosmopolitanism outlook, and individualization (Selchow, 2016). This section points toward three implications at the center of Beck's project: (1) the internal and external boundaries within and between existing nations are eroding; (2) individual governments are losing influence over individuals; and (3) both the construction of a cosmopolitan outlook and the individualization process agree that society lacks a master narrative that informs people about what is proper to do and to be. Individuals and nations alike take from a global Lego box that permits the construction of new, multi-faceted identities outside of traditional norms. The final section of the chapter offers communication ethics implications stemming from cyberspace as both global and national, which introduces cyber terrorism and cyber war as third-tier cyber attacks.

Communication Ethics Implications

This chapter contends that cyber terrorism and cyber war result from viewing cyberspace as either exclusively national or exclusively global; a dialectical approach to understanding cyberspace, however, attends to, and extends beyond, both these terms. The literature exploring this dialectic explains that the Internet re-arranges conceptions of borders since the days of Web 1.0. Furthermore, communication scholars note how these changes affect the flow of information across political, social, and economic borders. As noted by Eco (2006/2007), relations between nations fundamentally change as they lose the ability to have control over what information enters their borders, what their citizens can learn, and who can monitor the activities of citizens. Beck and Beck-Gernsheim's (2002) conceptions of the individuals who compose present-day nations and Beck's (2004/2006) cosmopolitan outlook inform ways that risk can be mitigated within the digital risk society with attention to both national and global considerations. Beck's both/and logic of the cosmopolitan methodology reveals communication ethics implications that can offer a first response to these third-tier cyber attacks.

Within the dialectical framework of this project, grounded in the scholarship of Kenneth Burke and David Gunkel, emerge new possibilities for understanding cyberspace along a national/global dialectic. First, Burke's (1941; 1945/1969) conceptualization of dialectic names the terms in tension—national and global borders. Cyberspace holds both national and global borders and results in a partially national and partially global platform. As users and nation states engage cyberspace, they must remember the ambiguous nature of cyber borders between and among countries. Gunkel (2007) recognizes the terms in contradiction within this dialectic and announces the postmodern recognition that a "synthesis" within cyberspace is beyond and otherwise than a combination of national and global borders; the space is wholly and fundamentally other. Cyberspace is neither exclusively national nor exclusively global but instead entirely different. A belief that cyberspace is exclusively national results in nations attempting to control web traffic and cyber access within their specific geographic boundaries; however, actors located in one country may commit what is considered illegal actions in another country while crossing only virtual borders but physically never leaving their home nations. A belief that cyberspace is entirely global denies the way that individual users in various countries can shape the space. Cyber terrorism and cyber war become paradigmatic results of the problematic misunderstandings of cyberspace as either national or global.

This chapter contends that cyber terrorism and cyber war emerge because of an unreflective misunderstanding about the national/global dialectic of cyberspace. While some scholars contend that nations exert control over their portion of cyberspace (Halavais, 2000; Hedley, 2003; Rogers, 2012), others contend that this space is global and beyond the scope of any individual nation (Dodge & Kitchin, 2001; Eco, 2006/2007; Gearing, 2014; Hedley, 2003; Weber, 2011). Although this chapter suggests both these contentions are to a certain extent true, cyberspace radically changes relationships between nations, people, and the physical world, as well as social, political, and economic boundaries (Davisson, 2011; Dodge & Kitchin, 2001; Eco, 2006/2007; Gearing, 2014; Hedley, 2003; Jiménez, Orenes, & Puente, 2010; McDonnell, 2009; Weber, 2011). Scholars thus note the ambiguous nature of cyberspace and the difficulty of categorizing response strategies to various cyber attacks (Chayes, 2015). Society must recognize the extent to which cyberspace exists along a national/global dialectic to offer adequate, lasting responses to cyber terrorism and cyber war. This chapter finds five implications:

1. There is a direct relation between cyber borders and international relations. The Internet, World Wide Web, and cyberspace re-organize the way that information enters a nation-state and permit both state and non-state entities to monitoring civilians. Rather than tracking the layout of this information by traditional maps, cyber cartographers can engage the practice of "spatialisation" (Dodge &Kitchin, 2001), or determine the layout of cyberspace through the various "media classes" (Halavais, 2000) and "cyber enclosures" (Hedley, 2003) that identify particular data use. A dynamic map of cyber data use will facilitate understandings of who is accessing cyberspace and how they are engaging the space.

2. Cyber terror and cyber war as third-tier cyber attacks emerge from a national/global dialectic. Cyber attacks fall within an ambiguous area "between war and peace" (Chayes, 2015) and, furthermore, the practices engaged as crime in times of peace

become a testing ground for attacks in times of war (Harnett, 2011). Cyber defenders can bolster their preparedness for cyber aggressions by recognizing that cyberspace exists wholly other than traditional, physical conceptions of nation states. Thus, data sharing and cyber treaties (Hodgson, 2016) between and among nations can help defend against the potential for cyber terrorism and cyber war.

3. Our rhetoric about cyber terror places us at the brink of cyber warfare. Despite the fact the term "cyber terrorism" is heavily circulated in common and academic parlance, scholars and government officials have yet to name an official cyber attack an act of cyber terrorism. However, government officials and experts employ the term cyber terrorism as a form of weaponized language (Stahl, 2016) to mobilize nations to war, which increasingly includes attacks on and through the cyber domain.

4. Beck and Beck-Gernsheim's (2002) notion of individualization permeates cyberspace—it gives individual users the power to craft and frame cyberspace in ways that influence nation states and accelerates the number of choices presented to individuals in a global platform. Cyberspace becomes a platform where persons can create an individual identity from a multiplicity of possibilities and divorces society from a master national narrative that grounds an understanding of what it means to be a good citizen. Cyberspace possesses an infinite amount of choices through which they may understand themselves.

5. Beck's (2004/2006) cosmopolitan outlook reflectively and thoughtfully combines national and international influences to prepare people to act in a global environment. While Beck and Beck-Gernsheim's (2002) individualization process describes an individual who becomes increasingly pre-occupied with the self and the

construction of personal identity, Beck’s (2004/2006) cosmopolitan outlook reflectively recognizes the interconnectedness of people across nation states. Cosmopolitan citizens recognize and appreciate the multiple traditions and sources that influence their identity and prepares them to function in a globalized world.

Cyber terrorism and cyber war reflect a misunderstanding of cyber borders and misconception that cyberspace is either a purely national or global space. Cyberspace, as a radically new space, combines national and global concerns on a wholly different platform. While the space offers global interconnectivity, the concerns and laws of individual nation states exert influence over the space. Although somewhat tied to geographic location, the space is also measured through spatalization practices that determine particular uses of cyberspace and generate new borders. Thus, cyberspace is neither exclusively national nor global, but an entirely new combination of both. After having reviewed three dialectical tensions characteristic of Web 2.0 (public/private, anonymity/identity, and national/global) and their associated cyber threats (cyber bullying, corporate cyber data theft, and cyber terrorism and cyber war), the final chapter returns to cyber attacks as a wicked problem and to a communication ethics framework that can guide analysis and inform response strategies.

Chapter 6

“This Is Not That”:

Re-conceptualizing the Dialectics of Cyberspace

Introduction

As noted previously and demonstrated throughout this project, cyber attacks are increasing in intensity and frequency. These attacks manifest in a variety of forms including the three tiers addressed throughout this work: cyberbullying, cyber theft, and cyber terrorism/cyber warfare. These attacks take the form of wicked crises that require attention and consideration from communication scholars. As I have contended, cyberspace is dialectical and distinctly other than physical spaces—in short, we cannot conflate “this” (cyberspace) with “that” (physical spaces). According to Arnett, communication ethics highlights difference and the important recognition that “this” is, indeed, not “that” (personal communication).[70] For instance, while an understanding of “this” pool can facilitate understandings of “that” ocean, modernity attempts to reject a recognition that the two are different. To assume that “this” is the same as “that” results in the mistaken conclusion that “this” and “that” ought to be engaged in an identical manner. We must never equate “this” and “that” as the same, lest we canon ball into the ocean without a life jacket. This guiding insight announces the relevance of communication ethics and particularly its attentiveness to and willingness to learn from difference as a first step in framing responses to cyber attacks.

This concluding chapter reviews cyberbullying, cyber theft, and cyber terrorism/cyber war as wicked crises and moves toward communication ethics

[70] In several Ph.D. seminars at Duquesne University during the early 21st century, Ronald C. Arnett employed the phrase “this is not that” to indicate the importance of distinctiveness and difference, especially as it relates to communication ethics, specifically with regard to the work of Emmanuel Levinas.

implications as a first response. First, I review the defining characteristics of wicked crises and situate acts of cyberbullying, cyber theft, and cyber terrorism and cyber war within this scope. The project recognizes these attacks as crises that call for ethical solutions. Second, the chapter returns to the dialectics that correspond with each tier of cyber attack—public/private, anonymity/identity, and national/global—to glean communication ethics insights about how these dialectics shape users' practices of cyber engagement and reflect commitments to particular goods. The chapter concludes by outlining summative thoughts and implications from the study.

The significance of this chapter lies in the articulation of communication ethics as a necessary resource that can address the clumsy solutions characteristic of the wicked crisis. The connection between ethics and clumsy solutions centers on the notion of learning from difference. Arnett, Fritz, and Bell (2009/2018) articulate learning as a central coordinate for communication ethics—a way to order the public sphere in a moment of metanarrative collapse and competing goods. By recognizing the different goods and practices protected and promoted in the public sphere, people can learn how their approach to understanding the world is similar to and/or different from that of others. The recognition of difference and the willingness to learn are necessary first steps to uncovering how we can understand a world situated within the multivocal nature of cyberspace. Stemming from this project's association between cyber attacks and the dialectical tensions of cyberspace, this chapter aims to synthesize these connections and illuminate communication ethics implications that can guide response strategies to cyber attacks as wicked crises.

Cyber Attacks as Wicked Crises

This section reviews the notion of "wicked problems" as introduced by Rittel and Webber (1973) and tracks its development into the articulation of "wicked crises" (Maier and Crist, 2017) in order to frame cyber attacks within this scope. Rittel and Webber (1973) introduce the notion of wicked problems as those that lacks clear resolution. They contend that wicked problems are wide in breadth, causing confusion between effective solutions and mere symptoms. When dealing with wicked problems, the language that we use to describe the issues frames public understanding and potential resolution strategies. Wicked problems are distinct in that they lack universally implemented remedies; what responded to the problem successfully in one instance may not in other situations. The serious nature of the wicked problem, however, urges prompt and direct response without allowing room for error. According to Rittel and Webber, wicked problems are complex, far reaching, and urgent by their very nature.

Maier and Crist (2017) develop Rittel and Webber's wicked problem into the notion of a wicked crisis. Working from the phenomenology of Jean-Luc Marion, they announce that wicked crises require us to recognize the experience of *being-in-crisis*—or attending to the crisis in all its complexity. Maier and Crist situate the wicked crisis with three characteristics: (1) "unpredictable, ill-defined and swiftly mutating"; (2) "clumsy solutions"; and (3) reducing public trust in institutions (p. 170). According to Maier and Crist, as we listen and work to understand wicked crises, we might begin to determine clumsy solutions that start conversations about response strategies for re-establishing trust. These solutions are considered starting points rather than end points; by allowing for trial and error, ambiguity, and multiple attempts, clumsy solutions recognize that one-size-fits-all solutions do not adequately respond to wicked crises. Instead, the wicked crisis demands attentiveness to a “this is not that” mindset, which attends to distinctive contexts. This section examines how cyberbullying, cyber theft, and cyber terrorism/ cyber war meet the criteria of a wicked crisis, which introduces possibilities for clumsy responses that make a first step toward potential resolutions that repair public trust in institutions.

Cyberbullying

As chapter 3 indicates, cyberbullying is a serious problem with consequences for individuals and interpersonal communication in public and private contexts. Cyberbullying meets the following three criteria of a wicked crisis:

1. Unpredictable, ill-defined, swiftly mutating. First, cyberbullying is unpredictable. Cyberbullying occurs through the posting of negative comments on social media profiles as well as in instances of humiliation and harassment as personal content (photos, messages, etc.) are re-distributed publicly. Users create personal profiles that receive peer responses that affect their public image in unpredictable ways. Furthermore, cyber communication denies the strict bounds of public or private life and becomes increasingly unpredictable as personal correspondence can be re-distributed in public platforms. Cyberspace alters patterns of human communication and interaction that increase the likelihood of cyberbullying.

Second, cyberbullying is ill-defined. There is not an agreed-upon definition of what constitutes cyberbullying—the term itself is broad. Early attempts to define cyberbullying from a communication perspective, offered by Anthony J. Roberto and Jen Eden (2010) and Roberto, Eden, Matthew W. Savage, Leslie Rasmos-Salazer, and

Douglas M. Deiss (2014), understand this first-tier cyber attack as the "*deliberate*" and "*repeated*" implementation of communication technology by users in isolation or collaboration with an intent to "*threaten or harm*" (Roberto et al., 2014, p. 98). The particular activities that fall within this definition remain unstated and disputed. A 2018 Pew Research Center study includes activities as diverse as name-calling, false rumors, unwanted sharing of explicit images, stalking, and physical threats as examples of cyberbullying (Anderson, 2018). The exact scope of what actions constitute cyberbullying and which do not remains unclear.

Third, cyberbullying is swiftly mutating. Because technology evolves at a rapid speed, particular methods of cyberbullying continually expand. For instance, returning to the claim that cyberbullying is ill-defined, technologies that exist today (such as SnapChat, Tinder, and similar platforms) were not in existence when the earliest definitions of cyberbullying emerged. These new technological platforms introduce unforeseen methods of cyberbullying that continually change the definition and alter the inherent practice of cyberbullying and its corresponding threats to users.

2. Clumsy solutions. The steps to resolve cyberbullying are not clear, often requiring that we begin with clumsy solutions. As reviewed in chapter three, there is dispute as to whether electronic-, computer-, and cyber-mediated communication improves or detracts from interpersonal communication and the human condition. Because questions about the influence of this alternative form of interpersonal communication continue, the proposed solutions about how to respond to social issues mediated on the platform are also unclear. Proposed solutions range from implementing bystander intervention programs (Brody & Vangelisti, 2016; High & Young, 2018) to institutionalizing corporate oversight and regulations (Arntfield, 2015; Milosevic, 2016). These resolution strategies offer points from which we can begin to explore possible responses to cyberbullying in the midst of unclear and impermanent solutions. While we have not yet found an undisputed answer to cyberbullying, clumsy solutions offer a starting point for trial and error responses.

3. Reduce trust in public institutions. The severe consequences of cyberbullying diminish public trust in institutions as they fail to resolve or eliminate instances of threat and harm (Arntfield, 2015; Milosevic, 2016; Primack & Johnson, 2017). Particular institutions called into responsibility are schools, social media corporations, and government-led organizations. Alvin J. Primack and Kevin A. Johnson (2017) depict a lack of trust in the schools to protect their students and faculty from cyberbullying. Similarly, Tijana Milosevic (2016) labels social media companies as liable for the activities occurring on their platforms and therefore urges them to take preventative measures against cyberbullying. Michael Arntfield (2015) demonstrates a complete lack of faith in present institutions to respond to issues of cyberbullying and suggests the need for cyber “enforcement agencies” to patrol and regulate online communication (p. 384). Cyberbullying extends beyond the reach of the schoolyard and corporation regulation; the public does not believe its existing institutions can shield them from acts of cyberbullying and calls for a radically new response system. Together, these characteristics label cyberbullying a wicked crisis.

Cyber Theft

As chapter 4 indicates, cyber theft is a poignant issue relevant to individual security and corporate reputations. Corporations are primary targets for cyber theft due to the massive amount of personal data they hold on record. Individuals interact with corporations through cyberspace within mixed notions of anonymity and identity that make them unaware of the specifics of data collection. They cannot answer who has access to my data, how is it used, and what security measures protect this sensitive information. Thus, cyber theft is a wicked crisis as it meets the following three criteria:

1. Unpredictable, ill-defined, swiftly mutating. First, cyber theft is unpredictable as corporations are often unaware that a data breech occurred and often do not inform stakeholders that their information has been compromised. New cyber theft tactics continually emerge to penetrate existing security measures in unconventional ways unanticipated by corporations. Due to the constantly evolving nature of cyber threats, corporations are not able to anticipate new ways that insurgent groups will target data. Thus, acts of cyber theft are unpredictable, often leaving corporations and stakeholders unaware of how and when cyber thieves compromise their information.

Second, cyber theft is ill-defined. Although the notion of cyber theft itself is obvious, the fact that it occurs in obscurity, is unknown, and can go undetected renders these acts ill-defined. As program designers engineer and re-engineer software and hardware with more sophisticated technology, the means of theft simultaneously become more sophisticated. The growth of cyberspace coincides with evolving cyber attacks. Increasingly sophisticated means of cyber theft obscure an agreed upon definition of what constitutes a cyber attack and appropriate response practices.

Third, cyber theft is swiftly mutating. A 2017 Pew Research Center study explicates that when users lack the knowledge of how to protect their online information, cyber thieves and hackers can rapidly steal data from them (Smith, 2017b). Cyber thieves engineer attacks within the constantly evolving landscape of cyberspace. This environment of swiftly increasing technological sophistication, which also renders cyber theft unpredictable and ill-defined, alters how cyber thieves access information, often leaving corporations' once-protected information unknowingly vulnerable. Cyber thieves adjust their tactics in response to corporate best practices for cyber security. The unpredictable, ill-defined, and swiftly mutating components of cyber theft make reliable, clear, and permanent solutions difficult to discern.

2. Clumsy solutions. As cyber theft tactics continually evolve, corporations must constantly update cyber security practices to protect user data. Importantly, the literature recognizes the ill-defined nature of cyber attacks and encourages response strategies that reflect the particularity of a given threat (Farbo & Cornelius, 2008; Schmidt, 2012; Skopik, Settanni, & Fiedler, 2016). In other words, a universal statement on cyber security that will neutralize the threat in every instance is not possible. Thus, organizations must engage clumsy solutions that simultaneously learn from the history of industry response patterns as well as from new methods that have not yet been tested. For organizations to prevent cyber theft, they must maintain industry recommendations for updating their systems to prepare for possible future intrusions, but also recognize that what worked in one instance may not in another. This means a response will undoubtedly be clumsy as organizations determine effective methods for dealing with various intrusions.

3. Reduce trust in public institutions. As a result of clumsy resolution strategies, users lose faith in the ability for public corporations to protect their data/identity. A 2017 Pew Research Center study shows evidence that Americans have low trust in “key institutions” due to this inability (Smith, 2017a, para. 3). Even prior to 2017, diminished trust in corporate data security measures corresponded with calls for the establishment of international centers to prevent cyber theft (Colvin, Garrie, & Rao, 2013; Skopik, Settanni, & Fiedler, 2016). This call for generating external organizations to monitor online activity exemplifies civilian lack of trust in corporations to keep their data safe.

Furthermore, advanced means for corporations to collect massive amounts of data on users perpetuates an environment devoid of trust. For instance, the 2018 controversies involving Facebook’s practice of sharing user data with third-party companies introduced debate about whether this instance constitutes a data breach or falls within the bounds of the publicly agreed-upon terms of use (Menand, 2018). Likewise, the summer of 2018 witnessed the onset of the European Union’s General Data Protection Regulation, which brought corporate use of cookies and other data collecting mechanisms to the forefront of public attention on a global scale (Powles, 2018). Public trust in corporations related to data use and security continues to decline (Osnos, 2018). This trend, along with the need for clumsy solutions and clarity in defining these threats, renders cyber theft a wicked crisis.

Cyber Terrorism and Cyber War

As chapter 5 discusses, cyberspace exists without marked boundaries in geographic locations and therefore requires a virtual re-conceptualization of borders that corresponds with and simultaneously breaks free from existing divides in the physical world. Cyberspace fundamentally changes notions of borders as users can act and send information across lines formerly separating nation states; cyberspace then becomes an alternative avenue to address international relations, making the threat of cyber terrorism and cyber war increasingly prevalent. Thus, cyber terrorism and cyber war pose wicked crises that meet the following three criteria:

1. Unpredictable, ill-defined, swiftly mutating. First, cyber terrorism and cyber war are unpredictable. The majority of scholars claim that an officially documented act of cyber terrorism or cyber war has yet to occur (Brenner, 2007; Conway, 2014; Stahl, 2016; Weimann, 2005), and therefore, the practical means of conclusively identifying the source of attack and the full knowledge of potential threats posed by these assaults remain opaque. While the 2007 cyber attacks on Estonia acted as a precursor to cyber terrorism and cyber war, we remain unaware of how these attacks could influence civilian life and government functionality. While cyberspace becomes an increasingly viable path for international conflict, the strategies for prevention, protection, and reaction are unprecedented and unpredictable.

Second, acts of cyber terrorism and cyber war lack an agreed upon definition. While the majority of scholars define cyber terrorism according to strict bounds that eliminate any previous cyber attack from falling within this label (Conway, 2014; Denning, 2007; Pollitt, 1998; Stahl, 2016), others consider the use of cyberspace by terrorist organizations as a first step into the realm of cyber terrorism (Minei & Matusitz, 2013; Weimann, 2006, 2015). Contested definitions surround the vernacular use of cyber terrorism and cyber war. In fact, Roger Stahl (2016) suggests that our public use of these phrases emerges within a rhetorical trope of weaponized language used to mobilize nations to arms, placing us at the cusp of cyber war. Antonia Chayes (2015) exemplifies this insight by describing cyber attacks within a murky spectrum somewhere between war and peace. As cyberspace re-conceptualizes existing borders between nation states, it completely alters how we understand international relations mediated through this online platform. For instance, the cyber distance between a user in London interacting with someone in Tokyo is equivalent to a user in London interacting with someone else in London. Cyberspace does not only make determinations about what constitutes cyber terrorism and cyber war unclear but also obscures cyber borders and physical conceptions of distance.

Third, acts of cyber terrorism and cyber war are swiftly mutating. Like cyber theft, cyber terrorism and cyber war evolve as a result of the constant updates to the hardware and software that mediate our experiences in cyberspace. Governments can be unaware of the entrance of hostile insurgents within enclosures of sensitive data that makes civilian well being vulnerable. Technological updates inherently bring possibilities for new ways to penetrate safe-guarded data and infrastructures. Here, we may draw another parallel to cyber theft in that cyber terrorist activities become exceedingly difficult to detect. For instance, Javier Argomaniz (2015) observes that simply shutting down terrorist websites only drives these activities further "underground" into the darkest realms of cyberspace (p. 264). As these activities move to the dark web, access to the content requires sophisticated knowledge that could quickly exceed tactics known by a nation's security or military forces. The constantly changing nature of cyberspace complicates issues of cyber terrorism and cyber war, necessitating clumsy attempts at resolution.

2. Clumsy solutions. The nature of cyberspace and these cyber threats complicate cyber defenses; at best, clumsy solutions can offer coordinates to guide governmental responses. Clumsy solutions involve learning best response strategies in the midst of uncertainty and urgency of response. Often clumsy solutions require continual points of reflection and effort as we navigate through an unknown and ambiguous terrain. Perhaps a place to start these solutions is through the establishment of Gabriel Weimann's (2006; 2015) "golden path," which permits some surveillance of civilian Internet use in the prevention of cyber terrorism while still upholding privacy as a fundamental value of democracy. Alternatively, Grant Hodgson (2016) suggests that governments establish international treaties to share information about cyber threats and successful response strategies. These cyber treaties would act as a common resource so that one nation could learn from the attacks incurred by another. Moving toward these clumsy solutions requires some ambiguity as governments respond to these threats to ensure strategic prevention.

3. Reduce trust in public institutions. A majority of the literature agrees that there has not been a documented cyber terrorist attack (Brenner, 2007; Conway, 2014, Weimann, 2005; Stahl, 2016). However, this literature recognizes the potential threats that cyber terrorism poses. Among these is Susan W. Brenner's (2007) characterization of cyber terrorism as a weapon of mass disruption that would target banks, transportation outlets, and medical institutions. When employed as a weapon of mass disruption, cyber terrorism diminishes trust in the government's ability to protect civilians and run the country. Cyber terrorism and cyber war threaten to reduce civilians' faith in governmental entities to protect them. Like cyberbullying and cyber theft, cyber terrorism and cyber war are wicked crises that meet the three defining criteria structuring this section.

This section has reviewed the ways in which cyberbullying, cyber theft, and cyber terrorism and cyber war fulfill Maier and Crist's (2017) qualifications, which frame the wicked crisis thus: (1) as "unpredictable, ill-defined and swiftly mutating"; (2) offering "clumsy solutions"; and (3) reducing public trust in institutions (p. 170). Importantly, Maier and Crist build upon the original framework of a wicked problem introduced by Horst and Rittel (1973). While Horst and Rittel did not allow for "trial-and-error" in response to wicked problems, insisting that those responsible had "no right to be wrong" (pp. 163, 166),[71] Maier and Crist alternatively stress that the best solutions to wicked crises are "clumsy" (p. 170). The clumsy solution supported by Maier and Crist opens room for action through trial and error. They emphasize that clumsy solutions act as starting points for offering thoughtful and contextually-grounded responses even when placed in situations shrouded in uncertainty. This clumsy solution approach allows practitioners to move from constant deliberation to the adoption of a particular framework that can respond to the problem within Horst and Rittel's (1973) original understanding of wicked problems as ethical by nature and judged as "good-or-bad" rather than "true-or-false" (p. 162). The clumsy solution permits the uncovering of communication ethics insights that permit wicked crises to speak in all their complexity. The next section turns to a communication ethics analysis in order to uncover goods that can illuminate clumsy solutions to the wicked crises of varying cyber attacks.

Communication Ethics: Examining the Dialectics of Cyberspace

This segment applies Arnett, Fritz, and Bell's (2009/2018) communication ethics literacy to uncover the differing goods and practices at stake in cyber attacks as a first

[71] These two principles of the wicked problem are problematic for underscoring potential solutions and correspond with Keith Grint's (2010) consideration that wicked problems lead to endless deliberation rather than action.

response to cyber threats. The goods and practices revealed by this analysis particularly highlight the fundamental component of learning from difference within communication ethics; the acknowledgment of difference counteracts modernity's temptation to confuse "this" for "that." Arnett et al. emphasize recognition of and willingness to learn from difference as necessary first steps to communication ethics. Without an understanding of the good that one protects and promotes, which thus motivates practices, one cannot as easily spot those of another. The discovery of difference prompts people to learn about other worldviews that diverge from their own; awareness of monologue[72] and a commitment to dialogue facilitate this learning. Learning from difference undergirds an imperative for understanding the dialectical nature of cyberspace as well as the goods and practices that characterize this space.

The dialectics of public/private, anonymity/identity, and national/global characterize Web 2.0 and uncover pertinent insights to understanding cyberbullying, cyber theft, and cyber terrorism and cyber war as wicked crises. These dialectics prompt consideration of whether cyberspace bolsters or detracts from interpersonal communication in public and private settings, whether it constructs new avenues for identity formation or facilitates anonymous action sometimes detrimental and other times advantageous to democratic society, and whether it lies between the borders of existing nations or constitutes a new territory. As Kenneth Burke (1941; 1945/1969) would recognize, cyberspace does each of these things simultaneously. These terms—public/private, anonymity/identity, national/global—live amid an unceasing give-and-

[72] While a dialogic approach to ethics centers Arnett, Fritz, and Bell's *Communication Ethics Literacy*, Arnett (2015) subsequently announces the importance of monologue in a series of essays addressing dialogic ethics. Arnett contends that attending to and being aware of monologic commitments offers one a glimpse into the goods and practices another holds as uncompromisable. This acknowledgement, in turn, becomes a first step toward effective and productive dialogue.

take. David Gunkel (2007), likewise, recognizes that these dialectics do not beget a synthesis, but rather render cyberspace as wholly and radically other; these dialectical properties collide and deteriorate within the virtual re-materialization and re-ordering of cyberspace. The terms at opposition in each of these dialectics illuminate a communication ethics good, which corresponds with practices that guide user engagement in cyber interactions.

When individual users protect and promote cyberspace as an extension of public life, their practices violate and impose themselves upon others who protect and promote cyberspace as an extension of private life—neither recognizing that cyberspace is a strange extension of subsets within both public and private spaces. Similarly, we find users protecting and promoting cyberspace within an understanding of participation as either anonymous or identifiable. Likewise, users engage cyberspace as an alternative platform for national or global action without clear knowledge of how virtual borders correspond with physical boundaries between nations. Each of these modes of engaging and understanding cyberspace reflects ethical considerations that guide scholarly debate about how each framework ultimately benefits or causes detriments to society. Modernity encourages a reductive mindset that subsequently confuses "this" (cyberspace as dialectical by nature) with "that" (cyberspace as equivalent to physical space) and results in the problematic consequences of cyber attacks. Thus, this project turns toward communication ethics analysis to attend to difference and offer a first response to these wicked crises.

Public and Private

Chapter 3 highlighted how cyberspace alters interpersonal communication in public and private settings. Public and private represent two competing goods that collide in cyberspace. Respecting the differences between these goods and how they structure cyberspace, as informed by the theoretical work of Hannah Arendt, can guide response strategies to counteract cyberbullying.

Public: goods and practices. Scholars recognize the ways in which cyber-mediated interactions fundamentally alter conceptions of public communication in positive (Anderson, 1994; Marletta, 2010; Rahimi, 2011) or negative (Jackson, 2009; Putnam, 2000) ways. Writing before the onset of the Web 2.0, Rob Anderson (1994) suggests that electronically-mediated communication offers renewed opportunities for public action in the physical world. Donna Marletta (2010) recognizes that digital meetings, when coupled with physical gatherings, can form groups capable of political action. Babak Rahimi (2011) eliminates the necessity of physical meetings altogether and suggests that political groups can form and take public action through cyberspace alone. Each of these views inherently emphasizes public life as a good that guides practices when participating in cyberspace.

Conversely, however, Robert Putnam (2000) announces problematic implications emerging from protecting and promoting cyberspace as an extension of public life. Specifically, he offers the early recognition that electronic media, and by extension digital media and cyberspace, distance and discourage people from civic engagement and thus limit public action. A reductive view of cyberspace as an extension to the public sphere limits users' ability to participate in meaningfully civic engagement opportunities.

In a similar vein, Maggie Jackson (2009) recognizes that dependence on digital devices tears at the potential to form a strong public sphere. Jackson also warns against the misconception that cyberspace and the public sphere align by emphasizing the inherently distinctive practices that correspond with each mode of engagement. As researchers contest the effects of cyberspace on public communication, their work reveals communication ethics commitments and understandings about how one ought to engage cyberspace.

Private: goods and practices. Similar to public communication, scholars dispute the benefits (Colleoni, Rozza, & Arvidsson, 2014; Flaxman, Goelm, & Rao, 2016; Walther, 1996) and deleterious effects (Carr, 2010, 2014; Putnam, 2000; Turkle, 2011) of cyber-mediated communication in private, personal relationships. When engaging cyberspace as an extension of private life, online practices contribute to relationship building and maintenance (Walther, 1996) as well as personal development (Colleoni, Rozza, & Arvidsson, 2014; Flaxman, Goel, & Rao, 2016). Users who commit themselves to engaging cyberspace as a private space invest significant time and energy in its ability to portray self-avatars in a virtual context and to use that profile as a principal means for private correspondence with others. Likewise, those committed to the private possibilities of cyberspace celebrate the capacity for users to gain a sense of control in determining what information they encounter online and thereby use cyberspace as a path toward learning from diverse perspectives (Colleoni, Rozza, & Arvidsson, 2014; Flaxman, Goel, & Rao, 2016). Those that recognize the positive effects of cyber communication stress the ability of the user to manipulate the platform to accomplish specific goods related to relationship growth and personal development.

Contrarily, others warn against practices of engaging cyberspace as an exclusively private sphere. For instance, Putnam (2000), who also announced the limits for public action to cyberspace, describes how cyberspace as a platform for private communication can both minimize interpersonal relationships and create what have more recently been termed echo chambers. Putnam warns that cyberspace diverts our attention away from public life and simultaneously trivializes our discourse within private contexts and furthermore urges that as communication technologies increasingly personalize our engagement with digital platforms, they limit the information one encounters based upon personal preference. Sherry Turkle (2011) also recognizes that electronic devices negatively affect interpersonal relationships as they isolate users, who become "alone together" in exclusively private contexts devoid of any public interaction. While some scholars announce the benefits of private online communication and others reject it, underlying insights emerge about how these modes of interaction move toward communication ethics goods and practices.

Communication ethics insights. Hannah Arendt (1958) informs user understandings of public and private spaces. Arendt's public is a space of recognition, where the community acknowledges the struggle that culminates in the accomplishment of great deeds. Arendt's private sphere allows the public domain to function by maintaining the conditions that sustain life. Importantly, Arendt notes the significance of protecting and promoting public and private life as separate spheres of the human condition that can problematically blur into the realm of the social. Arendt's social is a space blending aspects of public and private life into one conglomerate.

Arnett (2013) describes that the social replaces the struggle involved in great, immortal deeds (the public sphere) and overlooks the conditions that sustain life (the private sphere) for a celebration of personality, charisma, and individualism (the social sphere). Deborah Eicher-Catt (2013) problematizes the social by describing it as a mode of problematic discourse functions that either ideologically bind to inapplicable traditions or individualistically substitute personal preference for publicly agreed upon community standards. While maintaining concern about the social, Judith Butler (2015) announces interconnections between public and private life that fruitfully lead to communication and meaningful action. She explains that public life is often motivated by experiences occurring in private settings; these experiences do not necessarily constitute the social. Instead, the social emerges with the inability to distinguish the bounds of public and private action.

The public/private dialectic requires careful attentiveness or else leads to the problematic discourse of the social. Within cyber contexts, unrepresentative understandings of cyberspace as either "public" or "private" result in an indeterminate space that brings forth cyberbullying. Recognizing that cyberspace affects both our public and private lives offers a reconceptualization of this domain that can inform responses to cyberbullying. Just as cyberbullies, in their engagement with others, fail to recognize that their communication is both public and private, our general patterns of use online open vulnerabilities to these attacks. Regardless of whether this recognition would deter all cyberbullies from engaging in problematic online behaviors, understanding cyberspace as both public and private could reframe our engagement with the full acknowledgement that our practices cross unanticipated boundaries and reach unintended audiences within our public and private lives.

In cyberspace, the goods of public and private exist in tandem; an overemphasis on the private results in a neglect of the public and vice versa. Users must recognize the dual nature of cyberspace to understand and respond to cyberbullying adequately. Cyberbullies work to build themselves up through the social's perversion of public and private spheres. At times, cyberbullies operate actively with the assumption that their online behavior will exhibit a unique personality that garners celebration while, at other times, their behavior unknowingly reveals biases that fall within the problematic discourse function of ideological adherence (attacking all others who demonstrate difference of appearance, lifestyle, or opinion) or undue reliance on personal preference (harassing others based upon personal biases and prejudices). Arendt's work reminds us that we cannot allow our perceptions of cyberspace to blur into the realm of the social. Instead, we must diligently adhere to cyberspace as both a public and private realm—one that requires the union of the *vita contemplativa* and *vita activa* by urging users to think before acting. Within the context of this dialectical recognition, this thinking must center on how our cyber interactions influence others across public and private settings. This recognition offers an initial response to cyberbullying as a clumsy solution. Encouraging cyber users to recognize cyberspace as public and private and urging them to think before acting will not eliminate cyberbullying; however, it would offer a first step in deterring problematic communication patterns from well-intentioned users. With these communication ethics insights, Arendt's work reveals the potential for a first response to cyberbullying, as users recognize their embeddedness in cyber contexts that shape implications for their communication patterns.

Anonymity and Identity

Chapter 4 reviewed the manner in which cyberspace allows users to act anonymously and empowers them to construct their identities rhetorically. Anonymity and identity represent two contending goods that guide practices of engaging cyberspace. An understanding of the differences and interplay between these conflicting goods, alongside ethical and theoretical contributions from Ulrich Beck (1986/1992; 1992), inform corporate responses to cyber theft.

Identity: goods and practices. Scholars recognize how users construct their identities rhetorically in cyberspace (Brookey & Cannon, 2009; Brunskill, 2014; Eklund, 2011; Jordan, 2005; Kang & Yang, 2011; Walther, 1996; Zhang, 2008). This process consists of practices that reflect identity formation as a fundamental good of cyberspace. Specifically, those committed to the good of identity within cyberspace laud this platform's ability to liberate users from the constraints of identity creation and maintenance in the physical world. Mei Zhang (2008) and David Brunskill (2014) describes how this good of cyberspace lends itself to practices that allow users to create identities based upon a projected set of ideals that reflect agreed upon community standards of the good life. Furthermore, Robert Alan Brookey and Kristopher L. Cannon (2009) and Lina Eklund (2011) describe how cyberspace grants users a safe space to explore multiple avenues of identity without physical threats; their research emphasizes the exploration of gender identities, which may or may not coincide with gender identity in face-to-face contexts. Users can construct identities in cyberspace that mirror or fundamentally re-write the conventions of the physical world. The communication ethics practices of identity portrayal through cyberspace allow users to protect and promote desired qualities that simultaneously conceal others.

Anonymity: goods and practices. Alongside a recognition that users create rhetorical identities in cyberspace, one finds the contention that online activities permit users to act with varying degrees of anonymity. Scholars recognize this anonymity as both helpful (Akdeniz, 2002; Bargh & McKenna, 2004; Mahfood, Olliges, Astuto, & Suits, 2005; Simpson, 2005; Tsui, 2015) and harmful (DiMaggio et al., 2001; Williamson & Pierson, 2003). John W. Jordan (2005) announces how users can construct completely false identities that garner a community of attention, emphasizing an environment where we cannot always know who we interact with in an online context. Yaman Akdeniz (2002) and Lokman Tsui (2015) underscore the importance of online anonymity for free speech and the ability to speak out against oppressive governmental regimes. The good of online anonymity allows users to connect with others (Bargh & McKenna, 2004), explore identities (Simpson, 2005), and test engagement strategies for interacting with others in the physical world (Mahfood, Olliges, Astuto, & Suits, 2005).

Conversely, scholars recognize the threats of understanding cyberspace as a solely anonymous realm. Specifically, this misconception poses threats related to theft in an era where corporations can track IP addresses that essentially identify users and govern targeted marketing content based upon this information (DiMaggio, Hargittai, Neuman, & Robinson, 2001; Mullany, 2004). Additionally, this misconception can encourage a toxic atmosphere of hate speech (DiMaggio et al., 2001; Williamson & Pierson, 2003); in such instances, users overlook the fact that everyone engages cyberspace as embodied participants (Boler, 2007). What we say, do, and read online always occurs as performative actions mediated through a body, and furthermore, those practices contribute to identity formation that spans across virtual and physical contexts. Anonymity and identity act as cyber goods that govern practices of engagement and influence how users perform the good online. Whether advancing the good of anonymity or the good of identity, users engage cyber practices that announce communication ethics commitments.

Communication ethics insights. German sociologist Ulrich Beck (1986/1992) characterizes the “risk society.” The risk society emerged in a period of advanced, reflexive modernity and neoliberal capitalism. He contends that this era creates unlimited opportunities for economic growth alongside rapidly increasing levels of risk. In other words, we thoughtlessly flood the market with products to meet the modern and capitalistic goods of increased production, financial advancement, and technological efficiency. Beck (1992) focuses on risks in nuclear, chemical, genetic, and ecological contexts, contending that we threaten the destruction of life as we know it by allowing risk to reach unprecedented and unforeseeable heights. According to Beck (2013), our reliance on cyberspace and its corresponding patterns of use only advances the risk society, particularly within the scope of protecting one’s identity when interacting with unknown others (whether they be individuals phishing for information or institutions surveying our online activities). As the modern era protects and promotes goods and practices that align with neoliberal capitalism, it is individuals who are tasked with managing unending amounts of risk. Beck (1992) does not, however, leave us without hope; he suggests that the formation of a public sphere that further deliberates on new, emergent risks and their resolution assuage the potential for catastrophe.

Scholars further extend Beck's work on risk with an emphasis on cyberspace, software, and digital technologies (Deibert & Rohozinski, 2010; Federspiel & Brincker, 2010; Lupton, 2016). Deborah Lupton (2016) specifically focuses on the emergence of the digital risk society, articulating how cyberspace advances the desired goods of modernity and neoliberal capitalism and simultaneously rests massive risk upon individual users. She identifies three types of risk: (1) "digitized risk," which mediates and remediates information within a broadly conceived spectrum of truth and deceit; (2) "digital technology use," which inhibits individual well being by promoting practices such as online addiction, isolation, idleness, and cyber theft; and (3) "digital social inequality risks," which grant institutions the ability to survey user activities and discriminate access to content based upon social categories (pp. 304–306). Lupton's work uncovers the underlying connection between Beck's risk society and the anonymity/identity dialectic, particularly as it poses threats for cyber theft.

The ability for users to cloak portions of their identity strategically in online anonymity facilitates the potential for cyber theft. Cyberspace becomes an ideal platform for cyber theft as its potential for anonymous action coincides with individuals complacently allowing corporations to collect massive amounts of personal data stored in online platforms. Cyber theft falls within extensions of Beck's risk society as corporations use cyberspace to achieve the goods of modernity and neoliberal capitalism. However, cyberspace creates two façades related to the anonymity/identity dialectic; first, cyberspace is only truly anonymous when used by someone who understands the platform well enough to conceal unintentional identity cues, and second, particular modes of engagement limit users' ability to construct and control identity portrayals.

Inherent within cyberspace is a surreptitious identity generating mechanism governed by algorithms produced and maintained by institutional entities. Cyberspace is not anonymous unless users can strategically escape these modes of surveillance. As noted by Brenner (2007), determining the "attacker-attribution," or the person/institution at the source of the attack, is particularly difficult because cyber thieves have the technological prowess to divert cyber security barriers and mechanisms that track online users. Thus, cyber theft occurs because cyberspace fundamentally combines possibilities for anonymous and identifiable action. An overemphasis on the good of anonymity neglects considerations of identity, and vice versa. To misunderstand cyberspace as solely one or the other makes users and corporations vulnerable to cyber theft. To embrace cyberspace as existing with a dual realm of anonymity and identity allows users to counter the goods of reflexive modernity and neoliberal capitalism with clumsy attempts to manage inconceivable risk. Both anonymity and identity exist in tandem, and when users engage cyberspace with this recognition, communication ethics insights can help prevent and respond to cyber theft.

National and Global

Chapter 5 addressed how cyberspace restructures the existing borders between nation states along a national/global dialectic. The national and global poles of this dialectic represent two contending goods that shape user understandings of cyberspace. The work of Beck and Elisabeth Beck-Gernsheim (2002) and Beck (2004/2006) can offer insight on the interplay between these two goods and how they combine in cyberspace.

National: goods and practices. Scholars recognize that physical locations situated within national boundaries shape user engagement with cyberspace (Halavais, 2000; Hedley, 2003; Rogers, 2012). From a study of cyber borders in the era of Web 1.0, Alexander Halavais (2000) finds that hyperlinks are most likely to redirect users to other websites originating from and housed by servers within the home country of the search. In instances of cyber attacks, Steve Hedley (2003) suggests, the physical location of the cyberbully/hacker/cyber terrorist governs what law enforcement agency holds jurisdiction for arrest and apprehension. Richard Rogers (2012) further announces how physical locations dictate online experiences with the onset of corporate tracking mechanisms that determine a user's physical location. Those committed to the good of cyberspace as a virtual extension to national entities announce practices that actively protect and promote the nation state's ability to control and respond to cyber activity.

Global: goods and practices. Contrarily, other scholars recognize that cyberspace spans across and beyond the physical borders of nation-states (Dodge & Kitchin, 2001; Eco, 2006/2007; Gearing, 2014; Jiménez, Orenes, & Puente, 2010; McDonnell, 2009; Weber, 2011). Martin Dodge and Robert Kitchin (2001) recognize that cyberspace is a radically other space and call for a re-mapping. Also understanding how the Internet alters conceptions of space, Umberto Eco (2006/2007) announces the onset of changing international relations due to shifting notions of cyber borders between geographic locations and physical states. Rolf H. Weber (2011) and Amanda Gearing (2014), likewise, note how cyberspace permits information to cross international divides. In the protection and promotion of cyberspace as a global realm, communication ethics goods and practices emerge related to the free exchange of information and the use of cyberspace as a means to conduct and maintain international relations between nation states. Communication ethics commitments lead users to interact with cyberspace as either a virtual extension of the nation or an international and global realm existing outside of national bounds. These commitments produce particular goods and practices that provide insight into how cyberspace re-conceptualizes notions of cyber borders.

Communication ethics insights. Beck and Beck-Gernsheim (2002) and Beck (2004/2006) can inform communication ethics portrayals of cyberspace centered around national and global goods. Beck and Beck-Gernsheim (2002) inform the "national" end of the national/global dialectic. They suggest a theory of individualization, which recognizes a trend between reflexive modernity's placement of abounding risk upon individuals and the inability for individuals to organize collective and concerted action. Without embracing or advocating for the empowerment of sovereign individuals, Beck and Beck-Gernsheim identify a trend toward individualization that begins to break down existing notions of nations. For Beck and Beck-Gernsheim, an individualized world highlights the infinitesimal number of choices posed toward individuals that accelerate opportunities for personalization and customization but complicate possibilities for collective political action. Within an era of individualization, a mass of individuals replaces the nation as a collective entity; nations no longer represent their citizens but rather individuals acting separately come to create a disjointed notion of nation as they find ways to live for their fellow citizens, a concern to which Beck's (2004/2006) cosmopolitan outlook responds.

Beck (2004/2006) continues to extend this thought through the development of the cosmopolitan outlook. The cosmopolitan outlook engages the world in a manner that celebrates differences between cultures, which in turn empowers individuals to construct an understanding of the world from multiple perspectives. Responding to an era of individualization, the cosmopolitan outlook allows possibilities for individuals to think beyond the circumstances of the self to extend toward others from multiple cultures and traditions. Within a highly-individualized environment, the cosmopolitan outlook provides hope for people to connect with and live among one another in a globally-aware world. Speaking toward the global entity within the national/global dialectic, the cosmopolitan outlook pushes individuals to think reflectively about how their actions and choices influence a global context comprised of multiple cultures and traditions. In doing so, the cosmopolitan outlook helps to mitigate individual risk within contemporary society by encouraging individuals to learn from difference and to use these insights to inform a variety of response strategies to social issues. Together, Beck and Beck-Gernsheim's theory of individualization and Beck's proposed cosmopolitan vision suggest means of response to the risks posed by cyber terrorism and cyber war as the manifestation of misunderstanding cyberspace as either a national or a global entity.

As cyberspace changes notions of cyber borders, it denies the exclusive categories of either national or global; instead, cyberspace exists dialectically within and between these terms. When cyberspace is engaged solely as an extension of the nation, users forget that information is available globally, and governments overlook how cyberspace poses threats to international relations. When conceived of as exclusively international, users disregard the ways in which physical locations govern access to online content and perpetuate an environment akin to what Beck and Beck-Gernsheim call "individualization." To think of cyberspace, or any subset within it, as belonging solely to one nation fundamentally denies possibilities for collective action within or beyond physical boundaries. Beck's cosmopolitan outlook begins to offer a corrective that reminds us that we live in a global, both/and world. In the context of cyberspace, a cosmopolitan outlook begins to embrace both the global and national goods of cyberspace, which in turn can respond to instances of cyber terrorism and cyber war.

Misconceptions about and in response to the national/global dialectic advance the threats of cyber terrorism and cyber war. When users protect and promote practices that propagate assumptions that cyberspace belongs to a nation, they forget that this same platform connects them to a global network of users and thus could make them vulnerable to attack. Likewise, if users conceive of cyberspace solely according to practices that protect and promote it as a global platform, they miss the real ways in which physical locations govern access to content. Both misconceptions bring forth the potential for cyber terrorism and cyber war. Beck and Beck-Gernsheim and Beck announce communication ethics insights that move toward first steps for response.

This portion of the chapter has overviewed the communication ethics goods uncovered through an analysis of the public/private, anonymity/identity, and national/global dialectics. Arnett, Fritz, and Bell (2009/2018) acknowledge that in the postmodern recognition of metanarrative collapse, communication ethics offers a way to structure our interactions with one another. The notion of the "good," or the sense of what is proper to be and do, grounds the communication ethic through what is protected and promoted. Communication ethics are embodied and live in the practices associated with a given good; these goods and practices center on attentiveness to difference and a willingness to learn. Difference is an important first step for communication ethics;

difference creates the opportunity for learning and lays fertile ground for dialogue. Difference in communication ethics is key to understanding the goods and dialectics of cyberspace. The recognition that “this” is not “that” is essential for understanding cyberspace. While the metaphor of the Wild West can lend understanding to cyberspace, cyberspace is literally not the Wild West and cannot be engaged as such. By recognizing the differences between physical world conceptions of public, private, anonymity, identity, national borders and global borders and how they appear on cyberspace, we can offer a first response to cyber attacks as a wicked crisis in this historical moment. The final section of the chapter concludes with implications.

Concluding Implications

The final section of the project concludes with implications that emerge from this study. This chapter has proceeded by situating cyberbullying, cyber theft, and cyber terrorism and cyber war as wicked crises. Each of these attacks was established within the three characteristics of wicked crises: (1) they are unpredictable, ill-defined, and swiftly mutating; (2) they require clumsy solutions; and (3) they reduce trust in public institutions. The project suggests that to uncover coordinates for these clumsy solutions, a communication ethics analysis can announce the contending goods that are protected and promoted within these dialectics. The second segment of the chapter proceeded with this analysis of the goods that ground the dialectics of cyberspace: public, private, anonymity, identity, national, and global. When one of these goods is protected and promoted in insolation from the other, one loses a holistic understanding of cyberspace and opens room for cyber threats of bullying, theft, terrorism, and war. This project finds six implications:

1. Definitional problems surround current understandings of cyber attacks. As noted in the first section of this chapter, contemporary understandings of cyberbullying, cyber theft, and cyber terrorism/cyber war are ill-defined. Without publicly agreed upon standards for identifying what activities constitute each form of attack, we are left in the midst of confusion about how to respond. Determining coordinates for identification will assist individuals, corporations, and governments as they navigate the clumsy solutions necessitated by these wicked crises.

2. Current understandings of cyberspace are reductive and partial rather than representative and holistic. As we try to understand cyberspace, we apply a wide variety of physical world metaphors to conceptualize the space. However, each of these metaphors is reductive of the whole. The particular metaphor shapes our understanding and, while important for navigating cyberspace, must never be substituted for cyberspace—"this" is not "that." However, each of these metaphors lends a perspective that lends insight to our understanding of the overall development of the whole. In actuality, these metaphors are all valid for understanding cyberspace, but cyberspace is distinct from them all.

3. The dialectics of cyberspace render it wholly other than the physical world; we cannot confuse our familiarity with "this" (physical spaces and contexts) with the constantly evolving nature of "that" (cyberspace). The dialectical terms that collide in cyberspace—public/private, anonymity/identity, and global/national—create something radically other; each term is forever changed as a result of their collision. Any attempt to understand or engage cyberspace as solely or primarily characterized by one of these

terms completely misunderstands this platform and thus opens vulnerabilities to various cyber threats.

4. Communication ethics uncovers goods for the attackers and their targets. The goods at stake in cyber attacks illuminate how people conceive of cyberspace and thus the practices they engage in to protect and promote the space as such. A belief that cyberspace is exclusively public or private, offers either anonymity or identity, and is only national or global shapes how users will engage the space. Attentiveness to these goods and the dialectical recognition that cyberspace is all of them can provide lasting, adequate responses to cyber attacks.

5. Cyber attacks occur through the Internet and have drastic effects on cyberspace or the user experience with Internet and information and computer technologies. The Internet is distinct from cyberspace. While technological infrastructure is connected through the Internet, damage to these systems through a cyber attack will have severe implications on human health and well being through cyberspace. A conflation of these terms contributes to further misunderstandings of how to frame adequate, lasting responses.

6. Sebastian Mahfood, Ralph Olliges, Angela Astuto, and Betsy Suits (2005) offer an early "canon" of literature on cyberethics[73] (pp. 14–16). This canon introduces

[73] Their comprehensive cannon includes: *Computer Ethics* (Fetch, Vincent, & Kemnitz, 1983), *Computer ethics: A guide for a new age* (Johnson, 1984), *Ethics in an age of technology* (Barbour, 1992), *Society, ethics, and technology* (edited by Winston, Karsnitz, & Goldberg, 1993), *Computer ethics: Cautionary tales and ethical dilemmas in computing* (Forester & Morrison, 1994), *Computers, ethics, and social values* (Johnson & Nissenbaum, 1995), *Case studies in information and computer ethics* (Spinello, 1996), *The cyberethics reader* (Willard, 1996), *Cyberethics: Managing the morality of multimedia* (Lynch, 1996), *Morality and machines: Perspectives on computer ethics* (Edgar & Suny, 1997), *Social impact on computers* (Rosenberg, 1997), *Cyberlaw: The law of the Internet* (Rosenoer, 1997), *Ethics and technology: Innovation and transformation in community contexts* (Hart, 1997), *Virtual morality: Christian ethics in the computer age* (Houston, 1998), *Ethics and electronic information in the 21st century* (edited by Pourciau & Medina, 1999), *Computer and cyber law: Cases and materials* (Clifford, 1999), *Cyberethics: Social &*

coordinates for understanding the intersections between cyberspace and ethical considerations emerging within Web 1.0. This canon primarily includes resources for considering how to navigate the onset of the digitalized computer age in an ethical manner. To understand ethics within an era of Web 2.0, scholars should attend to ethicists who acknowledge cyberspace as a wholly other space and who understand cyberspace fundamentally as users' experiences with computer technologies. These recognitions would include communication ethicists, media ecologists, and philosophers attentive to phenomenology and existential hermeneutics. These additions maintain attentiveness to and appreciation of difference as it guides online action and emphasizes the experiential and interpretive frameworks that distinctively mark cyberspace. These approaches guide an understanding that cyberspace is other than the physical world and, likewise, do not confuse the experiential nature of cyberspace with technological terminology (e.g., the Internet, the World Wide Web, or social media).

moral issues in the computer age (edited by Baird, Ramsower, & Rosenbaum, 2000), *Computer Ethics* (Johnson, 2000), *Computers and ethics in the cyberage* (Hester & Ford, 2000), *Ethics and computing* (edited by Bowyer, 2000), *Internet ethics* (edited by Langford, 2000), *Code and other laws of cyberspace* (Lessig, 2000), *Internet & computer ethics for kids: (and parents & teachers who haven't got a clue)* (Schwartu, 2001), *CyberEthics* (Halbert & Ingulli, 2001), *Readings in cyberethics* (edited by Spinello & Tavani, 2001), *CyberEthics: Morality and law in cyberspace* (Spinello, 2001), *The ethics of cyberspace* (Hamelink, 2001), *Computer network security and cyber ethics* (Kizza, 2001), *The concise encyclopedia of the ethics of new technologies* (edited by Chadwick, 2001), *Cyberlaw: Your rights in cyberspace* (Ferrera, Reder, August, Schiano, & Lichtenstein, 2001), *Regulating Cyberspace: The policies and technologies of control* (Spinello, 2002), *Computers, ethics, and society* (edited by Ermann, Shauf & Williams, 2002), *Computer ethics, etiquette, and safety for the 21st-century student* (Willard, 2002), *Email and ethics: Style and ethical relations in computer-mediated communications* (Rooksby, 2002), *Society, ethics, and technology* (edited by Winston, Wainwright, Edelbach, & Hawes, 2002), *21st Century Guide to Cybercrime* (The United States Federal Government), *Computer ethics and professional responsibility: Introductory text and readings* (edited by Bynum & Rogerson, 2003), *Understanding computer ethics* (Fodor, 2003), *Computer and information ethics* (Woodbury, 2003), *Learning right from wrong in the digital age: An ethics guide for parents, teachers, librarians, and others who care about computer-using young people* (Johnson, 2003), *Cyberlaw: Text and cases* (Ferrera, Lichtenstein, Reder, Bird, & Schiano, 2003), *Pragmatist ethics for a technological culture* (edited by Keulartz, Korthals, Schermer, & Swierstra, 2003), *Computers in society: Privacy, ethics, & the Internet* (edited by George, 2003), *Ethics and technology: Ethical issues in an age of information and communication technology* (Tavani, 2004), *Readings in cyberethics* (edited by Spinello & Tavini, 2004), and *Cyberethics* (Halbert & Ingulli, 2005).

As cyberspace continues to evolve, new threats will undoubtedly emerge that necessitate further work on pertinent dialectics and their corresponding attacks. This project stands as a first attempt to represent the dialectical nature of cyberspace as distinctively other than physical world contexts. Misunderstandings about these dialectics produce misconceptions that make one vulnerable to cyber attacks. As these cyber attacks grow in intensity and severity, they act as wicked crises that lack clear and undisputed solutions. Instead, cyber attacks as wicked crises call forth clumsy solutions. Communication ethics analysis provides insight for uncovering these clumsy solutions with attentiveness to dialectical goods that acknowledge cyberspace in its distinctiveness. Communication ethics thus guides a first response to cyber attacks.

References

Aaviksoo, J. (2010). Cyberattacks against Estonia raised awareness of cyberthreats. *Defence Against Terrorism Review*, *3*(2), 13–22.

Abe, K. (2015). Ulrich Beck and Japan. *Theory, Culture & Society*, *32*(7/8), 339–342.

Ainscough, T. L., & Luckett, M. G. (1996). The Internet for the rest of us: Marketing on the World Wide Web. *The Journal of Consumer Marketing*, *13*(2), 36–47.

Akdeniz, Y. (2002). Anonymity, democracy, and cyberspace. *Social Research*, *69*(1), 223–237.

Allers, C. R. (2010). Undoing what has been done: Arendt and Levinas on forgiveness. *At the Interface / Probing the Boundaries*, *66*, 19–42.

Amoore, L., & De Goede, M. (Eds.). (2008). *Risk and the War on Terror*. London: Routledge.

Andersen, J. (2018). Archiving, ordering, and searching: Search engines, algorithms, databases, and deep mediatization. *Media, Culture & Society*, *40*(8), 1135–1150.

Anderson, M. (2018, Sept. 27). A majority of teens have experienced some form of cyberbullying. *Pew Research Center.* Retrieved from http://www.pewinternet.org/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/

Anderson, R. (1994). Anonymity, presence, and the dialogic self in a technological culture. In R. Anderson, K. N. Cissna, and R. C. Arnett (Eds.), *The Reach of Dialogue: Confirmation, Voice, and Community* (pp. 91–110). Cresskill, NJ: Hampton Press, Inc.

Anderson, R. (1982). Phenomenological dialogue, humanistic psychology, and pseudo-walls: A response and extension. *The Western Journal of Speech Communication*, *46*, 344–357.

Anderson, R., Cissna, K. N., & Arnett, R. C. (1994). Introduction. In R. Anderson, K. N. Cissna, and R. C. Arnett (Eds.), *The Reach of Dialogue: Confirmation, Voice, and Community* (pp. 1–6). Cresskill, NJ: Hampton Press, Inc.

Anderton, K. (2017, March 29). 8 Major Cyber Attacks of 2016 [Infographic]. *Forbes.* Retrieved from https://www.forbes.com/sites/kevinanderton/2017/03/29/8-major-cyber-attacks-of-2016-infographic/#2ad118d048e3

Arendt, H. (1958). *The Human Condition* (2nd ed.). Chicago, IL: The University of Chicago Press.

Argomaniz, J. (2015). European Union responses to terrorist use of the Internet. *Cooperation and Conflict*, *50*(2), 250–268.

Aristotle. (2018). *Rhetoric*. (C. D. C. Reeve Trans.). Indianapolis, IN: Hackett Publishing Company, Inc. (Original work published in Antiquity)

Arnett, R. C. (2018). Hannah Arendt: Story-laden action. In R. C. Arnett, A. M. Holba, & S. Mancino (Eds.), *An Encyclopedia of Communication Ethics: Goods in Contention* (pp. 21–25). New York, NY: Peter Lang Publishing, Inc.

Arnett, R. C. (2016). An immemorial obligation: Countering the eclipse of the Other. *Journal of Communication & Religion*, *39*(2), 7–21.

Arnett, R. C. (2015). The dialogic necessity: An acknowledging and engaging monologue. *Ohio Communication Journal*, *53*, 1–10.

Arnett, R. C. (2013). *Communication ethics in dark times: Hannah Arendt's rhetoric of warning and hope.* Carbondale: Southern Illinois University Press.

Arnett, R. C. (2012). Biopolitics: An Arendtian communication ethic in the public domain. *Communication and Critical/Cultural Studies*, *9*(2), 225–233.

Arnett, R. C. (1982). Rogers and Buber: Similarities, yet fundamental differences. *The Western Journal of Speech Communication*, *46*, 358–372.

Arnett, R. C. (1981). Toward a phenomenological dialogue. *The Western Journal of Speech Communication*, *45*, 201–212.

Arnett, R. C., Bell McManus, L. M., & McKendree, A. G. (2013). *Conflict between persons: The origins of leadership*. Dubuque, IA: Kendall Hunt Publishing Company.

Arnett, R. C., Fritz, J. M. H., & Bell McManus, L. M. (2018). *Communication ethics literacy: Dialogue and difference*. Los Angeles, CA: Sage Publications. (Original work published in 2009)

Arnett, R. C., Bell, L. M., & Fritz, J. M. H. (2010). Dialogic learning as first principle in communication ethics. *Atlantic Journal of Communication*, *18*(3), 111–126.

Arntfield, M. (2015). Toward a cybervictimology: Cyberbullying, routine activities theory, and the anti-sociality of social media. *Canadian Journal of Communication*, *40*, 371–388.

Arquilla, J., & Ronfeldt, D. (2001). Preface. In John Arquilla and Don Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. v–vi). Santa Monica, CA: RAND Corporation.

Bargh, J. A., & McKenna, K. Y. A. (2004). The Internet and social life. *Annu. Rev. Psychol.*, *55*, 573–590.

Baxter, L. A., & Montgomery, B. M. (1996). *Relating: Dialogues & dialectics*. New York, NY: The Guilford Press.

BBC News. (2019, January 31). Regulate social media to protect children, MPs urge. *BBC News*. Retrieved from https://www.bbc.com/news/technology-47056761

BBC News. (2017, May 13). NHS cyber-attack: GPs and hospitals hit by ransomware. Retrieved from http://www.bbc.com/news/health-39899646

Beck, U. (2013, Aug. 30). The digital freedom risk: too fragile an acknowledgement. *OpenDemocracy*. Retrieved from http://www.opendemocracy.net/can-europe-make-it/ulrich-beck/digital-freedom-risk-too-fragile-acknowledgment

Beck, U. (2006). *Cosmopolitan vision*. (C. Cronin Trans.). Cambridge: Polity Press. (Original work published in 2004)

Beck, U. (1992). From industrial society to the risk society: Questions of survival, social structure and ecological enlightenment. *Theory, Culture & Society*, *9*, 97–123.

Beck, U. (1992). *Risk society: Towards a new modernity* (M. Ritter Trans.). London, Newbury Park, New Delhi: Sage Publications Ltd. (Original work published in 1986)

Beck, U., & Beck-Gernsheim, E. (2002). *Individualization: Institutionalized individualism and its social and political consequences* (P. Camiller, Trans.). Los Angeles, CA: Sage Publications Inc.

Bell, V. (2005). On the critique of secular ethics: An essay with Flannery O'Connor and Hannah Arendt. *Theory, Culture & Society*, *22*(2), 1–27.

Bernard, T. S., Hsu, T., Perlroth, N., & Liber, R. (2017, September 7). Equifax says cyberattack may have affected 143 million in the U.S. *The New York Times*. Retrieved from https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

Biegel, S. (2001). *Beyond our control?: Confronting the limits of our legal system in the age of cyberspace*. Cambridge, MA: The MIT Press.

Blower, L. (2016). It's 'Because I am a woman': Realizing identity to reconstruct identity for the female auto*blog*raphical inquiry. *Convergence: The International Journal of Research into New Media Technologies*, *22*(1), 88–101.

Boler, M. (2007). Hypes, hopes and actualities: New digital Cartesianism and bodies in cyberspace. *New Media & Society*, *9*(1), 139–168.

Brenner, S. W. (2007). "At light speed": Attribution and response to cybercrime/terrorism/warfare. *The Journal of Criminal Law & Criminology*, *97*(2), 379–475.

Brody, N., & Vangelisti, A. L. (2016). Bystander intervention in cyberbullying. *Communication Monographs*, *83*(1), 94–119.

Brookey, R. A., & Cannon, K. L. (2009). Sex lives in Second Life. *Critical Studies in Media Communication*, *26*(2), 145–164.

Brownstein, O. L. (1965). Plato's *Phaedrus*: Dialectic as the genuine art of speaking. *Quarterly Journal of Speech*, *51*(4), 392–399.

Brunskill, D. (2014). The dangers of social media for the psyche. *Journal of Current Issues in Media and Telecommunications*, *6*(4), 391–415.

Bucci, S. (2012). Joining cybercrime and cyberterrorism: A likely scenario. In D. S. Reveron (Ed.), *Cyberspace and National Security* (pp. 57–68). Washington, DC: Georgetown University Press.

Burke, K. (1969). *A grammar of motives.* Berkley: University of California Press. (Original work published in 1945)

Burke, K. (1941). Four master tropes. *The Kenyon Review*, *3*(4), 421–438.

Butler, J. (2015). *Notes toward a performative theory of assembly*. Cambridge, MA: Harvard University Press.

C-SPAN (2016, October 4). Vice presidential debate spilt screen (C-SPAN) (Full Video) [Video File]. Retrieved from https://www.youtube.com/watch?v=RQ91ZqLh26s

C-SPAN (1994, March 29). Information superhighway (C-SPAN) (Full Video) [Video File]. Retrieved from https://www.c-span.org/video/?55624-1/information-superhighway

Calyptix. (2017, November 30). Biggest cyber attacks 2017: How they happened. *Calyptix Security.* Retrieved from https://www.calyptix.com/top-threats/biggest-cyber-attacks-2017-happened/

Carcasson, M., & Sprain, L. (2016). Beyond problem solving: Reconceptualizing the work of public deliberation as deliberative inquiry. *Communication Theory*, *26*(1), 41–63.

Carpio, G. G. (2018). Racial projections: Cyberspace, public space, and the digital divide. *Information, Communication & Society*, *21*(2), 174–190.

Carr, N. (2016). *Utopia is creepy: And other provocations*. New York, NY: W. W. Norton & Company.

Carr, N. (2014). *The glass cage: How our computers are changing us.* New York, NY: W. W. Norton & Company.

Carr, N. (2010). *The shallows: What the Internet is doing to our brains*. New York, NY: W. W. Norton & Company.

Cathcart, R., & Gumpert, G. (1994). Anonymity, presence, and the dialogic self in a technological culture. In R. Anderson, K. N. Cissna, and R. C. Arnett (Eds.), *The Reach of Dialogue: Confirmation, Voice, and Community* (pp. 157–172). Cresskill, NJ: Hampton Press, Inc.

Chayes, A. (2015). Rethinking warfare: The ambiguity of cyber attacks. *Harvard National Security Journal*, *6*, 474–519.

Cingel, D. P., & Olsen, M. K. (2018). Getting over the hump: Examining curvilinear relationships between adolescent self-esteem and Facebook use. *Journal of Broadcasting & Electronic Media*, *62*(2), 215–231.

Cissna, K. N., & Anderson, R. (1994). Communication and the ground of dialogue. In R. Anderson, K. N. Cissna, and R.C. Arnett (Eds.), *The Reach of Dialogue: Confirmation, Voice, and Community* (pp. 9–30). Cresskill, NJ: Hampton Press, Inc.

Clinton, H. R. (2017). *What happened?*. New York, NY: Simon & Schuster.

Colleoni, E., Rozza, A., & Arvidsson, A. (2014). Echo chamber or public sphere? Predicting political orientation and measuring political homophily in Twitter using big data. *Journal of Communication*, *64*, 317–322.

Collin, B. (1997). The future of cyberterrorism. *Crime and Justice International*, *13*(2), 15–18.

Colvin, C., Garrie, D. B., & Rao, S. (2013). Cyber warfare and the corporate environment. *Journal of Law & Cyber Warfare*, *2*(1), 2–24.

Condliffe, J. (2017, September 6). Hackers have the power to switch off American grid systems. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/the-download/608808/hackers-have-the-power-to-switch-off-american-grid-systems/

Constante Martins, R. (2015). The influence of Ulrich Beck's work on social-environmental studies. *Theory, Culture & Society*, *32*(7/8), 342–345.

Conway, M. (2014). Reality check: Assessing the (un)likelihood of cyberterrorism. In T. Chen, L. Jarvis, & S. Macdonald (Eds.), *Cyberterrorism*, (pp. 103–122). New York, NY: Springer.

Coombs, T. W., &. Holladay, S. J. (2018). Social issue qua wicked problems. *Journal of Communication Management*, *22*(1), 79–95.

Crable, B. (2003). Symbolizing motion: Burke's dialectic and rhetoric of the body. *Rhetoric Review*, *22*(2), 121–137.

Crable, B. (2000a). Defending Dramatism as ontological and literal. *Communication Quarterly*, *48*(3), 323–342.

Crable, B. (2000b). Burke's perspective on perspectives: Grounding Dramatism in the representative anecdote. *Quarterly Journal of Speech*, *86*(3), 318–333.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *14*, 13–21.

Crusius, T. W. (1988). Orality in Kenneth Burke's dialectic. *Philosophy and Rhetoric*, *21*(2), 116–130.

Crusius, T. W. (1986). A case for Kenneth Burke's dialectic and rhetoric. *Philosophy and Rhetoric*, *19*(1), 23–36.

Czosseck, C., Ottis, R., & Talihärm, A. (2011). Estonia after the 2007 Cyber attacks: Legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism*, *1*(1), 57–64.

Dahlberg, L. (2001). Computer-mediated communication and the public sphere: A critical analysis. *Journal of Computer-Mediated Communication*, *7*(1). Retrieved from https://authenticate.library.duq.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edselc&AN=edselc.2-52.0-0037537987&site=eds-live

Danidou, Y., & Schafer, B. (2011). 'Trust me, I'm a computer' – Trusted computing and the law between liability and responsibility. *Information & Communications Technology Law*, *20*(3), 185–199.

David Gunkel. (2016). Retrieved from http://gunkelweb.com/

Davisson, A. (2011). Beyond the borders of red and blue states: Google maps as a site of rhetorical invention in the 2008 presidential election. *Rhetoric & Public Affairs*, *14*(1), 101–124.

Dean, M. (1998). Risk, calculable and incalculable. *Soziale Welt*, *49*, 25–42.

Deborah Eicher-Catt. (2018). *Personal home page*. Retrieved from http://www2.york.psu.edu/~dle4/

Deborah Lupton. (2017). *University of Canberra.* Retrieved from https://www.canberra.edu.au/about-uc/faculties/arts-design/courses/communications-staff/lupton-deborah

Deibert, R. (2014, April 17). Interview at the Munk School of Global Affairs, University of Toronto.

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Society*, *4*, 15–32.

Denning, D. E. (2007). A view of cyberterrorism five years later. In K. Himma (Ed.), *Readings in Internet Security: Hacking, Counterhacking, and Society* (pp. 123–140). Boston, MA: Jones and Bartlett Publishers.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In J. Arquilla and D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239–288). Santa Monica, CA: RAND Corporation.

Desmond, W. (1985). Hegel, dialectic, and deconstruction. *Philosophy & Rhetoric*, *18*(4), 244–263.

DiMaggio, P., Hargittai, E., Neuman, W. R., & Robinson, J. P. (2001). Social implications of the Internet. *Annual Review of Sociology*, *27*, 307–336.

Dodge, M., & Kitchin, R. (2001). *Mapping cyberspace*. London, UK: Routledge.

Dorothy Denning. (n. d.). *Profile.* Retrieved from https://theconversation.com/profiles/dorothy-denning-308774.

Eco, U. (2007). *Turning back the clock: Hot wars and media populism* (A. McEwen, Trans.). Orlando, FL: Hartcourt, Inc. (Original work published in 2006)

Eicher-Catt, D. (2013). A semiotic interpretation of authentic civility: Preserving the ineffable for the good of the common. *Communication Quarterly*, *61*(1), 1–17.

Eklund, L. (2011). Doing gender in cyberspace: The performance of gender by female *World of Warcraft* players. *Convergence: The International Journal of Research into New Media Technologies*, *17*(3), 323–342.

Elizabeth Minei. (n. d.). *Biography*. Retrieved from http://www.baruch.cuny.edu/wsas/academics/communication/ElizabethMinei.htm

Ercolini, G. L. (2003). Burke contra Kierkegaard: Kenneth Burke's dialectic via reading Søren Kierkegaard. *Philosophy and Rhetoric*, *36*(3), 207–222.

Fabro, M., & Cornelius, E. (2008). Recommended practice: Creating cyber forensics plans for control systems. *DHS National Cyber Security Division Control Systems Security Program*, *Idaho Falls*, *Idaho 83415*, 1–43.

Federspiel, S. B., & Brincker, B. (2010). Software as risk: Introduction of open standards in the Danish public sector. *The Information Society*, *26*, 38–47.

Felt, M. (2017). New portrayals of cyberbullying as the product of unstable teen technological culture. *Canadian Journal of Communication*, *42*(5), 893–912.

Feng, B., Li, S., & Li, N. (2016). Is a profile worth a thousand words? How online support-seeker's profile features may influence the quality of received support messages. *Communication Research*, *43*(2), 253–276.

Fishman, D. (2004). Reading John Locke in cyberspace: Natural rights and "The Commons" in a digital age. *Free Speech Yearbook*, *41*(1), 34–54.

Flaxman, S., Goel, S., & Rao, J. M. (2016). Filter bubbles, echo chambers, and online news consumption. *Public Opinion Quarterly*, *80*, 298–320.

Foucault, M. (1978). *Discipline and Punish* (A. Sheridan, Trans.). New York, NY: Pantheon Books. (Original work published in 1975)

Frost, C. (2016). The revolution might be tweeted but the founding will not be: Arendt and Innis on time, authority, and appearance. *Canadian Journal of Communication*, *41*(2), 271–286.

Gálik, S. (2015). Influence of the Internet on the cognitive abilities of man: Phenomenological and hermeneutical approach. *Communication Today*, *6*(1), 4–15.

Gearing, A. (2014). Investigative journalism in a socially networked world. *Pacific Journalism Review*, *20*(1), 61–75.

Georgiadou, Y., Puri, S. K., & Sahay, S. (2006). The rainbow metaphor. *International Studies of Management & Organization*, *35*(4), 48–70.

Gerding, J. M., & Vealey, K. P. (2017). When is a solution not a solution? Wicked problems, hybrid solutions, and the rhetoric of civic entrepreneurship. *Journal of Business & Technical Communication*, *31*(3), 290–318.

Gilbert, C. J., & Lucaites, J. L. (2015). Bringing war down to earth: The dialectic of pity and compassion in Doonesbury's view of combat trauma. *Quarterly Journal of Speech*, *101*(2), 379–404.

Gómez, A. G. (2010). Disembodiment and cyberspace: Gendered discourses in female teenagers' personal information disclosure. *Discourse & Society*, *21*(2), 135–160.

Grabosky, P. (2007). Requirements of prosecution services to deal with cyber crime. *Crime Law Soc Change*, *47*, 201–223.

Greenfield, P. (2018, Feb. 25). Social media firms failing to protect young people, survey finds. *The Guardian.* Retrieved from https://www.theguardian.com/society/2018/feb/26/social-media-firms-failing-to-protect-young-people-survey-finds

Grint, K. (2010). The cuckoo clock syndrome: Addicted to command, allergic to leadership. *European Management Journal*, *28*, 306–313.

Gunkel, D. J. (2007). *Thinking otherwise: Philosophy, communication, technology*. West Lafayette, IN: Purdue University Press.

Gunkel, D. J., & Gunkel, A. H. (1997). Virtual geographies: The new worlds of cyberspace. *Critical Studies in Mass Communication*, *14*, 123–137.

Haigh, T., Russell, A. L., & Dutton, W. H. (2015). Histories of the Internet: Introducing a special issue of *Information & Culture*. *Information & Culture*, *50*(2), 143–159.

Halavais, A. (2000). National borders on the World Wide Web. *New Media & Society*, *2*(1), 7–28.

Hammer, D. (2000). Freedom and fatefulness: Augustine, Arendt and the journey of memory. *Theory, Culture & Society*, *17*(2), 83–104.

Han, S. (2016). The legacy of Ulrich Beck in Asia: Introduction. *Theory, Culture & Society*, *33*(7/8), 253–256.

Hartnett, S. J. (2011). Google and the "Twisted Cyber Spy" affair: US-Chinese communication in an age of globalization. *Quarterly Journal of Speech*, *97*(4), 411–434.

Hawisher, G. E., Selfe, C. L., Guo, Y., & Liu, L. (2006). Globalization and agency: Designing and redesigning the literacies of cyberspace. *College English*, *68*(6), 619–636.

Hayat, T., & Samuel-Azran, T. (2017). “You too, Second Screeners?” Second Screeners’ echo chambers during the 2016 U.S. elections primaries. *Journal of Broadcasting & Electronic Media*, *61*(2), 291–308.

Hedley, S. (2003). Nations, markets and other imaginary places: Who makes the law in cyberspace?. *Information & Communication Technology Law*, *12*(3), 215–224.

Heim, M. (1999). The cyberspace dialectic. In P. Lunenfeld (Ed.), *The Digital Dialectic: New Essays on New Media* (pp. 24–45). Cambridge, MA: MIT Press.

Heller, N. (2018, April 12). We may own our data, but Facebook has a duty to protect it. *The New Yorker*. Retrieved from https://www.newyorker.com/tech/annals-of-technology/we-may-own-our-data-but-facebook-has-a-duty-to-protect-it

Heng, Y. (2006). The ‘Transformation of War’ debate: Through the looking glass of Ulrich Beck’s world risk society. *International Relations*, *20*(1), 69–91.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, *4*(2), 49–60.

High, A. C., & Young, R. (2018). Supportive communication from bystanders of cyberbullying: Indirect effects and interactions between source and message characteristics. *Journal of Applied Communication Research*, *46*(1), 28–51.

Hilbert, M., Saifuddin, A., Cho, J., Liu, B., & Luu, J. (2018). Communicating with alogrithms: A transfer entropy analysis of emotions-based escapes from online echo chambers. *Communication Methods and Measures*, *12*(4), 260–275.

Hodgson, G. (2016). Cyber attack treaty verification. *I/S: A Journal of Law and Policy*, *12*(2), 231–260.

Hong, C., & Li, C. (2017). The effect of "anonymous reviewer": A study of anonymity, affect intensity, and message valence in the cyberspace. *Journal of Language and Social Psychology*, *36*(5), 504–524.

House of Lords Publications. (2007). *Personal internet security* (HL Paper 165—I). London: The Stationery Office Limited. Retrieved from http://www.publications.parliament.uk/pa/1d200607/1dselect/1dsctech/165/16502.htm

Hunt, E. L. (1920). Plato on rhetoric and rhetoricians. *Quarterly Journal of Speech*, *6*(3), 33–53.

Irwin, S. O. (2016). Media ecology and the Internet of things. *Explorations in Media Ecology*, *15*(2), 159–171.

Jackson, M. (2009). *Distracted: The erosion of attention and the coming dark age.* Amherst, NY: Prometheus Books.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993.

Janssens, E. (1968). The concept of dialectic in the ancient world. *Philosophy & Rhetoric*, *1*(3), 174–181.

Jiménez, A. G., Orenes, P. B., & Puente, S. N. (2010). An approach to the concept of a virtual border: Identities and communication spaces, *Revista Latina de Comunicación Social*, 65, 214–221.

Jonathan Matusitz. (n. d.). *Biography*. Retrieved from https://communication.ucf.edu/person/jonathan-matusitz/

Jordan, J. W. (2005). A virtual death and a real dilemma: Identity, trust, and community in cyberspace. *Southern Journal of Communication*, *70*(3), 200–218.

Judith Butler. (2018). *Faculty*. Retrieved from https://egs.edu/faculty/judith-butler

Just, N., & Latzer, M. (2017). Governance by algorithms: Reality construction by algorithmic selection on the Internet. *Media Culture & Society*, *39*(2), 238–258.

Kang, Y., & Yang, K. C. C. (2011). The rhetoric of ethnic identity construction among Taiwanese immigrants in the United States. *The Howard Journal of Communications*, *22*, 163–182.

Kaposi, D. (2009). The unbearable lightness of identity: Membership, tradition and the Jewish anti-Semite in Gershom Scholem's letter to Hannah Arendt. *Critical Discourse Studies*, *6*(4), 269–281.

Kelsey, J. T. G. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. *Michigan Law Review*, *108*(7), 1427–1451.

Kellerman, A. (2010). Mobile broadband services and the availability of instant access to cyberspace. *Environment and Planning A, 42*, 2990–3005.

Kharpal, A. (2017, August 17). HBO social media accounts hacked in another cyberattack. *CNBC: Tech*. Retrieved from https://www.cnbc.com/2017/08/17/hbo-social-media-accounts-hacked-in-another-cyberattack.html

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., & Boulton, W. R. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. *Information Systems Management*, *23*(2), 76–87.

Langellier, K. M. (2013). Storytelling, turning points, and wicked problems in performance studies. *Text & Performance Quarterly*, *33*(3), 214–219.

Lash, S. (2018). Introduction: Ulrich Beck: Risk as indeterminate modernity. *Theory, Culture & Society*, *35*(7/8), 117–129.

Lash, S. (2015). Remembering Ulrich Beck. *Theory, Culture & Society*, *32*(7/8), 336–339.

Lechte, J. (2018). Rethinking Arendt's theory of necessity: Humanness as 'way of life', or: the ordinary as extraordinary. *Theory, Culture & Society*, *35*(1), 3–22.

Lenhart, A. (2013, August 21). British teen's suicide puts cyber-bullying back in spotlight. *Pew Research Center*. Retrieved from: http://www.pewresearch.org/fact-tank/2013/08/21/british-teens-suicide-puts-cyber-bullying-back-in-spotlight/

Lichtenbaum, P., & Schneck, M. (2002). The response to cyberattacks: Balancing security and cost. *The International Lawyer*, *36*(1), 39–48.

Lin, Z. (2017). Re-imagined communities in Macau in cyberspace: Resist, reclaim and restructure. *Chinese Journal of Communication*, *10*(3), 229–245.

Lotz, A. D., & Ross, S. M. (2004). Toward ethical cyberspace audience research: Strategies for using the Internet for television audience studies. *Journal of Broadcasting & Electronic Media*, *48*(3), 501–512.

Lupton, D. (2016). Digital risk society. In A. Burgess, A. Alemanno, & J. O. Zinn (Eds.), *Routledge Handbook of Risk Studies* (pp. 301–309). New York, NY: Routledge.

MacDonald, S. H. (2002). Globalization and risk: A contingent response for democratic governance. *Administrative Theory & Praxis*, *24*(1), 31–54.

MacKinnon, L., Bacon, L., Gan, D., Loukas, G., Chadwick, D., & Frangiskatos, D. (2013). Cyber security countermeasures to combat cyber terrorism. In B. Akhgar & S. Yates (Eds.), *Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies* (pp. 234–257). Oxford: Butterworth-Heinemann.

Mahfood, S., Olliges, R., Astuto, A., & Suits, B. (2005). Cyberethics: Social ethics teaching in educational technology programs. *Communication Research Trends*, *24*(4), 3–22.

Maier, C. T. (2016). Education for the love of the world: Hannah Arendt's philosophy of education and communication studies. *Atlantic Journal of Communication*, *24*(5), 289–301.

Maier, C. T., & Crist, J. R. (2017). From 'wicked crisis' to responsive witness: Jean-Luc Marion and the American Roman Catholic sexual-abuse scandal. *Southern Communication Journal*, *82*(3), 164–174.

Manao, N. A., Rahim, A. A., & Taji, H.. (2015). Cyberspace identity theft: The conceptual framework. *Mediterranean Journal of Social Sciences*, *6*(4), 595–605.

Mancini, A. (2002). *Ancient egyptian wisdom for the Internet*. Washington, DC: University Press of America.

Marciano, A. (2014). Living in the VirtuReal: Negotiating transgender identity in cyberspace. *Journal of Computer-Mediated Communication*, *19*, 824–838.

Marletta, D. (2010). Hybrid communities to digital arts festivals: From online discussions to offline gatherings. *At the Interface / Probing the Boundaries*, *69*, 83–96.

Martin Dodge. (2017). *Dr Martin Dodge.* Retrieved from https://www.research.manchester.ac.uk/portal/en/researchers/martin-dodge(35ae33e1-02da-43e0-8fb8-ae8c19e5a041).html

Marx, K. (2013). *Capital*. Ware, Hertfordshire: Wordsworth Editions Limited. (Original work published 1867)

McDonnell, J. (2009). Crossing borders in virtual space. *Media Development*, *4*, 3–7.

McGraw, G. (2013). Cyber war is inevitable (Unless we build security in). *Journal of Strategic Studies*, *36*(1), 109–119.

Menand, L. (2018, June 18). "Why do we care so much about privacy?." *The New Yorker*. Retrieved from https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy

Meyrowitz, J. (1994). The separation of social place from physical place. In R. Anderson, K. N. Cissna, and R. C. Arnett (Eds.), *The Reach of Dialogue: Confirmation, Voice, and Community* (pp. 143–156). Cresskill, NJ: Hampton Press, Inc.

Meyrowitz, J. (1985). *No sense of place: The impact of electronic media on social behavior.* Oxford: Oxford University Press.

Milosevic, T. (2016). Social media companies' cyberbulling policies. *International Journal of Communication*, *10*, 5164–5185.

Minei, E., & Matusitz, J. (2013). Cyberterrorist messages: A semiotic perspective. *Semiotica*, *197*, 267–281.

Mishra, S., & Semann, G. (2010). Islam in cyberspace: South Asian Muslims in America Log In. *Journal of Broadcasting & Electronic Media*, *54*(1), 87–101.

Mitchell Dean. (2019). *Academia.edu.* Retrieved from http://cbs.academia.edu/MitchellDean/

Mitra, B., & Golz, P. (2016). Exploring intrinsic gender identity using Second Life. *Journal of Virtual Worlds Research*, *9*(2), 1–17.

Mullany, L. (2004). ‘Become the man that women desire’: Gender identities and dominant discourses in email advertising language. *Language and Literature*, *13*(4), 291–305.

Murray, J. S. (1988). Disputation, deception, and dialectic: Plato on the true rhetoric (*Phaedrus* 261–266). *Philosophy & Rhetoric*, *21*(4), 279–289.

Murray, J. W. (2002). Kenneth Burke: A dialogue of motives. *Philosophy and Rhetoric*, *35*(1), 22–49.

Mythen, G. (2013). Ulrich Beck, cosmopolitanism and the individualization of religion. *Theory, Culture & Society*, *30*(3), 114–127.

Newman, L. H. (2018, July 9). The worst cybersecurity breaches of 2018 so far. *Wired.* Retrieved from https://www.wired.com/story/2018-worst-hacks-so-far/

Ngai, C. S-B., & Singh, R. G. (2018). Using dialectics to build leader-stakeholder relationships: An exploratory study on relational dialectics in Chinese corporate leaders’ web-based messages. *International Journal of Business Communication*, *55*(1), 3–29.

Nobles, W. S. (1957). The paradox of Plato’s attitude toward rhetoric. *Western Speech*, *21*, 206–211.

O'Hara, L. L. S. (2017). Discursive struggles in "diabetes management": A case study using Baxter's relational dialectics 2.0. *Western Journal of Communication*, *81*(3), 320–340.

O'Reilly, T. (2007). What is Web 2.0: Design patterns and business models for the next generation of software. *Communications & Strategies*, *65*(1), 17–37.

O'Reilly, Tim. (2005, October 1). Web 2.0: Compact definition?. *Radar.* Retrieved from http://radar.oreilly.com/2005/10/web-20-compact-definition.html

Ohlin, J. D. (2017). Did Russian cyber interference in the 2016 election violate international law?. *Texas Law Review*, *95*, 1579–1598.

Ollier-Malaterre, A., Rothbard, N. P., & Berg, J. M. (2013). When worlds collide in cyberspace: How boundary work in online social networks impacts professional relationships. *Academy of Management Review*, *38*(4), 645–669.

Ollove, M. (2016, September 28). Increase in youth suicide prompts states to act. *The Pew Charitable Trusts: Stateline Article*. Retrieved from https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/09/28/increase-in-youth-suicide-prompts-states-to-act

Olson, K. K. (2005). Cyberspace as place and the limits of metaphor. *Convergence*, *11*(1), 10–18.

Osnos, E. (2018, December 19). How much trust can Facebook afford to lose?. *The New Yorker*. Retrieved from https://www.newyorker.com/news/daily-comment/how-much-trust-can-facebook-afford-to-lose

Oswald, M. (2017). Jordan's dilemma: Can large parties still be intimate? Redefining public, private and the misuse of the digital person. *Information & Communications Technology Law*, *26*(1), 6–31.

Pallen, M. (1995). Guide to the Internet: The World Wide Web. *BMJ: British Journal of Medicine*, *311*(7019), 1552–1556.

Papacharissi, Z. (2002). The virtual sphere: The Internet as a public sphere. *New Media & Society*, *4*(1), 9–27.

Pittaro, M. (2007). Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology*, *1*(2), 180–197.

Plato. (1995). *Phaedrus* (A. Nehamas & P. Woodruff, Trans.). Indianapolis, IN: Hackett Publishing Company. (Original work published in Antiquity)

Plato. (1987). *Gorgias* (D. J. Zeyl, Trans.). Indianapolis, IN: Hackett Publishing Company. (Original work published in Antiquity)

Pollitt, M. M. (2018). *People.* Retrieved from https://ischool.syr.edu/people/directories/view/mmpollit/

Pollitt, M. M. (1998). Cyberterrorism: Fact or fancy?. *Computer Fraud & Security*, *2*, 8–10.

Powles, J. (2018, May 25). The G.D.P.R., Europe's new privacy law, and the future of the global data economy." *The New Yorker.* Retrieved from https://www.newyorker.com/tech/annals-of-technology/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy

Primack, A. J., & Johnson, K. A. (2017). Student cyberbullying inside the digital schoolhouse gate: Toward a standard for determining where a "School" is. *First Amendment Studies*, *51*(1), 30–48.

Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community*. New York, NY: Touchstone Books by Simon & Schuster.

Rabinbach, A. (2004). Eichmann in New York: The New York intellectuals and the Hannah Arendt controversy. *October 108*. Retrieved from: https://www.mitpressjournals.org/doi/abs/10.1162/016228704774115735?journalCode=octo

Rafal Rohozinki. (2019). *International Institute for Strategic Studies*. Retrieved from https://www.iiss.org/people/cyber-space-and-future-conflict/rafal-rohozinski

Rahimi, B. (2011). The agonistic social media: Cyberspace in the formation of dissent and consolidation of state power in postelection Iran. *The Communication Review*, *14*, 158–178.

Ralón, L. (2012). "Interview with Michael Heim," Figure/Ground. March 3rd. Retrieved from http://figureground.org/fg/interview-with-michael-heim/

Ramasubramanian, S., Doshi, M. J., & Saleem, M. (2017). Mainstream versus ethnic media: How they shape ethnic pride and self-esteem among ethnic minority audiences. *International Journal of Communication*, *11*, 1879–1899.

Rantanen, T. (2015). Ulrich Beck—A cosmopolitan from Munich. *Global Media & Communication*, *11*(3), 317–321.

Rindner, G. (2017, August 7). The HBO hack: What we know (and what we don't). *Vox*. Retrieved from https://www.vox.com/2017/8/5/16095560/hbo-hack-details-game-of-thrones

Rittell, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, *4*(2), 155–169.

Rob Kitchin. (n. d.). *Prof Rob Kitchin*. Retrieved from https://www.maynoothuniversity.ie/people/rob-kitchin#1

Roberto, A. J., & Eden, J. (2010). Cyberbullying: Aggressive communication in the digital age. In T. A. Avtgis & A. S. Rancer (Eds.), *Arguments, aggression, and conflict: New directions in theory and research* (pp. 198–216). New York, NY: Routledge.

Roberto, A. J., Eden, J., Savage, M. W., Ramos-Salazar, L., & Deiss, D. M. (2014). Prevalence and predictors of cyberbullying perpetration by high school seniors. *Communication Quarterly*, *62*(1), 97–114.

Rogers, R. (2012). Mapping and the politics of web space. *Theory, Culture & Society*, *29*(4/5), 193–219.

Ronald C. Arnett. (2018). *Faculty*. Retrieved from https://duq.edu/academics/faculty/ronald-arnett

Ronald Deibert. (n. d.). Bio. Retrieved from https://deibert.citizenlab.ca/bio/

Rosenzweig, R. (1998). Wizards, bureaucrats, warriors, and hackers: Writing the history of the Internet. *The American Historical Review*, *103*(5), 1530–1552.

Sabine Selchow. (n. d.). *Dr Sabine Selchow*. Retrieved from https://sydney.edu.au/arts/history/staff/profiles/sabine.selchow.php#publications-by-type

Sales, N. A. (2013). Regulating cyber-security. *Northwestern University Law Review*, *107*(4), 1503–1568.

Schiappa, E. (1990). Did Plato coin rhetorike?. *The American Journal of Philology*, *111*(4), 457–470.

Schmidt, A. (2012). At the boundaries of peer production: The organization of Internet security production in the cases of Estonia 2007 and Conficker. *Telecommunications Policy*, *36*, 451–461.

Schraff, R. C., & Dusek, V. (Eds.). (2014). *Philosophy of technology: The technological condition: An anthology* (2nd ed.). Hoboken, NJ: Wiley Blackwell.

Selchow, S. (2016). The paths not (yet) taken: Ulrich Beck, the ‘cosmopolitized world’ and security studies. *Security Dialogue*, *47*(5), 369–385.

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129–136.

Siegel, K. M. (2007). Protecting the most valuable corporate asset: Electronic data, identity theft, personal information, and the role of data security in the information age. *Penn State Law Review*, *111*(3), 779–822.

Simpson, B. (2005). Identity manipulation in cyberspace as a leisure option: Play and the exploration of self. *Information & Communications Technology Law*, *14*(2), 115–131.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176.

Smale, A. (2015, Jan. 4). Ulrich Beck, sociologist who warned of technology, dies at 70. *The New York Times*. Retrieved from https://www.nytimes.com/2015/01/05/world/europe/ulrich-beck-sociologist-who-warned-of-dangers-of-technology-is-dead-at-70.html

Smith, A. (2017a, January 26). Americans and cybersecurity. *Pew Research Center.* Retrieved from http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

Smith, A. (2017b, March 22). What the public knows about cybersecurity. *Pew Research Center.* Retrieved from http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Sporer, K., & Toller, P. W. (2017). Family identity disrupted by mental illness and violence: An application of relational dialectics theory. *Southern Communication Journal*, *82*(2), 85–101.

Stahl, R. (2016). Weaponizing speech. *Quarterly Journal of Speech*, *102*(4), 376–395.

Stefanita, O., Corbu, N., & Buturoiu, R. (2018). Fake news and the third-person effect: They are more influenced than me and you. *Journal of Media Research*, *11*(3(32)), 5–23.

Stefanita, O., Udrea, G., Durach, F., & Corbu, N. (2018). Facebook use among Romanian graduate students: Influences on self-esteem and feelings of loneliness. *Journal of Media Research*, *11*(1(30)), 5–19.

Stephen Herzog. (2018). *People*. Retrieved from https://politicalscience.yale.edu/people/stephen-herzog

Steven P. Bucci. (2018). *The Heritage Foundation Staff.* Retrieved from https://www.heritage.org/staff/steven-bucci

Stohl, M. (2006). Cyberterrorsim: A clear and present danger, the sum of all fears, breaking point or patriot games. *Crime Law Soc Change*, *46*, 223–238.

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication*, *63*(3), 382–412.

Susan W. Brenner. (n. d.). *Directory Home: School of Law Directory. University of Dayton: School of Law*. Retrieved from https://udayton.edu/directory/law/brenner_susan.php

Suter, E. A., & Norwood, K. M. (2017). Critical theorizing in family communication studies: (Re)reading relational dialectics theory 2.0. *Communication Theory*, *27*(3), 290–308.

Tamboukou, M. (2013). Love, narratives, politics: Encounters between Hannah Arendt and Rosa Luxemberg. *Theory, Culture & Society*, *30*(1), 35–56.

Tanrikulu, T., Hüseyin, K., & Aricak, O. T. (2015). Sensibility development program against cyberbullying. *New Media & Society*, *17*(5), 708–719.

Tell, D. (2004). Burke’s encounter with ransom: Rhetoric and epistemology in ‘Four Master Tropes.’ *Rhetoric Society Quarterly*, *34*(4), 33–54.

Thames, R. (2018). Kenneth Burke: Bodies in purposeful motion. In R. C. Arnett, A. M. Holba, & S. Mancino (Eds.), *An Encyclopedia of Communication Ethics: Goods in Contention* (pp. 80–85). New York, NY: Peter Lang Publishing, Inc.

The World Health Report 2008. (2008). Retrieved from http://www.who.int/whr/2008/en/

Thomas, S. (2006). The end of cyberspace and other surprises. *Convergence: The International Journal of Research into New Media Technologies*, *12*(4), 383–391.

Tikk, E. (2011). Ten rules for cyber security. *Survival*, *53*(3), 119–132.

Toma, C. L. (2013). Feeling better but doing worse: Effects of Facebook self-presentation on implicit self-esteem and cognitive task performance. *Media Psychology*, *16*, 199–220.

Totaro, P., & Ninno, D. (2014). The concept of algorithm as an interpretative key of modern rationality. *Theory, Culture & Society*, *31*(4), 29–49.

Tsui, L. (2015). The coming colonization of Hong Kong cyberspace: Government responses to the use of new technologies by the umbrella movement. *Chinese Journal of Communication*, *8*(4), 447–455.

Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other*. New York, NY: Basic Books.

Tynes, B. (2016, August 24). Cyberbullying is a bigger problem than screen time addiction. *The New York Times*. Retrieved from https://www.nytimes.com/roomfordebate/2015/07/16/is-internet-addiction-a-health-threat-for-teenagers/cyberbullying-is-a-bigger-problem-than-screen-time-addiction

Umberto Eco. (n. d.). *Umberto Eco*. Retrieved from http://www.umbertoeco.com

Usher, N., Holcomb, J., & Littman, J. (2018). Twitter makes it worse: Political journalists, gendered echo chambers, and the amplification of gender bias. *The International Journal of Press/Politics*, *23*(3), 324–344.

Van den Bulck, H., & Moe, H. (2018). Public service media, universality and personalisation through algorithms: Mapping strategies and exploring dilemmas. *Media, Culture & Society*, *40*(6), 875–892.

Verweij, M., & Thompson, M. (Eds.). (2006). *Clumsy solutions for a complex world: Governance, politics and plural perceptions*. Houndmills: Palgrave Macmillan.

Vie, S. (2008). Technology as a site of struggle: The interplay of identity, morality, and power in four popular technologies. *Review of Communication*, *8*(2), 130–145.

Vogel, T. A. (2002). Dealing with cyber attacks on corporate network security. *The Practical Lawyer*, *48*, 35–46.

Vogl-Bauer, S. (2014). When disgruntled students go to extremes: The cyberbullying of instructors. *Communication Education*, *63*(4), 429–448.

Walker, K. M. (2007). Proposing a joint enterprise for communication and terrorism studies: An essay on identity formation and expression within the Arab public sphere. *Review of Communication*, *7*(1), 21–36.

Walters, R. (2016, December 2). Cyber attacks on U.S. companies in 2016. *The Heritage Foundation.* Retrieved from https://www.heritage.org/defense/report/cyber-attacks-us-companies-2016

Walther, J. B. (2017). The merger of mass and interpersonal communication via new media: Integrating metaconstructs. *Human Communication Research*, *43*, 559–572.

Walther, J. B. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. *Communication Research*, *23*(1), 3–43.

Walther, J. B. (1993). Impression development in computer-mediated interaction. *Western Journal of Communication*, *57*, 381–398.

Walther, J. B. (1992). Interpersonal effects in computer-mediated interaction: A relational perspective. *Communication Research*, *19*(1), 52–90.

Walther, J. B., Anderson, J. F., & Park, D. W. (1994). Interpersonal effects in computer-mediated interaction. *Communication Research*, *21*(4), 460–487.

Webb, L. (2015). Shame transfigured: Slut-shaming from Rome to cyberspace. *First Monday*, *20*(4).

Weber, R. H. (2011). Politics through social networks and politics by government blocking: Do we need new rules?. *International Journal of Communication*, *5*, 1186–1194.

Weimann, G. (2015). *Terrorism in cyberspace: The next generation*. New York, NY: Columbia University Press.

Weimann, G. (2008). The psychology of mass-mediated terrorism. *American Behavioral Scientist*, *52*(1), 69–86.

Weimann, G. (2006). *Terror on the Internet: The new arena, the new challenges*. Washington, DC: U.S. Institute of Peace Press.

Weimann, G. (2005). Cyberterrorism: The sum of all fears?. *Studies in Conflict & Terrorism*, *28*, 129–149.

Weimann, G. (2004, May 13). Cyberterrorism: How real is the threat?. *United States Institute of Peace Special Report.* Retrieved from https://www.usip.org/publications/2004/05/cyberterrorism-how-real-threat

Wickman, C. (2014). Wicked problems in technical communication. *Journal of Technical Writing & Communication*, *44*(1), 23–42.

Wieviorka, M. (2016). Ulrich Beck: Some ideas for tomorrow. *Theory, Culture & Society*, *33*(7/8), 311–316.

William, L., & Pierson, E. (2003). The rhetoric of hate on the Internet: Hateporn's challenge to modern media ethics. *Journal of Mass Media Ethics*, *18*(3&4), 250–267.

Willis, P. (2016). From humble inquiry to humble intelligence: Confronting wicked problems and augmenting public relations. *Public Relations Review*, *42*(2), 306–313.

Winkler, C. K. (2006). *In the name of terrorism: Presidents on political violence in the post-World War II era*. Albany: State University of New York Press.

Yen, A. C. (2002). Western frontier or feudal society?: Metaphors and perceptions of cyberspace. *Berkeley Technology Law Journal*, *17*, 1207–1264.

Young Lee, E., & Nelson, C. (2018). Can Detroiters dream again? The imagined dialectics of urban declines in Anthony Bourdain's Parts Unknown—Detroit. *Communication Studies*, *69*(4), 421–438.

Young, R., Subramanian, R., Miles, S., Hinnant, A., & Andsager, J. L. (2017). Social representation of cyberbullying and adolescent suicide: A mixed-method analysis of news stories. *Health Communication*, *32*(9), 1082–1092.

Zanini, M., & Edwards, S. J. A. (2001). The networking of terror in the information age. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 29–60). Santa Monica, CA: RAND Corporation.

Zappen, J. P. (2009). Kenneth Burke on dialectical-rhetorical transcendence. *Philosophy and Rhetoric*, *42*(3), 279–301.

Zhang, G., & Jacob, E. K. (2012). Reconceptualizing cyberspace: ‘Real’ places in digital space. *The International Journal of Science in Society*, *3*(2), 91–102.

Zhang, M. (2008). Connecting alumni around the world: A study of harmony, memory, and identity online. *China Media Research*, *4*(4), 85–91.

Zimmerman, H. (2012). Diverging strategies of remembrance in traditional and Web-2.0 on-line projects. *At the Interface / Probing the Boundaries*, *83*, 151–163.

22 U.S.C. (2010). Title 22—Foreign Relations and Intercourse. Retrieved from https://www.gpo.gov/fdsys/pkg/USCODE-2010-title22/html/USCODE-2010-title22.htm