# THREE ESSAYS ON INTERNATIONAL CYBER THREATS: TARGET NATION CHARACTERISTICS, INTERNATIONAL RIVALRY, AND ASYMMETRIC INFORMATION EXCHANGE

by

JACOB A. MAUSLEIN

B.A., Washburn University, 2007
M.A., Kansas State University, 2009

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Security Studies
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2014

# Abstract

As the Internet is progressively integrated into industrial and defense-related networks around the globe, it is becoming increasing important to understand how state and sub-state groups can use Internet vulnerabilities as a conduit of attack. The current social science literature on cyber threats is largely dominated by descriptive, U.S.-centric research. While this scholarship is important, the findings are not generalizable and fail to address the global aspects of network vulnerabilities. As a result, this dissertation employs a unique dataset of cyber threats from around the world, spanning from 1990 to 2011. This dataset allows for three diverse empirical studies to be conducted. The first study investigates the political, social, and economic characteristics that increase the likelihood of a state being targeted for cyber threats. The results show that different state characteristics are likely to influence the forms of digital attack targeting. For example, states that experience increases in GDP per capita and military size are more likely to be targeted for cyber attacks. Inversely, states that experience increases in GDP per capita and those that are more democratic are less likely to be targeted for cyber terrorism. The second study investigates the role that international rivalries play in cyber threat targeting. The results suggest that states in rivalries may have more reason to strengthen their digital security, and rival actors may be cautious about employing serious, threatening forms of cyber activity against foes because of concerns about escalation. The final study, based upon the crisis bargaining theory, seeks to determine if cyber threat targeting decreases private information asymmetry and therefore decreases conflict participation. Empirical results show that the loss of digital information via cyber means may thus illicit a low intensity threat or militarized action by a target state, but it also simultaneously increases the likelihood that a bargain may be researched, preventing full scale war by reducing the amount of private information held between parties.

# THREE ESSAYS ON INTERNATIONAL CYBER THREATS: TARGET NATION CHARACTERISTICS, INTERNATIONAL RIVALRY, AND ASYMMETRIC INFORMATION EXCHANGE

by

JACOB A. MAUSLEIN

B.A., Washburn University, 2007
M.A., Kansas State University, 2009

A DISSERTATION

submitted in partial fulfillment of the requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Security Studies
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2014

Approved by:

Major Professor
Jeffrey Pickering

# Abstract

As the Internet is progressively integrated into industrial and defense-related networks around the globe, it is becoming increasing important to understand how state and sub-state groups can use Internet vulnerabilities as a conduit of attack. The current social science literature on cyber threats is largely dominated by descriptive, U.S.-centric research. While this scholarship is important, the findings are not generalizable and fail to address the global aspects of network vulnerabilities. As a result, this dissertation employs a unique dataset of cyber threats from around the world, spanning from 1990 to 2011. This dataset allows for three diverse empirical studies to be conducted. The first study investigates the political, social, and economic characteristics that increase the likelihood of a state being targeted for cyber threats. The results show that different state characteristics are likely to influence the forms of digital attack targeting. For example, states that experience increases in GDP per capita and military size are more likely to be targeted for cyber attacks. Inversely, states that experience increases in GDP per capita and those that are more democratic are less likely to be targeted for cyber terrorism. The second study investigates the role that international rivalries play in cyber threat targeting. The results suggest that states in rivalries may have more reason to strengthen their digital security, and rival actors may be cautious about employing serious, threatening forms of cyber activity against foes because of concerns about escalation. The final study, based upon the crisis bargaining theory, seeks to determine if cyber threat targeting decreases private information asymmetry and therefore decreases conflict participation. Empirical results show that the loss of digital information via cyber means may thus illicit a low intensity threat or militarized action by a target state, but it also simultaneously increases the likelihood that a bargain may be researched, preventing full scale war by reducing the amount of private information held between parties.

# Table of Contents

List of Figures ... ix

List of Tables ... xii

Acknowledgements ... xiii

Dedication ... xiv

Chapter 1 - Introduction ... 1

Chapter 2 - Estimating the Likelihood of Cyber Threats, 1990-2009 ... 17

  Literature Review ... 18

  Linking Terrorism and Cyber Threats: Theoretical Development ... 24

  Research Design ... 36

    Cyber Dataset ... 36

    Dependent Variable ... 39

    Independent Variables ... 40

      Gross Domestic Product – Per Capita ... 40

      Military Size ... 40

      Regime Type ... 41

      Freedom of the Press ... 41

      International Conflict ... 41

    Methodology ... 42

  Results & Discussion ... 46

    ZINB & Rare Event Logistic Results ... 46

    Discussion ... 53

  Conclusion ... 57

Chapter 3 - International Rivalry and Cyber Attacks ... 61

  Literature Review ... 62

  Theoretical Development ... 67

  Research Design ... 74

    Dependent Variable ... 76

    Independent Variables ... 77

    Control Variables ... 79

GPD Per Capita ........ 80
Military Size ........ 81
Regime Type ........ 82
Population ........ 84
Geography ........ 85
Media Bias ........ 86
Methodology ........ 86
Results ........ 89
Discussion ........ 96
Conclusion ........ 100
Chapter 4 - The Impact of Cyber Espionage on International Crisis Bargaining ........ 103
Information and War ........ 104
Cyber Attacks and Information Exposure ........ 112
Research Design ........ 118
Dependent Variables ........ 118
Independent Variables ........ 120
Control Variables ........ 122
Regime Type ........ 122
Contiguity ........ 123
Military Capabilities ........ 124
Alliances ........ 124
Intergovernmental Organization Participation ........ 125
Economic Interdependence ........ 125
Prior Military Activity ........ 126
Media Bias ........ 126
Methodology ........ 126
Results ........ 129
Analysis ........ 135
Conclusion ........ 137
Chapter 5 - Conclusion ........ 140
References ........ 148

Appendix A - Chapter 2 Tables and Graphs ..... 163
Appendix B - Chapter 3 Tables and Graphs ..... 178
Appendix C - Chapter 4 Tables and Graphs ..... 183

# List of Figures

Figure A.1 Model 1 – GDP Per Capita: Global Averages........ 164
Figure A.2 Model 1 – GDP Per Capita: U.S. Averages........ 165
Figure A.3 Model 2 – GDP Per Capita: Global Averages........ 165
Figure A.4 Model 2 – GDP Per Capita: U.S. Averages........ 165
Figure A.5 Model 3 – GDP Per Capita: Global Averages........ 166
Figure A.6 Model 3 – GDP Per Capita: U.S. Averages........ 166
Figure A.7 Model 4 – GDP Per Capita: Global Averages........ 166
Figure A.8 Model 4 – GDP Per Capita: U.S. Averages........ 167
Figure A.9 Model 1 – Military Size: Global Averages........ 167
Figure A.10 Model 1 – Military Size: U.S. Averages ........ 167
Figure A.11 Model 2 – Military Size: Global Averages........ 168
Figure A.12 Model 2 – Military Size: U.S. Averages ........ 168
Figure A.13 Model 3 – Military Size: Global Averages........ 168
Figure A.14 Model 3 – Military Size: U.S. Averages ........ 169
Figure A.15 Model 4 – Military Size: Global Averages........ 169
Figure A.16 Model 4 – Military Size: U.S. Averages ........ 169
Figure A.17 Model 1 – Polity: Global Averages ........ 170
Figure A.18 Model 1 – Polity: U.S. Averages........ 170
Figure A.19 Model 2 – Polity: Global Averages ........ 170
Figure A.20 Model 2 – Polity: U.S. Averages........ 171
Figure A.21 Model 3 – Polity: Global Averages ........ 171
Figure A.22 Model 3 – Polity: U.S. Averages........ 171
Figure A.23 Model 4 – Polity: Global Averages ........ 172
Figure A.24 Model 4 – Polity: U.S. Averages........ 172
Figure A.25 Model 1 – Freedom of Speech: Global Averages........ 172
Figure A.26 Model 1 – Freedom of Speech: U.S. Averages ........ 173
Figure A.27 Model 2 – Freedom of Speech: Global Averages........ 173
Figure A.28 Model 2 – Freedom of Speech: U.S. Averages ........ 173
Figure A.29 Model 3 – Freedom of Speech: Global Averages........ 174

Figure A.30 Model 3 – Freedom of Speech: U.S. Averages .................................................... 174

Figure A.31 Model 4 – Freedom of Speech: Global Averages................................................. 174

Figure A.32 Model 4 – Freedom of Speech: U.S. Averages .................................................... 175

Figure A.33 Model 1 – Interstate Conflict: Global Averages................................................... 175

Figure A.34 Model 1 – Interstate Conflict: U.S. Averages ...................................................... 175

Figure A.35 Model 2 – Interstate Conflict: Global Averages................................................... 176

Figure A.36 Model 2 – Interstate Conflict: U.S. Averages ...................................................... 176

Figure A.37 Model 3 – Interstate Conflict: Global Averages................................................... 176

Figure A.38 Model 3 – Interstate Conflict: U.S. Averages ...................................................... 177

Figure A.39 Model 4 – Interstate Conflict: Global Averages................................................... 177

Figure A.40 Model 4 – Interstate Conflict: U.S. Averages ...................................................... 177

Figure B.1 Model 1 – Enduring Rivalry Dummy 1990-2001: Global Averages........................ 179

Figure B.2 Model 1 – Enduring Rivalry Dummy 1990-2001: U.S. Averages .......................... 180

Figure B.3 Model 2 – Strategic Rivalry Dummy 1990-2001: Global Averages ........................ 180

Figure B.4 Model 2 – Strategic Rivalry Dummy 1990-2001: U.S. Averages ........................... 180

Figure B.5 Model 3 – Enduring Rivalry Count 1990-2001: Global Averages.......................... 181

Figure B.6 Model 3 – Enduring Rivalry Count 1990-2001: U.S. Averages.............................. 181

Figure B.7 Model 4 – Strategic Rivalry Count 1990-2001: Global Averages........................... 181

Figure B.8 Model 4 – Strategic Rivalry Count 1990-2001: U.S. Averages .............................. 182

Figure B.9 Model 5 – Strategic Rivalry Count 1990-2009: Global Averages........................... 182

Figure B.10 Model 5 – Strategic Rivalry Count 1990-2009: U.S. Averages ............................ 182

Figure C.1 Model 1 – Interstate Wars (COW): Global Averages.............................................. 185

Figure C.2 Model 1 – Interstate Wars (COW): U.S. Averages ................................................. 185

Figure C.3 Model 2 – Interstate Wars (COW): Global Averages.............................................. 185

Figure C.4 Model 2 – Interstate Wars (COW): U.S. Averages ................................................. 186

Figure C.5 Model 3 – Interstate Wars (PRIO): Global Averages.............................................. 186

Figure C.6 Model 3 – Interstate Wars (PRIO): U.S. Averages.................................................. 186

Figure C.7 Model 4 – Interstate Wars (PRIO): Global Averages.............................................. 187

Figure C.8 Model 4 – Interstate Wars (PRIO): U.S. Averages.................................................. 187

Figure C.9 Model 5 – Interstate Wars (MIDs): Global Averages.............................................. 187

Figure C.10 Model 5 – Interstate Wars (MIDs): U.S. Averages ............................................... 188

Figure C.11 Model 6 – Interstate Wars (MIDs): Global Averages............................................ 188

Figure C.12 Model 6 – Interstate Wars (MIDs): U.S. Averages ................................................ 188

# List of Tables

Table 2.1 Summary Statistics ........ 43
Table 2.2 Zero-Inflated Negative Binomial & Rare-Event Logit Results ........ 48
Table 3.1 Summary Statistics ........ 87
Table 3.2 ZINB Dichotomous Estimates of Cyber Attack Event Counts ........ 90
Table 3.3 ZINB Count Estimates of Cyber Attacks ........ 91
Table 4.1 Summary Statistics ........ 127
Table 4.2 Correlates of War (COW) & PRIO Interstate War Rare-Event Logistic Results ....... 130
Table 4.3 Militarized Interstate Dispute (MID) Zero-Inflated Negative Binomial Results ....... 131
Table A.1 Fixed Effects Logit and Rare Event Logit Comparison ........ 163
Table A.2 Fixed Effects Results ........ 164
Table B.1 Fixed Effects Estimates of Cyber Attack Event Counts (Binary) ........ 178
Table B.2 Fixed Effects Estimates of Cyber Attack Event Counts (Count) ........ 179
Table C.1 Correlates of War (COW) & PRIO Interstate War Fixed Effects Results ........ 183
Table C.2 Militarized Interstate Dispute (MID) Fixed Effects Results ........ 184

# Acknowledgements

I would like to express my sincere gratitude to the committee members who helped guide this dissertation. In particular, I thank Dr. Jeff Pickering for helping me improve the focus of this research and providing me with countless comments and suggestions. I also thank him for always making time to work with me, despite his exceptionally busy schedule. To Dr. Craig Stapley, I thank you for many years of guidance and for providing me with an understanding of physical terrorism, which ultimately became one of the primary theoretical frameworks of this research. To Dr. Sabri Ciftci, thank you very much for taking the time to teach me the various empirical methods that made the study of this unique research topic possible. And to Dr. Michael Krysko, thank you for always challenging me and pushing me to think about this research in unique and innovative ways. I would also like to thank Dr. Amanda Murdie, who was kind enough to help guide me during the earliest days of this dissertation, and Dr. Joe Aistrup, who pushed me to explore research topics outside of political science and for giving me the opportunity to learn ArcGIS.

In addition, I want to thank my countless family, friends, and colleagues who have been a source of support and inspiration. While I am indebted to far too many people to list, I wish to personally acknowledge three of these individuals. To Dr. Stephen Nemeth, thank you for your friendship and guidance. To Dr. Jerome Sibayan, thank you for your help and overwhelming generosity. And to Dr. Tom Gould, thank you for the many opportunities you have given me since my earliest days at Kansas State University.

# Dedication

This work is dedicated to my unbelievably patient wife, Stephanie, and our beautiful daughter, Elloise. Stephanie is my best friend, as well as a constant source of support and encouragement. I could not have been blessed with a better partner, and this project would never have been a success without her. I would also like to dedicate this dissertation to my parents – Biff and Barb – both of whom instilled the importance of education into their sons.

# Chapter 1 - Introduction

During the early morning hours of September 6, 2007, a squadron of Israeli F-15s and F-16s departed from Ramat David Airbase in northern Israel. The objective of the mission was to destroy a suspected nuclear reactor site at Dayr ez-Zor in Northern Syria. Despite the technological supremacy of Israeli aircraft, Syrian radar was still capable of tracking potential enemies, giving the Syrian military time to organize its defense. In order to ensure the success of the mission, and increase the chances of all aircraft returning to Israeli airspace, both Syrian regional and national radar detection systems would need to be eliminated. To accomplish this feat, and with an expectation that such a mission would eventually be conducted, Israeli-paid contractors had previously been employed to covertly install unique software and hardware in the Syrian radar defense network. These seemingly harmless components, given a moment's notice, could be remotely activated by Israeli forces and effectively disable the radar system. On September 6, the tactic worked perfectly. By activating the software and hardware components, Israeli technicians hundreds of miles away were able to manipulate the radar and prevent the system from detecting the approaching aircraft. Israeli forces were then able to fly into Syrian airspace undetected, destroy the target, and return home without incident. This example demonstrates just one instance of the Internet, and networked technology, being adapted as a weapon of conflict between states (Handler 2012; Rid 2013).

Despite its humble beginnings, the Internet and World Wide Web have been adapted and adopted by states across the globe for a plethora of positive functions. This technology, much like the telegraph and radio before it, provides individuals with a means of communication and sharing ideas across broad geographic locations. In addition, the expansion of computing power and networked technologies has provided industries with the ability to automate many of the vital systems and social services we take for granted. For example, no longer do we see a lone police officer in the middle of a busy intersection directing traffic. This job was long ago replaced by automated traffic signals. In much the same vein, engineers have designed ever-more complex and "smart" electric grids integrated with computing and networked technologies. Computers can now predict and divert increased levels of electricity to locations in need, while at the same time maximizing efficiency at the plants responsible for generating that power (see Sioshansi 2011).

While there are a host of benefits and advantages associated with networked technology, Internet connectivity has also produced a wide variety of unintended consequences. At the extreme end of the spectrum, there are those actors that seek to employ the Internet as a weapon or as a means of accessing private information that would otherwise be impossible without a physical presence. These actors include nation-states, terrorist organizations, corporations, as well as private citizens. Such actors have used the Internet to conduct a wide variety of malevolent activities, such as pilfering sensitive documents related to the F-35 fighter project from Lockheed Martin, or using highly specific computer code to target centrifuges within the Iranian nuclear program. Thus, because of its widespread integration throughout much of the industrialized world, and notwithstanding its many benefits, the Internet could potentially be seen as a serious security vulnerability for militaries, corporations, and private citizens. This was a harsh reality the Syrian government and military learned in September 2007, and it is a reality that many states around the globe are learning within increasing regularity.

Despite the fact that the Internet has become a revolutionary tool of communication, and networked technology has been adopted by states across the globe, there are still a wide variety of questions yet to be answered regarding its role as a tool of foreign policy and conflict. This dissertation will thus offer an initial analysis of the use of the Internet by states, sub-state groups, and individuals for malicious purposes. In particular, this research will fill gaps in the current social science literature by examining the characteristics of states targeted for digital cyber threats, how participation in international rivalries impacts the prospect of being a target, and how cyber espionage can influence asymmetric information exchange and conflict participation. Theoretical foundations will be borrowed from current international relations research on terrorist targeting, interstate rivalries, and crisis bargaining. Such an approach is necessary, given the paucity of systematic studies on cyber threats. Additionally, these questions will be explored through the use of thorough empirical tests, in an effort to propel the current study of cyber threats beyond a descriptive approach. The dataset employed for this task is revolutionary in the study of cyber threats, and was built specifically to test a broad range of research questions like those posed in this dissertation. Finally, the ultimate goal of this research is to provide insight into some of the ways in which a revolutionary form of communication has become a security vulnerability for the many states that now use it for a host of vital functions.

Historians of technology, in particular, offer valuable insight on the way that new innovations such as the Internet develop new roles and purposes beyond those originally conceived (Bimber 1994; Kelly 2010; Naimi and French 2010; Nye 2006). David Nye (2006), for example, points out that, "deterministic conceptions of technology seem misguided when one looks closely at the invention, the development, and the marketing of individual devices" (31). Nye (2006) goes on to note, "even if one can predict which new technologies are possible and forecast which designs will thrive in the market, people may fail to foresee how they will be used" (44). The history of the Internet, which was conceived as a means of communication and research but has also been adapted into a major vulnerability and conduit for attack, most certainly exhibits the unpredictability of technology.

Communications technology has a long history of being unpredictable and having unintended impacts on interstate relations (Headrick 1991). A series of communications technology have been trumpeted as means to tie peoples more closely together and enhance prospects of world peace.[1] However, as Headrick shows, they are often quickly adapted by nations as a means of strengthening control over foreign territory and inflicting injury on their opponents. For example, the invention of the telegraph and the laying of cable around the world spurred a host of agreements between states to ensure transmission lines could cross international borders. Eventually, however, London's control over the bulk of these cables allowed the British empire to spread into parts of the world that were previously inaccessible or ungovernable by competing European powers.[2] In addition to integrating the telegraph as a military asset, the English used their strong monopoly on undersea cables as a foreign policy tool, as they would

[1] For example, during the 19th century, French diplomat and Suez Canal developer Ferdinand de Lesseps postulated that "men, by knowing one another, will finally cease fighting" (Headrick 1991, 274).

[2] This was demonstrated during the Indian rebellion of 1857, when the English faced a large and well-armed militia seeking to drive the European power out the Asian subcontinent. Despite the militia's robust membership, the Indians were hampered with poor and disorganized communication. The British, having established a stout Indian telegraph service consisting of over 7,000km of telegraph cable and 46 telegraph offices, were able to coordinate with military planners in southern India as well as in Britain itself regarding how to subdue the uprising. The British military incorporated telegraph technology to the point that new telegraph stations were established as the English army moved north and towards victory (Headrick 1991). According to Colonial Patrick Stewart, who accompanied British commander-in-chief General Colin Campbell during the Indian rebellion, British military telegraphers were able "to put the end of the telegraph wire in Sir Colin's hand wherever he went. No sooner were headquarters established at any spot, than the post and the wire were established also. It was the first time that the telegraph had been made to keep pace with the advance of an army in the field" (Headrick 1991, 52).

regularly spy on unencrypted transmissions of competing powers sent through British-owned lines.

The British domination of undersea cables and their effective use in military campaigns spurred other European powers, particularly France and Germany, to develop competing cable systems and rely on them more and more for private communication. Given that the early 20th century was an atmosphere of continental and international tension, the rapid adoption of communication systems like the telegraph and radio also began to expose the technologies' weaknesses. For example, German submarine warfare during World War I demonstrated that transatlantic telegraph cables could easily be cut, disrupting communication between continents and armies. Additionally, the rapid expansion of telegraph services led to the establishment of communication intelligence agencies. These agencies were responsible for intercepting and deciphering the private information of rival telegraphs and transmissions.

This need to control, and at times disrupt, the flow of communication and pilfer the confidential information transmitted through it would do little to ease tensions prior to World War I and World War II and played a major role in the conduct of these wars (Headrick 1991; Winkler 2008). Ultimately concerning the development and adoption of instantaneous transcontinental communications, Headrick (1991) observes, "international cooperation preceded international disagreements" (12). In other words, the adoption of communication technology like the telegraph required substantial agreement among states, however it also allowed for larger empires and more stable trade networks capable of enhancing military war machines. Thus, as suspicions and tensions grew, communications also contributed to international insecurity with the rise of targeted electronic communication disruption, sophisticated electronic espionage, and intelligence agencies (Headrick 1991).

Ironically, the British domination of telegraph cables, the vulnerability of transatlantic cables to submarine attack, and the active espionage being conducted by numerous European powers would also stir the United States to develop its own communication network. As Winkler (2008) points out, the United States had, "a desire to realign world communications in ways that would minimize Great Britain's predominant position, move the United States from the periphery to the center of the global cable and radio network, and apply the benefits of this transformation to the nation's standing and influence in the world" (4). As a result, World War I found the United States investing heavily into researching new formats of communication, including telephone, shortwave radio, and even satellites, that would be less susceptible to the weaknesses of conventional telegraph cables.[3] These innovations were meant to provide the United States with secure forms of communication that could be built and maintained by U.S. corporations, thus alleviating dependence on other states.

The interwar period in the United States found military planners building upon their early advancements in radio. As Millett (1996) observes, "the strategic uncertainty of the interwar period influenced development of radio communications security systems as well as the exploitation of radio beams (radar) for navigation and target acquisition" (341). World War I had demonstrated that the speed and security of communication were vital to success, and radio provided such attributes. During the Second World War, these radio resources proved to be an integral component of both Allied and Axis armies. However, despite advances in security and encryption, radio transmissions became vulnerable to enemy interception and jamming. This fear of espionage and a loss of communication would appear again shortly after the end of World

[3] The creation of the Radio Corporation of America (RCA) was a direct result of the US Navy's desire to ensure that America's international radio connections remained under U.S. control.

War II. In particular, the Cold War found the Soviet Union actively jamming Western radio transmissions. Thus, much like the telegraph, reliance on radio communications for strategic priorities carried both rewards and risks. Foes found ways to exploit technological weaknesses and hamper transmissions. Jamming, coupled with a fear of Communist espionage and nuclear attack, forced the United States to continue to build upon its earlier advances in communication technology. This ultimately led to sophisticated projects such as the ARPANET, a precursor to the Internet (Winkler 2008).

Much like the communication systems of the early 20th century, contemporary states are adopting the Internet as a foreign policy tool. The trajectory and exploitable weaknesses of this digital network were perhaps less well understood by its original developers than pioneers of telegraph and radio communications. The agency responsible for creating the Internet's predecessor was the consequence of another revolutionary piece of technology: satellite orbiters. On October 4, 1957, the Soviet Union launched Sputnik, the first manmade satellite to orbit the Earth. As a result of the Soviet's technological prowess, U.S. President Dwight D. Eisenhower mandated that the Pentagon ensure the United States catch up to the Soviet Union, and eventually surpass its defense-related technological innovation. As a result of DoD Directive 5105.15, the Advanced Research Projects Agency (ARPA) was created in February 1958. The agency's original mission was to prevent technological surprises, and support America's burgeoning space program (Ceruzzi 2008). Because of the exceptional amount of data being generated as a result of America's new space program, coupled with the wide geographic distribution of NASA's contractors, researchers began to postulate the feasibility of computers that could not only share data but also "talk" to each other. The new network would also serve a subsidiary purpose, similar in nature to the British telegraph system 60 years prior. The United

States wanted a reliable, robust system of communication that could be relied upon in the event of conflict with the Soviet Union.

The networking of computers was first discussed in a series of memos by MIT Professor and ARPA Computer Research Director J.C.R. Licklider in 1962. Licklider envisioned a "Galactic Network," or "a globally interconnected set of computers through which everyone could quickly access data and programs from any site" (Leiner et al. 1999). During the same time period, MIT PhD candidate Leonard Kleinrock was finishing his dissertation on packet switching. The idea of packet switching was revolutionary, since up to that point data transfers were routed directly from terminal to terminal via circuits. Packet switching allows data to be divided into segments, transmitted individually until they reach their destination, and then reassembled into the original message or data. While the dividing of data into packets was novel, it was the idea that the individual segments could be sent via different routes to their final destination that made researchers take notice of the theory. Combined, the concept of a "Galactic Network," and the ability to send data via packet switching would become the backbone of a truly revolutionary means of data and research sharing (Leiner et al. 1999). By 1969, Licklider's successor, Lawrence G. Roberts, had refined both the structure and specifications of the new network, dubbed the ARPANET. Later that year, "four host computers were connected together into the initial ARPANET, and the budding Internet was off the ground" (Leiner et al. 1999).

Throughout the 1970s and early-1980s, the ARPANET continued to grow through a barrage of new innovations. One of the earliest such innovations was email, which allowed the

Internet to become a forum for the immediate open exchange of ideas.[4] Email was quickly joined by the creation of the File Transfer Protocol (FTP), graphical user interface (GUI), and the point and click mouse. In addition to these new innovations, ARPA researchers began postulating various means of connecting the ARPANET to other networks. This project, dubbed the "Internet Program," was tasked with the creation of a worldwide network of networks. In 1976, ARPA staff successfully connected the ARPANET to other similar networks through the use of transmission control protocol/internet protocol (TCP/IP). This basic idea of connecting individual networks together without reconfiguring each network, and sans a centralized hub, is the basis of the modern-day Internet (Abbate 2000). The Internet evolved beyond its military foundation with ARPANET by the late 1980s, however. ARPANET had been stripped of much of its military research funding in the 1980s, and larger academic networks such as NSFNet had developed, and they would eventually become the backbone of Internet connectivity.

The transition of the Internet from a military project into a publicly-accessible tool was made possible as a result of several innovations. The first was the gradual integration of networking components and TCP/IP settings into personal computers throughout the 1980s and

[4] Ironically the Internet, which was designed as a means of quickly and efficiently sharing data, was initially standardized in the late 1960s and early 1970s by hand-typed letters. The standardization of the ARPANET was a result of the establishment of the Request for Comments (RFC) notes. These notes were originally exchanged by university researchers via the U.S. Postal Service (USPS) and were, "intended to be an informal, fast distribution way to share ideas with other network researchers" (Leiner et al. 1999). As it turns out, these RFC notes may have been among first loss of business the USPS suffered as a result of email. As noted by (Leiner et al. 1999), "Email has been a significant factor in all areas of the Internet, and that is certainly true in the development of protocol specifications, technical standards, and Internet engineering. The very early RCSs often presented a set of ideas developed by the researchers at one location to the rest of the community. After email came into use, the authorship pattern changed – RFCs were presented by joint authors with common view independent of their locations."

early 1990s.[5] Second, Tim Berners-Lee developed Hypertext Transfer protocol (HTTP) as well as the first web browser, named *World Wide Web*.[6] More popular browsers, namely *Mosaic* and *Netscape*, would follow and ultimately gave consumers the ability to search the Web from the comforts of their own homes. Abbate (2000) notes of web browsers, they "completed the Internet's transformation from a research tool to a popular medium by providing an application attractive enough to draw the masses of potential Internet users into active participation" (217). Ultimately, because of HTTP and the web browser, coupled with the ability of consumers to access these resources via their home computers, the decentralized and user-driven World Wide Web we know today largely came into being.

[5] Interestingly, Abbate (2000) notes that TCP/IP protocols were never mandated as an official specification of networking technology. Instead, it had become the de facto standard promoted by the U.S. government, as well as research groups in the United States and Europe. The protocol eventually became widespread through adoption by computer manufacturers, and became the de factor protocol around the world. The QWERTY typewriter keyboard followed a similar path in its widespread, global adoption.

[6] Berners-Lee was heavily influenced by authors of the computer counterculture during the 1960s and 1970s. Most notable of these authors was Ted Nelson, who called on ordinary people to learn computer technology. Seeking to "democratize" the Internet and information sharing, Nelson postulated that information should be linked together, as opposed to the conventional way of presenting information: linearly. Berners-Lee's adapted Nelson's theory and developed what is known as hypertext, or HTTP, which effectively linked pieces of information such as text, images, audio, and video on computers around the world (Abbate 2000). Because Berners-Lee's HTTP standard was built upon TCP/IP settings, which were a component in most personal computers, HTTP and web browsers gave ordinary users a means of easily accessing public information across the globe. Despite its many advantages, this innovation spurred a variety of unintended consequences. One such consequence of global information sharing, and the adoption of personal computers and Internet technology, is the rise of harmful activity such as contemporary cyber attacks, cyber terrorism, and cyber espionage.

The Internet and the "World Wide Web" thus developed in an often unforeseen and unpredictable manner.[7] There can be little doubt, however, that both concepts were founded upon an initial desire to share research and information in a peaceful, open atmosphere. According to Denning (1989), "most [early] users thought of the network as a way of communicating with colleagues, and a tool supporting collaboration" (531). In many regards, the purpose behind the Internet mirrored that of the telegraph and radio: safe, reliable communication. The notion expressed by Denning was also noted by Berners-Lee. When asked what he had in mind when he first developed the Web, he replied, "The dream behind the Web is of a common information space in which we communicate by sharing information. ...once the state of our interactions was on line, we could then use computers to help us analyze it, make sense of what we are doing, where we individually fit in, and how we can better work together" (Berners-Lee 1998). These were lofty goals, but they are becoming realized through the rapid spread of the Internet into the daily lives of countless billions around the world.

Despite the peaceful intentions of those who invented the Internet, the warning of historians of technology (Kelly 2010; Naimi and French 2010) regarding the negative and unpredictable aspects of technology apply equally to the present case.[8] And in a manner similar

[7] One of the most unique aspects of the Internet is the fact that it is an exceptionally user-generated and user-shaped entity. Abbate (2000) astutely notes that, "much of the Internet's success can be attributed to its users' ability to shape the network to meet their own objectives" (5).

[8] Despite the hope for "a better world to come," some historians of technology are less idealistic in detailing the unintended consequences of innovation. For example, Naimi and French (2010) point out that we should not be surprised when technologies are molded for purposes beyond their original intent. Citing Newtonian physics, they posit, "Technological innovation brings both new opportunities and new problems. And inevitably, adoption of technological innovations leads to adaption and uses not envisioned by the inventor. For every intended consequence, there will be an opposite and equal unintended consequence" (Naimi and French 2010, 4). Further, as Kelly (2010, 246) observes, "there are no technologies without vices and none that are neutral. There is no

to the telegraph and radio preceding it, the Internet suffers from a variety of weaknesses that states, as well as private users, are willing to exploit. These weaknesses exist both as a result of technical oversight, as well as the Internet's rapid adoption and adaption by states around the globe. Much of the Internet developed with little regard for digital security, or certainly less regard than exists today. A basic component of Internet connectivity, TCP/IP, for example, evolved into "a principal vulnerability that hackers use…to gain root access to a computer" (Garber 2000, 15). Additionally, the decentralized nature of the Internet allows users to remain largely anonymous, thereby lowering the risk of being caught.[9] Coupled with these physical attributes are the vulnerabilities inherent in the software designed to access the Web. Martin, Graham and Caines (2011) point out that, "weaknesses in operating systems, network operating systems, default configuration of network devices and firewalls, encryption, and poorly written applications" lay behind many digital vulnerabilities (10). A recent example of a weakness in coding was the Heart Bleed bug, which left the passwords of millions of Internet users vulnerable (Worthington 2014).

In conjunction with its physical and software attributes, the Internet provides a lucrative conduit through which to attack because of its complex integration into private industrial functions and national security networks in advanced states. Networked technology has been incorporated by private firms to help increase the efficiency of mass transit systems, power grids, nuclear facilities, air traffic control systems, water and sewer systems, and a number of other crucial components of infrastructure. As noted in the introductory example, governments have

powerfully constructive technology that is not also powerfully destructive in another direction, just as there is no great idea that cannot be greatly perverted for great harm."

[9] Because of its somewhat anarchic structure, the Internet, "has been a difficult place for policymakers seeking to enforce the laws of the real world" (Chharia 2013, 30).

infused Internet technology into services that aid national security, such as radar and communication systems. Unfortunately, integration by both groups has opened these systems up to covert access and thus makes them potential targets of state and sub-state groups. This provides a security vulnerability that could potentially impact relations between states, an issue that has yet to be thoroughly investigated with empirical analysis.

The study of the Internet as a conduit of attack and espionage, despite its benefits as a forum of free expression and information sharing, is an exceptionally important matter. The urgency in studying the Internet as a security threat is captured by Brenner (2009), who points out that, "If the chaos evolving in the cyberworld stayed in that virtual environment, we would have little or no reason to be concerned. Unfortunately, what happens in the cyberworld does not stay in the cyberworld; it migrates out into our world because cyberspace is not a true externality. It is simply a vector for human activity, both good and bad" (8). Thus, thanks to the Internet, what happens in Vegas is no longer guaranteed to stay in Vegas. While scholars continue to try to keep up by developing systematic knowledge on many phenomena associated with the Internet, there remain a wide variety of issues yet to be addressed. This dissertation is driven by the fact that researchers in the social sciences have largely overlooked how events on the Internet, and the exploitation of the Internet's weaknesses by a variety of groups, can impact the relations between states.[10]

In order to remedy this oversight, this dissertation investigates three basic, yet fundamental questions related to the Internet, its weaknesses, and its use as a conduit of attack and espionage. Because of the contemporary nature of this subject, coupled with the fact that

[10] This approach to studying communication was also adapted by Headrick (1991) in his study on telecommunications from 1851 to 1945.

social scientists have yet to rigorously investigate Internet vulnerabilities, the following three chapters will borrow from three diverse theoretical frameworks in the international relations literature. In particular, Chapter 2 focuses on a very basic, yet instrumental question in broadening our understanding of cyber threats: what state-based characteristics are most likely to increase the likelihood of being attacked via digital means. This research question allows scholars to generalize about the role of political, social, and economic factors in cyber threat targeting, and to forecast where attacks may be launched in the future. Because of the similarities in tactics between terrorist organizations and state- and sub-state hackers, the terrorism targeting literature will be used as a surrogate theoretical framework. In terms of the dissertation, this chapter also provides operationalizations of the different types of cyber threats studied throughout the empirical chapters, and an introduction to the dataset as well.

Chapter 3 relies upon the interstate rivalry literature in an effort to better understand the relationship between contentious relationships and the use of cyber attacks. More specifically, a relatively new line of research has emerged that suggests that interstate rivalries promote the use of low-intensity forms of conflict. These low-intensity forms of violence include terrorism, guerrilla combat, and perhaps even cyber threats. A recent descriptive study produced by Valeriano and Maness (2014), however, finds that rivalries are likely to reduce the use of cyber threats between states, given that they may lead to more destructive forms of combat. Chapter 3 will test this proposition with cross sectional, time-series empirical data to determine if states engaged in interstate rivalries are more likely to be attacked via the Internet.

Chapter 4 borrows from the crisis bargaining literature to study whether the loss of private, digital information influences the decisions of states to engage in armed conflict. This chapter is based upon the premise that states have private information, such as unique knowledge of their military strength and resolve. The incentive to misrepresent such information is, according to Fearon (1995), one of the primary reasons why bargaining situations break down into armed conflict. Chapter 4 argues that cyber threats release private information to the public that states would have otherwise kept private. This information includes tactical and military plans, the security of digital networks, and even weapon blueprints. With this information exposed, the targeted state can no longer misrepresent it in a bargaining situation, and would therefore be more likely to push for peace.

As noted earlier, in addition to the novel subjects being studied, this dissertation employs quantitative methods to provide a generalized view of Internet vulnerabilities and their impact on interstate relations. Up to this point, social science research has tended to study Internet vulnerabilities through case studies or other qualitative methods. While these studies have certainly increased our knowledge of specific cases, this dissertation presents the first attempt to date to produce generalizable results that can predict which state-based characteristics will increase the likelihood of being targeted for attack, how international rivalry can impact the use of low-intensity forms of violence such as digital attacks, and if the theft of digital information will deter states from engaging in armed conflict. In order to accomplish this feat, a unique dataset of attacks, terrorism and espionage from around the globe was subjected to a series of empirical tests.

Finally, because of the diverse nature of the subjects being studied and the theory being examined, each chapter was designed to largely stand as an isolated piece of research. As a result, each chapter has its own literature review, theoretical framework, research design, and results section. This method has the advantage of offering a more in-depth analysis of the particular type of digital attack being investigated and a more thorough look at the literature surrounding the theoretical framework.  Additionally, this method allows for a more efficient means of publishing this research in peer-reviewed academic journals with minimal editing.

# Chapter 2 - Estimating the Likelihood of Cyber Threats, 1990-2009

When Stephen Walt (1991) described what he saw as the "Renaissance of Security Studies," the spectrum of international security threats was in a period of transition. The nuclear stalemate that defined international relations throughout the Cold War had begun to crumble, ultimately replaced in the next decade by smaller, localized civil conflicts. At the dawn of the 21st Century, the world of Security Studies is once again in transition, and the definition of what constitutes "security studies" prescribed by Walt may be too narrow. Contemporary security threats can no longer be solely defined by physical military force, nor are they confined to a particular geographic location. Instead, states, terrorist organizations, and individuals alike have begun to increasingly rely on electronic means to cause physical damage, steal vital information, and strike fear into ordinary individuals. These new forms of electronic security vulnerabilities, collectively known as "cyber threats," have thus far been largely neglected within the empirical security studies and international relations literature.

While limited research exists that anecdotally posits the potential damage caused by a full-scale cyber attack (Clarke and Knake 2010), there is a substantial gap in the scholarly literature that attempts to adequately explain the characteristics of states that become targets of this new form of security vulnerability. Although broad anecdotes of the dangers of cyber threats abound, the lack of systematic empirical analysis from the scholarly community leaves vital computer networks around the world at risk. This essay will borrow theory from the social sciences and apply quantitative methods as a means of studying international cyber threats and expanding our understanding of cyber threat targeting.

## Literature Review

The study of cyber threats by social scientists remains in its infancy. In many respects, the present state of the social science cyber literature reflects the early approaches taken in researching physical terrorism. Young and Findley (2011) point out that the terrorism literature was dominated by descriptive research for decades until the events of September 11, 2001. It was only after such a horrific terrorist attack that many social scientists began to study the causes and targets of terrorism through more systematic qualitative and quantitative, large-N studies. Thus far, the study of cyber threats largely mirrors a descriptive, "pre-Sept. 11" approach; in particular, scholars focus on determining the possible effects of a cyber threat on the infrastructure of an industrialized nation (Clarke and Knake 2010), and formulating a wide-variety of definitions to help categorize cyber activity. The following review provides a broad representation of the current state of the social science literature as well as the identification of areas where research must still be conducted to aid in understanding this 21st Century security threat.

One of the key features of recent work on cyber threats is the categorization of cyber threats based on the origin of the attack and the intended motive. As a result, the literature can be divided based on the category of attack studied (e.g., cyber attacks, cyber terrorism, and cyber espionage). Each category maintains similar traits in scope and focus. These include a drive to conceptualize the type of activity undertaken, the threat it poses, and its potential effects on the digital infrastructure of the target state.

The first category investigates the use of cyber capabilities by state-based actors against the infrastructure of other states (Arquilla and Ronfeldt 1993; Betz 2012; Brenner 2007; Choucri and Goldsmith 2012; Devine 2008; Libicki 2000; Rawnsley 2005; Rid 2013; Trendle 2002).

These types of attacks are generally referred to as either cyberwar or *cyber attacks*. Given that cyber attacks can be used by any state, great or small to, “tilt the odds against an invading army and remove the certainty of success that once made aggression worthwhile,” the literature surrounding cyber attacks is quickly becoming more robust (Libicki 2000, 30).

On a broad scale, scholars have addressed whether or not cyber attacks are a viable threat that deserves military or clandestine attention. As early as 1993, the possibility of cyberwars and netwars were discussed in-depth, particularly relating to how globalization may lead to an increase in violent interactions and how technological shifts may alter the nature of conflict and warfare (Arquilla and Ronfeldt 1993; Betz 2012; Libicki 2000). More recently, authors such as Clarke and Knake (2010), who write for mainstream public consumption, take a sensationalized approach to explaining the effects of a full-scale cyber war against the United States. They do so by crafting rather haunting scenarios of destruction and loss of basic day-to-day services. Despite claims that a cyber component to combat may prove to be anything from a means of shoring up military power to a revolutionary addition to military tactics, many researchers do not take an alarmist point of view on the matter. Rid (2013), for example, takes the position that cyber attacks are not likely to achieve the level of damage foreseen by Clarke and Knake (2010). Instead, Rid argues that past cyber attacks fail to fit within Clausewitz’s concept of war, particularly that the use of force in war is violent, instrumental and political, three criteria that no single cyber attack meets. Ultimately, he concludes that cyber attacks will be used for one of three purposes: subversion, espionage or sabotage. Valeriano and Maness (2014) present evidence consistent with Rid’s analysis. They study the impact of cyberwar on international rivalry using Joseph Nye’s (2011) definition of cyberwar as a foreign policy tactic used by states against other states. Using quantitative analysis, they find that only 20 of 124 active rivalries have engaged in cyber conflicts, and those conflicts were limited in both magnitude and frequency. Thus, views on the viability and the impact of cyber attacks are mixed in the literature to date. The available evidence suggests, however, that cyber conflicts between states are rare and constrained events.

The information that we possess on cyber attacks is, however, limited. A number of studies focus solely on the U.S. and do not analyze the impact that cyber attacks have on other states (Clarke and Knake 2010; Hunt 2012). Additionally, the handful of cross-national studies of the subject are largely descriptive. It is thus safe to conclude that the literature on this important subject is in its infancy. There have been few attempts to develop rigorous theory to explain the phenomena, with Choucri and Goldsmith (2012) and Brenner (2007) standing out as exceptions. To date, Valeriano and Maness (2014) have produced the only quantitative study of cyber attacks. The focus of their study is narrow, however, as will be discussed below.

Perhaps the cyber attack literature is underdeveloped because, as Choucri and Goldsmith (2012) claim, "there is an enormous disconnect between the cyber realities of today and the theories of the twentieth century" (75). A large number of IR theories focus on nation-states, but a host of sub-state actors such as Anonymous and Al-Qaeda affiliated hackers also have the potential to cause serious damage via electronic means, potentially as much or more damage than traditional state actors (Choucri and Goldsmith 2012). Such attacks represent the second and most heavily researched category of cyber threats, *cyber terrorism*, defined here as cyber attacks on states by non-state entities.

The acknowledgment that much of Western society relies on network technology produces a powerful psychological component for the study of cyber terrorism. Weimann (2005) notes that, "psychological, political, and economic forces have combined to promote the fear of cyberterrorism. From a psychological perspective, two of the greatest fears of modern time are combined into the term ‘cyberterrorism.’ The fear of random, violent victimization segues well with the distrust and outright fear of computer technology” (131). Yet, despite the increased attention, the disagreements and focus of this literature largely mirror that of the cyber attack research. For example, some maintain that cyber terrorism is the next major security threat for the United States (Bunker 2000; Chu et al. 2009; Embar-Seddon 2002; Kohlmann 2006; Weimann 2005), while others find that concern over cyber terrorism may be misplaced (Conway 2002).

In contrast to the cyber attack literature, cyber terrorism research has placed a greater emphasis on defining what constitutes an act of cyber terrorism. Colarik (2006) notes that most definitions agree that cyber terrorism involves some form of, “premeditated, politically motivated attack” (46). Nuances in the definitions grow larger when the “cyber” component is addressed more thoroughly. In a definition provided by Lourdeau (2004), cyber terrorism is an attack committed via computer and telecommunication services. As suggested by Colarik (2006), other scholars define “cyber terrorism” simply as the point where terrorism meets cyberspace. If this is true, then any use of computer technology by terrorist organizations (such as sending emails to plan an attack or using Google to research potential targets) could categorically fall under the umbrella of “cyber terrorism.” To say the least, the difficulty in defining what constitutes physical “terrorism,” (see Hoffman 2006) coupled with the abstract nature of the Internet and electronic technology, produces a very diverse literature.

The third category of cyber threats in the social science literature is *cyber espionage*, which is the theft of private information from businesses and ordinary citizens (Fidler 2012; Guisnel 1997; Lewis 2011). While the financial threat of cyber espionage is particularly grave to industrialized nations, the literature on the issue is less substantial than for cyber attacks and cyber terrorism. One of the few book-length investigations of cyber espionage and its history was produced by Guisnel (1997). Despite the book's age, Guisnel provides an excellent history of primitive electronic espionage in the early 1990s, as well as a description of how states and corporations may employ computers to extract large volumes of digital secrets from rival computer networks for personal gain. The author points out that, "in the United States and Canada, threats by foreign powers against companies within both countries are perceived as threats to their national interests" (Guisnel 1997, 212). While Guisnel addresses how U.S. and Canadian intelligence communities combat potential economic losses, he spends very little time discussing the interests of others states and the potential loss of information they face.

More recent publications focus on the use of cyber espionage by governments and the prevention of such intrusions. Fidler (2012) addresses a variety of ways governments should address cyber espionage, ranging from classifying it as "just spying," to treating it as a potential act of cyberwar. In a commission report written by the Center for Strategic and International Studies (CSIS) for the Obama Administration, Lewis (2011) points out that a continued reliance on information technology infrastructure may require a massive overhaul of computer security regulations. Of the various cyber threats facing the United States, the commission asserts that espionage and cyber crime remain the greatest. It is noted that, "the Internet provides nation-states, their intelligence agencies, and cyber criminals with vastly expanded capabilities to illicitly acquire information. Economic espionage does the most damage: other nations steal technology, research products, and intellectual property" (Lewis 2011, 2). Lewis's report also demonstrates the most difficult aspect of studying cyber espionage - the security concerns of publicly announcing you were targeted. The commission estimates that 80 major U.S.

companies were targeted for cyber espionage in 2010, despite the fact that only two companies publicly announced they were targeted.

Although the categorization of cyber threats helps to both frame and focus research, literature on all of these threats suffers from two distinct problems. First, the literature is highly focused on addressing America's vulnerabilities. There are exceptions to this, such as Rawnsley (2005) who investigates information warfare and propaganda between China and Taiwan, and Trendle (2002) who researches a possible Arab-Israeli cyberwar. Many articles also refer to the Russia-Georgia and Russia-Estonia cyber events, but these cases are often used only as a framing device (Devine 2008). These examples aside, a vast majority of the current literature seeks to determine how cyber threats, particularly cyber attacks and cyber terrorism, may impact American infrastructure and how to protect against such intrusions. This may be due to the fact that the United States is targeted more than any other state, making it an excellent example for scholars to rely upon, or that American policymakers are the targeted audience for such research. In any case, the literature is vastly US-centric. The second problem that the literature faces is the lack of systematic social science research on the subject, in the form of either rigorous qualitative studies or large-N, quantitative work. The vast majority of the scholarship on the subject is descriptive in nature. The notable exception is the research conducted by Valeriano and Maness (2014), who perform a content analysis through *Google News* which demonstrates the rarity of cyber attacks between rival states. However, while the authors collect data to establish the rarity of cyber attacks, they do not develop theory to explain this paucity or provide empirical tests on the potential causes of cyber attacks.

The research conducted in this paper addresses the current holes in the cyber literature, while it simultaneously expands our understanding of cyber threat targeting. Contrary to the current literature, which often focuses on identifying the *effects* of a cyber attack and their policy implications, the research question of this paper focuses on the *cause*. In particular, what factors, be they economic, military, political, or social, cause a state to be the target of a cyber threat? In order to answer this question, an extensive cyber threat dataset encompassing attacks from around the world is tested using quantitative methods, thus expanding the literature beyond its current emphasis on US-based and descriptive, qualitative studies. This paper also draws largely from and expands upon terrorist targeting literature as a framework to establish targeting characteristics and ultimately determine whether those findings can be extrapolated to cover cyber threats as well.

## Linking Terrorism and Cyber Threats: Theoretical Development

One aspect of studying cyber threats that adds to the issue's complexity is the lack of an established theoretical framework. Considering the current focus of the cyber literature, a theoretical framework is not necessarily required given that many papers attempt to define the categories of cyber threats or predict the potential effects of a cyber threat. However, the aim of this paper is to study cyber threats using quantitative means to ascertain the attributes of targeted states. In an effort to avoid founding hypotheses on an ad-hoc series of assumptions, the theoretical groundwork for this paper is based upon the physical terrorism targeting literature. That literature has determined a number of potential attributes that increase the likelihood of a state being targeted for terrorism and, given similarities between terrorism and cyber threats, using it as an early proxy for cyber threat targeting seems appropriate.

While the terrorism targeting literature is a useful foundation to craft theory on cyber threat targeting, it is important to recall that the former literature is also in its infancy (Toft et al. 2010). In preparation for their study on terrorist targeting of critical infrastructure, Ackerman et al. (2007) note "…a paucity of material regarding the more general process of target selection by terrorist groups" (viii). This assertion is backed by Toft et al. (2010), concluding that, "while the body of literature on the causes of terrorism is vast, the subject of terrorism targeting is somewhat neglected" (4411). Adapting the terrorism targeting literature to study an issue like cyber threats is further complicated by the fact that many terrorism studies investigate the link between terrorist organization ideology and their specific targets (critical infrastructure, government foundations, etc.) After the terrorist attacks of September 11, 2001, a more concerted effort was made to study physical terrorist groups, understand the logic and psychology behind their motives, and grasp their decision-making processes. Thus far, the individuals and groups that utilize cyber threats have not received such attention. Ultimately, the theoretical foundation for this paper relies on the few broad, state-level characteristics established by the terrorism literature as a means of framing the possible characteristics of states targeted for cyber threats.

Despite the rarity of terrorism targeting literature, encompassing previously developed research to help frame the question of cyber threat targeting is a step that should be taken for two primary reasons. The first reason is for simplicity's sake. Since the use of broad quantitative data to study cyber threats is in its infancy, it may be prudent to reserve cyber-exclusive theory building until after exploratory research is concluded. The present paper, and the findings it produces, may be used to develop cyber-specific theory in the future, but it can also be used to test the similarities and differences between cyber and physical threat targeting.

The second reason to employ the terrorism literature is that while cyber attacks, cyber terrorism, and cyber espionage occur in the virtual realm, they do share common attributes with physical terrorism. Hoffman (2006) points out that all terrorist organizations have a single common trait: "they do not commit actions randomly or senselessly" (173). In most cases, the same is true of cyber tactics. According to Hasham et al. (2011), "advanced cyber threat groups are extremely patient, tending to invest heavily in the research and development of custom malicious code and clever means to exfiltrate data" (3). Historical cases also provide evidence of the heavily planned nature of cyber warfare. For example, Stuxnet was specifically developed by Western nations to seek out certain Iranian computers and impede the enrichment of nuclear material. Additionally, hactivist groups seek out specific targets for disruption. In the case of Anonymous, which arguably straddles the line between crime and terrorism, the loose affiliation of hackers often target specific groups  that they believe prevent the spread of free information (such as the RIAA, the FBI, or the Justice Department).

The potential damage caused by terrorism and electronic attacks are similar as well. For example, terrorist organizations seek to, "inflict psychological and physical damage on their targets" (Lewis 2002, 8). While cyber threats prior to Stuxnet rarely caused physical damage, the impact they can have on industries and customers that rely on computers could easily cause both psychological and physical damage.[11] According to Evans and Whittell (2010), the social impact of a successful cyber attack could be the equivalent of "a well-placed bomb" (n.p.). Leon Panetta, the U.S. Secretary of Defense, backed that assertion by comparing a theoretical cyber attack to the 9/11 terrorist attacks: "A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11. Such a destructive cyber terrorist attack could paralyze the nation" (Ratnam 2012, n.p.). Both forms of attack are also

[11] The Stuxnet virus was designed to physically destroy Iranian nuclear centrifuges. Once it infected the computers controlling the centrifuges, the virus automatically increased then decreased the speed in an effort to create vibrations. Stuxnet was successful in destroying several Iranian centrifuges and slowing the process of nuclear material enrichment for a short period of time.

typically performed covertly and can be exceptionally difficult to attribute to any particular group (Weimann 2005). Crenshaw (2012) points out that one of the most difficult obstacles to overcome when responding effectively to a physical terrorist attack is the attribution of responsibility. In regards to attributing cyber threats, Gordon Snow (2011), the Assistant Director of the FBI Cyber Division notes, “the current Internet environment can make it extremely difficult to determine attribution.” This assertion is backed by Weimann (2005), who states that many users (terrorists and state-sponsored hackers included) rely on anonymous “screen names,” making it exceptionally difficult for security agencies to track the user and ascertain their true identity.

Ultimately, the common attributes of physical terrorism and cyber threats suggest that they may share similar traits in targeting. Libicki et al. (2007) point out that al Qaeda chooses targets and attack modalities, “designed to inflict a large amount of damage on the economic foundations [of states with] military, political, and commercial power” (xiv). The goal of this paper is to determine if those economic, political, and social characteristics may also provide the incentive to target one particular state over another using cyber threats.

Of the many targeting factors studied within the terrorist literature, a state’s economic strength is one of the most robust lines of research. For example, Tavares (2004) and Piazza (2008a) find that wealthier nations are more likely to experience terrorist attacks. Tavares notes that one of the primary objectives of terrorist groups is to damage the economy of their target and to, “impose material cost on the population as a form of pressure on the society as a whole” (4). The findings of Tavares and Piazza are further backed by Blomberg et al. (2004). Their analysis indicates that democratic nations, in particular those with high incomes, experience high levels of terrorist activity.

Unlike an act of physical aggression, which can happen at any time and in any place, cyber threats require some form of technological infrastructure through which to direct the attack. One reason economically developed states may be prone to cyber threats is the fact that they tend to have the type of well-developed cyber infrastructure that is vulnerable to attack. Hawkins and Hawkins (2003) found that the 32 economically-robust states that make up the Organization for Economic Co-Operation and Development (OECD) are home to 95% of the world's Internet hosts. Rogers (2000) also finds that the Internet is primarily concentrated in wealthy and well-educated urban areas. Finally, Xiaoming and Kay (2004) demonstrate that per capita wealth is a primary factor in determining the spread of the Internet in Asian nations, and there is a strong relationship between a state's GDP and Internet penetration. They conclude that, "GDP per capita indicates a country's economic strength as well as individual wealth. The deployment of the Internet is a costly venture and only countries with strong economic power are able to build the Internet in such a way that it allows access to as many people as possible" (8). Ultimately, states with a strong economy or increasing economic growth may be more likely targets of cyber attacks and terrorism both because of their economic power and because they have the appropriate infrastructure available.

Literature on the causes of economic espionage provides additional insight. Similar to cyber espionage, economic espionage is state-sponsored, conducted covertly, difficult to detect until after-the-fact, and meant to harm a target nation through non-military means. According to a former French intelligence director, "In economics, we are competitors, not allies. America has the most technical information of relevance. It is easily accessible. So naturally your country will receive the most attention from the intelligence services" (Schweizer 1996). According to the SANS Institute, "the same people doing the military espionage are engaged in industrial espionage using the same or very similar techniques to steal information from organizations…" (Messmer 2008). States that are willing to use economic espionage as a means of achieving their goals would not target a state that has few economic secrets to hide, especially if economic power is just as important as military power. Instead, it would be more advantageous to seek information from states that have proven to be economically robust. The ultimate motive of those who use cyber threats could range from economic devastation (U.S. Congressional Research Service 2004) to technological leapfrogging via industrial espionage (Parkhe 1992), both of which require targets with robust economies and Internet infrastructure for success.

Ultimately, states with more robust economics could be targeted by cyber terrorists due to the increased economic damage they could cause if Internet connectivity were disrupted. Thus,

$H_1$: States that experience economic growth are more likely to be targets of cyber threats.

Economic strength can be converted into varying forms of state power, including military power. Terrorist actors tend use unconventional means precisely because they do not have the economic or military capabilities to challenge states on the traditional battlefield. Cyber threats from both states and sub-state actors may be used in a similar way – they challenge and weaken militarily superior actors. For example, in a 2001 interview with a leading Gaza Muslim activist, military superiority of the opposing force was addressed. The activist, in defense of the use of suicide terrorism, explained that, "we lack the arms [planes, missiles or artillery] possessed by the enemy" (Hoffman 2006, 155). In a summary of the interview, Hoffman notes that "(terrorist) attacks are considered to be a means of offsetting a numerically superior, better-armed, and better-equipped opponent." In other words, organizations that are faced with a stronger opponent equipped with superior military weaponry and technology are more likely to use unconventional tactics. The terrorist attacks of September 11th were a deadly example of this inverse relationship.

In many regards, the use of cyber threats (while not as deadly in practice as terrorist attacks) could act as another form of unconventional warfare. State actors, terrorist organizations, as well as individual actors in states with less-robust military options, could rely on cyber threats to target enemies they could not otherwise significantly impact through conventional means. The use of cyber threats by terrorist organizations against larger, better-equipped militaries, such as the United States and its allies, was (and still is) a particular concern during the protracted "War on Terror." According to Vatis (2001), "the United States and its allies must operate under the premise that military strikes against terrorists and their nation-state supporters will result in cyber attacks against U.S. and allied information infrastructures" (21). In fact, the United States Department of Defense issued a report in April 2013 stating that, "as more and more state and nonstate actors gain cyber expertise, its importance and reach as a global threat cannot be overstated" (Franzen 2013). As a result of this new unconventional use of digital force, cyber threats were listed as the most pressing danger facing the U.S. in 2013.

Given the reliance of terrorist organizations on unconventional tactics and the prospect that states with less robust military infrastructures may seek to target more powerful enemies through the use of cyber threats, we can postulate that,

$H_2$: As a state's military size increases, it will experience an increase in cyber threats.

Aside from economic and military factors, the terrorism literature has diverse findings on the role that regime type may play in the risk of violence. Eubank and Weinberg (1994; 2001), Li (2005), Pape (2003), Rogan (2010) and Savun and Phillips (2009) have all investigated the potential link between regime type and terrorist attacks. Eubank and Weinberg (2001) notably point out that, “democracy makes it possible for dissident groups of all sizes and shapes to wage campaigns of terrorist violence,” which opposes the view that democracies provide a peaceful means of conflict resolution (163). Thus, the democratic political process is not responsible for the rise of terrorism, but instead it is the liberal attributes of a democracy (freedom of speech, expression, etc.) that permit these groups to exist. More specifically, Eubank and Weinberg (1994; 2001) found that democratic societies are likely targets of attack as open societies allow terrorist groups to organize and carry out their attack with less chance of being noticed. These views are further expanded upon by Li and Schaub (2004). They note that, “…by guaranteeing citizen’s political rights and civil liberties, democracy allows terrorist groups much greater room to maneuver, lowering the costs and risks for committing terrorism” (242). Not all studies research the same conclusion (Eyerman 1998; Li 2005), but the bulk of the literature maintains that the liberties associated with democratic governance are also associated with higher levels of terrorist activities.

Given the increased mobility afforded to terrorist organizations by democratic states, target hardening becomes increasingly difficult for free societies. Terrorist organizations seek to minimize the impact of increased security in societies by randomizing their target selection or choosing an entirely new primary target. This finding is backed by Brandt and Sandler (2010) who agree that terrorists shift their attention to harder-to-defend targets where success is more probable. The authors point out that, “terrorists’ response to security upgrades is to direct attacks against the most vulnerable groups” (216).

Due to the unique nature of cyber targets, access to a target must generally be easily navigable in order to deliver the virus or other malicious code. The conduit of access is, in most cases, the Internet itself. As a result, those using cyber threats must look at how different states "harden" access to the Internet and adjust their plans accordingly to attack more easily accessible targets. Thus, the nature of Internet access and Internet freedom may play a crucial role in target selection.

Traditionally, democratic states are far more likely to embrace the Internet as a means of communication and free expression (Milner 2006). As a means of communication, the views and opinions expressed in emails, blog posts, and websites are protected under freedom of speech (Goldman 2010). As a result of the openness and freedom associated with the Internet in democratic states, users have the advantage of visiting any website they wish (within legal limits), have as many email accounts as they want, and open any attachment sent to them. In many cases, it is the responsibility of the end-user to have the appropriate security software available to protect their equipment from malicious code. The cheap deployment of web connectivity also means an increasing number of industries are interconnected, as well as allowing for the digital regulation of water, gas, and other vital systems. While the spread and use of Internet services has opened up new and exciting forms of communication and opportunities, it also increases the number of available targets.

In autocratic states, many leaders believe the Internet's disadvantages outweigh its benefits. According to Sussman (2000), "45 countries now restrict Internet access on the pretext of protecting the public from subversive ideas or violation of national security…they are all autocracies." For example, the Internet can provide uncensored information, which may ultimately "threaten the interests of the ruling groups in autocracies" (Milner 2006). Non-democratic ruling institutions do not necessarily rely on broad public support, thus some autocratic regimes largely impede the adoption of technologies perceived as threatening (Kalathil and Boas 2003). Even though many autocratic states are suspicious of the Internet and the free exchange of ideas, some have adopted the Web as a means of spreading propaganda and improving political control. For example, China has recognized that, "future economic growth…will depend in large measure on the extent to which the country is integrated with the global information infrastructure" (Milner 2006). In order to use the Internet to propel national goals, but also limit the free exchange of ideas, the Chinese government has implemented firewalls, routers, and filters to limit what its citizens and outside users can view. Additionally, Chinese "Internet police" regularly use surveillance and coercion to ensure users are not viewing restricted information. When viewed in a hard/soft target framework, the Internet infrastructure in an autocratic society is likely to be considered a "hard target."

These different approaches to the Internet can have a substantial impact on the ease of deploying a cyber threat, making government type a potentially important factor in predicting which states may be a future target. In democratic states, the Internet is an open forum for ideas and the free exchange of information. That free exchange includes the ability to send and open email attachments that may contain security-exploiting viruses. In essence, the Internet in a democratic state is a soft target. In terms of industry, democratic states also tend to be more interconnected and reliant on Internet technology than autocracies. If a state or group was seeking to disrupt the power and water supplies of an enemy coalition with a cyber attack, it would be much more logical to target a democratic state whose industries relied on a digital infrastructure to regulate production. Therefore, the third hypothesis for this paper is,

$H_3$: Democratic states are more likely to be targets of cyber threats than non-democracies.

In addition, scholars acknowledge that, "not all democracies have free media and sometimes media are free in countries that lack other democratic characteristics" (Whitten-Woodring 2009, 595; Van Belle 1997). As far as tactics go, terrorists may target states with the media necessary to provide the free publicity and exposure they seek to expand their cause (Enders and Sandler 1999). In much the same vein, groups using cyber tactics often rely on free media to explain their goals. For example, the hacking group Anonymous is well-known for publishing home-made YouTube videos explaining their target selection, why they are attacking that particular target, and usually a list of demands. A state without a free press, and access to video sharing sites such as YouTube, would largely nullify the ability of hacking groups to spread their message. Therefore, based on the findings of Eubank and Weinberg (2001) and Enders and Sandler (1999),

> $H_4$: States with greater freedom of the press will receive more cyber threats than states with less press freedom.

Finally, it is important to include factors beyond domestic indicators. Notably, the terrorist targeting literature explains that engagement in international conflict may create a grievance against the aggressing state. Burgoon (2006) points out that external conflict may, "spark internal tensions or terrorist action from or against foreigners involved in the conflict" (189). This is expanded upon by Savun and Phillips (2009) who note, "states that are highly involved in international affairs form or increase their already existing interests in other states. Regular interactions and contact between states sometimes lead to misunderstanding and create discontent" (888). The authors go on to note that it is unlikely for a terrorist organization to target a state that has not negatively impacted groups within the country in which it operates. Finally, in reference to the United States exclusively, Flint (2003) finds that "the U.S.'s role as target lies in its twentieth-century position as world leader or hegemonic power. The grievances associated with the United States' contemporary global role are a precondition of terrorist activity" (162).

Those states that are more engaged on the international stage, particularly when it comes to military conflict, make themselves a target for aggression due to the grievances they generate among target states and a range of sub-state actors. However, despite this finding, the logistical cost of planning, organizing, and executing a physical terrorist attack may not be an option for all groups to air their grievances. With their low cost of deployment, coupled with the fact that the target state's homeland can be struck without a physical presence, a cyber threat could become an invaluable asset for a group seeking retribution against a perceived invading army.

By including the number of international conflicts each state engages in per year, this study can evaluate how foreign policy decisions impact the likelihood of being targeted for a cyber threat. If the terrorist targeting literature can be applied to the study of cyber threats, then we can conclude that,

$H_5$: As the number of interstate conflicts a state engages in increases, the likelihood of it being targeted for a cyber threat will increase.

The theory offered for this paper presents a variety of factors that may contribute to cyber threat targeting. Clarifying the economic and political attributes of countries that are most likely to suffer cyber threats allows for a broader understanding of this emerging hazard and offers a different perspective from the more common question, "what are the effects of a cyber attack?" that is found in the mainstream literature. In order to determine those attributes, and due to the rare nature of publicized cyber threats against public, private, and government networks, a thorough content analysis was undertaken to create the dependent variable for this analysis. The following section details the data collection process, the operationalization of the variables, and the research methodology.

## Research Design

### *Cyber Dataset*

Given the sensitive nature of network security logs, many large companies and government agencies are reluctant to allow researchers access to their network data. In an effort to exhaust any possible resources of cyber threat data, every branch of the U.S. Armed Forces, the FBI, the CIA, the Department of Homeland Security, as well as private companies such as Microsoft, Google, Apple, and Symantec were contacted. All of these sources either denied the request for information or refused to return phone calls. As a result, only one option was left to build a cyber dataset: content analysis.

The cyber dataset employed in this quantitative analysis was assembled by Virtual Research Associates using an automated content analysis of the Reuters Global News Service. The search was limited to attacks that occurred between January 1, 1990 and December 31, 2011. Due to the lack of a common vernacular, many search terms were used to ensure the maximum number of cases was collected. A complete list of the search terms used is available in Appendix A. Ultimately, the raw dataset includes 15,879 cases.[15]

Once the raw dataset was complete, a process of coding was undertaken to weed out redundant cases and those that were not clear examples of cyber threats. After the raw dataset

[15] While the total number of raw cases in the original dataset is robust, the software used by Virtual Research Associates is unable to categorize between articles of events and other types of reports. For example, the search term “cyber” returned a host of cyber threat related events, however it also returned hundreds of articles dedicated to reviews of the Sony Cybershot camera. A similar issue was encountered by including the search term “hacked,” which returned stories of computers being hacked, as well as more gruesome articles of individuals being physically “hacked apart” in violent altercations. Due to the excessive number of non-cyber related articles in the raw dataset, each case was inspected to ensure it was an example of a computer or digital network attack or intrusion.

was pared down into potential cases of cyber threats, those were further investigated using the LexisNexis service. This process ensured the remaining cases were indeed examples of a cyber threat, and allowed for a clearer idea of who the target and suspected source of the threat was. Unfortunately, in many cases the source of the attack was either not listed or was deemed heavily suspect. Given this ambiguity, the present study is only able to investigate the characteristics of the targeted state. The LexisNexis service was also used to verify the date of the attack and to ensure the correct year was listed for the beginning of the threat or its first discovery.

The final step was to code the cases into one of three categories: cyber attack, cyber terrorism, and cyber espionage. These categories were operationalized based largely on Brenner (2009) and reflect the classifications found in the cyber literature. Those obscure or vague cases that could not be coded as a specific instance of cyber warfare, cyber terrorism, or cyber espionage remained in the broader cyber threat classification but was not included in the more specific categories.

The first category, cyber attack, is similar to Brenner's "cyberwarfare" in that these are cases in which a state government is suspected of being the source of an attack against another state. The term was changed from "cyberwarfare" to "cyber attack" due to the connotation of the former that these attacks occur during a period of war. In almost every instance this is not the case. An example of a "cyber attack" case would be the 2009 Chinese cyber attack on Taiwan in an effort to paralyze the island's government and economy. Due to the sophisticated nature of the network and the virus code, the 2009 intrusion into the North American power grid by Chinese and Russian hackers would also fall under this category (as no sub-state group has claimed responsibility for the attack).

The second category is cyber terrorism, which encompasses a wide variety of cases. At the most basic level, a case is deemed cyber terrorism if the suspected source of the cyber threat is a terrorist organization. For example, in 1998 the Internet Black Tigers (an offshoot of the Tamil Tigers) launched a digital assault on Sri Lankan embassy computers around the world. The cyber terrorism category will also include those cases known as "hactivism," in which websites are attacked and taken offline. Most forms of hactivism are distributed denial of service (DDoS) attacks, which are commonly associated with groups such as Anonymous. These cases are included under cyber terrorism because the source of the attack purposefully targets a specific group/website due to a political disagreement. If one subscribes to Hoffman's (2006) working definition of terrorism, "the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change," then disabling a website and preventing the dissemination of information could certainly lead to fear in the general population (40).

The last category is cyber espionage. This is a fairly straightforward category and will encompass cases where private, digital information was stolen or released to the public against the wishes of the target. Cases that would fall into this category include Chinese attacks on Google, which released email conversations between Chinese dissidents. The case of "Titan Rain," in which 10 to 20 terabytes of information was stolen from the Pentagon computer network, would also classify as cyber espionage.

Of course, a content analysis of cyber threat cases creates a variety of problems that must be acknowledged. Perhaps the most blatant is that a successful cyber threat, especially one that seeks to steal military or economic secrets, should remain relatively unknown. The fact that knowledge of a cyber threat was published signifies one of three outcomes: an attack was originally intended to do harm and the source wanted the target to know of the attack; a failed attack was originally intended to remain a secret but, was foiled prior to its completion; or a successful attack was originally intended to remain a secret, but was discovered after its execution.  All three scenarios have been included in the dataset, as it can be concluded that even a failed cyber threat was intended by the source to harm the target in some fashion.  Although data on a phenomena such as cyber threats will inevitably have limitations, the dataset built through proprietary content analysis software for this project offers, at the very least, an initial cut at understanding this complex category of activity.

### *Dependent Variable*

The primary dependent variable for this paper will be the aggregate number of cyber attack, cyber terrorism, and cyber espionage cases each state experienced each year from 1990 to 2009.  In addition to the primary dependent variable, a series of additional analyses will be conducted to determine if alternative state characteristics exist individually among cyber attacks, cyber terrorism, or cyber espionage.  This process is undertaken as a result of findings from the terrorism literature, particularly Young and Findley (2011), who note that studying domestic and transnational terrorism as the same phenomenon may lead to incorrect conclusions based on the differing motivations that guide them.  The dependent variables measuring cyber attacks, terrorism, and espionage were coded using the process described in the previous section.[16]

[16] The raw, uncoded cyber dataset provided by Virtual Research Associates was not tested, given the exceptional number of "junk cases" present in the data.  A more detailed description of these "junk cases" is provided in the previous footnote.

## *Independent Variables*

### *Gross Domestic Product – Per Capita*

Following past research in the terrorism literature, economic performance will be measured via gross domestic product (GDP) per capita. GDP per capita was chosen as the economic measure since, "an increase in domestic income…will result in more spending by consumers and governments on goods and services which will leave a positive impact on the growth of the industrial sector" such as an expansion of the communication system (Ullah et al. 2012). In addition, this measure was used in studies such as Piazza (2006), Krueger and Laitin (2008) and Li (2005). The argument will be made that as GDP per capita increases, so too will Internet infrastructure availability and the opportunity for increased targeting. [17]

The measure for gross domestic product (per capita) was borrowed from the World Development Indicators and Global Development Finance (WDI) dataset provided by the World Bank (World Bank 2013). The GDP per capita measure was heavily skewed; as a result it was logged to improve normality.

### *Military Size*

Military size is measured as the total number of "active duty miltiary personnel, including paramilitary forces if the training, organization, equipment, and control suggest they may be used to support or replace regular military forces" (World Bank 2013). As with the previous

[17] Despite a wide reaching literature on the subject, the number of Internet and broadband users will not be included in this analysis. This choice was made for two reasons. First, there is a high degree of correlation between Internet users and both polity and the economic variables. Second, Internet user statistics are historically undependable. According to van Dijk (2005, p. 46), "Internet statistics are notoriously unreliable because of defective sampling, nonresponse, and bad quality of much (marketing) telephone interviewing or Web surveys."

economic variables, military size was obtained from the World Bank WDI dataset (2013), and is logged for normality.

### *Regime Type*

Regime type data was provided by the Polity IV project (Marshall, Gurr and Jaggers 2012). The Polity IV data measures regime authority on a 21-point scale, ranging from -10 (hereditary monarchy) to +10 (consolidated democracy). Among a number of reasons, Polity IV data was used for consistency with other conflict studies (Plumper and Neumayer 2010).

### *Freedom of the Press*

The freedom of the press data was provided by the Quality of Government dataset. This measure "indicates the extent to which feedoms of speech and press are affected by government censorship, including ownership of media outlets" (QoG Codebook 2013, 69). Censorship is defined as any restriction placed on the freedom of the press, speech, or on musical or artistic expression. Each state is measured on a scale from 0 to 2, from complete government censorship (coded 0) to absolutely no government censorship of the media (coded as a 2). While the Freedom House measure is more commonly used as a measure of press freedom, a shift in the project's method of coding states in the early 1990s would have substanitally reduced the number of cases available in the analysis.

### *International Conflict*

International conflict data was derived from the Uppsala Conflict Data Program (UCDP)/PRIO armed conflict dataset (Gleditsch et al. 2002). Each state is assigned the number of international conflicts in which it engaged for each year of the analysis. For this particular measure of conflict, at least one side must be a state government and there must be at least 25 battle-related fatalities. Given the rarity of armed international conflict in the post-Cold War era, the PRIO measure, with it's relatively low threshold of violence, was deemed more approperiate than the Correlates of War measure, which only includes conflicts with 1,000 or more battle-related causulities.

### *Media Bias*

Because the independent variable is a content analysis of media reports provided by Reuters, a variable is included to control for any potential media bias that may exist in each state. The variable is a count of the total number of articles from Reuters concerning each country in each year of the analysis (Murdie and Peksen 2013). The natural log of the control is used for normality.

Below, Table 2.1 provides the descriptive statistics of the variables used in the analysis.

## *Methodology*

The data for this research is in a time series cross section format, with a target state/year unit of analysis. Since the dependent variable is comprised of event data, an event count model is the most appropriate choice. A Poisson model was eliminated as a possible option because it assumes that the data are independent and homogenous, which is an assumption that will not hold for the current dependent variable. Ultimately, a zero-inflated negative binomial (ZINB) was chosen for the models testing the cyber aggregate, terrorism, and espionage measures because of the abundance of zeros in the primary dependent variable. Of the 1,576 cases, there were only 338 non-zero observations. Both Vuong (Vuong 1989) and a variety of tests such as residual plots and AIC (Long and Freese 2005) confirmed that a zero-inflated model is preferable over a standard negative binomial estimate.

The use of zero-inflated models in the study of terrorism has gained increased popularity as studies become more complex. In their study of terrorist target preferences, Drakos and Gofas (2006) address the need for zero-inflated modeling. They point out that both Poisson and negative binomial models assume that the occurrence of zero counts is the result of a draw from the given sample. The authors state of the terrorism literature, "the observed zero counts in the sample might be the outcome either of a country that never experiences terrorism (always zero count) or of a country that did not experience terrorism in the given sample and the count could well be positive in another period" (81). The same logic applies to studies focused on cyber threats. Thus, researchers are left with two options to account for the overabundance of zeros in their dependent variable: zero-inflated Poisson (ZIP) or zero-inflated negative binomial. As noted, statistical tests confirmed a ZINB model is the optimal choice for this study.

**Table 2.1 Summary Statistics**

| | Obs. | Mean | Std. Dev. | Min. | Max. |
|---|---|---|---|---|---|
| All Cyber Threats (*coded*) | 3,754 | 0.07 | 0.72 | 0 | 24 |
| Cyber Attacks | 3,754 | 0.004 | 0.06 | 0 | 1 |
| Cyber Terrorism | 3,754 | 0.04 | 0.42 | 0 | 17 |
| Cyber Espionage | 3,754 | 0.03 | 0.34 | 0 | 11 |
| GDP Per Capita (Logged) | 3,586 | 7.80 | 1.64 | 4.16 | 12.13 |
| Military Size (Logged) | 3,194 | 10.55 | 1.86 | 4.61 | 15.24 |
| Polity | 3,169 | 2.76 | 6.75 | -10 | 10 |
| Freedom of Press | 3,303 | 1.06 | 0.74 | 0 | 2 |
| Interstate Conflict | 3,754 | 0.03 | 0.19 | 0 | 3 |
| Media Bias (Logged) | 3,579 | 5.85 | 2.24 | 0 | 12.37 |

While the coded aggregate, terrorism, and espionage dependent variables all converge successfully with a ZINB model, the cyber attack measure was unable to find convergence. This is attributed to the extremely rare nature of the event; out of 3,754 events, only 14 country-years experienced an attack. Of those 14 country-years with an event, only the United States in 2009 was targeted for more than one cyber attack. Given the exceptionally rare nature of cyber attacks, and the difficulty experienced by the ZINB in finding convergence, the decision was made to make the cyber attack variable dichotomous. This required changing the finding for the United States in 2009 from three cyber attacks to one, the remainder of the variable already ranged from 0 to 1. With this transformation, the cyber attack model was successfully tested using a rare event logit. Rare event logistic models were originally developed by King and Zeng (2001) in an effort to aid in the study of extremely rare events, such as war. The authors note that conventional logistic regressions tend to "sharply underestimate the probability of rare events," and are "grossly inefficient for rare events data" (137).

In addition to convergence difficulty, rare event panel data may encounter a number of methodological problems. For example, the aggregated cyber threat and cyber espionage models tested in this research suffer from autocorrelation, as confirmed via the Wooldridge test for panel data. Since AR processes cannot be incorporated into a ZINB estimates at this time, each model with autocorrelation includes a lagged version of the dependent variable as a control.

Additionally, given that the data is clustered by state, a means of accounting for group-level variation was undertaken. In particular, when confronted with clustered or grouped data, many scholars rely on fixed or random effects models (Clark and Linzer 2012). A series of spatial and temporal controls were added to test whether a fixed or random effects model would be preferred. The results of a Hausman specification test affirm that fixed effects models are a better fit. Unfortunately, ZINB and rare event logistic estimates are unable to accommodate fixed effects.[18] Additionally, according to Allison (2009), “in applications where the within-person variation is small relative to the between-person variation, the standard errors of the fixed effects coefficients may be too large to tolerate” (cited in Williams 2012, 2). This also applies to the present study, where measures such as polity, freedom of speech, and international conflicts vary little or not at all within states, but vary substantially across units. Given that the rare event models take into account the excessive number of zeros in the dependent variable, and the small within-group variation that exists across many of the model variables, the standard ZINB and rare event logit models were deemed to be the optimal choices.[19]

A Ramsey reset test also confirms the models suffer from omitted variable bias. However, the significance of this test was expected given that the theoretical framework utilized in this research is based on the study of a different phenomenon. While studies of both physical and digital aggression would likely include similar political, economic, and social variables, there simply must be additional factors that make a state the target of a cyber threat that have no bearing on physical terrorism. For example, measures of government and private funding dedicated to network security, offensive and defensive cyber capabilities, and other cyber-

[18] An attempt was made to run a negative binomial model with dummy variables for the different country codes. Unfortunately, this model proved to be too complex for STATA. Paul Allison notes this technique is a means of applying fixed effects to rare event panel data, but admits it “can be computationally demanding for conventional software if the number of individuals is large” (Allison 2012). Table A.1 in Appendix A reports the results of a fixed effects logit model, and the original rare event logit. The results are largely similar, aside from a shift in significance for the military size measure.

[19] Table A.2 in Appendix A provides the results of the fixed effects models, many of which demonstrate a difference in both indicator sign and significance when compared to the ZINB models. However, given the benefits of the ZINB model and the excessive number of zeros in the dependent variable, the zero-inflated negative binomial was deemed to be the more appropriate specification for this analysis.

exclusive factors are not the focus of terrorism targeting studies and thus are not included in this paper. Additionally, it must be acknowledged that the data necessary to measure many of those attributes are either notoriously unreliable or unavailable for scholars (van Dijk 2005). Given that this is the first attempt at quantifying the study of cyber threat targeting and the framework is based upon the study of a similar yet physical form of aggression, certain targeting characteristics are bound to be omitted. Omitted variables may thus be one of the limitations inherent in studies of phenomena that have received scant empirical attention in the past and in relatively new fields of research. Further research with new data will hopefully overcome this limitation.

Finally, each model was tested using a variance inflation factor (VIF) test, to ensure that correlation among the variables was not present. No serious correlation was found, particularly among the economic measures or the regime type/political freedoms measures.

## Results & Discussion

### *ZINB & Rare Event Logistic Results*

The analysis results are presented in Table 2.2. Much like a logistic regression, additional techniques are required to interpret the impact of each independent variable in a ZINB and rare event logistic regression. A host of different statistical tools are used to interpret coefficients, from incidence rate ratios (Savun and Phillips 2009) to more complex Monte Carlo simulations (Piazza 2011). For the purposes of this research, factors and marginal effects were utilized in providing an accurate interpretation of the coefficients (Dreher et al. 2010; Santifort-Jordan and Sandler 2014), and provide the predicted number of events at varying levels (typically a standard deviation increase) of the specified independent variable. Because the number of state/year combinations, however, it is unrealistic to specify the marginal effects for each. As a result, the global mean of the independent variables will be substituted for many of the analyses. However, it should be noted this technique only provides an estimate of the "average state" and may not necessarily reflect the targeting likelihood of a particular state. To aid in interpretation and to demonstrate the wide variation between the means of an average state and those of the United States, specialized marginal effects are reported throughout.[20] The following section will discuss the statistical findings of the regressions, and the next section will provide additional discussion, particularly highlighting how these findings compare to those of the terrorist targeting literature.

The results of the analyses demonstrate varying support for the hypotheses, dependent upon the particular cyber threat being studied. The first hypothesis, focusing on the relationship between GDP per capita and cyber threats, receives varying support across the four models. While the first model is statistically insignificant, the second model indicates that a one percent increase in GDP per capita will increase the number of cyber attacks by a factor of 2.33. Inversely, Model 3 demonstrates that a one percent increase in GDP per capita results in a decrease in cyber terrorism cases by a factor of 0.71. Surprisingly, GDP per capita is a statistically insignificant factor for states being targeted with cyber espionage, suggesting that a robust economic atmosphere is not necessarily attractive to those states, groups or individuals seeking to steal private information.

Concerning the substantive effects, the use of marginal effects sheds more light on the relationship between a robust economy and cyber threat targeting. For example, despite the

[20] Marginal effects graphs for the four models can be found in Appendix A.

**Table 2.2 Zero-Inflated Negative Binomial & Rare-Event Logit Results**

| | Model 1 | Model 2 | Model 3 | Model 4 |
|---|---|---|---|---|
| | *Aggregate Cyber* | *Cyber Attacks* | *Cyber Terrorism* | *Cyber Espionage* |
| *Inflated Negative Binomial* | | | | |
| GDP Per Capita (Logged) | 0.14 | 0.85** | -0.35* | 0.34 |
| | (0.93) | (2.06) | (-1.78) | (1.23) |
| Military Size (Logged) | 0.55*** | 1.43** | 0.02 | 1.27*** |
| | (3.97) | (2.30) | (0.10) | (6.68) |
| Polity | -0.13*** | 0.07 | -0.19*** | -0.13* |
| | (-3.90) | (1.15) | (-3.43) | (-1.68) |
| Freedom of the Press | 1.66*** | -0.10 | 2.04*** | 2.45*** |
| | (3.66) | (-0.12) | (2.69) | (2.58) |
| International Conflicts | 0.42 | 0.68 | 0.80** | -0.05** |
| | (0.74) | (1.02) | (2.02) | (-2.13) |
| Lagged D.V. | 0.02 | - - - | - - - | 0.05** |
| | (1.49) | | | (2.03) |
| Media Bias (Logged) | 0.18 | -0.45 | 0.77*** | -0.38*** |
| | (1.12) | (-1.47) | (3.56) | (-3.33) |
| Constant | -11.59*** | -26.63*** | -6.50** | -19.79*** |
| | (-4.12) | (-2.83) | (-2.13) | (-4.97) |
| *Inflated* | | | | |
| GDP Per Capita (Logged) | -0.24 | - - - | -0.90*** | -0.57 |
| | (-0.96) | | (-3.32) | (-0.61) |
| Military Size (Logged) | 0.50 | - - - | -0.13 | 1.98*** |
| | (1.34) | | (-0.28) | (2.76) |
| Polity | -0.18** | - - - | -0.21* | -0.46 |
| | (-2.08) | | (-1.79) | (-1.34) |
| Freedom of the Press | 2.84*** | - - - | 3.54*** | 8.75* |
| | (3.46) | | (2.91) | (1.75) |
| International Conflicts | 0.43 | - - - | 1.13** | -1.04 |
| | (0.68) | | (1.88) | (-0.98) |
| Lagged D.V. | -2.11** | - - - | - - - | -1.54*** |
| | (-2.26) | | | (-2.57) |
| Media Bias (Logged) | -0.93*** | - - - | -0.55 | -3.57*** |
| | (-2.67) | | (-1.40) | (-3.56) |
| Constant | 3.04 | - - - | 11.96** | 5.14 |
| | (0.60) | | (2.10) | (0.62) |
| *Model N* | *2,650* | *2,771* | *2,771* | *2,650* |

*(z statistics in parentheses)* * *p* < .10, ** *p* < .05, *** *p* < .01

statistically insignificant ZINB result, when testing the aggregate cyber data using global averages, the marginal effects show an increase of one percent in GDP per capita results in an increase in cyber threats by .3 percent. This finding is significant at the 10% level. For the United States, the impact of GDP per capita is more robust and significant at the 1% level of confidence: an increase in 1 percent in GDP per capita results in a 70 percent greater probability of a cyber threat. Marginal effects also shed more light on Model 2, which suggests a positive relationship between economic robustness and cyber attack targeting. When modeling global averages, a state would experience a 90% percent growth in cyber attacks for every 1 percent increase in GDP per capita. The United States would expect to see a similar increase in cyber attacks with every one-percent increase in GDP per capita. These findings broadly suggest that states with more robust economies are targets of state-sponsored cyber attacks. Additionally, increases in GDP per capita are shown to reduce cases of cyber terrorism. While the global marginal effects are insignificant, a one-percent increase in America's GDP per capita reduces cyber terrorism cases by 20%. The notion that increases in GDP per capita increase cyber attack targeting but decrease cyber terrorism targeting is interesting. It is possible that the resources that states devote towards defending against cyber attacks make it easier to defend against less sophisticated forms of cyber terrorism. In other words, states are able to overcome targeting hardening but non-state actors may have more difficulty. Finally, as expected, a one-percent increase in GDP per capita increases cyber espionage in the United States by 130%.

The second hypothesis investigates the relationship between cyber threats and military size. Three of the four analyses have statistically significant results and support the theoretical framework behind the hypothesis. In particular, Models 1, 2, and 4 demonstrate that an increase in military size increases the number of cyber threat cases by a factor of 1.73, 4.18, and 3.56 respectively. Using marginal effects and global averages, a one percent increase in military size would result in a .04 percent increase in total cyber threat cases. This increase jumps to 54 percent when U.S. averages are substituted. In Model 2, the marginal effects show that a one percent increase in the mean state military size results in a 143 percent increase in cyber attacks. Although considering the average state only sustains .004 cyber attacks a year, this increase is rather marginal. For Model 3, despite the insignificant ZINB result, marginal effects with U.S.

averages show that a one percent increase in military size results in 15 percent increase in cyber terrorism, or an additional .44 cases during a typical year. Finally, the marginal effects with U.S. averages for Model 4 predict that a one percent increase in military size results in 831 percent more cyber espionage cases. Since the United States sustains 3.4 cyber espionage cases on average per year, a one percent increase in military size could translate into almost 25 additional cyber espionage events. Surprisingly, the marginal effects with global averages were not significant, indicating that states with large armies are the target of cyber espionage far more often than the "typical" state.

The third hypothesis seeks to determine the impact of regime type on cyber threat targeting. Model 1 shows that a one point increase in the Polity IV scale decreases total cyber threat cases by a factor of .88. Models 3 and 4 also show a similar pattern, as an increase in Polity results in decreased cases of cyber terrorism and espionage by a factor of .83 and .88, respectively. The marginal effect results largely reassert the inverse relationship demonstrated by the ZINB models. For example, if the United States were to decline by one point on the Polity IV scale, it may experience an additional .26 cyber terrorism cases. In other words, these results show that increased democratic participation may reduce cyber targeting, which does not support the hypothesis framed previously.

These findings do, however, mirror a small subset of the terrorism literature which finds that democratic states experience a decline in violence. When combining a negative binomial model with the ITERATE database, Eyerman (1998) found that democracies experience fewer terrorist attacks than non-democracies. Additionally, Li (2005) models the heterogeneity that exists between democratic regimes and finds that democratic participation reduces the number of terrorist events. The present study supports this strain of the physical terrorism literature as democratic states do not experience as many cyber terrorism events as their autocratic counterparts. These results will be discussed further in the next section.

The fourth hypothesis tests a subsidiary of the terrorist literature focused on the freedom of expression within governments. Eubank and Weinberg (2001) claim that terrorism is more likely in democratic states due to the freedom of movement and expression afforded to its citizens, but Whitten-Woodring (2009) points out that not all democracies have the same level of freedoms. The theoretical assertion by Whitten-Woodring that increasing freedoms lead to higher levels of violence is largely supported by the present analysis. To test this hypothesis, a 3-point scale ranging from no freedom of speech to absolute freedom of speech is employed, and finds that an increase in the freedom of expression also increases cyber threats in general, as well as cyber terrorism and cyber espionage. More specifically, an increase in one point on the scale increases the number of cyber threats, terrorism, and espionage by a factor of 5.26, 7.69, and 11.59 respectively.

The marginal effects also largely reflect the conclusions of the three significant models. In particular, when employing U.S. means, a decline from a 2 to a 1 on the freedom of speech scale reduces the number of aggregate cyber threats by 6.5 annual events. While Model 2 does not produce a significant finding, the nuances of marginal effects demonstrate that an increase of one point on the scale decreases the number of cyber attacks on the average state by 0.1 events. A similar result is produced when substituting U.S. averages. For Model 3, the global marginal effects show that only those states coded as having no freedom of speech are statistically more likely to experience cyber terrorism. Finally, the marginal effects for Model 4 vary somewhat from the ZINB findings. For example, the results using global averages are all statistically insignificant, signaling that the freedom of speech has no relationship on cyber espionage targeting. When substituting U.S. averages, the results demonstrate that only states with absolute freedom of speech are statistically likely to be targeted for cyber espionage. This may suggest that there is a link between freedom of expression and the type of robust R&D that is likely to be a target of cyber espionage.

The fifth hypothesis investigates the proposed relationship between interstate conflict and cyber threat targeting. Unlike the other independent variables, this one seeks to determine the influence of foreign policy on the likelihood of targeting. The results show mixed support for the hypothesis that an increase in the number of international conflicts would result in an increase of cyber threats. The hypothesis is supported by Model 3, suggesting that states engaged in more armed conflicts abroad are likely to experience an increase in cyber terrorism by a factor of 2.23. However, Model 4 shows that states engaged in more conflicts will experience fewer cases of cyber espionage. In particular, engaging in one additional armed conflict will decrease the number of cyber espionage by a factor of 0.95.

The final set of marginal effects produce particularly robust findings, and provide insight into the models that were not outwardly significant. For example, the marginal effects with U.S. averages of Model 1 demonstrates that moving from zero conflicts to one will increase the number of total cyber threats by 3.9 cases. When employing global means, the marginal effects of Model 2 show that engaging in one additional armed conflict will increase the number of cyber attacks by 0.7 cases. Marginal effects with U.S. averages are statistically insignificant, however. For Model 3, marginal effects with U.S. averages shows that moving from zero conflicts to one will increase the number of cyber terrorism events by 0.7 cases, while the results with global averages are all statistically insignificant. Finally, the results for Model 4 with U.S.

averages demonstrate that engaging in one additional conflict will reduce cyber espionage by an average of 0.8 cases.

## *Discussion*

The results of this analysis provide some interesting insights into the nature of cyber threat targeting, as well as expanding upon the similarities and differences between cyber threat and physical terrorism targeting. As expected, the results demonstrate that the terrorism literature cannot be used as a "one size fits all" theoretical foundation for the broad study of cyber threat targeting. And while the theory did not explain all of the models, it provides the foundation for building cyber specific theory for different types of cyber threats. Thus, the inability to demonstrate a statistically significant finding to support a hypothesis is, in this case, an opportunity to learn about those social, political, and economic factors that increase targeting likelihood. This paper and the results produced provide future researchers with a springboard to test their own theories without solely relying on the terrorism literature as a guide.

More succinctly, this analysis demonstrates the varying characteristics that lead to states becoming targets of cyber attacks, cyber terrorism, and cyber espionage. The cyber literature, with statistical evidence produced by this analysis, provides further evidence that the mentality behind the use of cyber threats may vary to a high degree. For example, looking solely at the regression results, states that experience a decrease in GDP per capita, those that are more autocratic with higher levels of freedom of speech, and engage in more international armed conflicts are more likely to experience cyber terrorism. This is in contrast to those states faced with cyber espionage, which have larger armies, are more autocratic with some freedom of speech, and fewer international conflicts. Given these findings, it is becoming increasingly clear that cyber attacks, cyber terrorism, and cyber espionage may use the same digital network as a venue through which to operate, but the targets of those attacks and their intended goals are somewhat diverse.

In terms of the model results, the outcomes are varied and many find support in both the terrorism and cyber literatures, despite the fact that they did not always adhere to the expected direction of significance. For example, the finding that an increase in GDP per capita may lead to a decrease in cyber terrorism is similar to the results reported in Li (2005), who found that the level of economic development of a country (measured via GDP per capita) reduces the likelihood of being targeted for a transnational terrorist attack. This finding opposes the larger terrorism literature, specifically Tavares (2004) and Piazza (2008a) who find that wealthier nations are more likely to experience terrorist attacks. However, while cyber terrorism does not necessarily follow the same trajectory of physical terrorism, it should be noted that an increase in GDP per capita does significantly impact the likelihood of cyber attack targeting. This suggests that wealthier nations may invest more into computer network defense, which can deter terrorist organizations that often rely upon rudimentary forms of cyber terrorism such as denial of service attacks. However, the results show that the level of network defense capable of deterring cyber terrorists is not necessarily enough to deter nation-states from launching more sophisticated attacks.

In contrast to GDP per capita, military size appears to attract both cyber terrorism and cyber espionage. These results suggest that terrorist organizations are unable to compete directly with large, physical armies on the conventional battlefield. Thus, terrorist groups may choose to target the militarily superior foes in less conventional areas, such as the digital network many large armies rely upon for communication, tactical preparation, and information storage. Cyber terrorism attacks allow weaker groups to enact varying degrees of damage against a numerically superior foe that would have otherwise been impossible to perform through physical force. Additionally, states and groups that use cyber espionage also target states with larger militaries. This suggests that states with large militaries may also have advanced technology that other states covet. These include advanced forms of communication, more efficient weaponry, and advanced means of troop transport and deployment. Such technologies may very well be the target of cyber espionage cases. Additionally, groups and states may target the network infrastructures of states with large militaries seeking to find weaknesses or sensitive tactical information such as troop deployment schedules and future battle plans. A particularly successful case of cyber espionage could give a numerically disadvantaged, smaller nation a tactical advantage against a numerically-superior foe.

In addition to military size, the finding related to polity provides insight into the use of cyber threats against autocratic regimes. For example, the cyber terrorism results suggest that digital weapons such as distributed denial of service (DDOS) attacks are a tool of the repressed. For subjugated individuals in autocratic regimes without recourse through traditional politics and nonviolent demonstrations, cyber terrorism provides an opportunity to effectively challenge their stronger and better-equipped political opponents (Lichbach 1998). According to Still (2005), politically-motivated cyber tactics “show the general public and the media that they are standing up against the establishment to protect the rights of people around the world that are endangered by national or corporate oppression and greed” (2). In many regards, Still’s assertion of cyber terrorism tactics compliments Li’s (2005) theoretical argument that, “democratic participation reduces transnational terrorism [by increasing] satisfaction and political efficacy of citizens, reduces their grievances, thwarts terrorist recruitment, and raises public tolerance of counterterrorist policies” (294).

The findings related to regime type are coupled with the freedom of speech and press measure. For example, the regime type finding suggests that autocratic states are more likely to experience cyber terrorism. While the ZINB results for Model 3 show a significant and positive relationship, the marginal effects with global means demonstrate that only those states coded as a 0, which indicates complete government dominance over media, are statistically likely to be targeted for cyber terrorism. Thus, given the polity findings, we can speculate that autocratic states that suppress freedoms of speech are likely to experience more cyber terrorism than their democratic counterparts, further bolstering the assertion that cyber terrorism could be a weapon of the repressed.

Finally, the armed conflict involvement measures provide insight into the impact of foreign policy decisions and targeting likelihood. For example, Model 1 shows that if the United States were to engage in one interstate armed conflict, it could expect to be targeted for additional cyber threats. This result may give policymakers an additional factor to consider when contemplating whether to engage in interstate conflict: not only must they contemplate the security vulnerability of the troops being sent into battle, vital domestic network infrastructures may also be put into harm's way. Given the findings of the analysis, the U.S. should be particularly concerned about cyber terrorism and cyber espionage if armed conflict were to break out. Interestingly, the results for the interstate conflict measure were robust primarily when using U.S. averages, lending evidence to the notion that foreign policy decisions such as armed conflict engagement may only impact the domestic digital networks of global or regional military hegemons.

Perhaps most importantly for future quantitative analysis, this paper demonstrates the danger of studying cyber threats as a "group phenomena" without acknowledging the distinctive characteristics of cyber attacks, cyber terrorism, and cyber espionage.[21] As the results clearly show, the predictors across each model are not uniformly significant or signed. For this reason, one could not accurately posit that the results of Model 1 are representative of targeting state characteristics. If such an assertion was made, one would mistakenly believe that military size had a statistically significant impact on cyber terrorism targeting, or that GDP per capita was not a significant indicator of cyber attacks. Instead, researchers must acknowledge the nuances in the qualitative cyber literature, and apply those differences when categorizing the different types of cyber threats for analytical study. Failing to do so puts researchers in danger of committing a type one or type two error.

## Conclusion

In order to obtain a more complete understanding of the threat posed to digital networks by cyber attacks, cyber terrorism, and cyber espionage, scholars must use every tool at their disposal. This includes large-N, quantitative analyses as well as exploring examples of security vulnerabilities from past technological innovations. As alluded to in the first chapter, the vulnerabilities in many revolutionary forms of communication have been exploited by actors seeking advantages over rivals. For example, the radio transmissions of the United States were intentionally jammed by the Soviet Union as a means of limiting communication and preventing the spread of free information. The jamming of U.S. and other Western radio signals by the Soviets was part of the broader ideological and strategic struggle between the two powers. This historic example demonstrates that factors such as government ideology and power struggle

[21] In a similar fashion, Young and Findley (2011) found that research which combines international and domestic terrorism definitions may provide incorrect or inconclusive findings. In an attempt to prevent such problems, a variety of tactics have been developed to parse international from domestic terrorism cases (Enders et al. 2011).

could potentially increase the likelihood of state targeting through the vulnerabilities of other technological innovations. More broadly, the historical investigation shows that while the characteristics of those states targeted for cyber threats are unique, the broad problem of communication vulnerabilities and the notion that state characteristics may increase targeting are not necessarily unique.

Keeping historical examples in mind, the goal of this chapter was to determine if state characteristics increase the likelihood of targeting through a 21st century form of communication. By using a comprehensive dataset of cyber threats spanning 20 years, we can now provide a more accurate picture of those economic, political, and social characteristics likely to make a state the target of a digital attack. Additionally, the quantitative analysis conducted here further reinforces the categorization of cyber threats already present in the qualitative literature. Future quantitative studies should acknowledge those differences and incorporate them in order to help ensure the most accurate results possible.

Future studies can also build upon the work established here by continuing to gather and analyze cyber data. Although it is exceptionally difficult to do, one vital step in building a robust cyber dataset would be to incorporate the sources of cyber attacks, cyber terrorism, and cyber espionage. By only studying the targets of the threats, we are restricting our understanding of this phenomena to one side of a dyadic relationship. Once the source of these threats can be accurately identified, more robust directed dyadic studies can be performed. Additionally, more accurate measures of factors such as Internet penetration may be included as an independent variable or control. While there is a healthy literature linking Internet usage to both economics and polity, a singular measure of Internet usage would certainly aid in clarifying the impact it has on cyber targeting. Despite the fact that Internet penetration data does exist, it is exceptionally unreliable and the number of missing cases would have further limited the analysis conducted here. According to van Dijk (2005), "most survey data on computer and Internet penetration or use are too unreliable and invalid for us to be able to draw definite conclusions from them" (46).

Additionally, the analysis could benefit from a more robust measure of press and speech freedom. The measure used in this paper only categorized states based on a three-point scale, which overlooks many nuances in government control of media and the rights of private citizens to protest, assemble, and speak publicly. While the Freedom House measure of press freedom includes many of these nuances, it would also limited the temporal range of the study. Given the relatively new nature of cyber threats, a broad temporal range was desired to fully capture the maximum number of events as possible.

In terms of the results provided in this paper, future researchers should also delve deeper into the individual components of the analysis and help determine the causal mechanisms behind their significance. For example, what are the specific motivating factors behind hackers that choose to attack autocratic states more often than their democratic counterparts? This is another facet of cyber studies that could be aided by the terrorism literature, which has already invested significant research studying similar questions.

Ultimately, the quantitative study of cyber threats is a vital component of understanding a new generation of international security threats. Instead of focusing attention on defining what cyber threats are or what their effects may be, as a vast majority of the present literature does, this papers helps to fill one of the substantial quantitative gaps that currently exists. By relying on the unique dataset compiled for this project, research on cyber threats can now generalize beyond isolated events and seek to predict under what economic, political and social conditions cyber attacks, cyber terrorism, and cyber espionage are likely to occur. The endeavor to study such an abstract security threat may seem like a daunting task, but it is a necessary one to protect the vital digital networks that so many rely upon for basic social services.

# Chapter 3 - International Rivalry and Cyber Attacks

In the early months of 2013, the malicious spying software known as “MiniDuke” was deployed against Romania as well as a handful of other NATO countries. Once it was discovered by Romanian security experts, the software was immediately attributed to a rival nation, most likely one from the former Soviet Union (Patran 2013). This case was preceded by the high-profile Stuxnet virus used to temporarily disable Iranian nuclear facilities. The discovery of the virus by Iranian scientists led to a series of accusations by Iranian military officials, most of which were pointed towards Israel and the United States, both rivals of the Middle Eastern nation (Reuters News Agency 2011). Finally, in 2007, Estonia was targeted for a series of digital assaults that knocked government websites, including the Estonian president’s own site, offline. The country declared it was the first victim of cyber warfare, and immediately Estonian officials accused its northern rival, Russia, for the attacks (Myers 2007). As these cases demonstrate, cyber threats against national governments are often initially suspected to be the actions of a competing state.

The presence of conflict within rivalries has long been a focus of research in international relations. International rivals, states that view one another as competitors and enemies, have been found to engage in militarized disputes and wars more frequently than their non-rival counterparts (Colaresi et al. 2007; Dreyer 2012). While rival states are more likely to engage in armed conflict, a new form of violence has arisen that may also be used between antagonistic actors. This new form of assault, known collectively as cyber threats, involve the use of computer and network technology to disrupt or damage the information technology resources of a targeted state. Despite the fact that a full-scale cyber war has never occurred, and given their propensity for conflict, one must wonder if states engaged in rivalries are more likely to be targeted for cyber threats than neutral states. In order to shed light on this contemporary security issue, this study incorporates quantitative data on international cyber threats from 1990 to 2009 to determine if states engaged in rivalries are more prone to suffer cyber threats than non-rival states.

This paper will proceed in six parts. First, a review of the rivalry and cyber literatures will demonstrate trends within each respective field of study, and how the analysis conducted in this paper fills gaps in each. The second section will provide the theoretical framework employed to understand the use of cyber threats within international rivalries. That section is followed by the research design, a report of the regression results, and a brief discussion of those results. The final section concludes, and offers direction for further research.

## Literature Review

The international relations literature addressing interstate rivalries is particularly robust, especially when compared to the social science literature on cyber threats. Maoz and San-Akca (2012) parse the rivalry literature into three broad categories: the conditions that impact the frequency of conflict within rivalries (Conrad 2011; Findley et al. 2012; Maoz and San-Akca 2012; Vasquez 1995), the issues that lead to armed conflict (Colaresi and Thompson 2002; Rasler and Thompson 2006; Vasquez 1996) and the termination of rivalries (Bennett 1996; 1997; 1998; Goertz and Diehl 1995). This paper fits into the first category, but with a twist. Namely, instead of simply studying the frequency of armed conflict within rivalries, this study seeks to identify new types of force, less deadly than armed combat, that may be used against states embroiled in an international dispute. To do so, this study must first outline the scholarship that explores the use of conflict between interstate rivals, encompassing both armed conflict and more subtle forms of violence. Additionally, a brief overview of the social science cyber literature will be provided.

The use of force among interstate rivals has been addressed by a wide range of studies. Notably, many scholars choose to frame "force" between rivals in the form of traditional armed conflict (Goertz and Diehl 1993; Hensel 1996; Maoz and Mor 1996). While the use of conventional armed force is the most visible outlet of aggression between interstate rivals, Conrad (2011) differs from the traditional literature in his claim that the, "potential for militarized conflict, rather than armed physical conflict itself, can drive a state's consideration to use alternative forms of military force" (532). The author posits that alternative uses of force may include state-sponsored terrorism, a form of violence that had been largely overlooked in the rivalry literature. By analyzing the annual number of transnational terrorist attacks that occur in all countries between 1975 and 2003, Conrad determined that states involved in ongoing rivalries were victims of more attacks than states that were not part of an ongoing rivalry. Because the attribution of state-sponsorship in terrorism is exceptionally difficult, Conrad was only able to look at the target of such attacks, rather than investigating rivalry violence in the more traditional dyadic setup. However, given the findings, the author concludes, "logically, states involved in these hostile relationships are also likely to sponsor more terrorist attacks than states not involved in rivalries" (Conrad 2011, 546).

Conrad's question of whether states in a rivalry use alternative forms of violence has prompted additional scholarship on the matter. Findley et al. (2012) posit several reasons why rival states might use terrorist groups as a proxy for armed conflict. Most notably, the use of terrorist groups may help to "manage the strategic and political costs of rivalries," while traditional armed conflict is often viewed as costly and uncertain (236). The use of terrorism not only exacts real costs on the target through casualties and counterterrorism expenses, but it also has the potential to have positive domestic ramifications for politicians that support terrorist actors. For example, government officials may align themselves with terrorist organizations that garner popular support or sympathy in the country. In an analysis of terror events in politically-relevant directed dyads from 1968 to 2002, Findley et al. demonstrate that rivalry is a positive indicator of transnational terrorism. The authors conclude by noting their findings, "suggest that disputes between states have implications for a security threat – terrorism – that has commonly been regarded as a phenomenon driven by economic, political, and social features of individual states" (245).

Maoz and San-Akca (2012) also investigate the relationship between rivalry and violence. However, instead of focusing their analysis on the state sponsorship of terrorism, the authors investigate non-state armed groups (NAGs) such as ethnic or religious insurgents as well as guerilla organizations. The authors point out that states and NAGs who share mutual goals have several incentives to work together, particularly when the state is engaged in an enduring rivalry. For example, rivalries create opportunities for NAGs to acquire resources in order to sustain their operations. In the same manner, states may be eager to support NAGs as a means of imposing costs and inflicting causalities on a rival target. Examining an original dataset encompassing observations for 175 NAGs and 83 state supporters since the end of World War II, the authors show that the presence of rivalries increase the likelihood of cooperation among states and NAGs. Additionally, such cooperation is likely to escalate the tension between two rival states. This finding implies that, unlike state-sponsored terrorism and the anonymity that comes with such support, the backing of NAGs provide states with a more conspicuous means to target rival states.

The three studies conducted by Conrad (2011), Findley et al. (2012), and Maoz and San-Akca (2012) help demonstrate that rival states may not only engage in elevated levels of armed conflict, but they may also experience increased levels of terrorist and NAG attacks. The use of sub-state violence as a surrogate for more deadly state-to-state armed conflict raises the question of whether rivals use other forms of low-level violence, such as cyber threats, against their enemies. The term "cyber threat" encompasses a wide array of digital assaults on networked resources. These assaults are typically identified as cyber attacks, cyber terrorism, and cyber espionage. And while the targets and goals of these different forms of digital attack vary, they all rely on the same network infrastructure, they are all exceptionally difficult to trace back to the original source, and they can all be very effective. In fact, according to Evans and Whittell (2010), the social impact of a successful cyber attack could be the equivalent of "a well-placed bomb." This analogy was given support by Leon Panetta, the U.S. Secretary of Defense, who noted, "A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11. Such a destructive cyber terrorist attack could paralyze the nation" (Ratnam 2012, n.p.).

In contrast to the interstate rivalry literature, the cyber threat literature is still in its relative infancy. Many of the articles published on the issue rely heavily on anecdotal and descriptive evidence. One notable exception is the research produced by Valeriano and Maness (2014), who venture beyond descriptive information to quantify cyber attacks between rival states. The authors point out that deterrence, which plays heavily into conflict-prone rivalries, often provoke further conflict and extreme threats (Hensel and Diehl 1994; Vasquez 1993). As a result of the breakdown of deterrence, the authors posit that rivals may be less prone to use acts of cyber war due to fears of retaliation. In the event that cyber attacks are used, their impact would be exceedingly minimal due to deterrence dynamics. They also hypothesize that most cyber attacks should be limited to regional interactions, since the most dangerous rivalries are often driven by geographic contiguity (i.e., Russia and Georgia, Pakistan and India, Israel and Iran). In order to test their hypotheses, Valeriano and Maness build a dataset of cyber attacks using content analysis of the *Google News* service, and carefully code the suspected source and target of the attacks, as well as the nature of attack that was used. Finally, these attacks were compared to the 124 active and ongoing dyadic interstate rivalries from 2001 to 2011. Their analysis demonstrates that only 20 of 124 rivalries have employed cyber attacks, and most of those fall into the "lower end in terms of quantity" (17). Additionally, their statistics show that cyber attacks tend to be more common in regions dominated by a major regional power, such as China and India.

While Valeriano and Maness should be commended for their effort and early foray into the quantitative study of cyber threats, their analysis has limitations. For example, the authors do not perform statistical tests with control variables that help to establish causality. Thus, their conclusions do not provide researchers with any generalizable results, particularly regarding how participation in a rivalry statistically impacts the odds of being targeted for future digital attacks. Additionally, the authors use only Klein, Goertz and Diehl's rivalry data and not Thompson's (2001). While they note that they are only interested in dyads with the existence of militarized conflict, they fail to provide a clear theoretical reason to expect a correlation between past military conflict and the use of cyber threats in a rivalry relationship. Rivals that have not used armed conflict frequently may be just as prone to employ cyber weapons as those that have resorted to force, and Thompson's more inclusive rivalry data would have captured and even allowed differentiation among these different forms of rivalry. Finally, the authors explore just one type of cyber weapon, cyber attacks, while the possibility exists that rivals use a range of cyber weapons against one another. Despite these shortcomings, Valeriano and Maness have provided a thought-provoking addition to both the rivalry and cyber threat literature.

In sum, while scholars such as Maoz and San-Akca (2012) and Conrad (2011) have investigated the use of low-intensity forms of violence within international rivalries, the use of digital conflict between rival states has yet been studied using a broad cyber threat dataset. The research conducted by Valeriano and Maness (2014) takes an important first step toward building understanding on the issue, but additional work remains to be done. Most importantly, the full range of potential cyber threats need to be analyzed with generalizable empirical methods.

## Theoretical Development

As noted in the literature review, scholars largely agree that varying levels of armed conflict are common within international rivalries. As Thompson and Dreyer (2012) point out, “rivalry has a greater impact on increasing the probability of warfare than the democratic peace has in decreasing the probability of warfare” (17). While the importance of rivalry is unquestioned, scholars still disagree on issues such as the severity of armed attacks and the likelihood of conflict throughout the lifetime of an antagonistic relationship. Furthermore, the research conducted by Conrad (2011), Findley et al. (2012), and Maoz and San-Akca (2012) lend a unique dimension to the literature by demonstrating that states may use less conventional forms of violence, particularly terrorism and guerrilla support, against their enemies as a proxy for military combat. The purpose of this study is to determine if states embroiled in a rivalry also experience increased numbers of cyber threats.

Within the rivalry literature, there are two competing means of operationalizing the nature and conflict threshold of international antagonistic relationships. The first, and arguably most common, is the original conceptualization of rivalry formulated by Goertz and Diehl (1993) (Conrad and Souva 2011). This definition hinges of four components. The first is spatial consistency: "rivalries consist of the same pair of states competing with each other, and the expectation of a future conflict relationship is one that is specific as to whom the opponent will be" (Klein et al. 2006). In other words, the actors in rivalries are states, and all rivalries are dyadic. The second component is duration. In their original dataset, Klein and Goertz coined short-term rivalries as "proto-rivalries," and were included in the data along with enduring, long-term rivalries. For the 2006 dataset, Klein, Goertz and Diehl (2006) have dropped proto-rivalries, choosing instead to classify such relationships as isolated conflict. The third component is a history of armed conflict. As the authors note, "we saw 'rivalry relationships' as forming a particular subset of 'international relations'. We did not focus on 'relations' in general, but *militarized* and *conflictual* ones in particular" (Klein et al. 2006, 334). Finally, the last dimension of rivalries is the concept of linked conflict, in that rival states have a shared history that impacts contemporary events, and there is an expectation of conflict in the future.

In contrast to the data produced by Klein, Goertz and Diehl (2006), which is grounded on the assumption that rivals have a history of armed conflict, Thompson (2001) and Thompson and Dreyer (2012) operationalize rivalries in a different manner. According to Thompson (2001), Diehl and Goertz's original dataset and definition of rivalry falters because it, "assumes that a fairly substantial amount of militarized disputation must occur in order to create rivalry histories and futures" (569). Thompson disagrees with this approach, because it eschews the relationship of two states prior to their first military engagement. In other words, onset and termination dates of rivalries in datasets such as Diehl and Goertz are too reliant on "formal indicators" or historical events that may or may not accurately reflect when suspicions emerged between two belligerents. Thompson suggests a more "holistic" approach by interpreting historical evidence and classifying states as rivals based upon their perceptions of one another, and not solely on militarized conflict. Doing so avoids artificially censoring and truncating the rivalry data, however the construction of such a dataset also makes it less easily replicable (583). Thus, Thompson sees the coding of rivalries as a process that should categorize some competitors as threatening enemies, with a variable outcome that may include a level of explicit conflict ranging from hostile public statements to armed conflict.

As Conrad (2011) notes, "rivals always want to harm their opponents but are wary of the costs and uncertain outcomes associated with going to war, particularly given their ongoing and repeated interactions with each other" (534). Cyber threats, in the same manner as terrorism and state-sponsored guerrilla warfare, provide states with the opportunity to harm while potentially avoiding the uncertainty of war. And while the two definitions of what constitute a rivalry may differ, they both provide an incentive for the use of cyber threats. In the Klein, Goertz and Diehl definition, rivalry is defined by the presence of both armed conflict and the presence of an unresolved issue that precipitated the use of armed violence. Conrad (2011) points out that, "the characterizations of rivalries imply that even if armed conflict ends, the motivations for the initial use of force may persist. In other words, the original grievances that led to armed conflict still permeate the relationship" (533). The existence of this common issue, especially between periods of armed violence, may lead rival states to rely upon low-intensity, unconventional tactics in an effort to inflict injury upon their enemy and potentially gain an upper hand in the event of another armed confrontation. Rival states may also be targeted for cyber threats as a means of extorting concessions over the unresolved, mutual issue of contention.

Inversely, the Thompson and Dreyer rivalry definition is not founded upon a history of military conflict or the presence of a single divisive issue; instead it is based upon the presence of mutual distrust and shared animosity. Thompson (2001) "expressly avoids using armed conflict as a means of categorizing rivals and notes that rivals can involve 'latent threats' rather than actual military threats" (in Conrad 2011, 533). Thus, the possibility exists that both policymakers and military planners may rely upon unconventional tactics as a means of inflicting injury and damage on their rival's population, military, and infrastructure. More specifically, rival states may use cyber threats as a means of damaging their enemy's digital infrastructure or stealing private information with a reduced chance of discovery, and therefore a reduced chance of initiating an unwanted armed conflict. Thus, the use of cyber threats can undermine a rival's power, while increasing "uncertainty about the origin of the threat" (Kupperman et al. 1982).

The difficulty in attribution make cyber threats an optimal means of causing damage on a rival with minimal risk of precipitating armed conflict. According to Wheeler and Larsen (2007), "attribution is difficult and inherently limited. In particular, attackers can cause attacks to be delayed and perform their attacks through many intermediaries in many jurisdictions," thus hiding the true identity of the source (ES-2). This difficulty is attributed to the current architecture and policies that seek to govern the Internet. Hunker et al. (2008) note, "a combination of the Internet's architecture and the evolving administrative and governance systems that oversee the Internet make attributing a cyber attack extremely challenging" (5). In fact, attribution can be made more difficult through relatively simple tactics used by the hacker, such as deleting network logs, or as a result of system administrators being poorly trained in network security (Hunker et al. 2008). Further, attribution difficulty is supported by Gordon Snow (2011), the Assistant Director of the FBI Cyber Division, who admits that, “the current Internet environment can make it extremely difficult to determine attribution.” Ultimately, this characteristic satisfies a role in both rivalry definitions. For the Klein, Goertz and Diehl definition, attribution difficulty provides states with a means of softening their enemy and stealing private information during and between periods of armed conflict. For the Thompson and Dreyer definition, cyber threats give states the opportunity to inflict damage on their rival target without engaging in full-scale war. Cyber threats also mirror physical terrorism in that they provide the source state with “strategic ambiguity and plausible deniability,” while also providing a means of imposing costs on their target (Findley et al. 2012, 237; Conrad 2011).

In addition to the difficulty in attributing a cyber threat back to its original source, cyber threats can be used as a means of leveling the playing field between rivals of differing military power. This is a common argument made by scholars of state-sponsored terrorism. Findley et al. (2012) note that “state sponsorship of terrorism can enable a state to compensate for strategic weakness vis-à-vis rivals,” and that “states lacking the capacity to project traditional military power, or lacking strategic military assets, may actively use terrorist proxies to make up for this deficit” (237). Hoffman (2006) reiterates this point: “(terrorist) attacks are considered to be a means of offsetting a numerically superior, better-armed, and better-equipped opponent” (155). The same logic applies to the use of cyber threats. The code used to build and deploy cyber attack, cyber terrorism, and cyber espionage programs can be relatively cheap (Lewis 2010), they can pilfer much larger amounts of private information than physical espionage in a shorter period of time, they can substantially impact the economy of a targeted state (Lewis 2011), and they can have a devastating impact on civilian morale and military/state operations (Evans and Whittell

2010). In sum, weaker states with less-capable military equipment or those at a numerical disadvantage may rely upon unconventional forms of force to weaken their rivals, and help balance the terms of the next potential armed engagement.

Finally, a common trait among rivals is the large amount of time spent in the absence of armed conflict (Conrad 2011). Even during periods of peace, however, mutual grievances persist and the potential for conflict may be higher than non-rivals. As a result, rival states do not want to initiate an immediate armed conflict and must be more selective in their choice of policies towards their rival counterpart. Avenues of conventional diplomacy exist, however "states frequently choose additional military options" (Conrad 2011, 533). With the ever-increasing reliance of states on digital networks to control basic social services like communication and electric grids, the deployment of cyber threats, in conjunction with terrorism and guerrilla support, would potentially give rival states a plethora of non-military options to use during periods of relative peace to limit the potential for escalation to armed conflict.

While a theoretical and tactical justification exists regarding the use of unconventional violence in international rivalries, it should be noted that Valeriano and Maness (2014) rely upon an alternative theoretical justification for why rival states may *avoid* such low-level aggression. Despite the fact that many cyber threats are difficult to attribute to their source, Valeriano and Maness (2014) posit that, "due to the threat of retaliation and the ready possibility of actual direct combat, cyber operations will be limited in the international sphere" and between rival states (9). Thus, in contrast to the explanation above and the difficulty in attributing a cyber attack to its source (Hunker et al. 2008; Snow 2012; Wheeler and Larsen 2007), states may be reluctant to use cyber attacks in an effort to avoid "a conflict spiral and a never ending situation of continuous threats."

Despite the assertion that rival states seek to avoid conflict spirals, the use of deterrence such as threats of retaliation, alliances and military buildups often fail to obtain concessions from their enemy, and in some cases they may provoke further conflict (Hensel and Diehl 1994; Vasquez 1993). While it conflicts with their primary hypothesis, Valeriano and Maness admit that deterrence may not stop states from using more limited forms of cyber threats, such as cyber terrorism and cyber espionage. They conclude that, "rivals will tolerate cyberwar operations if they do not cross a line that leads directly into the loss of massive life," which may explain why minor acts of terror not directed at largely populated regions are common in international rivalries (Valeriano and Maness 2014, 7; Conrad 2011). Thus far, cyber threats have not been responsible for a substantial loss of life, and as noted may be an effective means of aggression between antagonistic actors without risking devolving into perpetual armed violence. This is particularly true, since cyber threats can be directed towards specific, non-vital digital networks that could cause disruption, and no causalities, in the targeted state. Their conclusion that rivals may tolerate cyberwar operations also supports the present theoretical framework, lending anecdotal support to the notion that states acknowledge they may be targeted for digital attack while engaged in an international rivalry, but may not respond unless the damage costs cross an unknown threshold.

As the literature review demonstrates, states in an antagonistic relationship are more prone to suffer terrorist attacks, and are also more apt to support guerrilla groups as a means of inflicting harm to a targeted enemy. This is founded upon the larger rivalry literature, which finds that conflict within antagonistic state relationships are statistically more likely to occur. Additionally, the present theoretical framework provides a justification that rival states have an incentive to employ cyber threats for a variety of different reasons. These reasons include inflicting damage on their rival counterpart during and between armed conflicts, providing a means of causing harm without engaging in war, plus the deniability and strategic ambiguity of cyber threats provides a minimal chance of retribution. Given the findings on the relationship between terrorist acts and rivalry, and the similar benefits of terrorism and cyber threats, we can posit:

*$H_1$: States involved in rivalries will experience an increased number of cyber threats.*

Because the most applicable study testing cyber threats and rivalry status, Valeriano and Maness, did not assess their findings using a regression analysis, this study will borrow components of the research design found in Conrad's (2011) terrorism study. The following section outlines the methods used to test the hypothesis, and operationalizes the dependent, independent, and control variables.

## Research Design

One of the more common estimation strategies in the rivalry literature, particularly those studies focused on state-sponsored terrorism and guerrilla group support, is the use of directed dyads (Findley et al. 2012). Other studies, such as Maoz and San-Akca (2012) incorporate triads which consist of the non-state armed group, the target of that group, and any potential supporters. The use of dyadic and triadic units of analysis are optimal for the study of rivalry, particularly because they aid in establishing casual links between indicators and patterns. They also allow researchers to examine the dynamic relationship of both origin countries and target countries (Findley et al. 2012). One of the drawbacks of dyads, or triads for that matter, is the substantial amount and accuracy of data required, particularly for the source state. For terrorism studies, the ITERATE dataset provides the nationality of the terrorist group suspected of committing the act of violence, giving researchers a better idea of the potential state sponsor of such violent acts.

As noted previously, despite the similar benefits between terrorism and cyber threats, it is much more difficult to identify the source of most digital assaults. Thus, while Valeriano and Maness do include the purported source of the cyber attacks analyzed in their study, one would be wise to approach their data on cyber attacks with caution. Relying on published news articles to supply the source of a cyber threat may lead researchers down the wrong path. For example, as noted previously, in 2007 a series of cyber attacks were launch against Estonia from Russian computer networks. Early published reports, especially those quoting the Estonian foreign minister, immediately placed blame for the attacks on the Russian government. However, as more information became available and the attacks were analyzed by professionals, it was eventually determined that a group of pro-government Russian youths were responsible for the attacks. While the legitimate source behind the attacks was eventually ascertained, in part because of the high-profile nature and attention given the attacks by the international media, the true source of many cyber threats remains a mystery.

Given the exceptionally difficult nature of attributing a cyber threat back to its actual source, employing a dyadic unit of analysis to study cyber threats in a rivalry situation may not be reliable. As Conrad (2011) notes in his study of terrorism, "the plausible deniability that states enjoy when supporting terrorist activities creates a similar plausible deniability in identifying those states for any data collection effort" (536). It is even more difficult to track down the culprit behind cyber activities, and this has a significant impact on the form the unit of analysis must take.

The present analysis thus focuses solely on the states that are targets of cyber attacks because target data can be deemed reliable. To test this paper's theory, the unit of analysis is the total number of cyber threats each state is targeted for each year from 1990 to 2001 or 2009, depending on the measure of rivalry being tested. The following sections outline the dependent and independent variables.

### *Dependent Variable*

The dependent variable for this study is the aggregated number of cyber threats each state sustains per year. Given that the aim of this research is to determine if states embroiled in rivalries sustain an increasing number of cyber threats than their non-rival counterparts, the cyber threat measure will not be subdivided into the specific categories of cyber attacks, cyber terrorism and cyber espionage. Theoretically, a rival state could target their enemy with all three types of digital assault, each with a specific purpose or means of inflicting economic, political or social harm.

At the time this research was conducted, no comprehensive cyber threat dataset has been developed for academic consumption. Given the sensitive nature of network security logs, many large companies and government agencies are reluctant to allow researchers access to their network data. In an effort to exhaust any possible resources of cyber threat data, every branch of the U.S. Armed Forces, the FBI, the CIA, the Department of Homeland Security, as well as private companies such as Microsoft, Google, Apple, and Symantec were contacted. All of these sources either denied the request for information or refused to return phone calls. As a result, a content analysis of published news reports was used to build a new data collection.

The cyber dataset employed in this quantitative analysis was assembled by Virtual Research Associates using automated content analysis of the Reuters Global News Service. The search was limited to attacks that occurred between January 1, 1990 and December 31, 2011. Due to the lack of a common vernacular, many search terms were used to ensure the maximum number of cases was collected. A complete list of the search terms used is available in Appendix A. Ultimately, the raw dataset includes 15,879 cases.

Once the raw dataset was complete, a process of coding was undertaken to weed out redundant cases and those that were not clear examples of cyber threats. After the raw dataset was pared down into potential cases of cyber threats, those were further investigated using the LexisNexis service. This process ensured the remaining cases were indeed examples of a cyber threat, and allowed for a clearer idea of who the target was and the legitimacy of the case. The date of the attack was also refined to ensure the correct year was listed for the beginning of the threat or its first discovery. The final, coded dataset used in this analysis contains 240 cases of international cyber threats from 1990 to 2009.

Of course, a content analysis of cyber threat cases creates a variety of problems that must be acknowledged. Perhaps the most blatant is that a successful cyber threat, especially one that seeks to steal military or economic secrets, should remain relatively unknown. The fact that knowledge of a cyber threat was published signifies one of three outcomes: an attack was originally intended to do harm and the source wanted the target to know of the attack; a failed attack was originally intended to remain a secret but was foiled prior to its execution; or a successful attack was originally intended to remain a secret, but was discovered after its execution. All three scenarios have been included in the dataset, as it can be concluded that even a failed cyber threat was intended by the source to harm the target in some fashion.

### *Independent Variables*

As noted previously, there are two definitions of rivalry that many scholars rely upon for their analysis. The first dataset, compiled by Klein, Goertz and Diehl (2006), provides an analysis of dyads with three or more militarized disputes from 1816 to 2001. This dataset is a departure from their previous operationalization of rivalry, eschewing the required minimum passage of time (10 years for proto-rivalries and 20 for enduring rivalries). As a result, the first independent variable for this analysis is a dichotomous variable indicating whether a state was in an enduring rivalry or not. The use of a dichotomous measure mirrors the technique used by Conrad (2011).

A second regression will be conducted to test an independent variable based on the Thompson and Dreyer (2012) rivalry dataset. As described earlier, this data is built using a historical analysis of state interactions, and thus contains a fewer number of rivalries than the Klein, Goertz and Diehl data. Also unlike the Klein, Goertz and Diehl dataset, the Thompson and Dreyer data covers the entire timespan of the dependent variable. This variable was built using the chronological list of rivalries found in the appendix of Thompson and Dreyer (2012). Like the first analysis, this variable will be a dichotomous measure of whether each state is engaged in at least one rivalry for each year, 1990 to 2001.

An additional set of regressions will be conducted that divert from Conrad's study. Instead of testing a dichotomous measure of rivalry participation, two variables have been created that indicate the total number of rivalries each state is involved in during each year for each rivalry definition. Thus, these independent variables allow the analysis to determine if increased rivalry participation leads to increased numbers of cyber threats, as opposed to the earlier analyses which simply measure if rivalry participation leads to increased cyber threats. In sum, four different independent variables have been created and will be analyzed to test the hypothesis: two dichotomous measures and two count measures.

It should be noted that the difference in operationalization between the two rivalry definitions creates a considerable variance in the number of rivalries each identifies. For example, Klein, Goertz and Diehl (2006) note that they, "code 183 cases that Thompson does not identify as rivalries, and Thompson codes 67 cases that we do not. These cases of disagreement are considerable and a nontrivial matter. The 67 Thompson rivalries that we do not identify comprise 39% of his cases, and the 183 rivalries in our data that he does not identify comprise 63% of our data" (346). As an example of the discrepancy in coding, Conrad and Souva (2011) cite the Nicaragua and Colombia dyad, which Klein, Goertz and Diehl code as a rivalry from 1994 to 2001. Thompson, on the other hand, does not consider this dyad to be a rivalry during that period of time. However, he does code the two states are being in an antagonistic relationship between 1979 and 1992. While the purpose of this paper is not to take a position on which measurement is more appropriate, analyzing both datasets will provide insight into whether past armed conflict or the perception of rivalry impacts the number of cyber threats a state is targeted for.

### *Control Variables*

The preceding section provides the two measures necessary to test the hypothesis. In addition, a variety of control variables must be included to ensure the analysis accurately captures the impact of rivalry on cyber threat targeting. Unfortunately, no previous research has studied cyber threats in a broad, quantitative manner. While Valeriano and Maness study the connection between cyber attacks and rivalry, they do not test their hypotheses with multivariate techniques. As a result of the lack of past quantitative research, and given the similarities between cyber threats and terrorism, this study will rely the terrorism targeting literature as a surrogate framework and adapt the common targeting factors as controls. These controls have many similarities to those employed by Conrad (2011).

***GPD Per Capita***

Of the many targeting factors studied within the terrorist literature, a state's economic strength is one of the most robust lines of research. Tavares (2004) and Piazza (2008b) find that wealthier nations are more likely to experience terrorist attacks. Tavares (p 4) notes that one of the primary objectives of terrorist groups is to damage the economy of their target and to, "impose material cost on the population as a form of pressure on the society as a whole". The findings of Tavares and Piazza are further backed by Blomberg et al. (2004). Their analysis indicates that democratic nations, in particular those with high incomes, experience high levels of terrorist activity.

Economically developed states may also be prone to cyber threats since they tend to have the type of well-developed cyber infrastructure that is vulnerable to attack. Hawkins and Hawkins (2003) found that the 32 economically-robust states that make up the Organization for Economic Co-Operation and Development (OECD) are home to 95% of the world's Internet hosts. Rogers (2000) also finds that the Internet is primarily concentrated in wealthy and well-educated urban areas. Finally, Xiaoming and Kay (2004) demonstrate that per capita wealth is a primary factor in determining the spread of the Internet in Asian nations, and there is a strong relationship between a state's GDP and Internet penetration. They conclude that, "GDP per capita indicates a country's economic strength as well as individual wealth. The deployment of the Internet is a costly venture and only countries with strong economic power are able to build the Internet in such a way that it allows access to as many people as possible" (8).[22]

[22] While data on Internet access could be used, it is extremely unreliable (van Dijk 2005).

The logged gross domestic product (per capita) data was taken from the World Development Indicators and Global Development Finance (WDI) dataset provided by the World Bank (World Bank 2013). The variable was logged to correct for a skewed distribution.

### *Military Size*

Terrorist actors tend use unconventional means precisely because they do not have the economic or military capabilities to challenge states on the traditional battlefield. For example, in a 2001 interview with a leading Gaza Muslim activist, military superiority of the opposing force was addressed. The activist, in defense of the use of suicide terrorism, explained that, “we lack the arms [planes, missiles or artillery] possessed by the enemy” (Hoffman 2006, 155). In a summary of the interview, Hoffman notes that “(terrorist) attacks are considered to be a means of offsetting a numerically superior, better-armed, and better-equipped opponent.” In other words, organizations that are faced with an opponent equipped with superior military weaponry and technology are more likely to use unconventional tactics.

Cyber threats from both states and sub-state actors may be used in a similar way – they challenge and weaken militarily superior actors. The use of cyber threats by terrorist organizations against better-equipped militaries, such as the United States and its allies, was (and still is) a particular concern during the protracted “War on Terror.” According to Vatis (2001), “the United States and its allies must operate under the premise that military strikes against terrorists and their nation-state supporters will result in cyber attacks against U.S. and allied information infrastructures” (21). In fact, the United States Department of Defense issued a report in April 2013 stating that, “as more and more state and nonstate actors gain cyber expertise, its importance and reach as a global threat cannot be overstated” (Franzen 2013). As a result of this new unconventional use of digital force, cyber threats were listed as the most pressing danger facing the U.S. in 2013.

The military size data were obtained from the World Bank WDI dataset (2013), and are logged for normality.

### *Regime Type*

Eubank and Weinberg (1994; 2001), Li (2005), Pape (2003), Rogan (2010) and Savun and Phillips (2009) have all investigated the potential link between regime type and terrorist attacks. Eubank and Weinberg (2001) notably point out that, "democracy makes it possible for dissident groups of all sizes and shapes to wage campaigns of terrorist violence," a perspective that runs counter to the view that democracies provide a peaceful means of conflict resolution (163). Eubank and Weinberg (1994; 2001) point out, however, that it is not necessarily the democratic political process that is responsible for the rise of terrorism, but rather the liberal attributes of a democracy (freedom of speech, expression, etc.) that permit dissident groups to exist. Democratic societies have a proclivity to become targets of attack because open societies allow terrorist groups to organize and carry out their attack with less chance of being noticed. These views are further expanded upon by Li and Schaub (2004) who note that, "…by guaranteeing citizen's political rights and civil liberties, democracy allows terrorist groups much greater room to maneuver, lowering the costs and risks for committing terrorism" (242).

Different views of the Internet can have a substantial impact on the ease of deploying a cyber threat, making government type a vital factor in predicting which states may be a future target. Traditionally, democratic states are far more likely to embrace the Internet as a means of communication and free expression (Milner 2006). As a result of the openness and freedom associated with the Internet in democratic states, users have the advantage of visiting any website they wish (within legal limits), have as many email accounts as they want, and open any attachment sent to them. In many cases, it is the responsibility of the end-user to have the appropriate security software available to protect their equipment from malicious code. The cheap deployment of web connectivity also means an increasing number of industries are interconnected, as well as allowing for the digital regulation of water, gas, and other vital systems. While the spread and use of Internet services has opened up new and exciting forms of communication and opportunities, it also increases the number of available targets.

In autocratic states, many leaders believe the Internet's disadvantages outweigh its benefits. According to Sussman (2000), "45 countries now restrict Internet access on the pretext of protecting the public from subversive ideas or violation of national security…they are all autocracies." Non-democratic ruling institutions also do not necessarily rely on broad public support, thus some autocratic regimes largely impede the adoption of technologies perceived as threatening (Kalathil and Boas 2003). Even though many autocratic states are suspicious of the Internet and the free exchange of ideas, some have adopted the Web as a means of spreading propaganda and improving political control. For example, China has recognized that, "future economic growth…will depend in large measure on the extent to which the country is integrated with the global information infrastructure" (Milner 2006). In order to use the Internet to propel national goals, but also limit the free exchange of ideas, the Chinese government has implemented firewalls, routers, and filters to limit what its citizens and outside users can view. When viewed in a hard/soft target framework, the Internet infrastructure in an autocratic society is likely to be considered a "hard target."

Due to the unique nature of cyber targets, access to a target must generally be easily navigable in order to deliver the virus or other malicious code. The conduit of access is, in most cases, the Internet itself. As a result, those using cyber threats must look at how different states "harden" access to the Internet and adjust their plans accordingly to attack more easily accessible targets. Thus, regime type and the nature of Internet access and Internet freedom may play a crucial role in target selection.

The regime classification data was provided by the Polity IV Project (Marshall and Jaggers 2002). The Polity IV data measures regime authority on a 21-point scale, ranging from -10 (hereditary monarchy) to +10 (consolidated democracy). Among a number of reasons, Polity IV data was used for consistency with other conflict studies (Plumper and Neumayer 2010).

### *Population*

Population is often included in terrorism studies both as a key component of the analysis or as a control variable (Krueger and Laitin 2008; Li 2005; Wade and Reiter 2007). For example, Krueger and Laitin (2008) find that population is a statistically significant predictor of terrorist origins, as well as a predictor of where terrorism would occur. Wade and Reiter (2007) include total population (logged) as a control, "following the supposition that larger states provide more targets and more areas against which to launch suicide terrorist attacks" (239).

In many regards, a larger population base also creates more opportunities and targets for states and non-state actors to attack using cyber threats. A larger population requires a larger and more sophisticated critical infrastructure for basic social services, such as electricity and water (FEMA 2011). Such complex critical infrastructure, particularly those controlled via networked workstations, opens up a wide variety of potential targets in which to inflict economic devastation. Additionally, if the goal of hackers is to create confusion and social panic, targeting states with robust populations provides a larger audience.

The measure of population included in this study, which is recorded in millions and logged for normality, comes from the Penn World Table dataset (Heston et al. 2012).

### *Geography*

Li and Schaub (2004), Li (2005) and Savun and Phillips (2009) have all included regional variables in their terrorism studies with varying success and significance. Enders and Sandler (2006) investigate geography directly by studying whether political shocks, such as the end of the Cold War and the terrorist attacks on September 11, 2001, resulted in increased terrorism in low-income countries and regions. They theorize that the 9/11 attacks resulted in a reduction of available, high-level targets in wealthy nations. As a result, terrorists have sought out targets in poor nations and specific regions (particularly the Middle East and Asia) where U.S. interests were readily accessible. Because of the conflicting results of previous studies and the shear lack of attention geography has received, Savun and Phillips (2009) state outwardly in their analysis that they could not develop a theoretical expectation regarding how regional variation could impact the likelihood of terrorism.

In this study, geographic measures are included partly as a means of absorbing cultural factors such as the adoption of the Internet and other targeted technologies (Savun and Phillips 2009). In his discussion of the Internet, David Nye (2006) points out that, "people adapted the Internet to a wide range of social, political, economic, and esthetic contexts, weaving it into the fabric of experience. Every culture continues to make choices about what to do with this new technology" (63). Indeed, the physical specifications of the Internet are virtually identical throughout the world, but the adoption, adaption, and social construction of the Internet may vary extensively due to cultural inclinations.

The inclusion of regional dummies is an established means of absorbing cultural variation within the terrorist targeting literature. As a result, this paper will replicate the technique used by Li and Schaub (2004) and include a regional dummy for each continent on the globe, excluding Antarctica. The regional dummies used in this research will differ slightly from those of Li and Schaub, as North and South America will be divided into individual indicators. Given the expectation that the United States is the most targeted state in the world, North America will be excluded from the analysis and used as a comparison case for the other regional dummies.

### *Media Bias*

Because the independent variable is a content analysis of media reports provided by Reuters, a variable is included to control for any potential media bias that may exist in each state. The variable is a count of the total number of articles from Reuters concerning each country in each year of the analysis (Murdie and Peksen 2013). The natural log of the control is used for normality.

Table 3.1 below provides the descriptive statistics of the variables used in the analysis.

## *Methodology*

The event data captures a relatively rare event, documented cyber attacks on countries. A series of statistical tests were performed, include Vuong (Vuong 1989) residual plots, and the AIC statistics (Long and Freese 2005), all of which confirm that a zero-inflated negative binomial is preferable over the standard negative binomial estimate.

After selecting the ZINB model, tests were conducted to ensure the model was correctly specified. A Durbin-Watson test determined that the model suffers from autocorrelation. To remedy this issue, a single lagged version of the dependent variable was added to the model as a control variable (Davis 2007).[23] A variance inflation factor (VIF) test also indicates that no serious multicollinearity exists.

Additionally, given that the data is clustered by state, a means of accounting for group-level variation was undertaken. In particular, when confronted with clustered or grouped data,

**Table 3.1 Summary Statistics**

| | Obs. | Mean | Std. Dev. | Min. | Max. |
|---|---|---|---|---|---|
| Cyber Threats | 3,754 | .07 | .72 | 0 | 24 |
| Klein, Goertz & Diehl (Dichotomous) | 2,212 | .46 | .50 | 0 | 1 |
| Klein, Goertz & Diehl (Count) | 2,212 | 1.10 | 2.41 | 0 | 39 |
| Thompson (Dichotomous) | 3,754 | .30 | .46 | 0 | 1 |
| Thompson (Count) | 3,754 | .49 | .98 | 0 | 6 |
| GDP per capita (logged) | 3,586 | 7.80 | 1.64 | 4.16 | 12.13 |
| Military Size (logged) | 3,515 | 10.54 | 1.87 | 3.91 | 15.24 |
| Regime Type | 3,169 | 2.76 | 6.75 | -10 | 10 |
| Total Population – 2011 (logged) | 3,493 | 1.91 | 1.88 | -3.20 | 7.19 |
| Media Bias (logged) | 3,579 | 5.85 | 2.24 | 0 | 12.37 |

[23] Without the lagged dependent variable, the Durbin-Watson statistic for all five models averaged 0.90. By including the lagged dependent variable as a control in each model, the Durbin-Watson statistic increased to roughly 2.20.

many scholars rely on fixed effects models (Clark and Linzer 2012). The results of a Hausman specification test were statistically significant at the .05 level, indicating that fixed effects should be used. A comparison of a fixed effects and basic ZINB models demonstrate some differences in both the significance and signs of the coefficients. Despite these differences, however, the ZINB specification is better suited to the present analysis. Fixed effects are unable to estimate the effect of variables that vary across individuals but not over time. In the case of the two independent variables, some states are in a constant number of rivalries throughout the studied period. Additionally, control variables such as regime type and geography may vary across states, but they have little or no within-state variation. Provided that the ZINB estimation more accurately models an excessive number of zeros in the dependent variable, and STATA is unable to estimate a ZINB model with fixed effects, the basic ZINB specification was deemed to be the optimal choice.[24]

Finally, in a fashion similar to a logistic regression, additional techniques are required in order to appropriately interpret the results of a ZINB model. The range of techniques used by researchers to interpret similar models include incidence rate ratios (Conrad 2011; Savun and Phillips 2009) as well as more complex Monte Carlo simulations (Piazza 2011). For the purposes of this research, two different means of interpretation will be implemented. For the dichotomous measures of the primary independent variables, incidence rate ratios (IRRs) will be used. For the more complex count measures of the independent variables, the regression results will be interpreted using IRRs as well as marginal effects (Dreher et al. 2010; Santifort-Jordan and Sandler 2014). In the cases where marginal effects are used, the global mean of the control variables will be used to calculate the estimation. However, it should be noted this technique

[24] The fixed effects model results are provided in Table B.1 and Table B.2 in Appendix B.

only provides an estimate of the “average state” and may not necessarily reflect the targeting likelihood of a particular state. To aid in interpretation and to demonstrate the wide variation between the means of an average state and those of the United States, specialized marginal effects are reported throughout.[25]

## Results

Table 3.2 below presents the first set of findings. Both models incorporate a dichotomous measure of rivalry, a technique similar to the analysis conducted by Conrad (2011).[26] While the analysis conducted by Findley et al., (2012) used dyads as a unit of analysis, their primary independent variable is also the presence of a rivalry between two states. Thus, one could consider their independent variable dichotomous as well, given that any given pair of states are either in a rivalry or they are not. Both studies find robust evidence that states in an antagonistic international relationship are more likely to sustain increased numbers of terrorist attacks than non-rivalry states, and supporting their hypotheses that rivalries can be defined by low-level conflict, as well as more deadly armed conflict.

Unlike the past terrorism studies, the results in the present analysis demonstrate a negative relationship between the use of cyber threats and participation in a rivalry. The first model tests the definition of rivalry prescribed by Klein, Goertz and Diehl (2006). The results show a state involved in a rivalry will see a decline in the number of cyber threats by a factor of

[25] Marginal effects charts for the five models can be found in Appendix B.

[26] Both models are studies of cyber threats from 1990 to 2001. Despite the fact that the Thompson and Dreyer data is coded to 2010, limiting Model 2 allows for a more accurate comparison with the Klein, Goertz and Diehl dataset which ends in 2001.

.20, holding all over variables constant. This finding is statistically significant at the 1% level of confidence. The second model, testing the definition of rivalry established by Thompson and

**Table 3.2 ZINB Dichotomous Estimates of Cyber Attack Event Counts**

| | Model 1 | | Model 2 | |
|---|---|---|---|---|
| | Coefficient | IRR | Coefficient | IRR |
| *Inflated Negative Binomial* | | | | |
| Enduring Rivalry – Binary (1990-2001) | -1.62***<br>(-2.87) | 0.20 | - - - | - - - |
| Strategic Rivalry – Binary (1990-2001) | - - - | - - - | -2.33***<br>(-3.57) | 0.10 |
| GDP per capita (logged) | -0.01<br>(-0.03) | 0.99 | -0.04<br>(-0.19) | 0.96 |
| Military Size (logged) | -0.37<br>(-0.72) | 0.69 | -0.50*<br>(-1.80) | 0.61 |
| Regime Type | -0.03<br>(-0.79) | 0.97 | -0.08**<br>(-2.34) | 0.92 |
| Total Population (logged) | 0.58**<br>(2.28) | 1.79 | 0.23<br>(1.15) | 1.25 |
| Media Bias (logged) | 1.28*<br>(1.86) | 3.60 | 2.33***<br>(5.81) | 10.30 |
| Geography – South America | -22.83***<br>(-19.87) | 0.00 | -17.90***<br>(-17.22) | 0.00 |
| Geography – Europe | -0.87<br>(-1.14) | 0.42 | -0.72<br>(-1.03) | 0.49 |
| Geography – Africa | -26.83***<br>(-26.22) | 0.00 | -23.33***<br>(-24.50) | 0.00 |
| Geography – Asia | 0.92<br>(1.46) | 2.52 | 2.65***<br>(4.20) | 14.23 |
| Geography – Oceania | 1.39**<br>(2.16) | 4.01 | 1.22**<br>(1.98) | 3.39 |
| Lagged D.V. | 0.01<br>(0.64) | 1.01 | -0.01<br>(-1.55) | 0.99 |
| Constant | -9.79***<br>(-2.82) | 0.00 | -17.07***<br>(-4.87) | 0.00 |
| *Inflated Logit* | | | | |
| State involved in rivalry? – KGD | -1.27<br>(-1.59) | -1.27 | - - - | - - - |
| State involved in rivalry? – Thompson | - - - | - - - | -7.09**<br>(-2.19) | -7.09 |
| GDP per capita (logged) | 0.54<br>(0.95) | 0.54 | 1.72**<br>(2.06) | 1.72 |
| Military Size (logged) | -0.52<br>(-0.55) | -0.52 | -1.93**<br>(-2.27) | -1.93 |

| | | | | |
|---|---|---|---|---|
| Regime Type | 0.04<br>(0.46) | 0.04 | 0.09<br>(1.29) | 0.09 |
| Total Population (logged) | 1.70**<br>(2.47) | 1.70 | 5.31**<br>(2.33) | 5.31 |
| Media Bias (logged) | -2.14**<br>(-2.08) | -2.14 | -2.51**<br>(-2.48) | -2.51 |
| Lagged D.V. | -0.56<br>(-1.17) | -0.56 | -0.35*<br>(-1.81) | -0.35 |
| Constant | 15.55*<br>(1.74) | 15.55 | 11.78<br>(1.47) | 11.78 |
| *Model N* | *1,460* | *1,460* | *1,463* | *1,463* |

* p < .10, ** p < .05, *** p < .01 (Z Scores in parentheses), Two-Tail Test; (Regional dummies not reported)

## Table 3.3 ZINB Count Estimates of Cyber Attacks

| | Model 3 | | Model 4 | | Model 5 | |
|---|---|---|---|---|---|---|
| | Coefficient | IRR | Coefficient | IRR | Coefficient | IRR |
| *Inflated Negative Binomial* | | | | | | |
| Enduring Rivalry – Count (1990-2001) | -0.20**<br>(-2.06) | 0.82 | - - - | - - - | - - - | - - - |
| Strategic Rivalry – Count (1990-2001) | - - - | - - - | 0.35<br>(1.36) | 1.42 | - - - | - - - |
| Strategic Rivalry – Count (1990-2009) | - - - | - - - | - - - | - - - | 0.52*<br>(1.78) | 1.69 |
| GDP per capita (logged) | -0.23<br>(-0.57) | 0.80 | -0.66<br>(-1.10) | 0.52 | 0.20<br>(1.33) | 1.22 |
| Military Size (logged) | -0.43<br>(-0.84) | 0.65 | -1.11**<br>(-2.28) | 0.33 | 0.01<br>(0.03) | 1.01 |
| Regime Type | -0.06**<br>(-2.01) | 0.95 | -0.06<br>(-0.85) | 0.94 | 0.04<br>(1.17) | 1.05 |
| Total Population (logged) | 0.25**<br>(2.50) | 1.29 | -0.13<br>(-0.37) | 1.14 | 0.04<br>(0.13) | 1.04 |
| Media Bias (logged) | 1.65***<br>(2.87) | 5.19 | 1.98*<br>(1.94) | 7.26 | 0.44***<br>(3.37) | 1.55 |
| Lagged D.V. | -0.05*<br>(-1.78) | 0.95 | -0.02<br>(-1.24) | 0.98 | 0.01<br>(0.69) | 1.01 |
| Constant | -8.69<br>(-1.60) | .000 | -0.19<br>(-0.06) | 0.83 | -7.17***<br>(-2.27) | 0.00 |

| | | | | | | |
|---|---|---|---|---|---|---|
| *Inflated Logit* | | | | | | |
| Enduring Rivalry – Count (1990-2001) | -0.21**<br>(-1.63) | -0.21 | - - - | - - - | - - - | - - - |
| Strategic Rivalry – Count (1990-2001) | - - - | - - - | 0.27<br>(1.02) | 0.27 | - - - | - - - |
| Strategic Rivalry – Count (1990-2009) | - - - | - - - | - - - | - - - | 0.45<br>(1.56) | 0.45 |
| GDP per capita (logged) | 0.10<br>(0.20) | 0.10 | -0.36<br>(-0.57) | -0.36 | -0.17<br>(-0.76) | -0.17 |
| Military Size (logged) | -0.14<br>(-0.22) | -0.14 | -0.81<br>(-1.19) | -0.81 | -0.08<br>(-0.18) | 0.08 |
| Regime Type | 0.04<br>(0.67) | 0.04 | 0.02<br>(0.18) | 0.02 | 0.08<br>(1.46) | 0.08 |
| Total Population (logged) | 0.60*<br>(1.83) | 0.60 | 0.44<br>(1.17) | 0.44 | -0.18<br>(0.48) | -0.18 |
| Media Bias (logged) | -0.86<br>(-1.45) | -0.86 | -0.44<br>(-0.41) | -0.44 | -0.42*<br>(-1.68) | -0.42 |
| Lagged D.V. | -0.71**<br>(-2.28) | -0.71 | -0.82<br>(-1.48) | -0.82 | -1.68<br>(-1.49) | -1.68 |
| Constant | 8.16<br>(1.04) | 7.01 | 16.22**<br>(2.41) | 16.22 | 7.56<br>(1.41) | 4.27 |
| *Model N* | *1,460* | *1,460* | *1,463* | *1,463* | *2,511* | *2,511* |

** p < .10, ** p < .05, *** p < .01  (Z Scores in parentheses),  Two-Tail Test*

Dreyer (2012) supports the conclusions from the first model. The analysis demonstrates that rivalries based on the perception of antagonism and not necessarily on a history of armed conflict reduce the number of cyber threats by a factor of .10. This finding is also statistically significant at the 1% level, holding the control variables constant.

When using marginal effects, the true impact of rivalry on cyber threat targeting becomes apparent, especially for the United States. First however, the results show that, when analyzing Model 1 using global means for the control variables, a state that shifts from being in no rivalries to being in at least one will experience negligibly fewer cyber threats. More specifically, it is predicted that a state in no rivalry will experience .0000000152 cyber threats annually from 1990 to 2001, while those states that do engage in a rivalry will experience .00000000987 annual cyber threats. This exceptionally marginal decline is attributed to the rare nature of cyber threats across much of the globe, especially during the 1990s and early 2000s. While the average number of cyber threats a "typical" state experiences declines only marginally when moving from non-rivalry to rivalry status, the impact is much more substantial for a state like the United States. When the U.S. average value for each control variable is substituted for the global values, the results show that moving from non-rivalry to rivalry participation will reduce the number of cyber threats against the U.S. by 22.65 events. Considering the United States sustains an average of 7.2 cyber threats per year, with a maximum number of 24 attacks in a single year, a decline of almost 23 events is substantial.

The marginal effects of Model 2 provide similar conclusions to Model 1. When averages for the United States are tested, the results show a drop of 20.85 cyber threats per year when moving from a status of non-rivalry to rivalry. Much like the first model, the decline in cyber threats for the average state are negligible. The average global state not participating in international rivalries could expect to be targeted for .000000174 cyber threats per year, while those in a rivalry are targeted for an average of .0000000252 threats per year.

The first two models represent a replication of the analysis conducted by Conrad (2011), particularly by reproducing the dichotomous measure of rivalry status and implementing similar controls. While the results of the current analysis do not support the conclusions of Conrad (2011), Findley et al. (2012) and Maoz and San-Akca (2012), specifically that rival states use low-level unconventional tactics during periods of peace, further study may shed additional light on the subject. Table 3.3 presents an initial step toward a more nuanced understanding of the relationship between rivalry and cyber threats. Models 3 and 4 expand upon a dichotomous measure of rivalry participation and specifies the number of rivalries each state is engaged in per year. Thus, Table 3.3 allows us to see the impact that participation in multiple rivalries has on cyber threat targeting, as opposed to the earlier analyses which simply models participation as a yes/no choice.

Table 3.3 provides the findings for Models 3 through 5.[27] Model 3 and Model 4 test a measure of rivalry from Klein, Goertz and Diehl as well as Thompson and Dreyer from 1990 to 2001. As noted previously however, these measures count the number of rivalries each state is in during each year of the analysis. The results for Model 3 show an increase in one rivalry will decrease the number of cyber threats by a factor of .82. For the "average country," this decrease is exceptionally marginal, much like Models 1 and 2. However, for a country like the United States, which is engaged in between 3 and 11 rivalries depending on the given year, the results are more noteworthy. The marginal effects predict that an increase from three rivalries to four will decrease the number of cyber threats by 2.8. This decrease becomes smaller, however, as the U.S. engages in more rivalries. For example, moving from ten rivalries to eleven only reduces the predicted number of cyber threats by .7 events.

While Model 3 shows a negative relationship between rivalries and cyber threats, the Thompson and Dreyer measure of rivalry tested in Model 4 paints a different picture. The results of Model 4 suggest that no statistically significant relationship exists between rivalries based on perception and cyber threat targeting. However, marginal effects results demonstrate that this relationship is statistically significant for the United States. Specifically, from 1990 to 2001, the United States engaged in one or two rivalries. The marginal effects results show that

[27] These models were run without regional dummies, due to a failure to find convergence. The omission of control variables from zero-inflated models as a result of a failure to find convergence is common in the literature (Findley and Young 2010; Morris and Slocum 2012). Negative binomial models with regional dummies also failed to converge, potentially as a result of the excessive number of zeros in the dependent variable.

moving from one rivalry to two will increase the predicted number of cyber threats by 1.96 events annually. From 1990 to 2001, the United States sustained an average of 6.1 cyber threats per year. Thus, an increase in one rivalry would raise the number of cyber threats by almost 32%.

Models 5 in Table 3.3 tests the same event count independent variables, but it expands the temporal range of the Thompson and Dreyer data from 1990 to 2009. This regression was conducted in order to take advantage of the full Thompson and Dreyer data, as well as incorporate more of the cyber threat data. The latter is particularly important, considering that cyber threats have continued to increase in volume throughout the studied period. Because the Klein, Goertz and Diehl measure is only coded from 1990 to 2001, extrapolating an additional eight years of data from the original twelve may have produced suspect results. As a result, the Klein, Goertz and Diehl measure was omitted.

Interestingly, the increased temporal range has shifted the Thompson and Dreyer measure from statistically insignificant to significant at the 10% level. Model 5 shows that an increase in one rivalry will increase the number of cyber threats by a factor of 1.68 events, holding all other variables constant. For the United States, which experienced between one and three rivalries per year between 1990 and 2009, an increase in one rivalry would result in an average of 3.83 additional cyber threats. Given that the United States averaged 5.8 cyber threats per year from 1990 to 2009, an increase in one rivalry could potentially increase the average number of cyber threats in the U.S. by 66%. When substituting global averages for the marginal effects analysis, an increase in one rivalry would result in approximately .001 additional cyber threats. However, the marginal effects show that only states that experience between zero and three rivalries are statistically more likely to be targeted for additional cyber threats.

# Discussion

The results of the ZINB analysis provide insight into the use of alternative forms of low-level conflict in international rivalries. Before now, such studies focused primarily on the use of state-sponsored terrorism and guerrilla warfare within antagonistic relationships, all of which found a positive relationship between such tactics and rivalry participation. The singular study, up to this point, which investigated cyber attacks and rivalries found that deterrence may be responsible for a decline in cyber threats amongst rivalry dyads. The present study, which expands upon the earlier work of Valeriano and Maness (2014) and adapts the general analytical framework of the terrorism studies, finds varying support for the hypothesis that states engaged in rivalries are more likely to experience increased numbers of cyber threats.

Models 1 through 3 lend statistical evidence to the argument made by Valeriano and Maness, namely in that rivalry participation is likely to reduce cyber threat targeting. The authors provide a series of explanations why this may be true, with the most convincing being that many governments, particularly the United States, consider cyber attacks to be an act of war. Thus, given the rationalist argument that war is both costly and risky, states may choose to avoid using cyber tactics to prevent an escalation of tension (Fearon 1995). This is in direct opposition to the results of studies such as Findley et al. (2012) and Conrad (2011), which find that rival states use terrorism as a proxy for armed conflict. However, as noted by Findley et al., rival states may actually tolerate a certain level of terrorist activity. Thus, given the relatively new and unknown impact that cyber threats may have, we can speculate that states have yet to define a "tolerable threshold" of damage sustained during a cyber threat that may warrant a more violent response. As a result, rivals are unwilling to use such tactics in fear of inciting a broader conflict than they had not originally prepared for. This is in contrast to physical terrorism, which given the findings of Findley et al. (2012) and Conrad (2011), many rival states seem to tolerate at a certain level without armed retaliation.

Alternatively, it is possible that states engaged in enduring rivalries have built up their cyber defenses, thus hardening any potential digital targets. This maneuver could be a result of their suspicious attitude toward rivals, whom have been willing to engage in armed conflict in the past. Thus, if states are willing to meet on the battlefield over a common issue, there may be very little incentive not to engage their rival in the digital domain as well. It is possible that states understand this threat, and have bolstered their digital defense as a proactive measure. Additionally, states in enduring rivalries may be wearier of admitting to the media that they were targeted for a cyber threat. Such media attention would provide both the source rival, and other potential rivals, with greater knowledge of the target state's security vulnerabilities.

While the findings of Models 1 through 3 support the conclusions made by Valeriano and Maness, the incorporation of an event count measure of rivalry participation somewhat complicates matters. Model 3, which tests the Klein, Goertz and Diehl definition, finds that increases in rivalry participation reduce the number of cyber threats a state will experience, backing the theoretical foundation of the earlier cyber attack study. However, the definition of rivalry proposed by Thompsons and Dreyer (states are rivals if they perceive each other to be hostile) ultimately produces different results. Models 4 and 5 show that an increase in rivalry participation results in an increase in cyber threat targeting, which refutes the deterrent theory of Valeriano and Maness and supports the terrorism studies of Findley et al. and Conrad. A potential explanation for the different findings is the varying definition of what constitutes a rivalry.

As noted, Thompson and Dreyer rely on a detailed analysis of the historical record to determine if animosity exists between two states. While this method results in fewer identified rivalries than the Klein, Goertz and Diehl data, such relationships are not necessarily defined by a history of armed conflict. As Fearon (1994) points out in his crisis bargaining analysis, "If crises are characterized by private information and costly signaling, then states will 'select themselves' into or out of crises according these prior beliefs, and this fact will have implications for subsequent inferences and choices" (245). In sum, Fearon's bargaining perspective asserts that past military engagement unveils previously-held information from both actors in a dyad that each had wanted to keep private. This information includes their willingness to engage in armed conflict. For the Klein, Goertz and Diehl definition of rivalry, such states are included in the dataset only if they have a history of repeated prior military conflict. Thus, these states have a better idea of each other's willingness to engage in armed conflict. This may explain the negative relationship between rivalry participation and cyber threat targeting found in Models 1 and 3, as states are unwilling to provoke a rival into a broader conflict.

Inversely, Thompson and Dreyer's measure of rivalry is not predicated on a history of armed conflict, but merely on the perception of national leaders towards a perceived enemy. That is not to say that these rival states do not engage in armed conflict, but it is not a necessary component to be included in the dataset. Given Fearon's assertion that past military conflict provides each state with private information, particularly the point at which each actor is willing to engage in war, the method of coding employed by Thompson and Dreyer may explain the positive relationship between rivalry status and increased cyber threat targeting. As Models 4 and 5 demonstrate, states that are coded as being perceived as rivals but not necessarily engaging in past military conflicts are more likely to be targeted for cyber threats. This may be a result of increasing levels of withheld private information by each state; such private information includes their willingness to engage in combat. Given that two perceived foes have less information about each other, such states may be more willing to use cyber threats in ignorance of their target's tolerance of violence. Alternatively, the lack of armed conflict may increase the number of "soft targets" which are more accessible for cyber threats. The armed conflict experienced by enduring rivals may have compelled states to harden their networks and implement other means of defense.

Finally, the overall significance of the control variables, and the use of terrorism as a framework for the study of cyber threats, should be noted. Surprisingly, the GDP per capita measure was statistically insignificant in every model except one, although the one significant result in Model 2 demonstrates the expected positive relationship between cyber threats and economic robustness. Military size and regime type are also relatively poor predictors of cyber threats in these models, as they are only significant in two models each. The results for military size both show that increases in military size reduce cyber threats, suggesting that larger militaries are more capable of defending against digital assaults. Additionally, the significant regime type findings demonstrate that democratic states are less likely to experience cyber threats, lending evidence to the notion that digital attacks may be a weapon of the repressed and used against autocratic regimes. And lastly, the population control is statistically significant in three models, and suggests that more populous states are more likely to be targeted by cyber threats.

As the general lack of significance for many of the controls show, the use of the terrorism targeting literature as a framework is not necessarily the most appropriate means of studying cyber threats. With that being said, however, given that the study of cyber threats is still in its infancy, and the characteristics of targeted states has yet to be established, incorporating general state characteristics such as regime type, GDP per capita, population and military spending are *currently* the best means to study digital threats. In the future, additional factors such as Internet penetration rates, broadband usage, and other specific digitally-related indicators should be included. Unfortunately, at the time of this research, many of those variables are unreliable and are limited both temporally and spatially (van Dijk 2005). Researchers should not be discouraged from studying cyber threats due to limited data access, but rather should adapt previous research and theoretical frameworks until such time as a dedicated cyber threat research agenda can stand on its own.

## Conclusion

The historic examples of communication vulnerabilities outlined in the first chapter provide a wealth of instances in which international rivalries play a role in targeting as well as the development of more advanced communications technology. For example, according to Steele and Stein (2002, 31), "as Great Power rivalry reemerged in the latter part of the nineteenth century, competition in telegraph communications was one domain for that rivalry." The authors note that British domination of cables, as well as a fear of espionage, spurred the French and Germans to develop their own competing telegraph systems. However, in time those states began to establish their own espionage programs, especially prior to World War I. In particular the French heavily targeted the transmissions of Germany, which was a rival with whom France had several previous military engagements (Headrick 1991). Thus, interstate rivalries and a fear of espionage not only impacted which states adopted telegraph technology, but rivalry also influenced the targets of newly-established espionage programs. Another example, as noted in the previous chapter, was the Soviet jamming of Western radio signals in an effort to prevent contact with West Berlin and to prevent the spread of free information in Soviet-controlled areas. While such targeting may have been partly the result of ideological differences, those differences were a principle foundation of the rivalry that persisted between the U.S. and Soviet Union throughout the Cold War.

Building upon the historic examples of the early 20th century, the results produced by this analysis help shed light on the impact of rivalry situations and the exploitation of 21st century communication technology. In particular, this study provides statistical support for earlier research on cyber threats in rivalry situations, as well as building upon terrorism research by exhibiting the similarities and differences between these two unconventional forms of violence. This paper also demonstrates that the definition of rivalry and the measurement style of that indicator can have a dramatic impact on a study's results.

Ultimately, this research was designed as a "first cut" into the quantitative study of cyber threats and international rivalries. As a result, a host of additional questions have yet to be answered. For example, this research lends credibility to the argument that cyber threats are used by states in tense, potentially volatile interstate relationships. The next logical step is to study the impact of cyber threats in crisis bargaining situations, principally to determine if cyber threats have any effect on states' decisions to engage in armed combat. Such a study would incorporate the bargaining theory literature, which was briefly touched upon earlier. Additionally, more in-depth case studies should be conducted on rival states and their use of cyber threats. An excellent example would be the relationship between Pakistan and India, states which have engaged in armed conflict and tense standoffs in the recent past, are considered perpetual rivals, and have been known to use cyber threats against each other. Alternatively, the rivalry between Argentina and Great Britain is worthy of study, as these rival states have not fought a war since the beginning of the Information Age, but have recently used cyber attacks against rival targets.

In sum, the quantitative study of cyber threats is still in its infancy. However, each study that is conducted, using both qualitative and quantitative methods, helps to clarify a largely unexplored subject. While a large-scale cyber war has never, and hopefully will never occur, research such as this helps to prepare states for potential digital assaults by detecting targets, identifying where such attacks may originate, and where security should be bolstered to defend against such attacks. Given the exceptional harm that cyber threats could unleash against an increasingly digitized world, it is important for scholars to establish and build upon a robust research agenda focused on unraveling the many unanswered questions that surround digital vulnerabilities. This research, and the research that came before it, are hopefully only the first wave of studies investigating this 21st century security threat.

# Chapter 4 - The Impact of Cyber Espionage on International Crisis Bargaining

In 2005, network security professionals in the United States detected a significant increase in cyber espionage activity originating from mainland Chinese servers. As military and civilian personnel investigated the intrusions further, the objective and damage of the attacks became more and more startling. According to published reports, hackers in the Chinese province of Guangdong had secretly assaulted U.S. military, government, and contractor computer networks for several years in complete secrecy (Crowell 2010, 16). The information taken by the hackers included sensitive documents, some of which were related to the F-35 fighter project overseen by Lockheed Martin (Clarke and Knake 2010). Ultimately, it was concluded that “Titian Rain,” the designated name for the attacks, resulted in a loss of between 10 and 20 terabytes of digital information from U.S. servers. To put the loss of information into more concrete terms, if a human were to physically steal the amount of information taken digitally during Titan Rain, the accumulated documents would total ten copies of the *Encyclopedia Britannica* (that’s 32 volumes and 44 million words, ten times over) (Clarke and Knake 2010).

The example of Titan Rain is just one of many cases of cyber espionage that have exposed states’ private information to a host of international actors, including rival states. While cyber espionage and other cyber attacks have been widely investigated through case studies and a handful of quantitative studies, the impact of cyber espionage on state interactions has yet to be addressed. To remedy this research oversight, the focus of this study will be to investigate whether the loss of private, digital information – particularly through cyber attacks – can impact the decision of rational state leaders to engage in armed conflict. In order to study this complex topic, a theoretical foundation will be built upon the crisis bargaining model. As the next section will address, one of the central tenants of the crisis bargaining model is the assumption that peaceful relations between states can break down because of the incentive to misrepresent and withhold private information. This paper will seek to determine if states targeted for cyber attacks and cyber espionage cases, such as Titan Rain, will seek peace more often than their untargeted counterparts due to the release of private information which provides clarity on the two states' bargaining range.

The following research will proceed in six parts. The next section outlines the crisis bargaining model, with a particular emphasis on the findings of Fearon (1995) and those scholars who have adapted the crisis bargaining model in their own research. The second section provides an investigation of cyber espionage, and the information that can exposed through such attacks. The third section contains a description of the variables to be tested, followed by the analysis results and a discussion of the findings. The final section will conclude, and provides direction for additional research.

## Information and War

The crisis bargaining model is a widely used means of investigating the interaction between states, and in particular why those interactions may lead to armed conflict. According to the common rationalist perspective of conflict, there are five contributing factors that may lead to the outbreak of war: 1.) anarchy; 2.) expected benefits greater than expected costs; 3.) rational preventative war; 4.) rational miscalculation due to lack of information; 5.) rational miscalculation or disagreement about relative power. Of these five potential causes, Fearon (1995) broadly notes that "the standard rationalist arguments fail to either address or to adequately explain what prevents (rational) leaders from reaching ex ante bargains that would avoid the costs and risks of fighting" (380). Through a process of elimination, Fearon eventually parses the list down to two primary causes of bargaining breakdowns: "private information about relative capabilities or resolve and incentives to misrepresent such information," as well as the inability to uphold a bargain (381).

The first rationalist mechanism that leads to interstate conflict, and the focus of this paper, is the incentive of rational states to misrepresent private information. Such private information includes the willingness to engage in combat, as well as military strength and new weapon technology. Because states have an incentive to avoid war, they should also have a desire to obtain a favorable resolution to the issue of contention. As a result, Fearon (1995) predicts that states, "have an incentive to exaggerate their true willingness or capability to fight" (395). Doing so provides states with both short-term and long-term advantages, including the possibility of concessions from an existing foe and deterring future challengers. Thus, even though states should rationally seek peace, they may be willing to exaggerate or misrepresent private information if it accomplishes a greater end. While this implies that rational states are seeking a peaceful resolution through the misrepresentation of information, it could also trigger the war they were aiming to avoid. Additionally, states have an incentive to conceal hidden capabilities or resolve, particularly if such information would make them militarily vulnerable. As Fearon (1995) states, "combined with the fact of private information, these various incentives to misrepresent can explain why even rational leaders may be unable to avoid the miscalculations of relative will and power that can cause war" (396).

The link between asymmetric information exchange and bargaining breakdowns is further addressed by Goemans (2000), who points out that, "if both sides knew how the pie would be divided after the war, both would be better off if they divided accordingly before the war" (24). With this in mind, Powell (2002) further explains Fearon's (1995) theory. In his example, two states ($S_1$ and $S_2$) engage in a series of bargaining moves. In this game, $S_1$ can make a take-it-or-leave-it offer to $S_2$, which has the option to accept the offer (maintain peace) or reject it (engage $S_1$ in war). If the states were to have complete information, then $S_1$ can safely make the maximum acceptable demand of $S_2$ without risking armed conflict. Without complete information however, which is typically the case in a bargaining situation, $S_1$ may demand more than $S_2$ is willing or able to give. As a result, $S_2$ has only two choices: initiate another round of bargaining or militarily engage $S_1$. This example demonstrates how private information, and the incentive to misrepresent information, creates inefficiencies in bargaining situations and could ultimately lead to conflict.

In terms of the quantitative study of asymmetric information and crisis bargaining, scholars have relied upon a variety of proxies to measure both formal and informal information exchange between states. As Bell (2013) notes, "a central dilemma associated with this literature results from the difficulties in empirically testing many of the theoretical models that point to information and uncertainty as important conditioning factors in the march to war" (453). Despite this difficulty, scholars have come up with innovative means to conceptualize the exchange of information during bargaining situations. At a very specific level, scholars have focused attention on intangible state information that can be gathered by outside actors. Namely, these state characteristics include power (Bearce et al. 2006; Reed 2003), resolve (Fearon 1994; 1997; Morrow 1989) as well as domestic political conditions (Smith 1996; Tarar 2006).

First, with regard to state power, the dynamic relationship between dyadic power parity and information has been analyzed by Reed (2003) among a number of others (Fey and Ramsay 2011; Reed et al. 2008). The author starts with the assumption of past studies, which often show that dyads of states which are power preponderant are often more peaceful than those at power parity. However, in contrast to this common argument that the distribution of power is a central cause of conflict, Reed (2003) maintains that "uncertainty about the distribution of power is as important a predictor of the probability of conflict as is the observed balance of power" (633). Through the use of Bayesian statistics to evaluate the credibility of this bargaining model, Reed is able to demonstrate that as states approach parity, information asymmetries are at their highest point. Thus, this information asymmetry is a contributing factor in the increased chances of conflict between at parity dyads.

Bearce et al. (2006) also investigate state power, particularly by integrating the impact of joint military alliances on the spread of information both within the alliance, and the signal it sends to outside actors. The authors follow Leeds (2003), who noted that alliance participation provides information to external actors, and expand upon that proposition by theorizing alliances could provide even more information to internal participants. Resting their theoretical framework on the premise that asymmetric information exchange can lead to conflict, the authors find that participation in alliances does indeed impact information exchange. This impact, however, is conditional. Their analysis demonstrates that, within alliances, information exchange matters most for dyads of states at or near parity. Theoretically, these are states that have the highest degree of information asymmetry, and are the most likely to engage in armed conflict due to a bargaining breakdown. Inversely, for power preponderant dyads of states where the outcome of a military engagement would be relatively certain, the environment of information exchange provided by an alliance is less important. This is due to the reduction of asymmetric information inherent in a power-preponderant relationship.

In addition to state power, audience costs and resolve are also pieces of information that can expose both state and leadership weaknesses as well as the willingness to fight or seek peace. As an example, Fearon (1994) investigates how audience costs influence international dispute escalation, particularly focusing on how states' leaders are impacted by domestic political conditions. In a formal analysis that estimates that "crises are public events carried out in front of domestic political audiences," Fearon (1994, 577) finds that audience costs do in fact have an impact on the decisions leaders make regarding conflict escalation. Notably, the analysis suggests that leaders who are most sensitive to audience costs are always the least likely to back down in disputes that become public contests. As far as crisis bargaining is concerned, the model demonstrates how state structures might impact signaling and information exchange. For example, if mobilizing troops produces a higher audience costs for democratic leaders than for their authoritarian counterparts, then it is conceivable that democratic states would be less likely to bluff through a physical display of force. Ultimately, audience costs are in some circumstances a visible display of resolve, and can play an important role in information exchange during crisis bargaining situations.

Coupled with the idea that domestic audience costs can impact leadership decisions, domestic political conditions can send signals to outside actors regarding state resolve to engage in armed conflict. In his investigation of diversionary foreign policy, Smith (1996) points out that electoral prospects can have a significant impact on the foreign policy decisions of democratically elected leaders. For example, when reelection is assured, rational leaders are able to make unbiased policy decisions, taking into consideration only international factors. This is also true when a government has no prospect of being reelected. However, Smith's model supports the idea that when foreign policy decisions could impact the prospect of reelection, governments are more likely to engage in violent foreign policy objectives. As a result, outside states that may be the target of such aggression tend to be more conciliatory and less confrontational during periods of uncertain election outcomes (Clark 2003; Mitchell and Prins 2004). Smith's model shows that state information, when it is exposed through election cycles, can impact the behavior of other states, particularly when violent diversionary actions are possible.

While the state characteristics of power, resolve and domestic political conditions provide hints regarding the available bargaining range and therefore the willingness of the state to engage in conflict, the outward exposure of these characteristics are privy to the level of state external transparency. External transparency "allows other states to observe political events and other state characteristics" (Bell 2013, 457). Thus, in order for outside actors to gauge the power, resolve, and domestic political conditions of a bargaining partner, some level of external transparency must be present.

Defining what constitutes external transparency, and whether it is synonymous with democratic regimes, has produced a wide range of findings. For example, Hollyer et al. (2011) point out that the presence of elections alone is not enough to sufficiently classify a state as democratic, and that transparency must be included as a part of defining political regimes. They point to the case of the U.S. State Department and their reaction to the Wikileaks scandal, which "makes clear that democratic governments strategize according to, rely upon, and even promote the degree of obfuscation they enjoy in policymaking" (Hollyer et al. 2011, 1193). Hollyer et al. define transparency as the willingness of a government to release policy-relevant information, and they find that democratic states are inherently more transparent than their autocratic counterparts. Thus, a minimalist definition of democracy (initially introduced by Schumpeter in

1942) actually covers more than just the presence of elections, given the relationship between information transparency and free elections.

The link between external transparency and crisis bargaining was further investigated by Bell (2013). In his study, Bell assumes two key elements from the bargaining literature and adapts them to study strategic conflict avoidance. First, interstate conflict results from a breakdown in bargaining between states. If perfect and complete information were available to both sides, a visible bargaining space preferred by both actors would always be present. Second, negotiated outcomes acceptable to both parties can be complicated by information asymmetries and uncertainty (Bell 2013). With these foundations in mind, Bell explains that externally transparent states are inherently at a disadvantage in terms of information asymmetry during bargaining situations, given the difficulty in withholding and misrepresenting such private information. As a result, Bell hypothesizes that externally transparent governments are less likely to initiate conflict, particularly for diversionary purposes. Through a large-N study, Bell shows that external transparency levels may impact whether states initiate MIDs, and therefore contributes to both the crisis bargaining as well as the diversionary theory literatures.

Of course, not all recent findings support the bargaining model. Some formal approaches have produced results that run counter to bargaining assumptions. Slantchev (2003) offers one prominent example by investigating war as a process of bargaining, not as the outcome of bargaining failure.[28] What makes Slantchev's model unique is his approach in studying a set of actor's actions during conflict. He points out that, "Once war is disaggregated from a lottery over exogenous outcomes into a process where war aims arise endogenously, it is possible to make a subtle distinction between two types of costs that are associated with conflict: the ability

[28] This idea harkens back to Clausewitz's definition of war as a continuation of politics by other means.

to bear costs and the ability to impose costs" (123). This new approach to studying war allows for the possibility that states "condition negotiation strategies on their performance in the war and that such strategies depend on their ability to impose costs in unforeseen ways" (124). Ultimately, Slantchev finds that, despite the assumption of complete information, war is still possible because states utilize conditional strategies that "make war aims dependent on actions in the model" (131).

While formal models such as Slantchev's continue to add important nuance to our understanding of the bargaining process, empirical literature to date has been largely supportive of Fearon's (1995) rationalist explanations for war (Danilovic and Clare 2010). However, the previous research focuses on intangible state characteristics that may influence asymmetric information exchange, such as power, domestic political conditions, and external transparency. In other words, research up to this point generally includes state characteristics that cannot be easily manipulated by other states. Instead, the characteristics of power, regime type, external transparency, etc. are domestic attributes and may be, for some states, largely time-invariant. Additionally, as noted in the external transparency literature, the type of political regime has a major impact on the kind of information that is exposed to the outside world, and what kind of information can be used during crisis bargaining situations. While the previous literature has certainly expanded our understanding of conflict outbreak, the research conducted in this paper will take a different approach to information exchange. Instead of assuming states can, to some degree, control the private information that is exposed to outside forces, the present analysis will determine if private information that is unwillingly and forcefully exposed through cyber attacks can impact states' propensity for conflict.

## Cyber Attacks and Information Exposure

The scholarly literature focused on cyber attacks and information loss is relatively sparse. This is particularly true of the cyber espionage literature. Cyber espionage is the theft of private information from government, military, corporate and personal computer networks (Fidler 2012; Guisnel 1997; Lewis 2011). Guisnel (1997) offers one of the few book-length investigations of cyber espionage. Despite the book's age, Guisnel provides an excellent history of primitive electronic espionage in the early 1990s, as well as a description of how states and corporations may employ computers to extract large volumes of digital secrets from rival computer networks for personal gain. The author points out that, "in the United States and Canada, threats by foreign powers against companies within both countries are perceived as threats to their national interests" (Guisnel 1997, 212). While Guisnel addresses how U.S. and Canadian intelligence communities combat potential economic losses, he spends very little time discussing the interests of other states and the potential loss of information they face.

A series of more recent publications has addressed potential government responses to acts of cyber espionage. These responses range from classifying it as "just spying" to treating it as a potential act of cyber warfare (Fidler 2012). Focusing specifically on the United States, Lewis (2011) notes that a massive overhaul of computer security regulations is needed to stay ahead of hackers. A Center for Strategic and International Studies (CSIS) notes that, "the Internet provides nation-states, their intelligence agencies, and cyber criminals with vastly expanded capabilities to illicitly acquire information. Economic espionage does the most damage: other nations steal technology, research products, and intellectual property" (Lewis 2011, 2). What has yet to be addressed, however, is how this loss of private information impacts relations between states and their propensity for conflict.

While acts of cyber espionage are most often attributed with a loss of private information, the nature of that private information can vary greatly. For example, at the most extreme level, cases such as Titan Rain can lead to the loss of massive amounts of sensitive or even classified data. Exceptional acts of cyber espionage are, of course, not limited only to the United States. On March 20, 2013 South Korean computer networks were targeted by a sophisticated espionage campaign that was believed to have originated in North Korea. The attack was accomplished by unleashing a piece of malicious code which "extracted classified information, including data related to U.S. forces in South Korea and military exercises carried out jointly by American and South Korean troops" (Gayathri 2013). According to a report released by McAfee Labs, the attack was designed explicitly to gather intelligence on military networks. Additionally, the malicious code may have been in operation since 2009, leaving terabytes of private information in danger of being stolen.

While some attacks are focused on classified military information, others target the economic assets of private businesses. A 2013 McAfee report on cyber espionage breaks malicious cyber activity down into six parts: "the loss of intellectual property and business confidential information, cybercrime, the loss of sensitive business information (including possible stock market manipulation), opportunity costs (including service and employment interruptions), the additional costs of securing networks, and reputational damage to the hacked company" (3). When combined, the global financial loss is roughly $400 billion a year. While the global GDP was roughly $70 trillion in 2011, a particularly costly act of cyber espionage against a nationalized industry could substantially impact the GDP of a smaller nation.

The same report further addresses the potential damage to national security by economic espionage. It notes that, "the theft of military technology could make nations less secure by strengthening potential opponents or harming export markets in aerospace, advanced materials, or other high-tech products" (4). Furthermore, the McAfee staff point out that acts of cyber espionage also improve cyber warfare capabilities. Finally, cyber espionage can "shift the terms of engagement in favor of foreign competitors" (4). For the United States, the loss of sensitive, proprietary information via cyber espionage has led to "extensive damage" among the U.S. private technology firms involved with stealth, missile and nuclear capabilities (17). Thus, it is clear that while some cases of cyber espionage do not actively target government servers, as they did in Titan Rain or the South Korean attacks of 2013, attacks directed at business interests can have a substantial impact on the security of states and the private information they possess as well.

In addition to the loss of private information via cyber espionage, other types of cyber threats can result in a release of information. A cyber attack is the use of cyber capabilities by state-based actors against the infrastructure of other states. There is little doubt, especially in the United States, regarding the serious nature of cyber attacks against both private and government computer networks. According to Martin Libicki, a senior management scientist at the Rand Corporation, cyber attacks are an "unprecedented threat to U.S. national security" (U.S. Congress 2013). For example, the U.S. security company Mandiant has determined that a branch of the Chinese military has been infiltrating the computer systems responsible for regulating critical U.S. infrastructure, such as electric power grids and gas lines (Langfitt 2013). According to Dan McWhorter, who oversees one of the company's intelligence units, "If you have the ability to steal the documents, you could have just as easily crashed the hard drives. From a national security standpoint, that's very scary" (Langfitt 2013). Thus, while the aim of a hacking operation may not necessarily be the extraction of digital information such as blueprints or other sensitive data, hackers do learn that aspects of the target state's network infrastructure is vulnerable. This is tactical information that could be put to use, especially during bargaining situations: the targeted state knows it has potentially devastating security vulnerabilities, and the source state knows it can exploit that vulnerability if conflict is initiated. Finally, the targeted state would be unable to misrepresent the robustness of its digital security, particularly if the vulnerability is published by the press. Ultimately, both cyber espionage and cyber attacks expose private information, both tangible and intangible, that could be used against the targeted state in a crisis bargaining situation.

Given the nature of cyber attacks and their ability to expose private information, the bargaining model provides an excellent framework from which to test the impact of the involuntary disclosure of private information on interstate conflict. This proposition can be adapted to fit Powell's earlier example of inter-state bargaining. Acts of cyber espionage and other cyber attacks can expose states' private information, creating an atmosphere where either $S_1$ can safely make a maximum demand of $S_2$, or where $S_2$ knows the relative strength of $S_1$'s willingness to engage in armed conflict if the demand is rejected. This scenario is, however, dependent entirely on which state is targeted by the cyber threat. In other words, if $S_2$ is the targeted state, $S_1$ can make the maximum demand since it has additional information $S_2$ would have preferred to remain private. If $S_1$ is targeted (either before or after the demand), $S_2$ may be able to determine the foe's willingness to fight. Ultimately, both war and inefficiency are results of asymmetric information. And while the present study cannot investigate crisis bargaining as a dyadic relationship, due to the exceptional difficulty in attributing cyber attacks to their true source (see Crenshaw 2012), the basic example explained here provides a framework in which cyber attacks may increase the amount of information that is available during the bargaining process, thereby reducing inefficiencies and reducing the outbreak of conflict.

Slantchev's (2003) results support the theoretical foundation of this study as well. Slantchev (2003) suggests that, "The process of war can be usefully viewed as a contest, in which both sides attempt to reduce the opponent's ability to impose costs on them while simultaneously trying to impose costs on the opponent, thereby improving their own bargaining position" (127). Although Slantchev's models address bargaining during conflict, the same "contest" can exist prior to the outbreak of war. The use of espionage and other tactics (in the case of this paper, cyber attacks and cyber terrorism) could easily be used by belligerents in an ex ante bargaining situation to both impose costs on the enemy (steal information) as well as reduce the opponent's ability to impose costs on them (use that information to increase defenses where necessary, increase one's bargaining range, etc.). As Schelling (1966) points out, "the power to hurt…is a kind of bargaining power." Cyber threats do hurt, although the damage is not always visible. The damage can come in the form of a reduction in morale, the loss of information, a loss of tactical advantage, or a reduction in the targeted state's bargaining leverage. Thus, if one subscribes to Fearon's (1995) theoretical framework and the findings of Schelling and Slantchev, it could be said that the denial of the ability to hurt will undermine the bargaining position of the opponent. This assertion strikes at the heart of this research, and ultimately sums up the primary hypothesis:

> $H_1$: A state that is targeted for cyber espionage or other cyber threat will suffer a loss of private information, and therefore will engage in fewer armed conflicts.

While the bargaining theory posits that conflict is less likely when information asymmetry is reduced, it is possible that states targeted for cyber threats may engage in more non-combat international disputes. The use of non-combat options to retaliate against states which engage in unwanted cyber activity may be an option some states would consider, but it is of course one that runs the risk of increasing tension. For example, the United States and its allies have imposed a series of increasingly harsh economic sanctions against Iran for its sponsorship of terrorist organizations and the continued development of a nuclear program. These actions have increased tension between Iran and the Western coalition, however that tension has not manifested as armed combat. In the same vein, as cyber attacks become more and more sophisticated and as the amount of information loss grows, it is understandable that targeted states begin to press the suspected attack source to cease their activities. In a 12-page report submitted to Congress in 2011, the Pentagon noted that it would, "respond to hostile attacks in cyberspace as we would to any other threat to our country" (Alexander 2011). One such response would be the use of force short of war or conflict (Blechman and Kaplan 1978; Fordham and Sarver 2001), such as threats, mobilizations, etc. against the suspected source of the attack (Sanger and Bumiller 2011). These options have already been discussed by U.S. officials for use against the Chinese government. However, in 2011, President Obama decided against such measures as to avoid increasing international tension and as to not damage the economic ties between the two states.

Considering the bargaining theory proposition that asymmetric information exchange reduces armed conflict, we must still conclude that states targeted for cyber attacks (including cyber espionage) may retaliate via non-armed means. These means include public condemnation, troop mobilizations, and border fortifications which may heighten tensions between states, which are not intended to result in armed conflict. Thus, given this prospect, we can hypothesize that:

$H_2$: A state that is targeted for cyber espionage or other cyber attacks will suffer a loss of information, and will engage in more international, non-armed disputes.

The next section outlines the variables used to tests these propositions, followed by a presentation and analysis of the results.

## Research Design

As noted above, this study explores the impact of information exposure through cyber threats on conflict participation. Because data attributing many cyber threats to their original source is notoriously unreliable, the model described below is based upon a state-year unit of analysis. The data in this analysis ranges from 1990 to 2005 because of the limitations of various datasets, and encompasses 149 states.

### *Dependent Variables*

Three dependent variables will be analyzed to test the hypotheses previously described. The first dependent variable will be the total number of interstate wars each state is involved in per year using the Correlates of War (COW) data (Gleditsch et al. 2002). The data encompass interstate conflicts from 1816 to 2007, however the temporal range for this study will be limited to the 1990-2005 time period. In order to classify as an interstate war, the conflict must involve sustained combat, involve organized armed forces, and result in at least 1,000 battle-related combatant fatalities within a twelve-month period (Sarkees and Wayman 2010). Additionally, for a state to be coded as a participant in an interstate war, it must either commit 1,000 troops to the war or suffer 100 battle-related deaths. This measure is used to test the first hypothesis, namely that cyber attack targeting reduces participation in bloody, large-scale conflicts due to information loss.

While the most common measure of conflict arguably comes from the Correlates of War project, other measures exist and are used in the international relations literature. Most notably, the UCDP/PRIO dataset classifies armed conflict as: “a contested incompatibility that concerns government and/or territory where the use of armed force between two parties, of which at least one is the government of a state, results in at least 25 battle-related deaths” (Themner and Wallensteen 2013). As Gleditsch et al. (2002) point out, there are disadvantages to the COW definition of conflict. Namely, there are several protracted conflicts that have accumulated more than 1,000 deaths over the course of the event, however no single year of the conflict breaks the 1,000-casualty threshold. As a result, these conflicts are not included in the COW dataset. With the lower, 25-casualty threshold, the UCDP/PRIO dataset can capture these events for study. Given that this study is only interested in interstate conflicts, only conflicts between internationally recognized states will be included in the dataset. This measure of conflict will also test the first hypothesis.

The third dependent variable also comes from the Correlates of War project, and was incorporated into a wide variety of the IR literature, including Bell’s (2013) study of conflict and bargaining. The COW Militarized Interstate Dispute data (MID) contains interstate incidents from 1816 to 2010 (Ghosn, Palmer and Bremer 2004). These incidents are coded on a scale from 1 to 5 based on the dispute’s level of hostility, ranging from “no militarized action” (1) to “join interstate war” (5). Because this measure is used to test the second hypothesis, namely that states targeted for cyber attacks are more prone to enter non-violent disputes, MIDs classified as “4” and “5” have been dropped from the dataset. As a result, this variable measures non-violent actions such as threats, alerts, and mobilizations.

### *Independent Variables*

At the time this research was conducted, no comprehensive cyber threat dataset has been developed for academic consumption. Given the sensitive nature of network security logs, many large companies and government agencies are reluctant to allow researchers access to their network data. As a result, Virtual Research Associates, who used an automated content analysis of the Reuters Global News Service, assembled the independent variables included in this analysis. The search was limited to cases of cyber attacks that occurred between January 1, 1990 and December 31, 2011. Due to the lack of a common vernacular, many search terms were used to ensure the maximum number of cases was collected. A complete list of the search terms used is available in Appendix A. Ultimately, the raw dataset includes 15,879 cases.

Once the raw dataset was compiled, a process of coding was undertaken to weed out redundant cases and those that were not clear examples of cyber threats. For example, one of the search terms was “Cyber,” which resulted in a large number of cyber attack, cyber terrorism, and cyber espionage cases. Unfortunately, it also returned a large number of cases focused on the Sony “Cybershot” camera. Such cases were removed from the dataset. After the raw dataset was pared down into potential cases of cyber threats, those were further investigated using the LexisNexis service. This process ensured the remaining cases were indeed examples of a cyber threat, and allowed for a clearer idea of who the target and, occasionally, suspected source of the threat was. The date of the attack was also refined to ensure the correct year was listed for the beginning of the threat or its first discovery.

Of course, a content analysis of cyber threat cases creates a variety of problems that must be acknowledged. Perhaps the most blatant is that a successful cyber threat, especially one that seeks to steal military or economic secrets, should remain relatively unknown. The fact that knowledge of a cyber threat was published signifies one of three outcomes: an attack was originally intended to do harm and the source wanted the target to know of the attack; a failed attack was originally intended to remain a secret but was foiled prior to its execution; or a successful attack was originally intended to remain a secret, but was discovered after its execution. All three scenarios have been included in the dataset, particularly since the publication of a security breach is a public acknowledgement that private-information exposure has occurred.

The primary independent variable for this study was derived from the coded cyber data. This variable is the aggregate number of cyber espionage cases each state sustains per year. This measure is operationalized based upon the definitions of cyber espionage provided by Guisnel (1997), Fidler (2012), and Lewis (2011), and encompass cases where private, digital information was stolen or released to the public against the will of the target. Cyber espionage exposes private information at varying levels of confidentiality and demonstrates that security vulnerabilities exist in the targeted state's digital network infrastructure. Such vulnerabilities could be exploited in the event of armed conflict.

In addition to the total number of cyber espionage cases per year a state experiences, a separate analysis will be conducted which includes the sum total of cyber warfare and cyber terrorism cases each state experiences from 1990 to 2005. Cyber warfare is defined as cases where there is substantial evidence the attack was sponsored or initiated by a national government or military. Inversely, cyber terrorism cases encompass those where the suspected source was a non-state group, such as Anonymous. By including the sum number of cyber warfare and cyber terrorism cases, this variable can measure how varying digital vulnerabilities impact the likelihood of conflict. As noted above, cyber warfare and cyber terrorism may not necessarily result in the loss of tangible, sensitive information, however it does provide outside actors with knowledge of security vulnerabilities. With the increasing reliance of industrialized nations on computers and other networked technology to provide basic human services such as water and electricity, not to mention the military application of such networked services, exposing vulnerabilities in such systems most certainly could be defined as a loss of private information that states could no longer misrepresent.

## *Control Variables*

Given the scarcity of quantitative cyber attack research, and the unique approach it provides on asymmetric information exchange, a comparable analysis has yet to be produced from which to glean basic control variables. As a result, this analysis will borrow controls from the conflict and bargaining theory literature, in an effort to ensure the relationship between conflict propensity and cyber attack targeting is being appropriately measured. It should be noted, however, that because the present model is based on a country-year framework, many dyadic indicators of conflict cannot be included. These dyadic indicators include similarity in preferences, sometimes measured via UN voting affinity (Gartzke and Jo 2002), as well as specific measures of geographic contiguity. Despite these omissions, there are still several controls that can be added to build the strongest model possible.

### *Regime Type*

The first control variable in the model is regime type. The inclusion of regime type helps to satisfy several possible contributing factors of interstate conflict involvement. First, audience costs have been demonstrated to impact how states initiate or respond to threats. Fearon (1994) noted that, “because it is easier to punish leaders in democracies than in autocracies, democratic leaders should on average face greater audience costs than autocratic leaders, other things equal” (Tarar and Leventoglu 2009, 819). In other words, democratic leaders are better able to signal their willingness and resolve to fight than their autocratic counterparts, lending evidence to the idea that public commitments are both a means of credibly conveying information and can be used as bargaining leverage (Fearon 1997; Schelling 1960). A number of empirical studies, including Eyerman and Hart (1996), Gelpi and Griesdorf (2001), and Prins (2003), have demonstrated that democratic regimes are more susceptible to varying levels of audience cost.

In addition to audience costs, regime type is also an indicator of external transparency. As noted earlier, external transparency can impact the amount of private information that is exposed to outside actors. This private information includes public support for the national leadership, the size and determination of the opposition, as well as the general preparedness for potential conflict. Bell's (2013) finds that such external transparency limits democratic leaders' ability to engage in diversionary tactics by limiting their bargaining range. As noted earlier, Hollyer et al.'s (2011) analysis of external transparency concluded that democracies are inherently more transparent than their autocratic counterparts.

In order to control for the natural transparency of most democratic states, coupled with the impact of audience costs on leadership signaling, regime type is included as the first control variable. It is anticipated that as regimes grow more democratic, their conflict propensity diminishes because of bargaining space increases. The regime type variable will be borrowed from the Polity IV project, which categorizes each state based on a 21-point scale (-10 being a hereditary monarchy to +10 being a consolidated democracy).

### *Contiguity*

In addition to regime type, territoriality can have a significant impact on conflict propensity. More specifically, territorial disputes have been demonstrated to be especially prone to escalate (Reiter 1999; Souva and Prins 2006). This monadic model includes a measure indicating each state's total number of contiguous neighbors by land or sea. It is assumed that states with a larger number of borders have a greater likelihood of being involved in a territorial dispute with a neighbor, thereby heightening the chances of conflict. The contiguity data for this project was borrowed from the COW project (Correlates of War Project; Stinnett et al. 2002).

### *Military Capabilities*

In addition to contiguity, which gives states an opportunity to initiate and participate in conflict, it is important to measure a state's military capabilities (Lai and Slater 2006; Most and Starr 1989). Accordingly, COW's Composite Index of National Capabailties (CINC) score is included in the model to control for disparity in military capabilities across the interstate system. The CINC score is an average of six measures of a state's power: total population, urban population, military personnel, military expenditures, primary energy consumption, and iron and steel production. The natural log of the CINC score is used, both for normality and to "capture the declining marginal effects of increases in power" (Quackenbush and Rudy 2009, 275).

### *Alliances*

The literature regarding the impact of alliance membership on conflict is mixed (Prins 2010), however some models suggest that alliance membership can increase the risk of war (Leeds 2003; Ray 1990; Senese and Vasquez 2004). Alliances may, for example, "embolden members to engage in conflict with the belief that they have a network of states to support them" (Lai and Slater 2006, 120). And, as noted earlier, alliance participation can have an impact on information exchange. The present measure was derived from the dyadic COW data on alliance membership, and is the total number of alliances a state is a member of per year.

### *Intergovernmental Organization Participation*

Much like the alliance literature, research focused on state participation in intergovernmental organizations (IGOs) has produced mixed results. Oneal and Russett (1999) find that MID involvement is reduced by shared memberships in IGOs, while Gartzke et al. (2001) find that IGO membership increases low-level conflict. More recently, Anderson et al. (n.d.) find that the relationship between IGO membership and conflict propensity is impacted by a temporal element. Notably, their results find that IGO membership during the Cold War reduced the likelihood of militarized conflict, but increased conflict in the post-Cold War era. Because of the potential impact of IGO membership on interstate conflict, country-year IGO membership data was borrowed from the Correlates of War Project and included as a control variable. The variable is measured as the total number of IGO memberships per state, per year from 1990 to 2005.

### *Economic Interdependence*

Economic interdependence also has an impact on the likelihood of interstate conflict. Although Russett and Oneal is include this variable as a fundamental leg of their Kantian peace triangle, a number of studies find evidence that raises questions about the pacifying notion of economic interdependence (Goldsmith 2013; Kleinberg et al. 2012; Prins 2010). Some studies even suggest interdependence may be associated with higher levels of conflict (Goldsmith 2013). A greater value of trade may thus have the potential to either decrease or increase a state’s conflict propensity. Economic interdependence (trade) is operationalized as imports plus exports divided by GDP in this study (Prins 2010). The COW national trade data supplied the import and export statistics, while GDP data was taken from the World Bank. The natural log of this variable is used for normality.

### *Prior Military Activity*

States that have used force and initiated conflict in the past may be more prone to use similar tools in the future (Levite, Jentleson and Berman 1992). As a result, a lagged dependent variable will be included to control for past military activity.[29] Additionally, including a lagged dependent variable controls for the effects of autocorrelation (Beck and Katz 1995).

### *Media Bias*

Because the independent variable is a content analysis of media reports provided by Reuters, a variable is included to control for any potential media bias that may exist in each state. The variable is a count of the total number of articles from Reuters concerning each country in each year of the analysis (Murdie and Peksen 2013). The natural log of the control is used for normality.

## *Methodology*

As demonstrated in Table 4.1, interstate wars and MIDs are rare events in the post-1990 timeframe. Given the overabundance of zeros in the sample, an ordinary least squares (OLS) model is inappropriate for all three measures. OLS models also allow for negative values; this assumption is not theoretically compatible with the dependent variables tested in this analysis. Given the limitations and assumptions of OLS models, more appropriate regression models were needed to accurately measure the relationship between interstate conflict and information loss. Since the COW measure of conflict is binary (one either participates in a war or not), and rare, a rare event logistic model is used. King and Zeng (2001) note that conventional logistic

[29] While Oneal and Russett (2001) suggest including lags for three years to adequately capture the complex temporal interaction between states, the relatively low number of years investigated in the present study necessitates a single lag to avoid losing too much information.

**Table 4.1 Summary Statistics**

| | Obs. | Mean | Std. Dev. | Min. | Max. |
|---|---|---|---|---|---|
| Correlates of War (COW) | 2,980 | 0.02 | 0.13 | 0 | 1 |
| PRIO | 2,980 | 0.04 | 0.19 | 0 | 1 |
| Militarized Interstate Disputes (MID) | 3,051 | 0.29 | 0.73 | 0 | 8 |
| Cyber Espionage | 2,980 | 0.02 | 0.25 | 0 | 7 |
| Cyber Attacks & Cyber Terrorism Sum | 2,980 | 0.04 | 0.47 | 0 | 17 |
| Regime Type | 2,556 | 2.58 | 6.81 | -10 | 10 |
| Contiguity | 2,984 | 5.72 | 3.46 | 0 | 29 |
| CINC (logged) | 2,971 | -7.34 | 2.47 | -13.82 | -1.69 |
| Alliances | 3,006 | 1.65 | 2.08 | 0 | 21 |
| IGO Membership | 2,984 | 56.96 | 22.29 | 1 | 129 |
| Economic Interdependence (Logged) | 2,592 | -0.57 | 0.66 | -3.57 | 3.94 |
| COW (Lagged) | 2,785 | 0.02 | 0.13 | 0 | 1 |
| PRIO (Lagged) | 2,785 | 0.04 | 0.19 | 0 | 1 |
| MID (Lagged) | 2,858 | 0.29 | 0.73 | 0 | 8 |
| Media Bias (logged) | 2,844 | 6.07 | 2.22 | 0 | 12.37 |

regressions tend to “sharply underestimate the probability of rare events,” and are “grossly inefficient for rare events data” (137).

The second dependent variable, PRIO interstate conflict, is also analyzed using a rare event logistics model. While the dataset includes six country-years where states are involved in more than one interstate war, the variable’s exceptionally low variance prevented a convergence while attempting a ZINB model. As a result, the PRIO measure of conflict was recoded as a dichotomous measure.

The third dependent variable tests a slightly parsed version of the MID dataset. In particular, those events coded as a use of force or war were removed from the data. While MIDs classified as threats and displays of force are far more common than interstate war, they are still relatively rare. Since a number of states engage in more than one MID during a given year of the sample, this dependent variable is analyzed using a zero-inflated negative binomial (ZINB) model. A Vuong test (Vuong 1989), residual plot, and AIC statistics (Long and Freese 2005) all indicate that the ZINB model is preferable over the standard negative binomial estimate as well as both the standard Poisson and rare event Poisson models.

Additional tests are also conducted to ensure that my estimates are correctly specified. Durbin-Watson tests determined that the MID and PRIO models suffered from autocorrelation. A single lagged version of the dependent variable was added to each model to remedy the issue (Davis 2007). As noted above, there are strong theoretical reasons to include such a variable in all six models. Additionally, all three models are clustered by the state. Hausman specification tests were conducted to determine if fixed or random effects models should be employed to account for the group-level variation. The Hausman test results for all the models suggest fixed effects should be implemented. A comparison of rare event and fixed effect models for the

COW and PRIO measures resulted in identical coefficient significance for three of the four models.[30] Because of the similarity between the two and the rare nature of interstate conflict, the rare event logit was deemed more appropriate. For the MID model, STATA is unable to include fixed effects as a parameter in a zero-inflated negative binomial. Standard fixed effects negative binomial estimates produce results consistent with the ZINB model. ZINB estimates are considered preferable given the rarity of MIDs. Lastly, variance inflation factor (VIF) tests were run and indicate that probabilistic levels of multicollinearity did not exist in any of the models.

Finally, the coefficients of rare event logistic and ZINB models cannot be interpreted as easily as those in an OLS. Scholars have used a wide variety of techniques to facilitate interpretation, including incidence rate ratios (IRRs) (Conrad 2011; Savun and Phillips 2009) and Monte Carlo simulations (Piazza 2011). Marginal effects are employed in this study (Dreher et al. 2010; Santifort-Jordan and Sandler 2014). In an effort to distinguish between the findings of an "average state" and a hegemonic state, like the U.S., specialized marginal effects will be reported throughout.

## Results

Empirical results are presented in Tables 4.2 and 4.3. Table 4.2 provides the results of Models 1 through 4, which test the COW and PRIO definitions of war. Table 4.3 contains models 5 and 6, which test the impact of cyber espionage and cyber attacks/terrorism on short of war MIDs. The results of these models demonstrate varying support for the theory and hypotheses outlined previously.

[30] The fixed effects results can be found in Appendix C, Tables C.1 and C.2.

Model 1 tests the impact of cyber espionage cases on interstate war, as defined by the Correlates of War project. The rare event logit results demonstrate that an increase of one cyber espionage case will decrease the number of COW interstate wars by a factor of .65. Marginal effects with global averages shows that an increase in one cyber espionage case will decrease the number of interstate wars by .44 events. More specifically, an average state that experiences seven cases of cyber espionage (the maximum number of events in a single state-year in the dataset) is predicted to be involved in three less interstate wars than a similar state that

**Table 4.2 Correlates of War (COW) & PRIO Interstate War Rare-Event Logistic Results**

| | Model 1<br>*COW War* | Model 2<br>*COW War* | Model 3<br>*PRIO War* | Model 4<br>*PRIO War* |
|---|---|---|---|---|
| Cyber Espionage | -0.44**<br>(-1.99) | - - - | 0.70***<br>(7.04) | - - - |
| Cyber Attack & Terrorism | - - - | -0.03<br>(-0.32) | - - - | 0.33***<br>(8.63) |
| Regime Type | -0.08*<br>(-1.89) | -0.08*<br>(-1.83) | -0.04*<br>(-1.73) | -0.04*<br>(-1.66) |
| Contiguity | -0.09**<br>(-2.00) | -0.07<br>(-1.47) | -0.04<br>(-1.13) | -0.04<br>(-1.22) |
| Alliance Participation | 0.11**<br>(1.96) | 0.07<br>(1.43) | -0.26***<br>(-3.93) | -0.23***<br>(-3.57) |
| CINC (logged) | 0.15<br>(0.71) | 0.13<br>(0.62) | 0.51**<br>(2.49) | 0.49**<br>(2.36) |
| IGO Membership | 0.01<br>(0.69) | 0.01<br>(0.71) | 0.01<br>(0.57) | 0.01<br>(0.53) |
| Economic Interdependence (logged) | -0.40*<br>(-1.79) | -0.33<br>(-1.53) | -0.54*<br>(-1.92) | -0.57**<br>(-1.98) |
| COW (lagged) | 0.33<br>(0.27) | 0.30<br>(0.24) | - - - | - - - |
| PRIO (lagged) | - - - | - - - | 5.41***<br>(10.17) | 5.45***<br>(10.19) |
| Media Bias (logged) | 0.56**<br>(2.10) | 0.50*<br>(1.94) | -0.13<br>(-0.71) | -0.13<br>(-0.68) |
| Constant | -7.97**<br>(-2.13) | -7.75**<br>(-2.08) | -1.50<br>(-0.53) | -1.69<br>(-0.59) |

** p < .10, ** p < .05, *** p < .01 (Z Scores in parentheses), Two-Tail Test*
*Model 1 & 2 N = 2,126; Model 3 & 4 N = 2,126*

## Table 4.3 Militarized Interstate Dispute (MID) Zero-Inflated Negative Binomial Results

| | Model 5 | | Model 6 | |
|---|---|---|---|---|
| | Coefficient | IRR | Coefficient | IRR |
| *Inflated Negative Binomial* | | | | |
| Cyber Espionage | .02<br>(0.42) | 1.02 | - - - | - - - |
| Cyber Attack & Terrorism | - - - | - - - | 0.03<br>(1.42) | 1.03 |
| Regime Type | -0.01<br>(-0.52) | 0.99 | -0.01<br>(-0.47) | 0.99 |
| Contiguity | 0.03**<br>(2.13) | 1.03 | 0.03**<br>(2.33) | 1.03 |
| Alliance Participation | 0.02<br>(1.60) | 1.02 | 0.02<br>(1.55) | 1.02 |
| CINC (logged) | 0.04<br>(0.46) | 1.04 | 0.04<br>(0.45) | 1.04 |
| IGO Membership | -0.00<br>(-0.51) | 1.00 | -0.00<br>(-0.47) | 1.00 |
| Economic Interdependence (logged) | 0.10<br>(0.81) | 1.10 | 0.10<br>(0.86) | 1.11 |
| MID (lagged) | 0.19***<br>(3.79) | 1.20 | 0.18***<br>(3.61) | 1.20 |
| Media Bias (logged) | 0.20**<br>(2.49) | 1.22 | 0.19**<br>(2.42) | 1.21 |
| Constant | -1.90<br>(-1.64) | 0.15 | -1.85<br>(-1.61) | 0.16 |
| *Inflated Logit* | | | | |
| Cyber Espionage | 0.04<br>(0.07) | 0.04 | - - - | - - - |
| Cyber Attack & Terrorism | - - - | - - - | -0.04<br>(-0.22) | -0.04 |
| Regime Type | -0.01<br>(-0.26) | -0.01 | -0.01<br>(-0.23) | -0.01 |
| Contiguity | -0.06<br>(-1.22) | -0.06 | -0.06<br>(-1.18) | -0.06 |
| Alliance Participation | -0.12<br>(-1.58) | -0.12 | -0.12<br>(-1.54) | -0.12 |
| CINC (logged) | -0.08<br>(-0.39) | -0.08 | -0.07<br>(-0.38) | -0.07 |
| IGO Membership | 0.02**<br>(2.03) | 0.02 | 0.02**<br>(2.06) | 0.02 |
| Economic Interdependence (logged) | 0.21<br>(0.88) | 0.21 | 0.22<br>(0.91) | 0.22 |

| | | | | |
|---|---|---|---|---|
| MID (lagged) | -1.80**<br>(-2.47) | -1.80 | -1.81**<br>(-2.40) | -1.81 |
| Media Bias (logged) | -0.06<br>(-0.34) | -0.06 | -0.07<br>(-0.41) | -0.07 |
| Constant | -0.37<br>(-0.14) | -0.37 | -0.28<br>(-0.11) | -0.28 |

** p < .10, ** p < .05, *** p < .01 (Z Scores in parentheses), Two-Tail Test*
*Model 5 & 6 N = 2,129*

experiences zero cyber espionage cases. When substituting U.S. averages in the marginal effects, the results show that zero and one cyber espionage events are statistically insignificant in decreasing interstate war involvement. However, each additional case of cyber espionage may reduce the number of interstate conflicts by .44 events.[31]

Model 2 replaces the cyber espionage predictor with a measure combining cyber attack and cyber terrorism cases. The rare event logit results show that these forms of digital attack are not statistically significant in the reduction of interstate conflict. However, marginal effects with global averages gives us a more in-depth look at this relationship. The marginal effect results predict that increasing numbers of cyber attacks and terrorist events do slightly reduce the number of interstate wars. Specifically, increasing the number of cyber attacks and cyber terrorism cases by one decreases the number of interstate wars by approximately .02 events. While these results are not spectacular, they do support the first hypothesis. Substituting U.S. averages, the marginal effects predict a similar relationship between cyber attack/terrorism and interstate war participation. However, only three through eleven attacks are statistically likely to reduce the number of interstate wars in the United States.

Model 3 tests a different operationalization of interstate war, provided by UCDP/PRIO. As noted previously, this dependent variable differs from that of the COW definition by

[31] Graphs for the twelve marginal effect analyses can be found in Appendix C.

including interstate conflicts with as few as 25 battle-related deaths in a given year. This unique, more robust operationalization produces starkly different results from those of Models 1 and 2. In particular, Model 3 demonstrates a strong, positive statistical relationship between cyber espionage and PRIO interstate conflict. The rare event logit results show that an increase in one cyber espionage case may increase the number of interstate conflicts by a factor of 2.01. This same relationship is shown when using marginal effects and global averages. The marginal effect results predict that each additional cyber espionage case will increase the number of interstate conflicts by approximately .7 events. The same relationship and increase in interstate conflict is exhibited when U.S. averages are substituted in the marginal effects.

Model 4 also relies upon the UCDP/PRIO definition of war, but includes the combined cyber war/terrorism measure. Like Model 3, the results demonstrate a positive and statistically significant relationship between cyber threats and an increase in war involvement. In this case, an increase in one cyber attack or cyber terrorism event increases the number of wars by a factor of 1.39. Marginal effects with global and U.S. averages reinforce the findings of the rare event logit. With global averages, an increase in one cyber attack/terrorism case increases the number of wars by approximately .3. Interestingly, the statistical significance of the findings only applies to states that experience up to fifteen cyber attack/terrorism cases. Any attacks beyond that are not predicted to impact conflict propensity. When substituting U.S. averages, the marginal effects show a similar increase of .3 wars for every additional cyber attack or cyber terrorism case sustained. This finding is statistically significant for up to seventeen attacks, with the exception of ten and eleven attacks which are statistically insignificant in increasing war involvement.

The final two models, the results of which can be found in Table 4.3, test the second hypothesis. In particular, it is theorized that cyber espionage, attacks, and terrorism may reduce war involvement due to a decrease in information asymmetry, however it may increase tensions between the target and the suspected source. As a result, Models 5 and 6 test the cyber espionage and cyber attack/terrorism predictors with MIDs. The first set of ZINB results in Table 4.3 outwardly suggests that there is no statistical relationship between cyber espionage and MID participation. Marginal effects with global averages provide a more in-depth look at this relationship, and reveals that cyber espionage may indeed have some minor impact on MID participation. Namely, states that are targeted for zero through two cyber espionage attacks are statistically likely to be involved in slightly more less-than-conflict MIDs, although the increase is not spectacular. Interestingly, three or more cyber espionage attacks are not statistically more likely to increase a state's MID involvement. Marginal effects with U.S. averages also demonstrate that increasing cyber espionage increases MID participation. Each cyber espionage case increases the number of MIDs with U.S. involvement by approximately .05 cases. Unlike the results with global averages, American MID involvement is statistically likely to increase as cyber espionage targeting increases.

Lastly, Model 6 tests the relationship between cyber attack and cyber terrorism targeting and MID participation. The results largely mirror those of Model 5, with the ZINB outwardly suggesting that no statistically significant relationship exists. However, marginal effects give us a more detailed picture. When using global averages, the results show that states targeted by cyber espionage are likely to be involved in increasing numbers of less-than-conflict MIDs. In particular, each cyber espionage case increases the number of MIDs by approximately .006. While this is not a significantly robust increase, it should be noted that the average state is only involved in .18 MIDs (categorized as a 3 and below) per year. Thus, each cyber espionage case equates to a 3% increase in MID participation. The same relationship is exhibited when U.S. averages are used. The marginal effects demonstrate the each cyber espionage case sustained by the U.S. increases MID involvement by approximately .08 MIDs. Given that the U.S. experiences an average of .71 MIDs per year, an increase in .08 MIDs per cyber espionage case equals an increase in MIDs of almost 10%.

## Analysis

One of the unique aspects of the present analysis, which has been neglected in past bargaining studies, is the involuntary nature of the information exposure being studied, namely covert cyber espionage, warfare, and terrorism events. The models above give us a better understanding of the relationship between information exposure and conflict participation. Overall, the use of marginal effects and rare event models demonstrate varying support for the two hypotheses. In terms of cyber threat targeting and armed conflict, the rare event logistic models are split in their support of the notion that information and security vulnerability exposure may play a role in reducing conflict participation. More explicitly, Models 1 and 2 support the theory that vulnerabilities exposed through digital attacks give outside actors, particularly other states, a more detailed idea of the targeted state's preparedness, potential vulnerabilities in their security apparatus, and detailed information regarding issues such as troop positions and weapon capabilities. Given this unwanted exposure, the results of these models suggest that targeted states may be more willing to bargain for peace than engage in armed conflict, especially those conflicts capable of inflicting more than 1,000 causalities. These results broadly support the findings of bargaining scholars, and lend additional empirical support for bargaining theory.

Additionally, through different operationalizations of armed conflict, the results suggest that targeted states differ in their reaction to cyber threats and the prospect of low-intensity conflict. In particular, Models 3 and 4 demonstrate that states targeted for cyber espionage, cyber attacks, and cyber terrorism are more likely to engage in combat with casualty rates lower than those defined by the COW data. These findings suggest that the information exposed by cyber threats may be enough to persuade a state to bargain for peace when the risk for serious combat is high. However, they may also be willing to initiate low intensity conflict in response to cyber attacks and espionage. Such actions on the part of the targeted may be a form of violent and particularly clear signaling, indicating that they are unwilling to tolerate the exploration and exploitation of their digital vulnerabilities. This unwillingness to tolerate such activity is tempered, however, by the prospect of violent conflict with a potential for high thresholds of causalities.

While Hypothesis 1 received varying support from the analysis, the results suggest that states are more likely to be in involved in MIDs, and thus lending support to Hypothesis 2. In particular, these MIDs were limited to those that involve less-than-war levels of action, such as public condemnation, economic sanctions, verbal warnings, and mobilizations. This finding, like those of Models 3 and 4, suggest that targeted states recognize the dangerous security vulnerabilities that are exposed through cyber attacks, and are willing to use forceful measures short of combat to counter and potentially deter them. Also like the previous results, the increase in MID participation may be an indication that states are becoming less willing to ignore the damage caused by cyber attacks. Given the increased effectiveness of cyber attacks, and the empirical evidence that increased targeting leads to increased low-intensity combat and less-than-combat MID involvement, it is conceivable that states are beginning to incorporate the active defense of their digital networks into their foreign policy portfolios.

## Conclusion

The first chapter of this dissertation points out that vulnerabilities in communication technology are not a unique problem. And despite not being specifically tied to the bargaining literature, the accounts of 20th century communication demonstrates that states have historically attempted to pilfer information to gain an upper hand on their opponents. This use of espionage is demonstrated by a plethora of European powers on telegraph cables prior to World War I. While the British had the most robust global cable system, and had actively spied on the unencrypted messages of its users, the French had the largest and most successful decryption operation among the great powers. Prior to the outbreak of World War I, the French had at least partially broken the codes of many of its continental rivals, as well as the United States (Headrick 1991). Shortly before the war, the French even shared with the British private information stolen from a mutual enemy: the Germans. During the war, espionage allowed the belligerents to determine where enemy troops would be stationed, and where attacks would be launched. While the use of espionage prior to World War I clearly did not prevent the outbreak of conflict, as postulated by the chapter's theoretical framework and the larger bargaining theory literature, it does demonstrate that states are willing to use the vulnerabilities in communication technology to gain an upper hand on their opponents, and reduce the amount of private and misrepresented information available to the opposing side.

Concerning the present chapter, the results of this analysis lend additional empirical evidence to the growing study of interstate crisis bargaining. However, instead of focusing attention on public sources of intangible information, such as regime type, external transparency, or domestic political conditions, the present research investigates how the loss of truly private information through covert, digital means can impact a state's combat decisions. This analysis suggests that scholars should not ignore how the actions of external actors, through the use of cyber tactics, reduce information asymmetry and the denial of the targeted state to misrepresent its private information. The results also note that while states targeted for cyber attacks tend to shy away from large-scale armed combat, they are more willing to engage combat where causalities may be lighter, as well as short of combat MIDs. Thus, the use of cyber espionage, warfare, and terrorism to steal information and expose security vulnerabilities may lead to heighten tensions between states, while they simultaneously reduce the probability of full scale war.

Of course, additional research should focus on the relationships between of cyber espionage, information asymmetry, and conflict. Due to present data limitations and the exceptional difficulty in attributing cyber threats to their true source, this analysis was based upon a state-year model. Hopefully future improvements in attack attribution and data collection methods will provide the means to conduct a dyadic study of the cyber/information/conflict relationship. This would allow for a more complex, inclusive study that incorporates additional independent variables commonly used in other bargaining studies. The dyadic framework would also allow for more clarification regarding how cyber attack targeting impacts both MID initiation and continuation.

Ultimately, the increasing capacity of cyber attacks to cause widespread damage and steal previously unfathomable amounts of private information warrants increased attention from the scholarly community. This study is the first to incorporate the growing empirical body of literature surrounding the bargaining theory to investigate how cyber attacks reduce information asymmetry, and therefore impact state interactions.  Further research will lend additional clarification and new insight into how states both use and react to this unique 21st century security threat.

# Chapter 5 - Conclusion

This dissertation offers researchers a new means of studying the relationship between cyber threats and international relations. Previously, the social science literature focused much of its attention on descriptive studies and probing the vulnerabilities of American digital networks. However, cyber threats are not solely an American, or even a Western, problem. With over 2 billion people worldwide using the Internet, the danger of cyber threats against digital networks is now a global problem. It thus seems appropriate for scholarly research to begin to produce less U.S.-centric and more generalizable scholarship. In many regards, cyber research mirrors that of the terrorism literature prior to the attacks of 9/11. It was only after those attacks that social scientists began in earnest to study physical terrorism through generalizable, empirical analyses. Given the vulnerabilities inherent in cyber networks, it would seem wise to begin rigorous studies of cyber threats before a 9/11-like event occurs. As a result, the present research breaks from the norm and aims to study the nature of cyber threats and how they impact, and are impacted by, international relations through empirical analysis. Such an approach provides policymakers, and scholars, with a far more intricate picture of cyber threats and their role as a tool of foreign policy. To do so, this dissertation has employed a unique dataset of almost two decades of cyber attack, cyber terrorism, and cyber espionage cases from across the globe. With this innovative data, we can expand beyond the descriptive and U.S.-centric approach of past studies. With this objective in mind, this dissertation has investigated three important questions.

The second chapter of this dissertation focuses on the first of these questions. While the subject itself may seem rather simplistic in nature, it has yet to be addressed and is exceptionally important: which economic, political, and social characteristics make a state more likely to be targeted for cyber threats? Given a paucity of social science research on the subject, the theoretical foundation of this chapter is based upon the terrorist targeting literature. As noted, there are a host of similarities between the tactics employed by physical terrorists and those of computer hackers. These include a careful selection of the target, the potential physical and psychological damage, and the difficulty in attributing an attack to any particular state or group. As a result, the terrorism literature provides an appropriate theoretical surrogate for this initial research. The results show that different state characteristics are likely to influence the forms of digital attack targeting. For example, states that experience increases in GDP per capita and military size are more likely to be targeted for cyber attacks. Inversely, states that experience increases in GDP per capita and those that are more democratic are less likely to be targeted for cyber terrorism. Interestingly, those states with increasing levels of press freedom and those that engage in more international conflicts are more likely to be targeted for cyber terrorism. Finally, increasing military size and press freedom are both statistically likely to increase cyber espionage targeting, while increases in a state's level of democracy and international conflict involvement decrease targeting.

Overall, the empirical results of Chapter 2 are novel in the cyber threat literature, and unique in that they can be generally applied to any state around the globe. As noted, a vast majority of the current cyber literature, particularly the research that focuses on targeting, gives priority to the attributes that make the United States a popular target. The analysis and marginal effects results conducted in Chapter 2 demonstrate that the characteristics that make the United States a target may not necessarily increase the odds of targeting for the "average state," and vice versa. This suggests that states are not targeted equally, and the results of descriptive studies focused on the U.S. may not necessary apply to other nations. Additionally, the results show that the use of the physical terrorism literature is not the most efficient surrogate theoretical framework for the study of cyber threats. Despite similarities between the two forms of unconventional attack, the analysis suggests that the characteristics likely to increase terrorist attacks may not translate into additional cyber threat targeting. Such empirical results help to illuminate the differences between the two forms of violence, and lend further insight into the problem of international cyber threats.

The third chapter narrows the analysis of cyber threat targeting, but analyzing such activity through the lens of international rivalry. In particular, this chapter seeks to determine if states that engage in international rivalries are more likely to be targeted for cyber threats than neutral states. Traditionally, the rivalry literature has focused on interstate conflict or MIDs as the typical, violent interaction between rivals. However, more recently, researchers such as Conrad (2011) and Findley et al. (2012) have begun to investigate how rivalries increase the use of alternative forms of violence. The authors argue that, given the exceptionally high cost of armed interstate conflict, states may be more willing to use terrorist organizations as a proxy to inflict injury. In both studies, the scholars found that rivalry participation is a positive indicator of terrorist activity. This chapter seeks to determine if the same logic applies: does participation in international rivalries increase cyber threat targeting? Interestingly, when employing a dichotomous measure of rivalry, the empirical results show that engaging in additional enduring and strategic rivalries reduces the number of aggregate cyber threats a state would experience. This negative relationship is also present when using a count measure of enduring rivalries. However, the results show that engaging in additional strategic rivalries will marginally increase the number of cyber threats a state experiences. This suggests the threat posed by rivalry may compel states to enhance their digital network security, or that states are hesitant to employ digital means against rivals.

The results of chapter three contribute knowledge to both the rivalry as well as cyber threat literature. For example, much of the rivalry literature relies heavily on analyzing one operationalization of rivalry or another. These operationalizations are generally those of either Klein, Goertz, and Diehl (2006) or Thompson and Dreyer (2012). Interestingly, but perhaps not surprisingly, the definition of rivalry and the temporal range employed in an analysis can have a significant impact on the results. In the case of the present research, those factors influenced the support each model lent to the hypothesis. In the future, rivalry scholars should consider including both definitions of rivalry to test how past military engagement impacts their results. Additionally, this chapter lends further understanding of the factors that may increase cyber threat targeting. While states engaged in rivalries with a violent past are likely to experience a decrease in cyber threats, those states viewed negatively by others are statistically likely to experience additional attacks. This suggests that the manner in which a particular state is viewed internationally, regardless of past military activity, can have serious implications for their digital networks' security. Thus, domestic factors such as those explored in Chapter 2 may not play the only role in targeting. Together, Chapters 2 and 3 give cyber researches a much better perspective of the threat digital networks face, and the state characteristics that may increase the likelihood of targeting.

The fourth chapter deviates from cyber threat targeting, and investigates how cyber threats impact crisis bargaining situations. In particular, Fearon (1995) notes that interstate wars are a consequence of bargaining breakdowns, often caused by states withholding and misrepresenting private information. This chapter is based on the assumption that cyber threats, especially cyber espionage, release information that the targeted state would have rather kept private. As a result, the targeted state would be more likely to seek peace in bargaining situations, as opposed to engage in armed conflict. The results, however, are mixed in their support of this hypothesis. Specifically, different types of cyber threats have varying impacts on the types of conflicts states engage in. For example, increasing number of cyber espionage, cyber attack, and cyber terrorism events are statistically likely to increase the number of low-intensity conflicts a state engages in. However, increasing numbers of cyber espionage cases are found to decrease participation in wars with over 1,000 causalities. States may thus be willing to initiate or participate in low scale force following cyber attacks but the release of private information and the enhanced bargaining prospects that result reduces the chances of full scale war.

Much like the previous chapters, Chapter 4 produces novel results and illuminates both an established literature and the burgeoning cyber literature. As far as bargaining theory is concerned, this chapter takes an exceptionally unique perspective of asymmetric information exchange by investigating how actual, private information loss can impact conflict propensity. Prior to this study, the bargaining literature focused on proxy forms of information loss, including transparency and alliance participation. While these proxies do have an impact on conflict participation, they are not forms of tangible information that a state could easily misrepresent or keep private. By using cyber espionage as a measure of information exposure, this chapter establishes how the loss of tangible data, which could have been misrepresented or withheld by the targeted state, impacts the likelihood of conflict. Again, much like the rivalry literature and the testing of only one definition of rivalry, many bargaining scholars focus heavily on one particular form of conflict, be it major armed encounters or less-bloody MIDs.

This chapter deviates from that norm, and incorporates varying levels of conflict intensity. The results show that information loss through cyber espionage and other cyber threats can significantly impact participation in different forms of conflict. This is a technique that should be adopted by bargaining theory researchers, in order to determine if proxy factors such as transparency have varying impacts on conflict. Additionally, the chapter demonstrates that cyber threat targeting can influence the behavior of states, especially when it comes to conflict participation. While it may deter states from engaging in bloody wars, it will actually increase the likelihood of low-intensity conflict.

The three empirical chapters of this dissertation provide unique, innovative insight into the threats facing digital networks across the globe. However, the chapters also add to the history of communication vulnerabilities, which have been present in varying forms of communication throughout the twentieth century. Such vulnerabilities include espionage of telegraph cables, and signal jamming of radio transmissions. The exploitation of the Internet as a weapon or tool of combat is simply another manifestation of a problem that has existed for quite some time. In addition, these chapters highlight the use of the Internet as a tool of foreign policy by states, as well as expanding upon the weaknesses of the Internet described in Chapter 1. Specifically, the Internet was originally conceived as a means of reliable communication during a period of increased international tension. However, the Internet's inventors never conceived of the Web being used as a conduit of attack. A vast majority of the previous social science literature provided anecdotal evidence that the Internet was being used in such a manner. This dissertation adds to that literature by quantifying this global security problem, and investigating how cyber threats impact (and are impacted by) international relations.

As noted previously, however, this dissertation only serves as a “first cut” in the quantitative study of cyber threats. Additional research is needed in order to gain a comprehensive grasp of this security threat. Robust quantitative data like that employed in this study will prove invaluable in future analyses. This dataset will thus continue to be updated and studied in order to fuel future research. In order to understand the finer details of cyber threat targeting, the dataset will also require more refined coding in the future. Specifically, the targets of individual attacks could be coded based on their industry or nature. For example, attack targets could be denoted as financial (such as banks), government, military (such as DoD networks), business, or private. Such a coding scheme would allow scholars to investigate which industries or entities are more likely to be targeted, and furthermore how the targeting of a specific industry impacts relations between states. The dataset would also benefit from more robust information on the source of specific attacks. Unfortunately, accurately attributing attacks to a specific state, organization, or individual using the raw data provided by Virtual Research Associates was exceptionally difficult for this data. Future advancements in attribution may permit for increased certainty regarding the source of attacks, allowing researchers to conduct dyadic investigations. While these data improvements would obviously add to our collective understanding of cyber threats as an international security threat, they do not detract from the novel results produced in this research.

Ultimately, by employing three different theoretical foundations and unique quantitative data, this dissertation provides a groundbreaking perspective on international cyber threats. Future work can build upon this research by continuing to expand the cyber data and utilizing it to test new theories. Only through methodologically rigorous studies can social scientists help explain the intricate nature of why states and sub-state groups use cyber threats, the international environments in which they are more likely to be used, and how they impact relations between states. As Internet technology is increasingly adopted as a component of industrial and national security networks, the danger of cyber threat targeting will only continue to rise. Instead of waiting until a "digital 9/11" to explore these subjects in-depth, this dissertation will hopefully provide social scientists with the tools necessary to begin empirical studies of this 21st century security threat.

# References

Abbate, Janet Ellen. 2000. *Inventing the Internet*. Cambridge, MA: The MIT Press.

Ackerman, G., P. Abhayaratne, J. Bale, A. Bhattacharjee, C. Blair, L. Hansell, A. Jayne, M. Kosal, S. Lucas, K. Moran, L. Seroki, and S. Vadlamudi. 2007. "Assessing Terrorist Motivations for Attacking Critical Infrastructure." Center for Nonproliferation Studies: Monterey Institute of International Studies.

Alexander, David. 2011. "U.S. Reserves Right to Meet Cyber Attack with Force." *Reuters.com*. 15 Nov 2011. Available at: www.reuters.com/assets/print?aid=USTRE7AF02Y20111116

Allison, Paul D. 2009. *Fixed Effects Regression Models*. Thousand Oaks, CA: Sage Publications.

Allison, Paul D. 2012. "Beware of Software for Fixed Effects Negative Binomial Regression." 2012 June 8. Accessed January 2, 2014. Available at: www.statisticalhorizons.com/fe-fnbreg.

Anderson, Christopher C., Sara McLaughlin Mitchell and Emily Schilling. Unpublished Manuscript. "Kantian Dynamics Revisited: Time Varying Analyses of Dyadic IGO-Conflict Relationships." Available at: www.saramitchell.org/arms.pdf.

Arquilla, John and David Ronfeldt. 1993. "Cyberwar is Coming." *Comparative Strategy*, 12(2): 141-165.

Bearce, DH, KM Flanagan KM and KM Floros. 2006. "Alliances, Internal Information, and Military Conflict Among Member-States." *International Organization*, 60(3): 595-625.

Beck, Nathaniel and Jonathan N. Katz. 1995. "What To Do (and Not To Do) With Time-Series Cross-Section Data." *American Political Science Review*, 89(3): 634-647.

Bell, Sam R. 2013. "What You Don't Know Can Hurt You: Information, External Transparency, and Interstate Conflict, 1982-1999." *Conflict Management and Peace Science*, 30(5): 452-468.

Bennett, D. Scott. 1996. "Security, Bargaining, and the End of Interstate Rivalry." *International Studies Quarterly*, 40(2): 157–184.

Bennett, D. Scott. 1997. "Measuring Rivalry Termination." *Journal of Conflict Resolution*, 41(3): 227–254.

Bennett, D. Scott. 1998. "Integrating and Testing Models of Rivalry." *American Journal of Political Science*, 42(4): 1200–1232.

Berners-Lee, Tim. 1998. “The World Wide Web: A Very Short Personal History.” Available at: http://www.w3.org/People/Berners-Lee/ShortHistory.html.

Betz, David. 2012. “Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed.” *Journal of Strategic Studies*, 35(5): 689-711.

Bimber, Bruce. 1994. “Three Faces of Technological Determinism.” in *Does Technology Drive History*. eds Merrit Roe Smith and Leo Marx. Cambridge, MA: MIT Press.

Blechman, Barry M. and Stephen S. Kaplan. 1978. *Force Without War: U.S. Armed Forces As a Political Instrument*. Washington, D.C.: The Brookings Institution.

Blomberg, S. Brock, Gregory D. Hess and Akila Weerapana. 2004. “Economic conditions and terrorism.” *European Journal of Political Economy*, 20(2004): 463-478.

Brandt, Patrick T. and Todd Sandler. 2010. “What Do Transnational Terrorists Target? Has it Changed? Are We Safer?” *Journal of Conflict Resolution*, 54(2): 214-236.

Brenner, Susan W. 2007. “’At Light Speed’: Attribution and Response to Cybercrime/Terrorism/Warfare.” *The Journal of Criminal Law and Criminology*, 97(2): 379-475.

Brenner, Susan B. 2009. *Cyberthreats: The Emerging Fault Lines of the Nation State*. Oxford: Oxford University Press.

Bunker, Robert R.J. 2000. “Weapons of Mass Disruption and Terrorism.” *Terrorism and Political Violence*, 12(1): 37-46.

Burgoon, Brian. 2006. “On Welfare and Terror: Social Welfare Policies and Political-Economic Roots of Terrorism.” *The Journal of Conflict Resolution*, 50(2): 176-203.

Ceruzzi, Paul E. 2008. *Internet Alley: High Technology in Tysons Corner, 1945-2005.* Cambridge, MA: The MIT Press.

Chharia, Rajesh. 2013. “Internet Governance and Cybersecurity.” In *MIND Co:llaboratory Discussion Paper Series No. 1, Internet and Security*, ed. Wolfgang Kleinwachter. October 2013. Available at: http://en.collaboratory.de/images/b/bb/Mind_06berlin.pdf.

Choucri, Nazli and Daniel Goldsmith. 2012. “Lost in cyberspace: Harnessing the Internet, international relations, and global security.” *Bulletin of the Atomic Scientists*, 68(2): 70-77.

Chu, Hai-Cheng, Der-Jiunn Deng, Han-Chieh Chao, and Yueh-Min Huang. 2009. “Next Generation of Terrorism: Ubiquitous Cyber Terrorism with the Accumulation of all Intangible Fears.” *Journal of Universal Computer Science*, 15(12): 2373-2386.

Clark, DH. 2003. “Can Strategic Interaction Divert Diversionary Behavior? A Model of U.S. Conflict Propensity.” *Journal of Politics*, 65(4): 1013-1039.

Clark, Tom S. and Drew A. Linzer. 2012. "Should I Use Fixed or Random Effects?" *The Society for Political Methodology*. Available at: polmeth.wustl.edu/media/Paper/ClarkLinzerREFEMar2012.pdf

Clarke, Richard A. & Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: HarperCollins.

Colaresi, Michael P. and William R. Thompson. 2002. "Strategic Rivalries, Protracted Conflict, and Crisis Escalation." *Journal of Peace Research*, 39(3): 263-287.

Colaresi, Michael P., Karen Rasler and William R. Thompson. 2007. *Strategic Rivalries in World Politics: Position, Space and Conflict Escalation*. Cambridge: Cambridge University Press.

Colarik, Andrew M. 2006. *Cyber Terrorism: Political and Economic Implications*. Hershey, PA: Idea Group Publishing.

Conrad, Justin. 2011. "Interstate Rivalry and Terrorism: An Unprobed Link." *Journal of Conflict Resolution*, 55(4): 529-555.

Conrad, Justin and Mark Souva. 2011. "Regime Similarity and Rivalry." *International Interactions*, 37: 1-28.

Conway, Maura. 2002. "What is Cyberterrorism?" *Current History*, Dec: 436-442.

Correlates of War Project. *Direct Contiguity Data, 1816-2006*. Version 3.1. Online: http://correlatesofwar.org.

Crenshaw, Martha. 2012. "Justice Delayed." *Foreign Policy*, 4 Oct 2012. Available at: http://www.foreignpolicy.com/articles/2012/10/04/justice_delayed.

Crowell, Richard M. 2010. "War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare." *Naval War College.* Available at: www.carlisle.army.mil/DIME

Danilovic, Vesna and Joe Clare. 2010. "Deterrence and Crisis Bargaining." In *International Studies Compendium*, ed. Robert A. Denemark. New York: Wiley-Blackwell Publishers.

Davis, William. 2007. "Public Opinion, Security Threats, and Foreign Policy Formation: A Theoretical Framework and Comparative Analysis." The Florida State University DigiNole Commons. Available online: http://diginole.lib.fsu.edu/etd/814/.

Denning, Peter J. 1989. "The ARPANET after Twenty Years." *American Scientist* 77(Nov-Dec): 530-535.

Devine, Jack. 2008. "Tomorrow's Spygames." *World Policy Journal*, 25(3): 141-151.

Drakos, Konstantinos and Andreas Gofas. 2006. "In Search of the Average Transnational Terrorist Attack Venue." *Defence and Peace Economics*, 17(2): 73-93.

Dreher, Axel, Martin Gassebner, and Lars-H. Siemers. 2007. "Does Terrorism Threaten Human Rights? Evidence from Panel Data." *Journal of Law and Economics*, 53(1): 65-93.

Dreyer, David R. 2012. "Issue Intractability and the persistence of International Rivalry." *Conflict Management and Peace Science*, 29(5): 471-489.

Embar-Seddon, Ayn. 2002. "Cyberterrorism: Are We Under Siege?" *American Behavioral Scientist*, 45(6): 1033-1043.

Enders, Walter and Todd Sandler. 1999. "Transnational Terrorism in the Post-Cold War Era." *International Studies Quarterly*, 43(1): 145-167.

Enders, Walter and Todd Sandler. 2006. "Distribution of Transnational Terrorism among Countries by Income Class and Geography after 9/11." *International Studies Quarterly*, 50(2): 367-393.

Enders, Walter, Todd Sandler, and Khusrav Giabulloev. 2011. "Domestic Versus Transnational Terrorism: Data, Decomposition, and Dynamics." *Journal of Peace Research* 48(3): 319-337.

Eubank, William and Leonard Weinberg. 1994. "Does Democracy Encourage Terrorism?" *Terrorism and Political Violence*, 6: 417-443.

Eubank, William and Leonard Weinberg. 2001. "Terrorism and Democracy: Perpetrators and Victims." *Terrorism and Political Violence*, 13: 155-164.

Evans, Michael and Giles Whittell. 2010. "Cyberwar declared as China hunts for the West's intelligence secrets." *Times Online*, 8 March, 2010.

Eyerman, Joe. 1998. "Terrorism and Democratic States: Soft Targets or Accessible Systems." *International Interactions* 24(2): 151-170.

Eyerman, Joe and Robert A. Hart Jr. 1996. "An Empirical Test of the Audience Cost Proposition: Democracy Speaks Louder than Words." *Journal of Conflict Resolution*, 40(4): 597-616.

Fearon, James D. 1994. "Signaling versus the Balance of Power and Interests: An Empirical Test of a Crisis Bargaining Model." *The Journal of Conflict Resolution*, 38(2): 236-269.

Fearon, James D. 1995. "Rationalist Explanations for War." *International Organizations*, 49(3): 379-414.

Fearon, James D. 1997. "Signaling Foreign Policy Interests: Tying Hands versus Sinking Costs." *Journal of Conflict Resolution*, 41(1): 68-90.

FEMA. 2011. "Strategic Foresight Initiative: U.S. Demographic Shifts." Available Online.

Fey, Mark and Kristopher W. Ramsay. 2011. "Uncertainty and Incentives in Crisis Bargaining: Game-Free Analysis of International Conflict." *American Journal of Political Science*, 55(1): 149-169.

Fidler, David P. 2012. "Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think." *International Journal of Critical Infrastructure Protection*, 5(2012): 28-29.

Findley, Michael and Joseph K. Young. 2010. "More Combatants, More Terror? An Empirical Test of the Outbidding Thesis." Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1676551.

Findley, Michael G., James A. Piazza, Joseph K. Young. 2012. "Games Rivals Play: Terrorism in International Rivalries." *The Journal of Politics*, 74(1): 235-248.

Flint, Colin. 2003. "Terrorism and Counterterrorism: Geographic Research Questions and Agendas." *The Professional Geographer*, 55(2): 161-169.

Fordham, Benjamin O. and Christopher C. Sarver. 2001. "Militarized Interstate Disputes and United States Uses of Force." *International Studies Quarterly*, 45(3): 455-466.

Franzen, Carl. 2013. "Cyber threats at the top of US intelligence report for the first time." *The Verge*, 15 April 2013. Available at: http://www.theverge.com/2013/4/15/4227598/cyber-threats-at-the-top-of-us-intelligence-report-for-the-first-time

Garber, L. 2000. "Denial-of-Service Attacks Rip the Internet." *Computer* 33(4): 12-17. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=839316&isnumber=18132.

Gartzke, Erik and Dong-Joon Jo. 2002. *United Nations General Assembly Voting, 1946-1996*. Version 3.0. http://www.colombia.edu/~eg589/datasets.

Gartzke, E. Q. Li and C. Boehmer. 2001. "Investing in the Peace: Economic Interdependence and International Conflict." *International Organization*, 55(92): 391-438.

Gayathri, Amrutha. 2013. "Cyber Espionage Campaign Aims to Steal Classified Information Relating to South Korea, US Militaries: McAfee." International Business Times. 2013, 9 July. Available at: http://www.ibtimes.com/cyber-espionage-campaign-aims-steal-classified-information-relating-south-korea-us-militaries-mcafee.

Gelpi, Christopher F. and Michael Griesdorf. 2001. "Winners or Losers: Democracies in International Crises, 1918-1994." *American Political Science Review*, 95(3): 633-647.

Ghosn, Faten, Glenn Palmer, and Stuart Bremer. 2004. The MID3 Data Set, 1993-2001: Procedures, Coding Rules, and Description. *Conflict Management and Peace Science*, 21: 133-154.

Gleditsch, Nils Petter, Peter Wallensteen, Mikael Eriksson, Margareta Sollenberg and Håvard Strand. 2002. Armed Conflict 1946–2001: A New Dataset. *Journal of Peace Research*, 39(5): 615–637.

Goemans, Hein. 2000. *War & Punishment: The Causes of War Termination and The First World War.* Princeton, NJ: Princeton University Press.

Goertz, Gary, and Paul F. Diehl. 1993. "Enduring Rivalries: Theoretical Constructs and Empirical Patterns." *International Studies Quarterly*, 37: 147-171.

Goertz, Gary, and Paul F. Diehl. 1995. "The Initiation and Termination of Enduring Rivalries: The Impact of Political Shocks." *American Journal of Political Science*, 39: 30–52.

Goldman, Brett. 2010. "The Democratic Dilemmas of Cyber-Terrorism and the Internet." *Publications in Contemporary Affairs*, 16 Feb 2010. Available at: <http://www.thepicaproject.org/?page_id=279>.

Goldsmith, Benjamin E. 2013. "International Trade and the Onset of Escalation of Interstate Conflict: More to Fight About, or More Reasons Not to Fight?" *Defence and Peace Economics*, 24(6): 555-578.

Guisnel, Jean. 1997. *Cyberwars: Espionage on the Internet*. New York: Plenum Trade.

Handler, Stephenie Gosnell. 2012. "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare." *Stanford Journal of International Law*, 48(1): 209.

Hasham, Salim, David Craig and Philip Grosch. 2011. "Are you compromised but don't know it? A new philosophy for cyber security." PwC Technology Consulting Services. Available at: www.pwc.com/ca/technology-consulting.

Hawkins, Eliza Tanner and Kirk A. Hawkins. 2003. "Bridging Latin America's Digital Divide: Government Policies and Internet Access." *Journalism and Mass Communication Quarterly,* 80(3): 746-665.

Headrick, Daniel R. 1991. *The Invisible Weapon: Telecommunications and International Politics, 1851-1945.* Oxford: Oxford University Press.

Hensel, Paul R. 1996. "Charting a Course to Conflict: Territorial Issues and Interstate Conflict, 1816-1992." *Conflict Management and Peace Science*, 15(1): 43-73.

Hensel, Paul R. and Paul F. Diehl. 1994. "It Takes Two to Tango: Nonmilitarized Response in Interstate Disputes." *Journal of Conflict Resolution*, 38(3): 479-506.

Heston, Alan, Robert Summers and Bettina Aten. 2012. Penn World Table Version 7.1. Center for International Comparisons of Production, Income and Prices at the University of Pennsylvania.

Hoffman, Bruce. 2006. *Inside Terrorism*. New York: Columbia University Press.

Hollyer, James R., B. Peter Rosendorff, and James Raymond Vreeland. 2011. "Democracy and Transparency." *The Journal of Politics*, 73(4): 1191-1205.

Hunker, Jeffrey, Bob Hutchinson, and Jonathan Margulies. 2008. *Role and Challenges for Sufficient Cyber-Attack Attribution*. Dartmouth College: Institute for information Infrastructure Protection. Available at: handle.dtic.mil/100.2/ADA468859

Hunt, Edward. 2012. "US Government Computer Penetration Programs and the Implications for Cyberwar." *IEEE Annals of the History of Computing*, July-September: 4-21.

Kalathil, Shanthi, and Taylor Boas. 2003. *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Washington, DC: Carnegie Endowment for International Peace.

Kelly, Kevin. 2010. *What Technology Wants*. New York, NY: Penguin Group.

King, Gary, and Langche Zeng. 2001. "Logistic Regression in Rare Events Data." *Political Analysis*, 9: 137–163.

Klein, James P., Gary Goertz, and Paul F. Diehl. 2006. "The New Rivalry Dataset: Procedures And Patterns." *Journal of Peace Research*, 43(3), 331-348.

Kleinberg, Katja B., Gregory Robinson and Steward L. French. 2012. "Trade Concentration and Interstate Conflict." *The Journal of Politics*, 74(2): 529-540.

Kohlmann, Evan F. 2006. "The Real Online Terrorist Threat." *Foreign Affairs*, 85(5): 115-124.

Krueger, Alan B. and David Laitin. 2008. "'Kto Kogo?': A Cross-Country Study of the Origins and Targets of Terrorism," in *Terrorism, and Economic Development, and Political Openness* (eds. Philip Keefer and Norman Loayza). Cambridge, MA: Cambridge University Press.

Kupperman, Robert H., Debra van Ostpal, and David Williamson, Jr. 1982. "Terror, the Strategic Tool: Responses and Control." *The Annals of the American Academy of Political and Social Science*, 463(1): 24-38.

Lai, B. and D. Slater. 2006. "Institutions of the Offensive: Domestic Sources of Dispute Initiation in Authoritarian Regimes, 1950-1992." *American Journal of Political Science*, 50(1): 113-126.

Langfitt, Frank. 2013. "U.S. Security Company Tracks Hacking to Chinese Army Unit." NPR. 19 Feb 2013. Available at: www.npr.org/2013/02/19/172373133/

Leeds, Brett Ashley. 2003. "Do Alliances Deter Aggression? The Influence of Military Alliances on the Initiation of Militarized Interstate Disputes." *American Journal of Political Science*, 47(3): 427-439.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Lawrence G. Roberts, and Stephen Wolff. 1999. *Brief History of the Internet*. Internet Society. Available at: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Leiner

Levite, Ariel, Bruce Jentleson and Larry Berman, eds. 1992. *Foreign Military Intervention: The Dynamics of Protracted Conflict*. New York: Columbia University Press.

Lewis, James A. 2002. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats". Washington, D.C.: Center for Strategic & International Studies.

Lewis, James A. 2010. "Thresholds for Cyberwar." Washington, D.C.: Center for Strategic and International Studies. Available at: http://csis.org/files/publication/101001_ieee_insert.pdf.

Lewis, James A. 2011. "Cybersecurity Two Years Later." *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. <http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf>

Li, Quan. 2005. "Does Democracy Promote or Reduce Transnational Terrorist Incidents?" *The Journal of Conflict Resolution* 49(2), 278-297.

Li, Quan and drew Schaub. 2004. "Economic Globalization and Transnational Terrorism: A Pooled Time-Series Analysis." *Journal of Conflict Resolution*, 48(2): 230-258.

Libicki, Martin. 2000. "Rethinking War: The Mouse's New Roar?" *Foreign Policy*, 117(Winter): 30-32/34-43.

Libicki, Martin, Peter Chalk and Melanie Sisson. 2007. "Exploring Terrorist Targeting Preferences." Santa Monica, CA: RAND Corporation. Available at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA463029.

Lichbach, Mark Irving. 1998. *The Rebel's Dilemma (Economics, Cognition, and Society)*. Ann Arbor, MI: University of Michigan Press.

Long, J. Scott and Jeremy Freese. 2005. *Regression Models for Categorical Outcomes Using Stata*. Second Edition. College Station, TX: Stata Press.

Lourdeau, Keith. 2004. *Judiciary Subcommittee on Terrorism, Technology, and Homeland security, Cyber Terrorism. Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI, Washington, D.C., 24 February 2004.*

Maoz, Zeev, and Ben D. Mor. 1996. "Enduring Rivalries: The Early Years." *International Political Science Review*, 17(2): 141–160.

Maoz, Zeev and Belgin San-Akca. 2012. "Rivalry and State Support of Non-State Armed Groups (NAGs), 1946-2001." *International Studies Quarterly*, 56: 720-734.

Marshall, Monty G. and Keith Jaggers. 2007. “Polity IV Project: Dataset Users’ Manual.” George Mason University and Center for Systemic Peace. Available at: http://www.systemicpeace.org/polity/polity4.htm.

Martin, Brady, Thomas Graham and Kezron Caines. 2011. “Threats to Information: A Study of SANS and Educause.” Unpublished Manuscript. Available at: http://www.cameron.edu/uploads/69/a2/69a2e510bc8a76920d18866deca69a92/3_Vulnerabilities_Trends.docx.

McAfee. 2013. “The Economic Impact of Cybercrime and Cyber Espionage.” *Center for Strategic and International Studies*. July 2013. Available at: www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

Messmer, Ellen. 2008. “Cyber Espionage Seen as Growing Threat to Business, Government.” *Network World*, 17 January, 2008. Available at: <http://www.networkworld.com/news/2008/011708-cyberespionage.html>.

Millett, Allan R. 1996. “Patterns of Military Innovation in the Interwar Period.” In *Military Innovation in the Interwar Period*, eds. Williamson Murray and Allan R. Millett. Cambridge, UK: Cambridge University Press.

Milner, Helen V. 2006. “The Digital Divide: The Role of Political Institutions in Technology Diffusion.” *Comparative Political Studies*, 39(2): 176-199.

Mitchell, Sara McLaughlin and Brandon C. Prins. 2004. “Rivalry and Diversionary Uses of Force.” *Journal of Conflict Resolution*, 48(6): 1-25.

Morris, Nancy A. and Lee Ann Slocum. 2012. “Estimating Country-Level Terrorism Trends Using Group-Based Trajectory Analyses: Latent Class Growth Analysis and General Mixture Modeling.” *Journal of Quantitative Criminology*, 28: 103-139.

Morrow, JD. 1989. “Capabilities, Uncertainty, and Resolve: A Limited Information Model of Crisis Bargaining.” *American Journal of Political Science*, 33(4): 941-972.

Most, B.A., and H. Starr. 1989. *Inquiry, Logic, and International Politics*. Columbia: University of South Carolina Press.

Murdie, Amanda and Dursun Peksen. 2013. “The Impact of Human Rights INGO Shaming on Sanctions.” *The Review of International Organizations*, 8(1): 33-53.

Myers, Steven Lee. 2007. “‘E-stonia’ Accuses Russia of Computer Attacks.” *The New York Times*, 18 May 2007. Available at: http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html?_&_r=0.

Naimi, Linda L. and Richard Mark French. 2010. *The Unintended Consequences of Technological Innovation: Bluetooth Technology and Cultural Change*. Available at: http://www.internetjournals.net/journals/tir/2010/July/Paper%2002.pdf.

David, Joseph S. 2006. *Technology Matters: Questions to Live With*. Cambridge, MA: The MIT Press.

Nye, Joseph S. 2011. "Nuclear Lessons for Cyber Security." *Strategic Studies Quarterly*, (Winter): 18-38.

Oneal, J.M. and B. Russett. 1999. "The Kantian Peace: The Pacific Benefits of Democracy, Interdependence, and International Organizations, 1885-1992." *World Politics*, 52(1): 1-37.

Oneal, John R. and Bruce Russett. 2001. "Clear and Clean: The Fixed Effects of the Liberal Peace." *International Organization*, 55(2): 469-485.

Pape, Robert A. 2003. "The Strategic Logic of Suicide Terrorism." *American Political Science Review*, 97(3): 343-361.

Parkhe, Arvind. 1992. "U.S. National Security Export Controls: Implications for Global Competitiveness of U.S. High-Tech Firms." *Strategic Management Journal*, 13(1), 47-66.

Patran, Ioana. 2013. "Romania believes rival nation behind 'MiniDuke' cyber attack." *Reuters News Agency*, Mar 1 2013. Available at: http://www.reuters.com/assets/print?aid=USBRE9200OO20130301.

Piazza, James A. 2006. "Rooted in Poverty? Terrorism, Poor Economic Development, and Social Cleavages." *Terrorism and Political Violence*, 18(1): 159-177.

Piazza, James A. 2008a. "Incubators of Terror: Do Failed and Failing States Promote Transnational Terrorism?" *International Studies Quarterly*, 52: 469-488.

Piazza, James A. 2008b. "Do Democracy and Free Markets Protect Us From Terrorism?" *International Politics*, 45: 72-91.

Piazza, James A. 2011. "Poverty, minority economic discrimination, and domestic terrorism." *Journal of Peace Research*, 48(3): 339-353.

Plumper, Thomas and Eric Neumayer. 2010. "The Level of Democracy During Interregnum Periods: Recoding the Polity2 Score." *Political Analysis*, 18(2): 206-226.

Powell, Robert. 2002. "Bargaining Theory and International Conflict." *Annual Review of Political Science*, 5(June): 1-30.

Prins, Brandon C. 2003. "Institutional Instability and the Credibility of Audience Costs: Political Participation and Interstate Crisis Bargaining, 1816-1992." *Journal of Peace Research*, 40(1): 67-84.

Prins, Brandon C. 2010. "Interventions and Uses of Force Short of War." In *The International Studies Encyclopedia, Volume VII,* ed Robert A Denemark. Oxford: Wiley-Blackwell.

Quackenbush, Stephen L. and Michael Rudy. 2009. “Evaluating the Monadic Democratic Peace.” *Conflict Management and Peace Science*, 26(3): 268-285.

QoG Codebook. 2013. “The QOG Standard Dataset Codebook.” Unviersity of Gothenburg. Available at: http://www.qogdata.pol.gu.se/codebook/codebook_standard_20dec13.pdf

Rasler, Karen A., and William R. Thompson. 2006. “Contested Territory, Strategic Rivalries, and Conflict Escalation.” *International Studies Quarterly*, 50(1): 145–167.

Ratnam, Gopal. 2012. “Cyberattacks Could Become as Destructive as 9/11: Panetta.” *Bloomberg*, 11 Oct. 2012: n. pag. Available at: http://www.bloomberg.com/news/2012-10-12/cyberattacks-could-become-as-destructive-as-9-11-panetta.html

Rawnsley, Gary D. 2005. “Old Wine in New Bottles: China-Taiwan Computer-Based ‘Information Warfare’ and Propaganda.” *International Affairs*, 81(5): 1061-1078.

Ray, J.L. 1990. “Friends as Foes: International Conflict and Wars Between Formal Allies” in *Prisoners of War? Nation-States in the Modern Era,* eds. C. Gochman and A. Sabrosky. Lexington: Lexington Books.

Reed, William. 2003. “Information, Power, and War.” *The American Political Science Review*, 97(4): 633-641.

Reed, William, David H. Clark, Timothy Nordstrom and Wonjae Hwang. 2008. “War, Power, and Bargaining.” *The Journal of Politics*, 70(4): 1203-1216.

Reiter, Dan. 1999. “Military Strategy and the Outbreak of International Conflict: Quantitative Empirical Tests, 1903- 1992.” *Journal of Conflict Resolution*, 43(3): 366-387.

Reuters News Agency. 2011. “Iran accuses Siemens over Stuxnet virus attack.” *Reuters News Agency*, Apr 17 2011. Available at: www.reuters.com/assets/print?aid=USTRE73G0NB20110417.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Rogan, Randall G. 2010. “Jihad Against Infidels and Democracy: A Frame Analysis of Jihadist Ideology and Jurisprudence for Martyrdom and Violent Jihad.” *Communication Monographs*, 77(3): 393-413.

Rogers, E.M. 2000. “The Communication of Innovation: The Need for Internet Access Multiplies Along with Obstacles.” *CNN*. Available at: <http://www.cnn.com/SPECIALS/2000/virtualvillages/story/essays/rogers/>.

Sanger, David E. and Elisabeth Bumiller. 2011. “Pentagon to Consider Cyberattacks Acts of War.” *The New York Times Reprints*, 31 May 2011. Available at: www.nytimes.com/2011/06/01/us/politics/01cyber.html?_&_r=0

Santifort-Jordan, Charlinda and Todd Sandler. 2014. “An Empirical Study of Suicide Terrorism: A Global Analysis.” *Southern Economic Journal*, 80(4): 981-1001.

Sarkees, Meredith Reid and Frank Wayman 2010. *Resort to War: 1816 - 2007.* CQ Press.

Savun, Burcu and Brian J. Phillips. 2009. “Democracy, Foreign Policy, and Terrorism.” *The Journal of Conflict Resolution*, 53(6): 878-904.

Schelling, Thomas. 1960. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press.

Schelling, Thomas C. 1966. *Arms and Influence*. New Haven, CT: Yale University Press.

Schweizer, Peter. 1996. “The Growth of Economic Espionage: America is Target Number One.” *Foreign Affairs* 75(1), 9-14.

Senese, Paul D. and John Vasquez. 2004. “Alliances, Territorial Disputes, and the Probability of War: Testing for Interactions.” In *The Scourge of War*, ed. Paul Diehl. Ann Arbor: The University of Michigan Press.

Sioshansi, F.P. 2012. *Smart Grid: Integrating Renewable, Distributed & Efficient Energy*. Waltham, MA: Elsevier Academic Press.

Slantchev, Branislav L. 2003. “The Principle of Convergence in Wartime Negotiations.” *American Political Science Review*, 97(4): 621-632.

Smith, Alastair. 1996. “Diversionary Foreign Policy in Democratic Systems.” *International Studies Quarterly*, 40(1): 133-153.

Snow, Gordon M. 2011. “Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism,” Washington, D.C.: 22 April 2011. Available at: http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism.

Souva, Mark and Brandon C. Prins. 2006. “The Liberal Peace Revisited: The Role of Democracy, Dependence, and Development in Militarized Interstate Dispute Initiation, 1950-1999.” *International Interactions*, 32(2): 183-200.

Steele, Cherie and Arthur A. Stein. 2002. “Communications Revolutions and International Relations.” In *Technology, Development, and Democracy: International Conflict and Cooperation in the Information Age*, ed. Juliann Emmons Allison. SUNY Series in Global Politics. Albany, NY: State University of New York Press.

Still, Brian. 2005. “Hacking for a Cause.” *First Monday*, 10(9): 1-14.

Stinnett, Douglas M., Jaroslav Tir, Philip Schafer, Paul F. Diehl, and Charles Gochman. 2002. "The Correlates of War Project Direct Contiguity Data, Version 3." *Conflict Management and Peace Science* 19(2): 58-66.

Sussman, Leonard. 2000. “The Internet and Press Freedom” *Freedom House*. <http://www.wpfc.org/site/docs/pdf/Publications/Working%20Papers-Conf%20Booklet.pdf>.

Tarar, Ahmer. 2006. “Diversionary Incentives and the Bargaining Approach to War.” *International Studies Quarterly*, 50(1): 169-188.

Tarar, Ahmer and Bahar Leventoglu. 2009. “Public Commitment in Crisis Bargaining.” *International Studies Quarterly*, 53: 817-839.

Tavares, José. 2004. “The open society assesses its enemies: shocks, disasters and terrorist attacks.” *Journal of Monetary Economics*, 51: 1039-1070.

Themner, Lotta and Peter Wallensteen. 2013. “Armed Conflict, 1946-2012.” *Journal of Peace Research*, 50(4): 509-521.

Thompson, William R. 2001. “Identifying Rivals and Rivalries in World Politics.” *International Studies Quarterly*, 45(4): 557-86.

Thompson, William R. and David R. Dreyer. 2012. *Handbook of International Rivalries, 1494-2010*. Washington, D.C.: CQ Press.

Toft, Peter, Arash Duero and Arunas Bieliauskas. 2010. “Terrorist targeting and energy security.” *Energy Policy*, 38(2010): 4411-4421.

Trendle, Giles. 2002. “Cyberwar.” *The World Today*, 58(4): 7-8.

Ullah, Asmat, Mohib Ullah Khan, Shahid Ali and Syed Waqar Hussain. 2012. “Foreign Direct Investment and Sectorial Growth of Pakistan Economy: Evidence from Agricultural and Industrial Sector (1979 to 2009).” *African Journal of Business Management*, 6(26): 7816-722.

U.S. Congress. House of Representatives. Subcommittee on Europe, Eurasia, and Emerging Threats. 2013. *Cyber Attacks: An Unprecedented Threat to U.S. National Security*. 113th Congress, 2nd Session, 21 March.

U.S. Congressional Research Service. 2004. “The Economic Impact of Cyber-Attacks (RL32331), prepared by Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel.” Available at: <http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf>.

Valeriano, Brandon and Ryan Maness. 2014. “The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011.” *Journal of Peace Research*. Forthcoming. Available at: http://wpsa.research.pdx.edu/meet/2012/manessvaleriano.pdf.

Van Belle, Douglas. 1997. “Press Freedom and the Democratic Peace.” *Journal of Peace Research* 34(4): 405-414.

van Dijk, Jan. 2005. *The Deepening Divide: Inequality in the Information Society*. Thousand Oaks, CA: Sage Publications.

Vasquez, John. 1993. *The War Puzzle*. Cambridge: Cambridge University Press.

Vasquez, John A. 1995. "Why Do Neighbors Fight? Proximity, Interaction, or Territoriality." *Journal of Peace Research*, 32(3): 277-293.

Vasquez, John A. 1996. "Distinguishing Rivals That Go to War from Those That Do Not: A Quantitative Comparative Case Study of the Two Paths to War." *International Studies Quarterly*, 40(4): 531-558.

Vatis, Michael. 2001. "Cyber Attacks During the War on Terrorism: A Predictive Analysis." Dartmouth College: Institute for Security Technology Studies.

Vuong, Quang H. 1989. "Likelihood Ratio Tests for Model Selection and Non-Nested Hypotheses." *Econometrica*, 57(2): 307-333.

Wade, Sara Jackson and Dan Reiter. 2007. "Does Democracy Matter? Regime Type and Suicide Terrorism." *Journal of Conflict Resolution*, 51(2): 329-348.

Walt, Stephen M. 1991. "The Renaissance of Security Studies." *International Studies Quarterly*, 35(2), 211-239.

Weimann, Gabriel. 2005. "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict & Terrorism*, 28: 129-149.

Wheeler, David A. and Gregory N. Larsen. 2003. "Techniques for Cyber Attack Attribution. Institute for Defense Analysis." IDA Paper P-3792.

Whitten-Woodring, Jenifer. 2009. "Watchdog of Lapdop? Media Freedom, Regime Type, and Government Respect for Human Rights." *International Studies Quarterly*, 53:595-625.

Williams, Richard. 2012. "Panel Data 3: Conditional Logit/Fixed Effects Logit Models." Accessed January 2, 2014. Available at: www3.nd.edu/~rwilliam/stats3/Panel03-FixedEffects.pdf.

Winkler, Jonathan Reed. 2008. *Nexus: Strategic Communications and American Security in World War I*. Cambridge, MA: Harvard University Press.

World Bank. 2013. "World Development Indicators 2013." Washington, DC: World Bank.

Worthington, Elise. 2014. "Internet Security Expert Says No Such Things as Online Privacy." May 12. http://www.abc.net.au/news/2014-05-12/internet-security-expert-says-no-such-thing-as/5445830 (1 May 2014).

Xiaoming, Hao and Chow Seet Kay. 2004. "Factors Affecting Internet Development: An Asian Survey." *First Monday* 9(2), 1-22.

Young, Joseph K. and Michael G. Findley. 2011. "Promise and Pitfalls of Terrorism Research." *International Studies Review*, 13: 411-431.

# Appendix A - Chapter 2 Tables and Graphs

## Virtual Associates Search Terms

The following search terms were used to ensure as many cases of cyber threats as possible were detected: botnet, Chinese firewall, computer worm, cyber, cyber attack, cyber crime, cyber espionage, cyber sabotage, cyber spying, cyber terror, cyber terrorism, cyber threat, cyber war, cyber warfare, cyberattack, cyber-attack, cybercrime, cyber-crime, cyberespionage, cyber-espionage, cyber-sabotage, cyberspace, cyber-space, cyberterror, cyber-terror, cyberterrorism, cyber-terrorism, cyberthreat, cyber-threat, cyberwar, cyber-war, cyberwarfare, cyber-warfare, DDoS, denial of service, distributed denial of service, firewall, GhostNet, hacked, hacker, hackers, hacking, hacktivism, industrial espionage, LulzSec, Moonlight Maze, Pentagon firewall, power grid, Red Hacker Alliance, rootkit, Stuxnet, Titan Rain, Trojan horse virus, and Trojan horse.

## Chapter 2 Additional Tables and Results

### Table A.1 Fixed Effects Logit and Rare Event Logit Comparison

| | (1 – Fixed Effects) | (2 – Rare Event) |
|---|---|---|
| | Attacks | Attacks |
| GDP Per Capita (Logged) | 3.41** | 0.85** |
| | (2.38) | (2.06) |
| Military Size (Logged) | -0.21 | 1.43** |
| | (-0.07) | (2.30) |
| Polity | 0.31 | 0.07 |
| | (0.44) | (1.15) |
| Freedom of the Press | 1.27 | -0.10 |
| | (1.26) | (-0.12) |
| International Conflicts | 1.86 | 0.68 |
| | (1.15) | (1.02) |
| Media Bias (Logged) | -0.46 | -0.45 |
| | (-0.73) | (-1.47) |
| Constant | - - - | -26.63*** |
| | | (-2.83) |

*(z statistics in parentheses)* * *p* < .10, ** *p* < .05, *** *p* < .01

## Table A.2 Fixed Effects Results

| | Model 1 | Model 2 | Model 3 | Model 4 |
|---|---|---|---|---|
| | *Aggregate Cyber* | *Cyber Attacks* | *Cyber Terrorism* | *Cyber Espionage* |
| GDP Per Capita (Logged) | 0.08** | 3.41** | 0.07*** | 0.01 |
| | (2.40) | (2.38) | (2.94) | (0.51) |
| Military Size (Logged) | -0.03 | -0.21 | -0.03 | -0.01 |
| | (-0.86) | (-0.07) | (-1.20) | (-0.37) |
| Polity | 0.00 | 0.31 | 0.00 | -0.00 |
| | (0.07) | (0.44) | (0.18) | (-0.12) |
| Freedom of the Press | 0.01 | 1.27 | 0.00 | 0.00 |
| | (0.28) | (1.26) | (0.11) | (0.23) |
| International Conflicts | -0.01 | 1.85 | -0.04 | -0.03 |
| | (-0,17) | (1.15) | (-0.78) | (-0.96) |
| Lagged D.V. | 0.19*** | - - - | - - - | 0.34*** |
| | (9.74) | | | (18.57) |
| Media Bias (Logged) | 0.04** | -0.46 | 0.05*** | -0.00 |
| | (2.09) | (-0.73) | (3.92) | (-0.26) |
| Constant | -0.45 | - - - | -0.48 | 0.04 |
| | (-0.88) | | (-1.35) | (0.20) |
| *Model N* | *2,650* | *129* | *2,771* | *2,650* |

*(z statistics in parentheses)*; * *p* < .10, ** *p* < .05, *** *p* < .01; Models 1, 3 & 4 were run with xtreg, Model 2 was run with xtlogit

## Figure A.1 Model 1 – GDP Per Capita: Global Averages

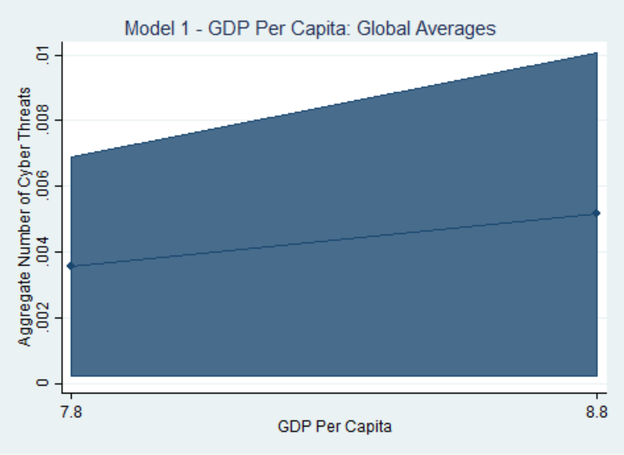


Figure A.2  Model 1 – GDP Per Capita: U.S. Averages

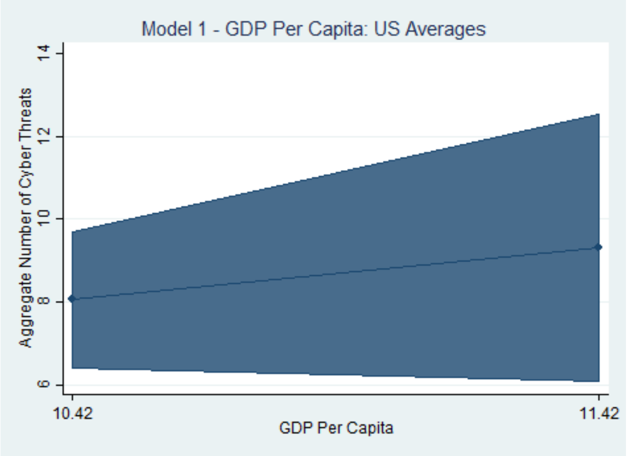


Figure A.3  Model 2 – GDP Per Capita: Global Averages

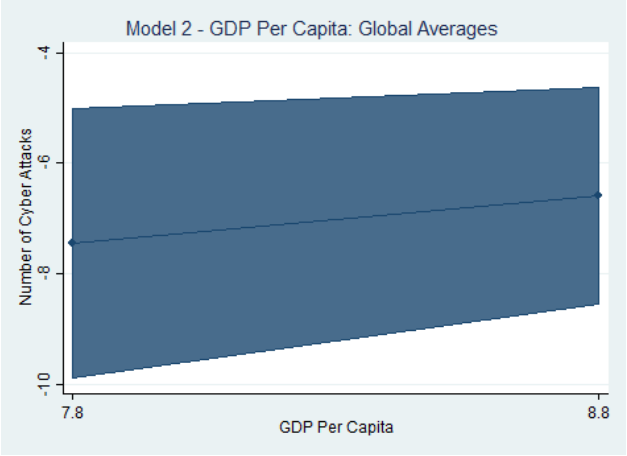
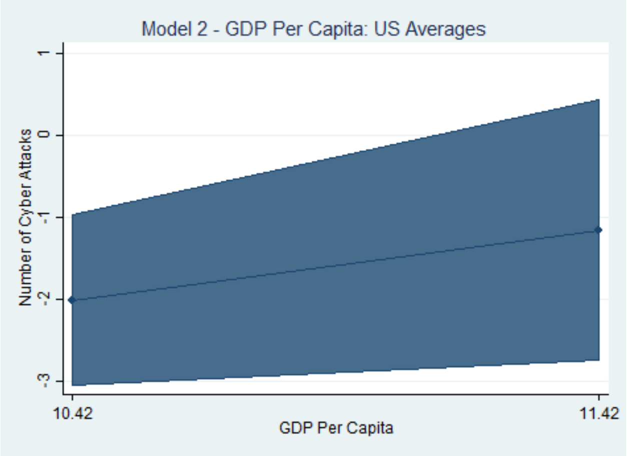
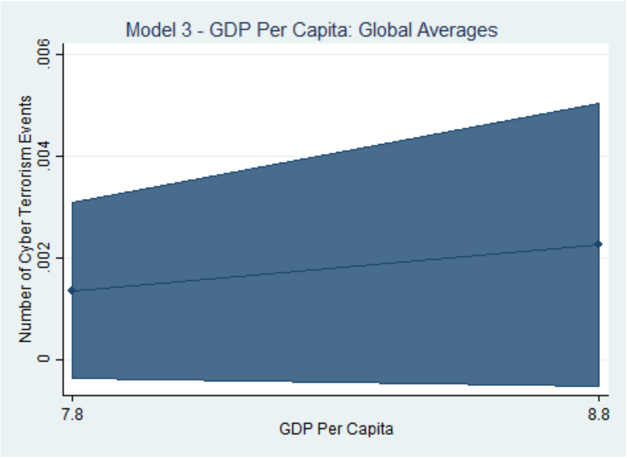


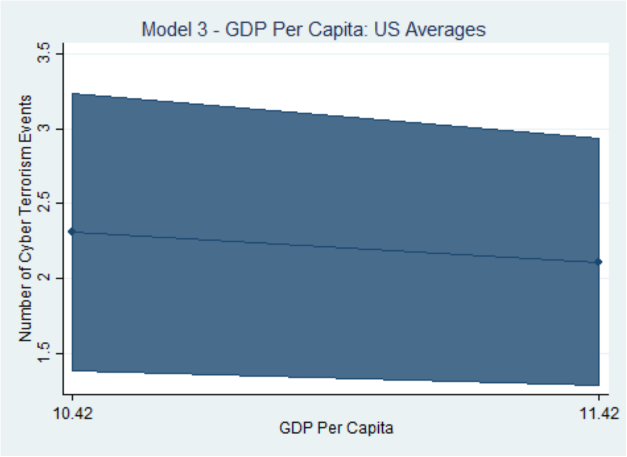
Figure A.4  Model 2 – GDP Per Capita: U.S. Averages



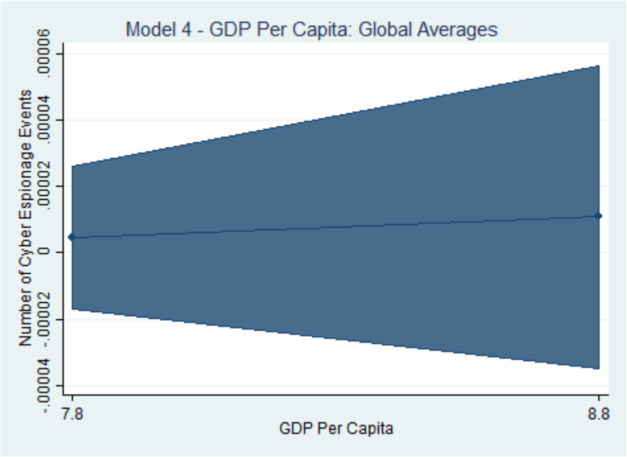
### Figure A.5  Model 3 – GDP Per Capita: Global Averages



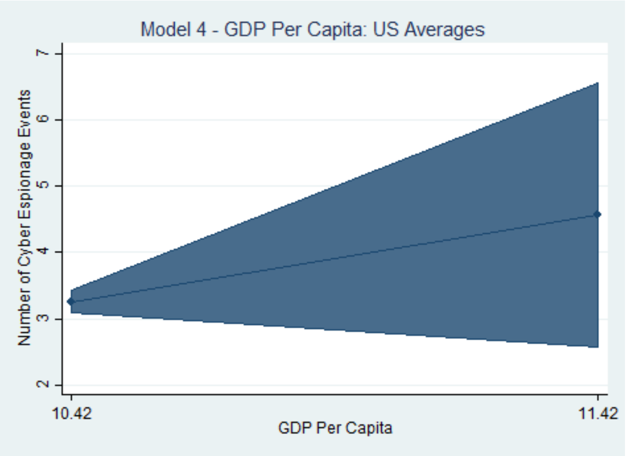
### Figure A.6  Model 3 – GDP Per Capita: U.S. Averages



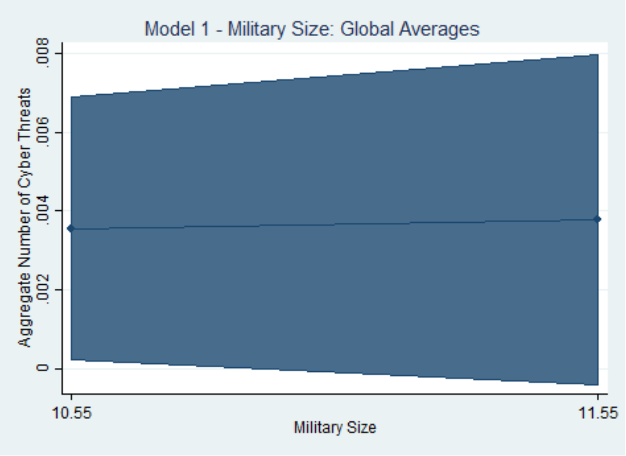
### Figure A.7  Model 4 – GDP Per Capita: Global Averages



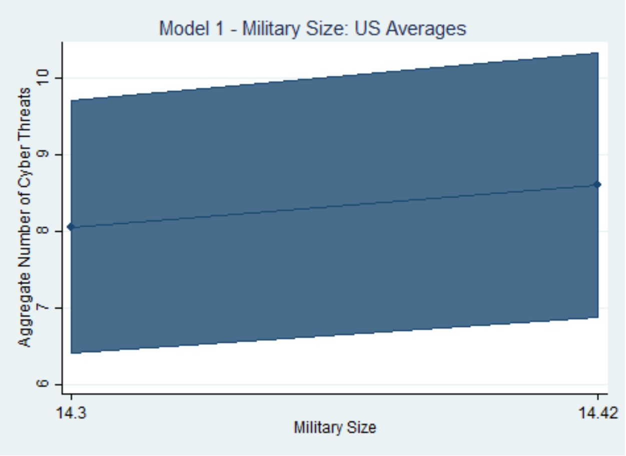
## Figure A.8  Model 4 – GDP Per Capita: U.S. Averages



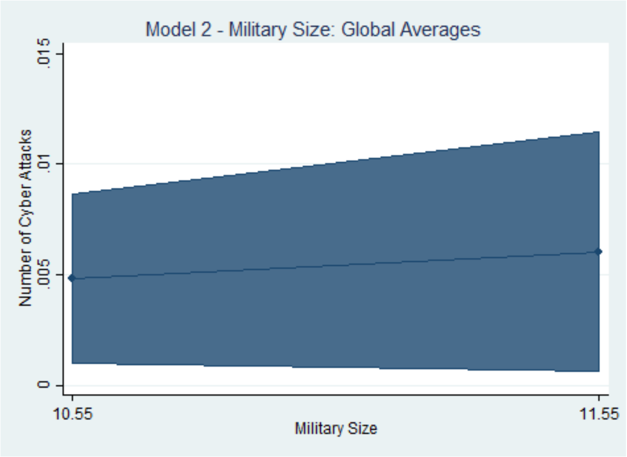
## Figure A.9  Model 1 – Military Size: Global Averages



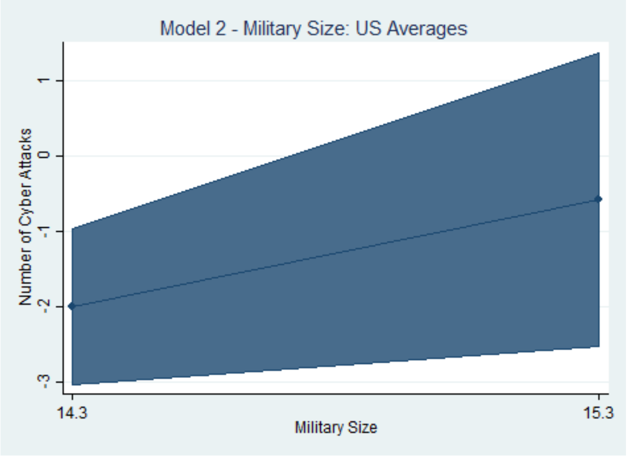
## Figure A.10  Model 1 – Military Size: U.S. Averages



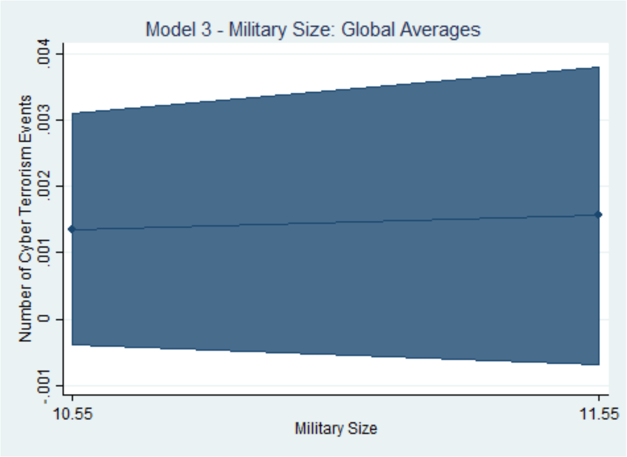
### Figure A.11  Model 2 – Military Size: Global Averages



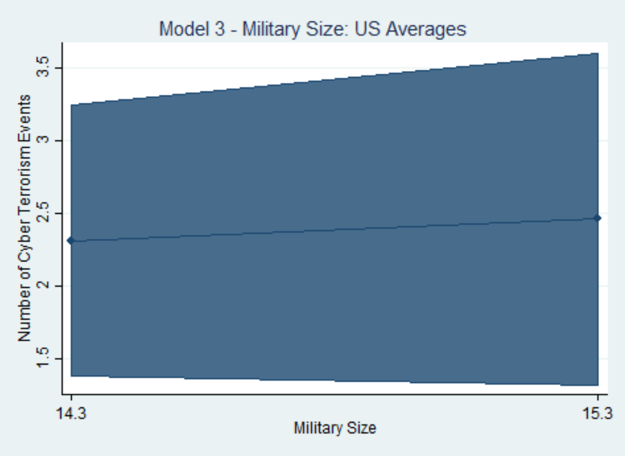
### Figure A.12  Model 2 – Military Size: U.S. Averages



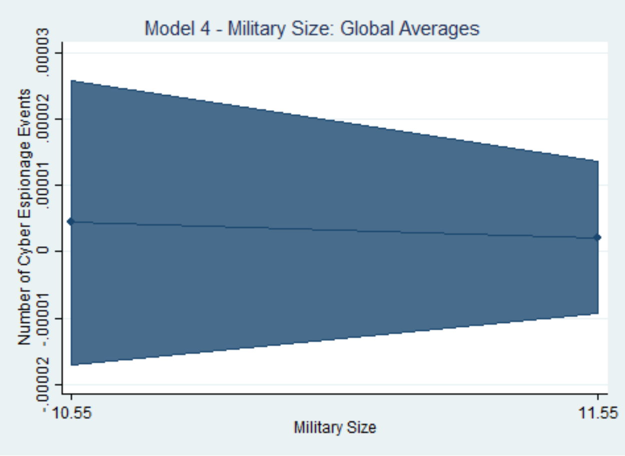
### Figure A.13  Model 3 – Military Size: Global Averages



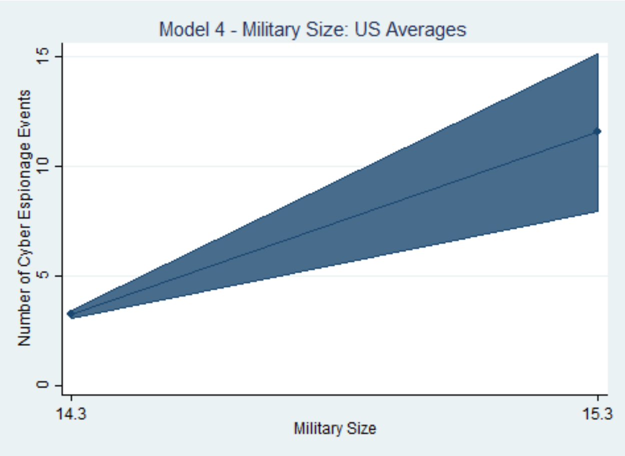
### Figure A.14  Model 3 – Military Size: U.S. Averages



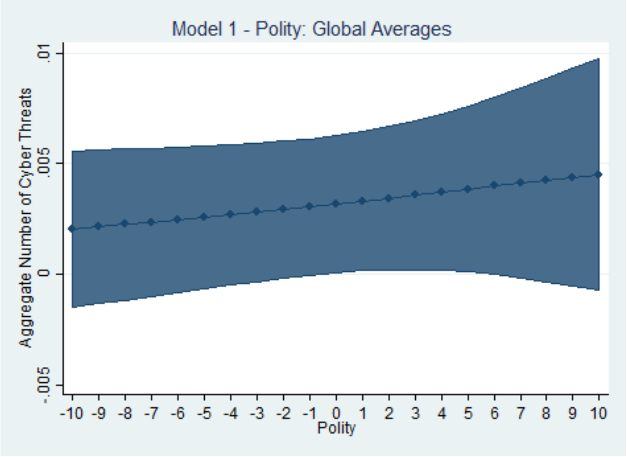
### Figure A.15  Model 4 – Military Size: Global Averages



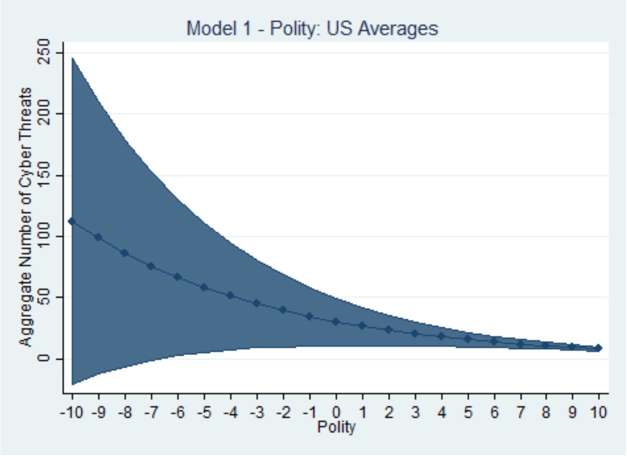
### Figure A.16  Model 4 – Military Size: U.S. Averages



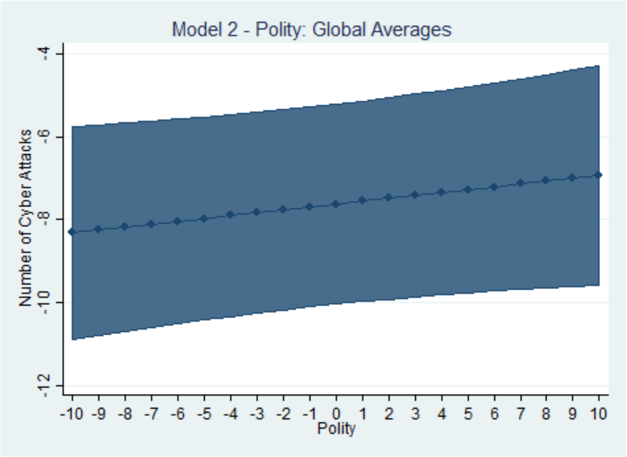
### Figure A.17 Model 1 – Polity: Global Averages



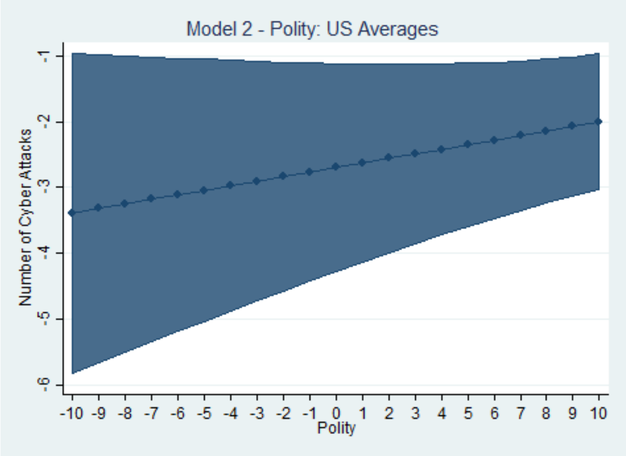
### Figure A.18 Model 1 – Polity: U.S. Averages



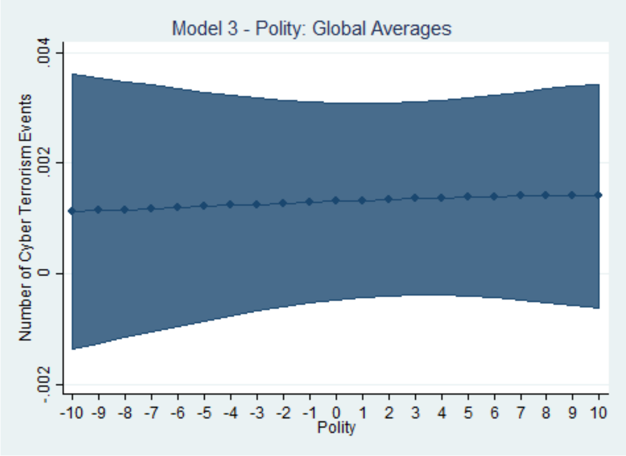
### Figure A.19 Model 2 – Polity: Global Averages



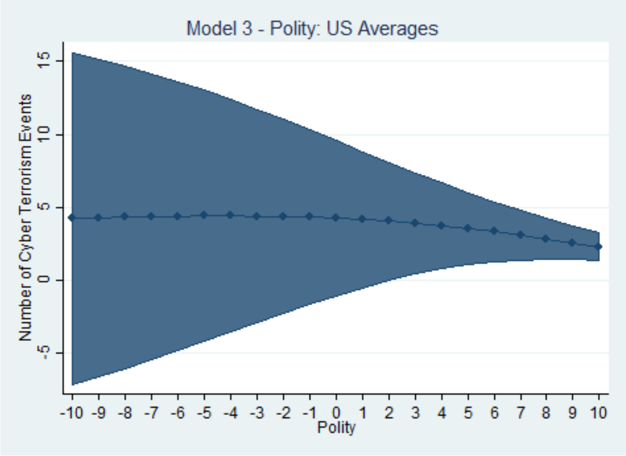
### Figure A.20 Model 2 – Polity: U.S. Averages



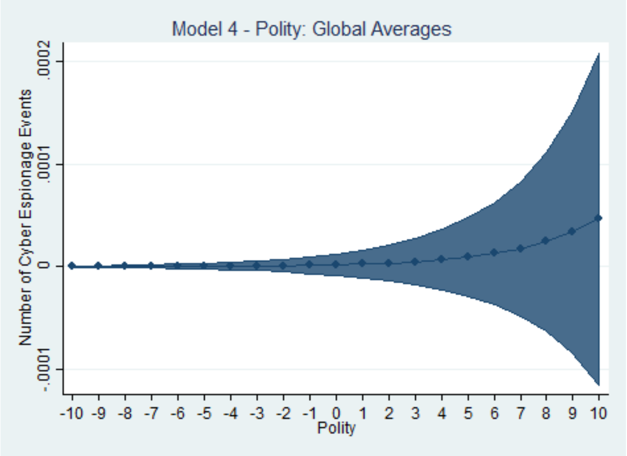
### Figure A.21 Model 3 – Polity: Global Averages



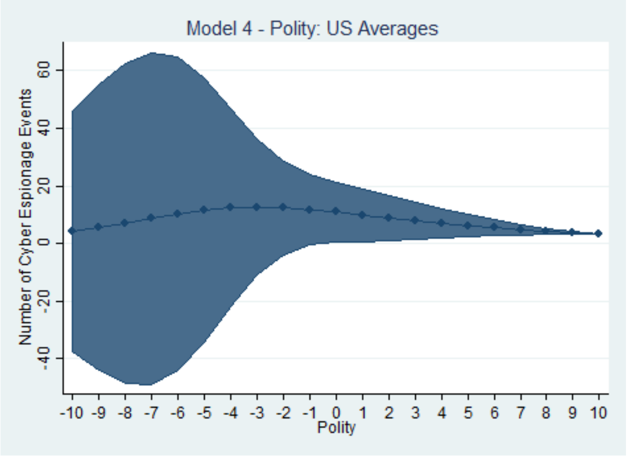
### Figure A.22 Model 3 – Polity: U.S. Averages



## Figure A.23 Model 4 – Polity: Global Averages



## Figure A.24 Model 4 – Polity: U.S. Averages



## Figure A.25 Model 1 – Freedom of Speech: Global Averages

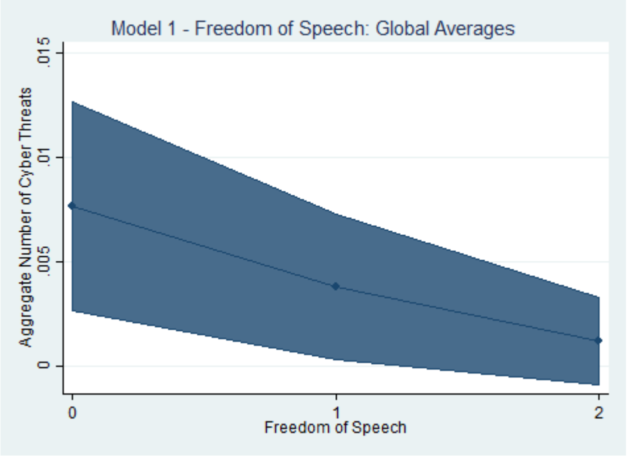


Figure A.26  Model 1 – Freedom of Speech: U.S. Averages

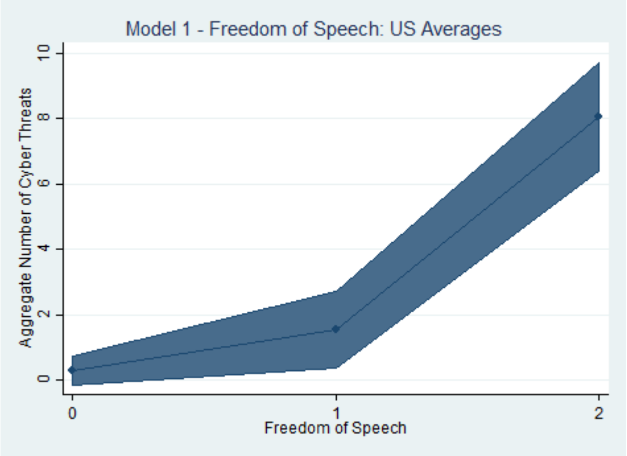


Figure A.27  Model 2 – Freedom of Speech: Global Averages

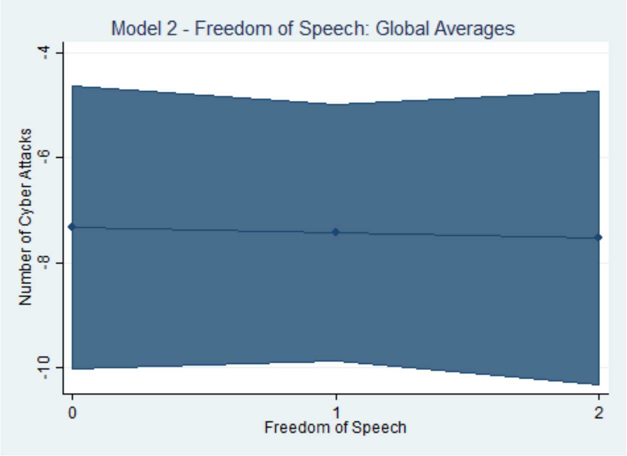
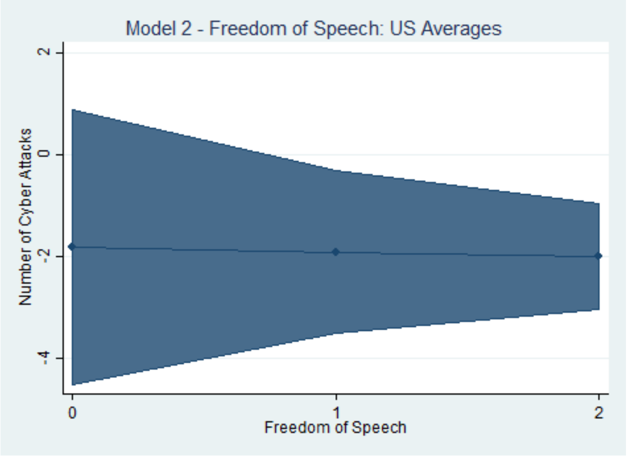
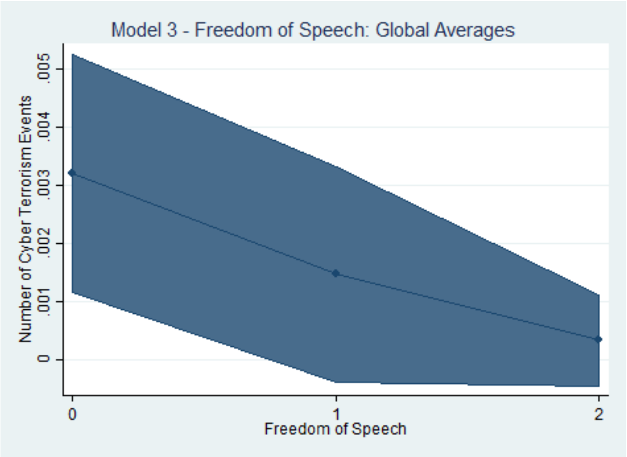


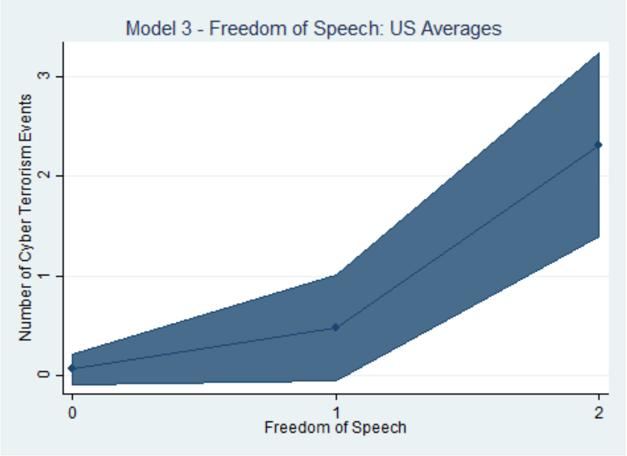
Figure A.28  Model 2 – Freedom of Speech: U.S. Averages



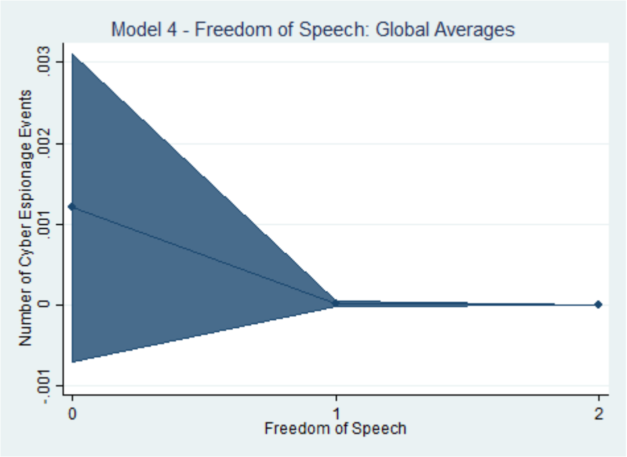
### Figure A.29 Model 3 – Freedom of Speech: Global Averages



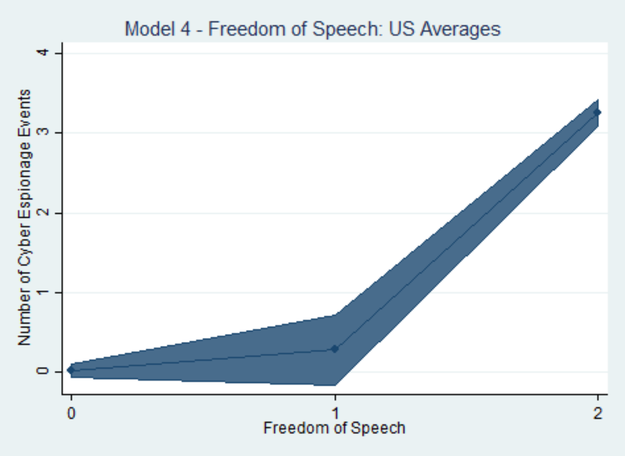
### Figure A.30 Model 3 – Freedom of Speech: U.S. Averages



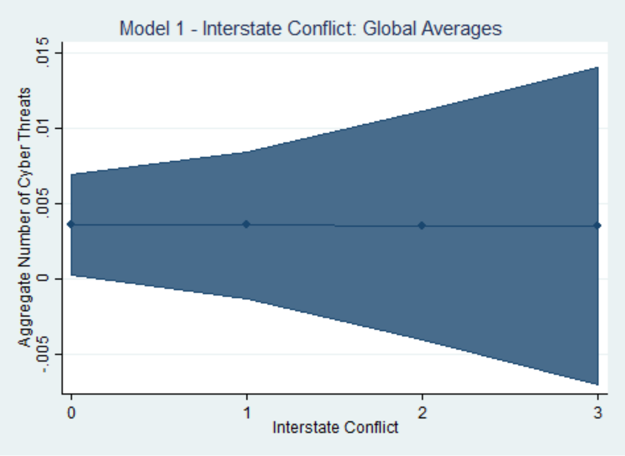
### Figure A.31 Model 4 – Freedom of Speech: Global Averages



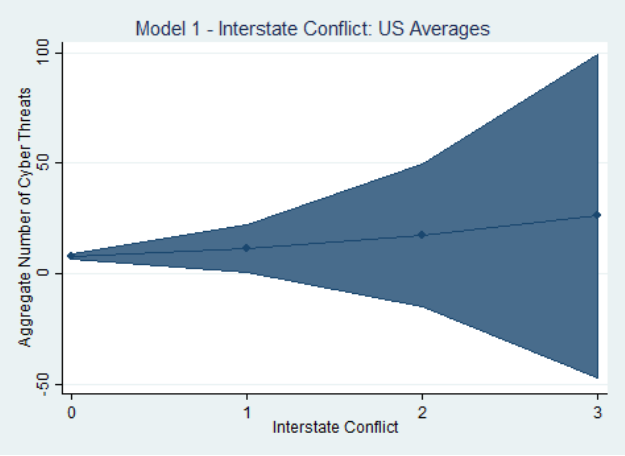
## Figure A.32 Model 4 – Freedom of Speech: U.S. Averages



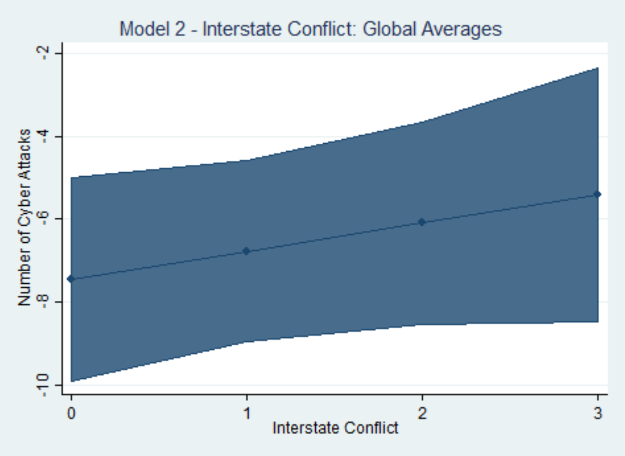
## Figure A.33 Model 1 – Interstate Conflict: Global Averages



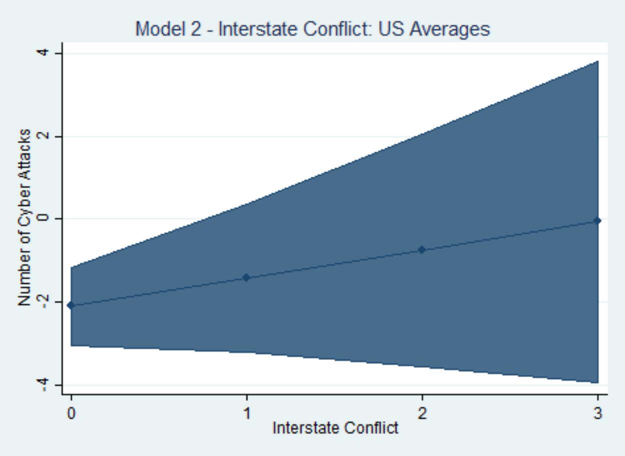
## Figure A.34 Model 1 – Interstate Conflict: U.S. Averages



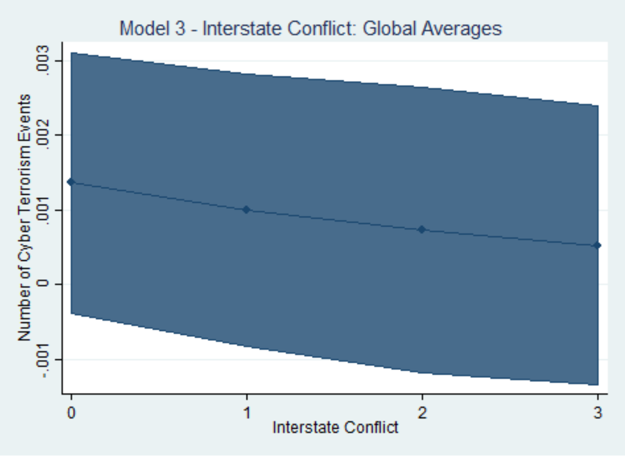
## Figure A.35  Model 2 – Interstate Conflict: Global Averages



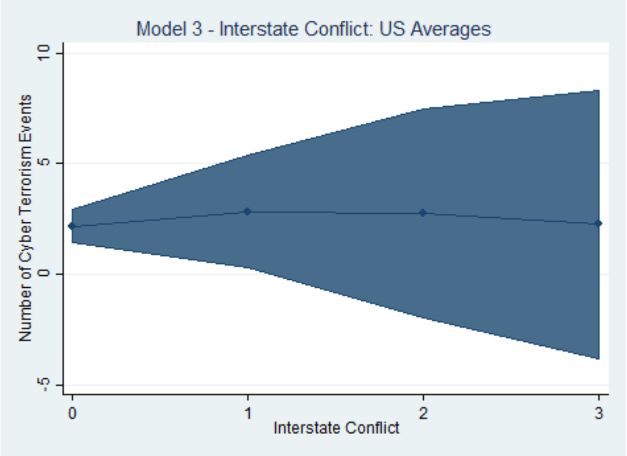
## Figure A.36  Model 2 – Interstate Conflict: U.S. Averages



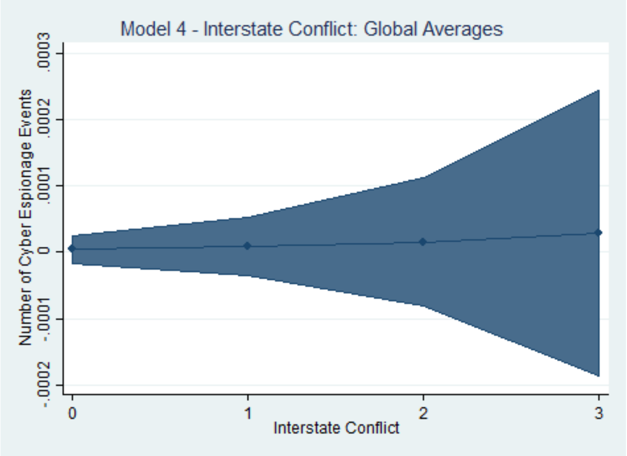
## Figure A.37  Model 3 – Interstate Conflict: Global Averages



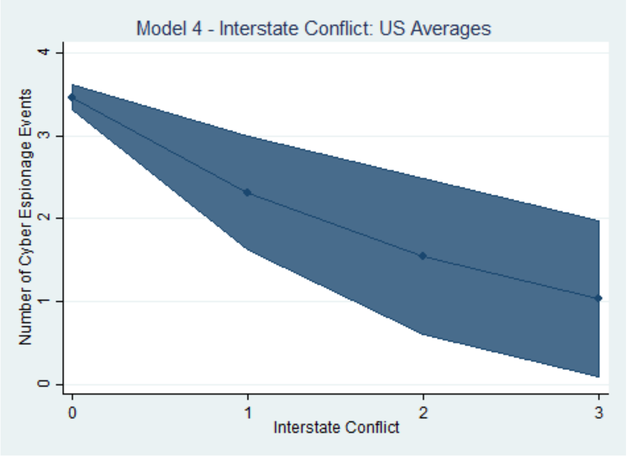
### Figure A.38 Model 3 – Interstate Conflict: U.S. Averages



### Figure A.39 Model 4 – Interstate Conflict: Global Averages



### Figure A.40 Model 4 – Interstate Conflict: U.S. Averages



# Appendix B - Chapter 3 Tables and Graphs

## Chapter 3 Additional Tables and Results

### Table B.1 Fixed Effects Estimates of Cyber Attack Event Counts (Binary)

| | Model 1<br>Coefficient | Model 2<br>Coefficient |
|---|---|---|
| Enduring Rivalry – Binary (1990-2001) | -0.02<br>(-0.35) | - - - |
| Strategic Rivalry – Binary (1990-2001) | - - - | 0.14<br>(1.38) |
| GDP per capita (logged) | 0.17*<br>(1.82) | 0.17*<br>(1.84) |
| Military Size (logged) | -0.09<br>(-1.25) | -0.10<br>(-1.39) |
| Regime Type | -0.00<br>(-0.52) | -0.00<br>(-0.37) |
| Total Population (logged) | 0.60*<br>(1.92) | 0.73**<br>(2.25) |
| Media Bias (logged) | 0.06<br>(1.49) | 0.06<br>(1.54) |
| Lagged D.V. | 0.22***<br>(7.97) | 0.22***<br>(7.92) |
| Constant | -1.97**<br>(-1.97) | -2.22**<br>(-2.21) |
| *Model N* | *1,460* | *1,463* |

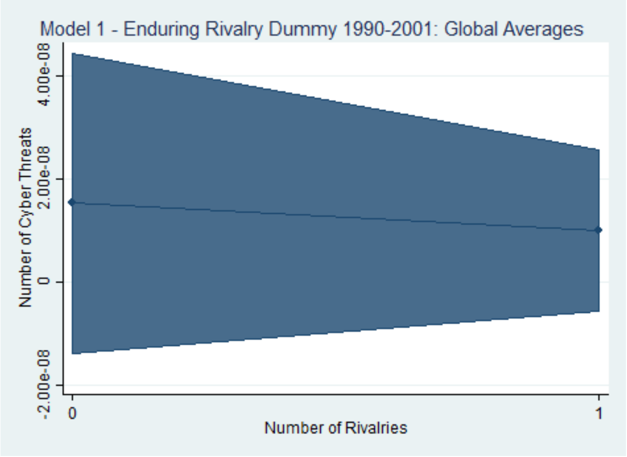
** p < .10, ** p < .05, *** p < .01 (Z Scores in parentheses), Two-Tail Test; (Regional dummies omitted due to collinearity)*

### Table B.2 Fixed Effects Estimates of Cyber Attack Event Counts (Count)

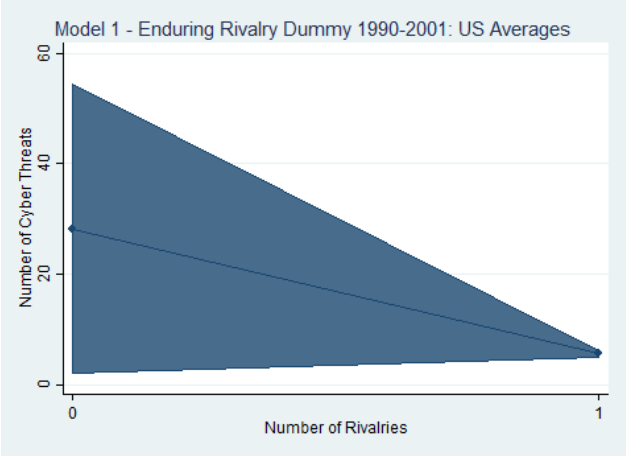
| | Model 3<br>Coefficient | Model 4<br>Coefficient | Model 5<br>Coefficient |
|---|---|---|---|
| Enduring Rivalry – Count (1990-2001) | -0.12***<br>(-5.19) | - - - | - - - |
| Strategic Rivalry – Count (1990-2001) | - - - | 0.28***<br>(4.48) | - - - |
| Strategic Rivalry – Count (1990-2009) | - - - | - - - | 0.19***<br>(4.59) |
| GDP per capita (logged) | 0.12<br>(1.30) | 0.17*<br>(1.88) | 0.06*<br>(1.81) |
| Military Size (logged) | -0.08<br>(-1.23) | -0.11<br>(-1.63) | -0.06<br>(-1.37) |
| Regime Type | -0.01<br>(-0.75) | -0.00<br>(-0.25) | 0.00<br>(0.33) |
| Total Population (logged) | 0.57*<br>(1.86) | 0.85***<br>(2.71) | 0.21<br>(1.55) |
| Media Bias (logged) | 0.06*<br>(1.73) | 0.06<br>(1.60) | 0.04**<br>(2.26) |
| Lagged D.V. | 0.19***<br>(6.49) | 0.21***<br>(7.42) | 0.18***<br>(8.99) |
| Constant | -1.49<br>(-1.51) | -2.48**<br>(-2.51) | -0.66<br>(1.26) |
| *Model N* | *1,460* | *1,463* | *2,511* |

** p < .10, ** p < .05, *** p < .01  (Z Scores in parentheses),  Two-Tail Test*

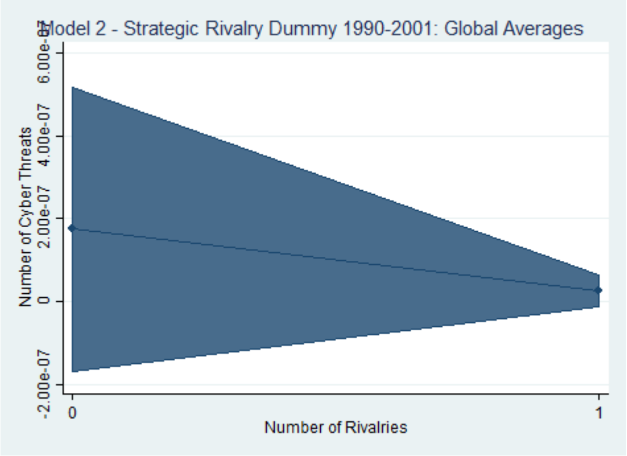
### Figure B.1 Model 1 – Enduring Rivalry Dummy 1990-2001: Global Averages



### Figure B.2 Model 1 – Enduring Rivalry Dummy 1990-2001: U.S. Averages



### Figure B.3 Model 2 – Strategic Rivalry Dummy 1990-2001: Global Averages



### Figure B.4 Model 2 – Strategic Rivalry Dummy 1990-2001: U.S. Averages

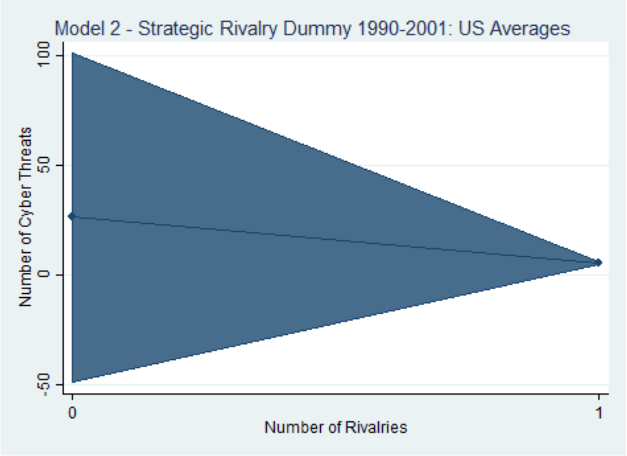


**Figure B.5 Model 3 – Enduring Rivalry Count 1990-2001: Global Averages**

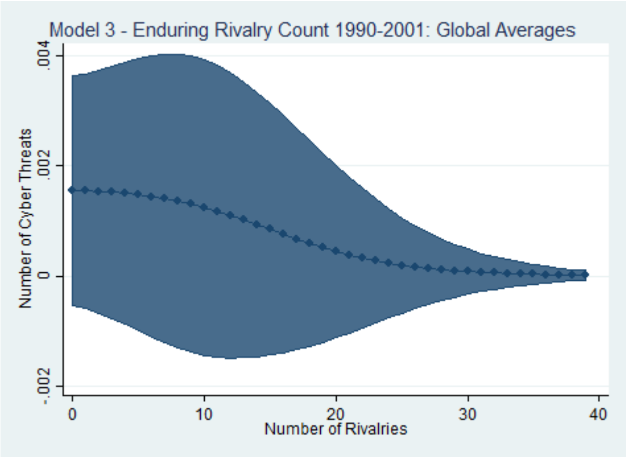


**Figure B.6 Model 3 – Enduring Rivalry Count 1990-2001: U.S. Averages**

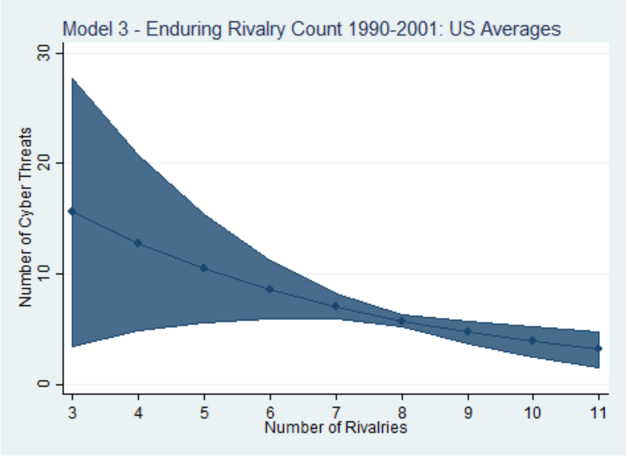
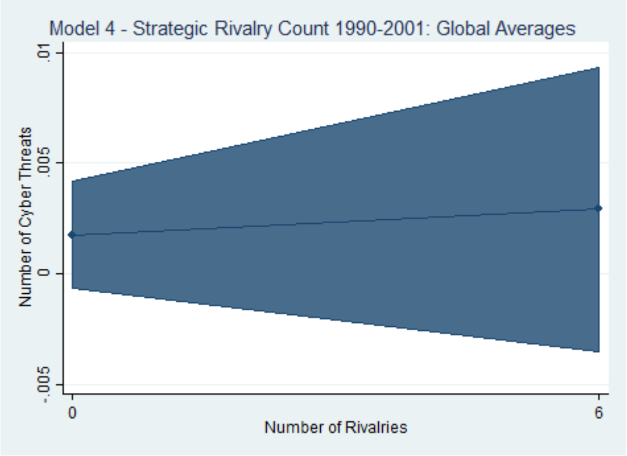
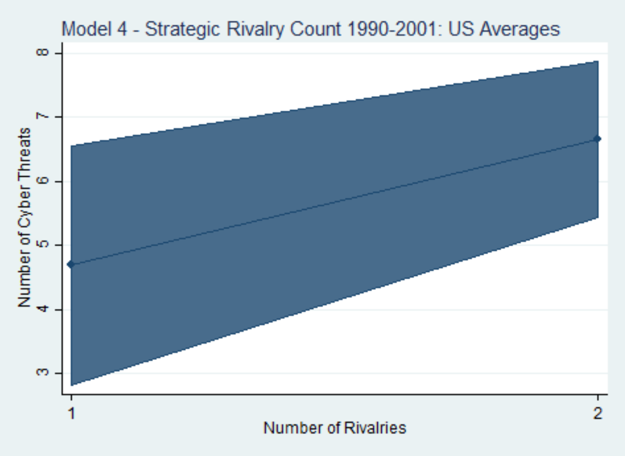


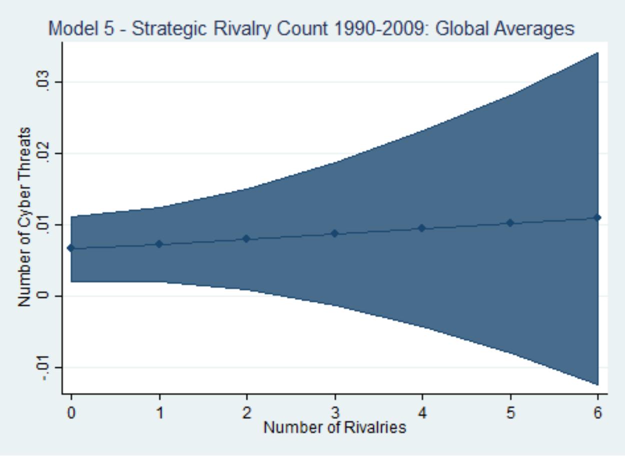
**Figure B.7 Model 4 – Strategic Rivalry Count 1990-2001: Global Averages**



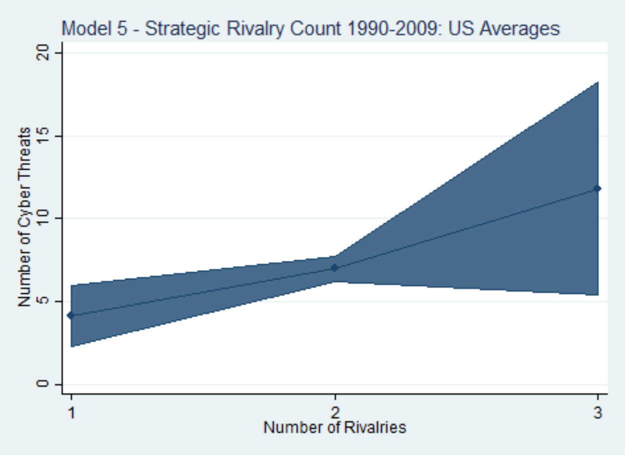
## Figure B.8 Model 4 – Strategic Rivalry Count 1990-2001: U.S. Averages



## Figure B.9 Model 5 – Strategic Rivalry Count 1990-2009: Global Averages



## Figure B.10 Model 5 – Strategic Rivalry Count 1990-2009: U.S. Averages



# Appendix C - Chapter 4 Tables and Graphs

### Table C.1 Correlates of War (COW) & PRIO Interstate War Fixed Effects Results

| | Model 1 | Model 2 | Model 3 | Model 4 |
|---|---|---|---|---|
| | *COW War* | *COW War* | *PRIO War* | *PRIO War* |
| Cyber Espionage | -0.05***<br>(-3.87) | - - - | 0.01<br>(0.61) | - - - |
| Cyber Attack & Terrorism | - - - | 0.01<br>(0.95) | - - - | 0.01*<br>(1.65) |
| Regime Type | 0.00<br>(0.57) | 0.00<br>(0.56) | -0.00<br>(-0.18) | -0.00<br>(-0.18) |
| Contiguity | -0.05***<br>(-3.70) | -0.05***<br>(3.63) | -0.02*<br>(-1.83) | -0.02*<br>(-1.80) |
| Alliance Participation | -0.00<br>(-0.12) | -0.00<br>(-0.11) | -0.00<br>(-0.12) | -0.00<br>(-0.12) |
| CINC (logged) | -0.02<br>(-0.91) | -0.02<br>(-0.89) | -0.03<br>(-1.53) | -0.03<br>(-1.55) |
| IGO Membership | -0.00**<br>(-2.46) | -0.00**<br>(-2.50) | -0.00<br>(-0.83) | -0.00<br>(-0.87) |
| Economic Interdependence (logged) | 0.00<br>(0.08) | 0.00<br>(0.01) | -0.00<br>(-0.43) | -0.00<br>(-0.43) |
| COW (lagged) | -0.07***<br>(-3.00) | -0.07***<br>(-3.18) | - - - | - - - |
| PRIO (lagged) | - - - | - - - | 0.47***<br>(30.93) | 0.47***<br>(31.01) |
| Media Bias (logged) | 0.00<br>(0.58) | 0.00<br>(0.47) | -0.00<br>(-0.28) | -0.00<br>(-0.36) |
| Constant | 0.30*<br>(1.75) | 0.30*<br>(1.75) | -0.00<br>(-0.03) | -0.01<br>(-0.04) |

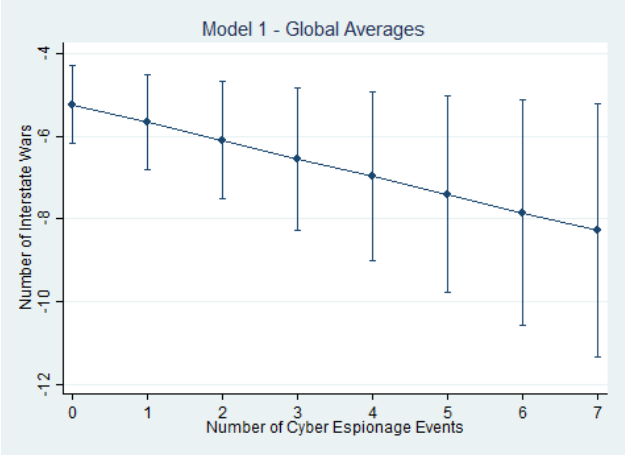
** p < .10, ** p < .05, *** p < .01 (Z Scores in parentheses), Two-Tail Test*
*Model 1 & 2 N = 2,126; Model 3 & 4 N = 2,126*

### Table C.2 Militarized Interstate Dispute (MID) Fixed Effects Results

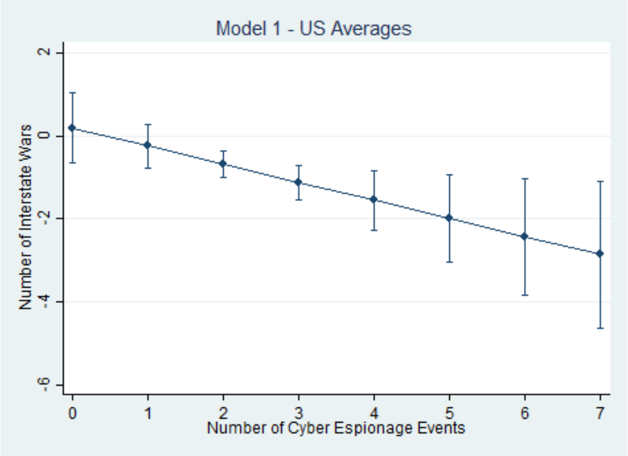
| | Model 5 | Model 6 |
|---|---|---|
| | Coefficient | Coefficient |
| *Inflated Negative Binomial* | | |
| Cyber Espionage | .13* | - - - |
| | (1.92) | |
| Cyber Attack & Terrorism | - - - | 0.14*** |
| | | (4.71) |
| Regime Type | 0.00 | 0.00 |
| | (0.56) | (0.57) |
| Contiguity | 0.04 | 0.04 |
| | (0.54) | (0.61) |
| Alliance Participation | 0.11*** | 0.11*** |
| | (3.61) | (3.69) |
| CINC (logged) | 0.10 | 0.09 |
| | (0.91) | (0.87) |
| IGO Membership | 0.00 | 0.00 |
| | (1.33) | (1.24) |
| Economic Interdependence (logged) | 0.00 | 0.00 |
| | (0.11) | (0.10) |
| MID (lagged) | 0.23*** | 0.22*** |
| | (10.27) | (2.69) |
| Media Bias (logged) | 0.06*** | 0.06*** |
| | (2.91) | (2.69) |
| Constant | -0.22 | -0.23 |
| | (-0.26) | (-0.28) |

** p < .10, ** p < .05, *** p < .01 (Z Scores in parentheses), Two-Tail Test*
*Model 5 & 6 N = 2,129*

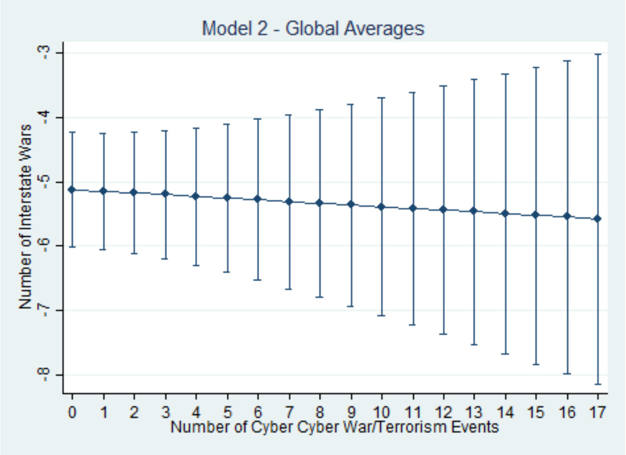
### Figure C.1 Model 1 – Interstate Wars (COW): Global Averages



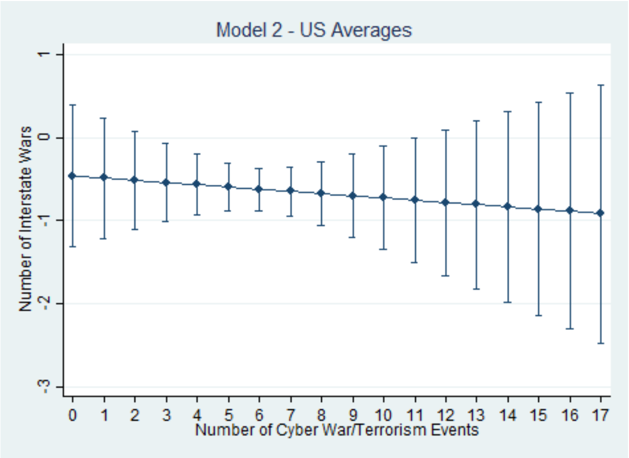
### Figure C.2 Model 1 – Interstate Wars (COW): U.S. Averages



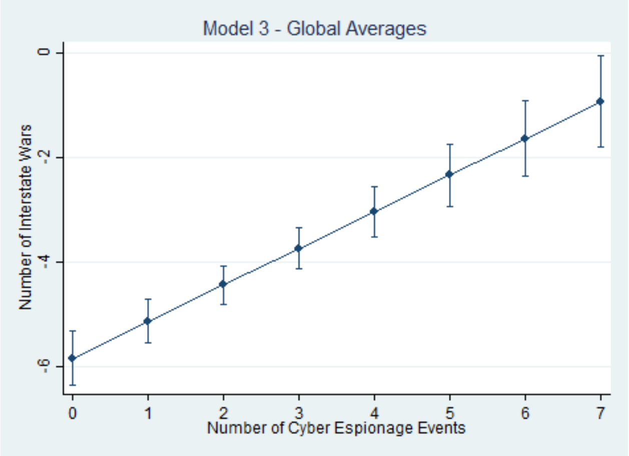
### Figure C.3 Model 2 – Interstate Wars (COW): Global Averages



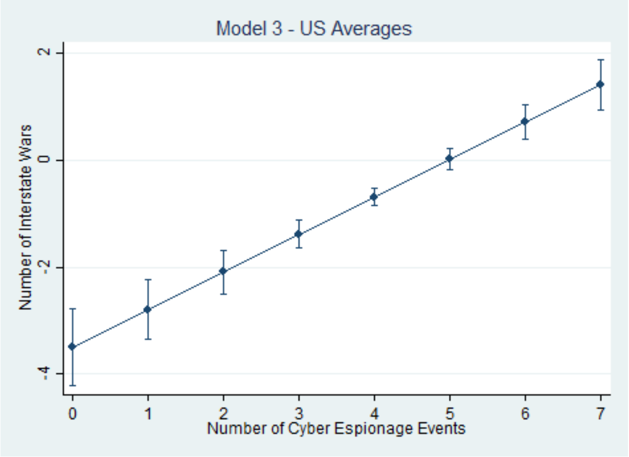
### Figure C.4 Model 2 – Interstate Wars (COW): U.S. Averages



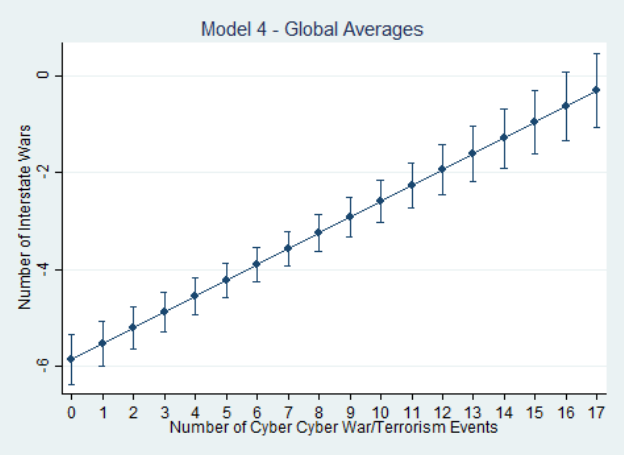
### Figure C.5 Model 3 – Interstate Wars (PRIO): Global Averages



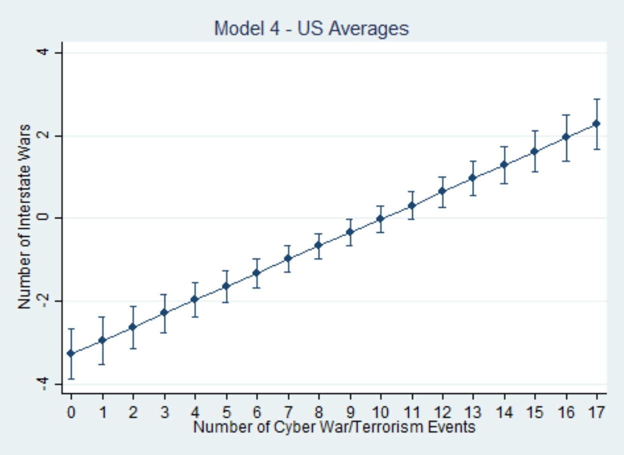
### Figure C.6 Model 3 – Interstate Wars (PRIO): U.S. Averages



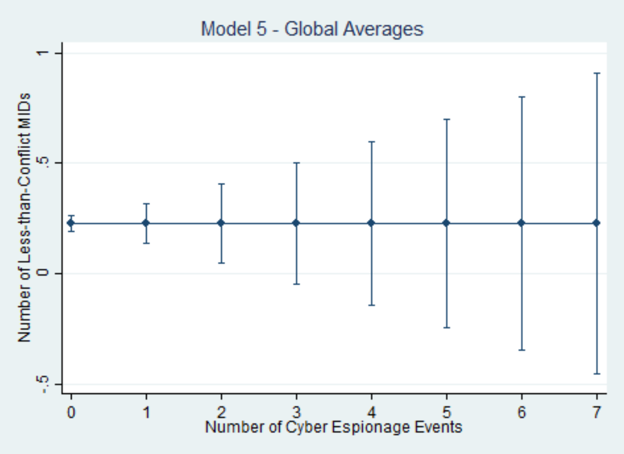
### Figure C.7 Model 4 – Interstate Wars (PRIO): Global Averages



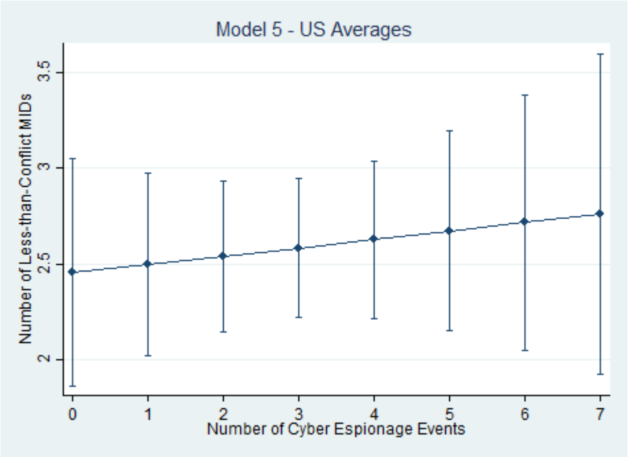
### Figure C.8 Model 4 – Interstate Wars (PRIO): U.S. Averages



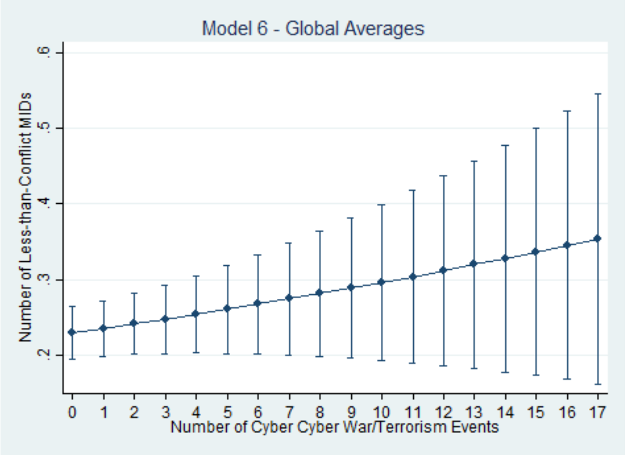
### Figure C.9 Model 5 – Interstate Wars (MIDs): Global Averages



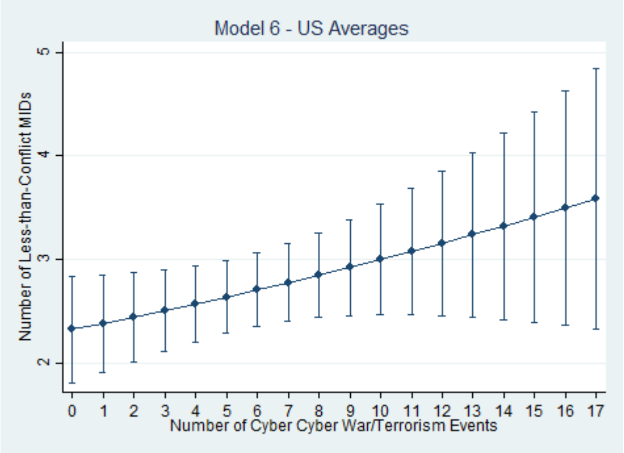
### Figure C.10 Model 5 – Interstate Wars (MIDs): U.S. Averages



### Figure C.11 Model 6 – Interstate Wars (MIDs): Global Averages



### Figure C.12 Model 6 – Interstate Wars (MIDs): U.S. Averages


Model 6 - US Averages
Number of Less-than-Conflict MIDs
Number of Cyber Cyber War/Terrorism Events