ANALYSIS OF CYBER INCIDENTS BETWEEN DYADIC RIVALS

by

Barry Edwin Newell

A thesis

submitted in partial fulfillment

of the requirements for the degree of

Master of Arts in Political Science

Boise State University

August 2016

BOISE STATE UNIVERSITY GRADUATE COLLEGE

DEFENSE COMMITTEE AND FINAL READING APPROVALS

of the thesis submitted by

Barry Edwin Newell

Thesis Title: Analysis of Cyber Incidents Between Dyadic Rivals

Date of Final Oral Examination: 13 June 2016

The following individuals read and discussed the thesis submitted by student Barry Edwin Newell, and they evaluated his presentation and response to questions during the final oral examination. They found that the student passed the final oral examination.

Michael Allen, Ph.D. Chair, Supervisory Committee

Brian Wampler, Ph.D. Member, Supervisory Committee

Michael Touchton, Ph.D. Member, Supervisory Committee

The final reading approval of the thesis was granted by Michael Allen, Ph.D., Chair of the Supervisory Committee. The thesis was approved for the Graduate College by Jodi Chilson, M.F.A., Coordinator of Theses and Dissertations.

ACKNOWLEDGEMENTS

There are many I need to acknowledge for their advice and guidance over the last year. First to Dr. Michael Allen for serving as Chairman of my Supervisory Committee as well as encouraging me to continue with my education. I would also like to thank Dr. Brian Wampler and Dr. Mike Touchton for serving on my Supervisory Committee and giving advice over the last year. Thanks is also given to Dr. Ross Burkhart who I've known from the very beginning of my collegiate career and who encouraged me to pursue my master's degree.

I would also like to acknowledge my fellow students in my cohort: Anna, Evan, Sally, and Tyler. It was a whirlwind of a year and I'm glad to have gone through this journey with you all.

To my family, friends, and roommates, you all gave me so much unconditional support and love when I needed it. And to the Almighty, I thank Him for the blessings He has bestowed upon my life.

ABSTRACT

Cyber conflict between states is a growing trend. There is a large body of research on cyber conflict, but there is very little quantitative analysis to support the theories or to assist in predicting future use of cyber operations. Using a logistic regression analysis, this thesis studies cyber conflicts between dyadic rivals from 2001 to 2011 to answer under what conditions cyber incidents occur between dyadic rivals in the past in the hopes to better analyze and predict future cyber incidents. The data demonstrate that the geographic proximity between dyads increases the probability of a cyber incident occurring while any or both of the dyads holds membership in NATO causes a decrease in the probability that cyber operations occur between dyadic rivals. The share of military personnel, military expenditure, and energy consumption is not enough to explain cyber incident trends. The results also show that many of my variables are conditional upon each other for their significance. It is imperative that states address the issues surrounding cyber conflict as the trend is increasing. At the present, the fear of retaliation will always be present as some argue that cyber defensive capabilities will never overtake cyber offensive capabilities as the latter is constantly transforming and evolving while the former is constantly playing "catch up."

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE: INTRODUCTION

As the world becomes more dependent upon cyberspace, states will have to address how to prevent and respond to a cyber incident, using both offensive and defensive capabilities. The use of cyber operations as part of a state's military strategy is increasing, particularly among dyadic rivals. As the cyber realm is already becoming the next anarchic frontier, states are developing offensive and defensive capabilities to protect their growing cyber dependence for the development, advancement, and maintenance of their infrastructure. There are plenty examples of state-on-state cyber incidents using distributed denials of service (DDoS), intrusions, sabotage, website defacement, Trojan horses, worms, and viruses such as the use of the Stuxnet worm, cyberespionage by China, and numerous cyber incidents attributed to Russia. It is interesting to note that the general trend has not been cyber incidents that could cripple their opponent, but rather incidents that serve more as a nuisance than anything serious. The use of cyber operations as military strategy is becoming a popular choice for states because it is relatively inexpensive, can be deployed relatively quickly, and the ability for perpetrators of an attack to remain anonymous. Anonymity is crucial if you are attempting to gather intelligence and attack your rival without causing escalation. Some scholars view the risks behind the use of cyber operations as low, but depending on the severity of an operation, they can have some serious costs and could lead to heightened escalation or retaliation against the attacking state.

Although there is a large body of research on cyber conflict and cyber incidents, there is very little quantitative analysis to support the theories or to assist in predicting future use of cyber operations. This thesis seeks to answer what has caused cyber incidents between dyadic rivals in the past in the hopes to better analyze and predict future cyber incidents. A better analysis is needed for a state to develop their cyber capacity and regulations properly. A better understanding will also assist states to address legal issues when cyber incidents occur between each other.

The extant literature varies on the causes of cyber conflict. My research centers on the research carried out by Valeriano and Maness (2014). Cyber operations are considered a part of asymmetric warfare and while many scholars argue that asymmetric warfare is commonly thought to be used solely by weak states, Breen and Geltzer (2011) demonstrate that strong states also employ asymmetric tactics. This assertion is backed by the data collected by Valeriano and Maness (2014). Breen and Geltzer (2011) argue that states that have computerized infrastructures and depend upon cyberspace become vulnerable to cyber incident. In seeking to explain and analyze reasons why a state would use cyber operations against another state, in any way, it is clear that no methodology, or approach, is self-sufficient and that various paradigms need to be brought together to produce stronger analysis. There are many challenges facing the study of cyber operations such as limited data and the anonymity of cyberspace.

There are currently conflicting claims regarding the threat posed to national security. There is a lack of empirical evidence that supports the claim that cyber operations are a significant threat to national security. My thesis contributes to our understanding by

drawing upon an existing database to expand our knowledge on cyber conflict between dyadic rivals.

I argue that historic animosity between dyadic rivals is a significant factor in the employment of cyber operations. Looking at all of the literature there is a lack of consistency in defining rivalry. For this thesis, I use Valeriano's definition of dyadic rivalry "a constant competition and struggle between two or more actors over some stake or issue with a high degree of salience, but the issues at stake may vary over time" (Valeriano 2013). I am using that definition to stay consistent with previous scholarship as I use Valeriano and Maness' data and dyadic rivalry list, and seek to build upon their scholarship. I also argue that regionalism plays a significant impact on the probability of the occurrence of a cyber incident. This holds true as 41 of the 52 dyads used in my dataset are contiguous and 29 of the dyads have capitals that are less than 1000-miles apart while 40 dyads have capitals less than 2000-miles apart.

I argue that military strength, alliances with world powers, and cyber structure development plays a crucial role in the decision to employ cyber operations rather than or in conjunction with conventional military strategies. To analyze this, I test the following hypotheses about under what circumstances a cyber incident is likely to occur:

> Hypothesis 1: All else being equal, as dyadic disparity increases, a state is likely to employ cyber operations against a rival when that rival possesses a larger share of power in the dyad.
>
> Hypothesis 2: All else being equal, as the share of power between dyads equalizes, states will be more likely to employ cyber operations against their rival when that rival is a member of NATO.

This thesis has the following chapters: existing literature, methodology, data analysis, case study, and conclusion. In the literature review I discuss previous research concerning my dependent variable. In the methodology section, I describe my dependent variable, state the conceptual definition of the dependent variable, identify the unit of analysis, explain the importance of the dependent variable, identify my key independent variables, their conceptual definitions, and my expectations on how the independent variables will affect the dependent variable. In the data analysis section, I give a summary of my dataset, identify the model I am using, provide the results, and analyze the results. In the conclusion, I summarize my argument as well as discuss the implications this has on existing literature and for policy makers.

CHAPTER TWO: EXISTING LITERATURE

This chapter is an overview of existing scholarship concerning dyadic rivalry, asymmetric warfare, the threat posed by cyber conflicts, and cyber conflicts between dyadic rivals. The chapter starts with two articles concerning differing perspectives on dyadic rivalry and conflict. I do this to illustrate how the behavior of dyadic rivals helps explain the growing trend of cyber incidents. Next, I provide two articles on the differing points of view of asymmetric warfare. I use these two articles as two of my hypotheses propose that it is the weaker of two states who is likely to employ cyber operations against their rival. Please note that in this chapter, some authors being cited use terms like "cyber warfare" and "cyberattacks", but I employ different terminology.

Vasquez (1996) argues that not all interstate enduring rivalries experience wars. Vasquez's rivalry escalation theory focused upon the "two path" war. The first path is where dyadic rivals are at war over disputed territory that may be held by one of the rivals or even a third party. The second path is when rivals that are not in a territorial dispute are pulled into an ongoing war by a third party (Vasquez, 1996). Vasquez defines rivalry as "relationship characterized by extreme competition, and usually psychological hostility, in which the issue positions of contenders are governed primarily by their attitude toward each other rather than by the stakes at hand" (Vasquez, 1996: 532) This article compares several datasets on dyadic rivalry and show the lack of uniformity in definition and

measurement of rivalry. Vasquez's article sets the foundation for a great deal of future scholarship.

Rasler and Thompson (2000) argue against Vasquez's "two paths to war" theory by stating that major powers are also concerned with positional issues. They devised a "2 path, 2 issue" theory where rival dyads that share borders are more likely to go to war than those rivals who do not share borders and non-contiguous rivals are more likely to be involved with a multilateral war than contiguous (border sharing) rivals. Therefore, it's not just rivalry that affects future conflicts, but the type of rivalry. They found three patterns in their research: there are more non-contiguous rivals than contiguous ones, dyadic wars are scarce, and joining into wars has become a new norm in the international system. These patterns are not explained by spatial issues alone, but need to incorporate positional issues as well. Contiguous dyadic rivals are more likely than non-contiguous dyadic rivals to be involved with spatial conflicts, and non-contiguous dyadic rivals are more likely to get involved with conflicts on positional issues than contiguous dyadic rivals (Rasler and Thompson, 2000).

Cyber operations fall under the category of asymmetric strategy that has traditionally been attributed to the weaker state (Arreguín-Toft, 2001). Arreguín-Toft argues that asymmetric conflict outcomes are explained by strategic interactions. Power does not imply victory in an asymmetric conflict, but the resolve of the state does. Arreguín-Toft introduces the reader to the Strategic Interaction Thesis where there are two strategies: attack and defense. Within each strategy there are two approaches: direct and indirect. The two approaches for attack strategy are direct attack and barbarism and for defense strategy are direct defense and guerilla warfare strategy (GWS). The author notes

that the attacker is synonymous with strong states and defense strategies are synonymous with weaker states. The interaction of same-approach favors strong actors, while opposite-approach interactions favor the weak. A direct attack would win against a direct defense, but fail against GWS. Arreguín-Toft focuses solely on physical military strategies and does not include any analysis on cyber operations.

Breen and Geltzer (2011) argue asymmetric strategies, such as cyber operations, it is not solely the province of weak states, but is also a strategy that is employed by strong states. Breen and Geltzer defined "asymmetric strategy" as the ability to "transform an adversary's perceived strength into a vulnerability, often by revealing one's own perceived vulnerability as a strength" (Breen and Geltzer, 2011: 41). They argue that it is the use of the strategy that defines the strategy, not the strength of the state or actor using it. As cyberspace continues to develop and states continue to become interconnected to it, and therefore dependent on, cyber operations are emerging as a significant threat, particularly in the hands of those with "large amounts of intellectual capital and technical expertise," characteristic of a strong state (Breen and Geltzer, 2011, p. 50).

Caplan (2013) argues that cyberspace has become the fifth domain of warfighting along with land, sea, air, and space. She states that there is a considerable threat from cyberattacks against the critical infrastructure of the United States. It is also shown that the United States military is dependent upon the civilian communications infrastructure which is insecure and makes the military extremely vulnerable to attacks. Citing Richard Clarke, there are four reasons that the United States is the most vulnerable state: dependency of critical infrastructure on cyberspace, critical infrastructures are privately owned and unregulated, private companies lobby for cyber deregulation, and the military is highly

susceptible to cyberattacks. Caplan (2013) also discusses the history of cyberwarfare, but in addition to the well-known cases of cyberwarfare attributed to Russia, China, and the United States, he also mentions cyber incidents between India and Pakistan, Hamas and Israel, Turkey and Armenia, Hezbollah and Israel, and Indonesia and Malaysia. She also covers the attack on US satellites as well as the Duqu virus (Stuxnet 2.0). To fix the vulnerabilities and reduce the susceptibility to attacks, Caplan (2013) suggests that the United States needs to adopt an aggressive cybersecurity strategy to better protect state institutions and more importantly the national critical infrastructure.

Lewis (2002) analyzes the growing dependency, and vulnerability, that states have on cyberspace and the threat terrorists pose via cyberattacks to critical infrastructures. He concludes that while computers and networks are vulnerable to attacks, he argues that critical infrastructures are not vulnerable to cyberattacks. To come to this conclusion, Lewis used these methods: first, he looked at the history of physical attacks on critical infrastructure; second, he compared cyber incidents and their effects to "routine infrastructure failures" and their effects; third, he assessed the dependency of critical infrastructures on computer networks and their security protocols; and lastly, he analyzed whether or not cyber incidents can achieve the goals of terrorists. From this he finds that cyberattacks are less effective than physical attacks in crippling critical infrastructure and that cyberattacks do not cause any greater damage than a routine disruption, and therefore not a threat to national security. He states that much of the hype concerning cyberwarfare is not supported by evidence. One thing I have noticed so far in reading through these sources is that those who support the idea that cyberwarfare is a significant threat to national security are qualitative papers citing very few sources while those papers that

oppose the idea that cyberwarfare is a significant risk are often quantitative ones with numerous sources.

Hansen and Nissenbaum (2009) analyzes cyberwarfare and cyber security through the Copenhagen School, which is a theory used in security studies that suggests "securitization" is a speech act in that governments will apply certain terms that will get a heightened response from society that something previously disregarded as a low priority will be seen as a threat. This theory often applied to non-democratic styles of government as "securitization" is often used by governments to bypass the democratic processes to pass regulatory measures on a policy such as cyberspace. This theory postulates that actors will maximize their utility by creating an order of preferences (Hansen and Nissenbaum 2009). Every state has differences in their level of cyber interconnectedness as well as infrastructure development and styles of government that will cause states to prioritize cybersecurity differently.

Valeriano and Maness (2014) use a quantitative analysis approach to analyze cyber incidents between states. They analyze cyber incidents between states that exist in a pre-existing rivalrous environment. They use the terms "cyber incidents" and "cyber disputes" rather than terms like "cyberattacks" or "cyberwarfare"; cyber disputes contain cyber incidents. They argue that cyberwarfare does not result in any deaths, which is why cyber incidents and cyber disputes are more useful as terms (Valeriano and Maness 2014). The term of cyber incident is defined as action by one state to penetrate another state's computers or networks for the purposes of causing damage or disruption. I use cyber operations to represent the overall cyber strategy of a state wherein cyber operations may contain cyber disputes and cyber incidents. Their research centers on the analysis of 110

cyber incidents and 45 cyber disputes, and observing only rivalries (of which there are 126 rivals) which incorporate a multiparadigmatic approach that brings into account not just data, but also history, social, and cultural context into the analysis (Valeriano and Maness 2014). They collected their data by performing searches on Google News using specific terms to find the duration of an incident or dispute, who initiated it, the objective of the incident or dispute, whether or not a third party was involved, if one or both of the states had issued any official statements about the incident or dispute, and the severity of the incident or dispute. They found that only 13% of the 110 cyber incidents had a severity of 3 (out of a possible 5) and the average was 1.62. For cyber disputes, the average severity was 1.71. Only 20 of the 126 rivals entered into a cyber dispute which boils down to only 4 of them being pre-existing rivalries. Based on this analysis, they conclude that cyber operations are exaggerated and that cyber disputes exist primarily between rivals co-located within the same geographical area, particularly if a major regional power also exists within the region. The exceptions to regionalism are the United States and China, two of the most prominent actors in cyberspace. Valeriano and Maness also conclude that restraint (what others call deterrence) has kept most states from using cyber operations, fearing retaliation and the fact that cyber defense has not kept up with offensive cyber tactics (Valeriano and Maness 2014).

The existing literature has expanded the scholarship on their respective subject, but alone does not explain the increasing trends of cyber conflicts between dyadic rivals. What can be taken away from the existing literature is that past conflict, geographic proximity, and asymmetric capabilities will have an impact on the occurrence of future conflict. With this thesis, I seek to expand the scholarship by incorporating analysis of the growing

number of cyber incidents with the previous theories of dyadic rivalry and asymmetric warfare.

A few states illustrate these points. Russia, for example, shows that strong states can and do use cyber operations, often against weaker states. Russia is accused of, but has never admitted to, using cyber operations against Chechnya, Estonia, Georgia, Ukraine, Lithuania, and Kyrgyzstan. The most significant use of cyber operations was in Georgia in which cyber operations were employed in conjunction with physical attacks (Breen and Geltzer 2011). Although not a part of conflict, Russia performed a DDoS attack (a type of cyberattack) against Estonia in 2007 that was thought to be in response to the Estonian government removing pro-Russian statues from public view (Clarke and Knake, 2010). China is also a great example of a strong state using cyber operations, but in this case they more often employ cyberespionage than any other type of cyber operations. Asymmetric strategies, such as cyber operations, were often linked to weak states as it is often the only choice for them to choose, but that is no reason to reject the notion that strong states may also employ asymmetric strategies. Such strategies are based on economics; for strong states it could be the most effective and efficient strategy, and due to the ambiguous and anonymous nature of cyber operations can allow states to attack others with less fear of reprisal (Breen and Geltzer 2011).

CHAPTER THREE: METHODOLOGY

Much of the literature analyzes cyber operations on a case-by-case basis or when analyzing dyadic rivals focuses on physical warfare. The research conducted by Valeriano and Maness (2014) was based on the construction of a dataset looking only at cyber incidents that occurred between dyadic rivals, but did not focus on what caused a state to employ cyber operations against a rival rather than traditional military strategies. My dataset contains 52 dyadic rivals over 11-years making 572 observations possible for each variable, but I must make clear that for some of my independent variables there is missing data. The unit of analysis for this thesis is the dyadic rival.

My dependent variable, "Incident", is a binary variable and indicates the occurrence of a cyber incident in a given country in a given year. It is measured as a zero (0), for no incident, and one (1), for an incident. I define "cyber incident" as "individual operations launched against a state" (Maness and Valeriano 2014: 349). The data for this variable comes from the dataset "Cyber Conflict Data Project for the years 2001-2011" compiled by Valeriano and Maness. The Valeriano and Maness (2014) data, however, is limited to observations where cyber incidents occurred between dyadic rivals. My dataset expands upon their work, but includes all dyadic rivals rather than those where only a cyber incident occurred. Valeriano and Maness (2014) use open source information, in their case Google News Search, to produce a dataset that looked at duration of cyber incidents, who initiated the cyber incident, the goals of the initiator, whether or not a third party was involved, if

either governments issued official statements, and the severity of the cyber incident. They have thus built a data set that can be replicated for future use, when more incidents occur.

The independent variables used in this are: "Share of GDP (Gross Domestic Product)", "Share of EnCon" (Energy Consumption), "Share of PEC" (Primary Energy Consumption), "Share of Personnel", "Share of Expenditures", "ln (Distance)", and "Membership in NATO." For *Share of GDP*, *Share of EnCon*, *Share of PEC*, *Share of Personnel*, and *Share of Expenditure*, the values display the share of power in that respective variable between the two rivals. I accomplished this by dividing the weaker rival by the sum of the two rivals. I do this because conflicts are likely to escalate between dyadic rivals under conditions of power parity, rather than power preponderance, and power transitions, versus power shifts (Geller 1993).

The *Share of GDP* variable measures the share of the combined GDP between the two rivals. I define GDP as the "sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products." (World Bank 2016) This raw data for each rival is a continuous variable and is in current US Dollar, but the *Share of GDP* variable can only range from 0 to .5 where 0 indicates that the weaker state shares none of the GDP and .5 indicates that the GDP is evenly shared between the two rivals. With the missing data in *Share of EnCon* and *Share of PEC*, I am using GDP as a proxy variable for energy consumption. I expect that as the share of GDP increases the probability of a cyber incident between dyadic rivals will increase.

The *Share of EnCon* variable is based upon data that is continuous measuring energy consumption in units of kilograms of oil equivalent (United Nations 2015). *Share*

of ENCON, like *Share of GDP*, ranges from 0 to .5 where 0 indicates that the weaker state has no share and .5 indicates that the amount of energy consumed is evenly shared between the two rivals. This variable is used as a proxy variable to indicate a state's cyber infrastructure dependence.

The variable *Share of PEC* shows the share of "Primary Energy Consumption" which is the summation of consumption of coal, petroleum, electricity, and natural gas into a common unit of measure which is one thousand metric ton coal equivalents (Correlates of War Project 2014: 4). This data was collected from the Correlates of War National Material Capabilities dataset. This variable also ranges from 0 to .5 and I expect that as the share of Primary Energy Consumption increases the probability of a cyber incident will increase.

Share of Personnel shows the share of the combined numbers of military personnel of the dyad. The Military Personnel data shows "the size of state armies" and is measured in the thousands (Correlates of War Project 2014). This data was collected from the Correlates of War Project who gathered the data from US Arms Control and Disarmament Agency (ACDA). I define military personnel as "troops under the command of the national government, intended for use against foreign adversaries, and held ready for combat as of January 1 of the referent year." (Correlates of War Project 2014) The data only counts "those troops under the command of the national government" and include "active, regular military units of the land, naval, and air components." (Correlates of War Project 2014) The *Share of Personnel* variable also ranges from 0 to .5, and I expect that as the share of military personnel (as an indicator of military strength) increases so will the probability of the occurrence of a cyber incident.

The *Share of Expenditure* variable measures the share of "the total military budget for a given state for a given year" (Correlates of War Project 2014: 4) and is collected from the Correlates of War National Material Capabilities dataset. The raw data is measured in thousands of current year U.S. dollars (Correlates of War Project 2014). Both of these variables are interval-level variables and are indicators of military capabilities. *Share of Expenditure* ranges from 0 to .5, and I expect that the share of Military Expenditure increases the probability that a cyber incident will occur.

The *ln (Distance)* variable is the natural log of the straight line distance between the capitals of the two rivals. Because of rivals against the United States, the data is slightly skewed and logging the data will reduce the variance and improve the normal distribution of the variable.

The *Membership in NATO* variable is a control variable that simply measures whether or not a state is a member of the North Atlantic Treaty Organization. This variable is measured as a 0 or 1 where 0 indicates that neither of the rival states are members and 1 indicates that one or both of the rivals are members of NATO. This data was collected from the NATO website which lists what states are members.

CHAPTER FOUR: DATA ANALYSIS

This chapter includes a summary of my data, the models I use to test my hypotheses, and the results of my analysis.

Summary of Data

Table 1: Summary of Data

Variable	N	Mean	Std. Dev.	Min	Max
Incident	572	.128	.334	0	1
ln(Distance)	572	6.719	1.188	4.352	8.843
Share of GDP	572	.221	.155	-.008	.498
Share of Personnel	354	.236	.153	0	.499
Share of Expenditure	309	.179	.151	0	.471
Share of EnCon	404	.298	.125	.067	.499
Share of PEC	364	.168	.165	.0001	.495
NATO	572	.327	.469	0	1

Table 1 is a summary of my dependent and independent variables. This summary shows the number of observations (N), Mean, Standard Deviation (Std. Dev.), Minimum (Min) and Maximum (Max) of my dependent variable and independent variables. The mean for *Incident* indicates that there are more dyadic rivalries that did not experience a cyber incident in a given year; of my 52 dyadic rivals, only 20 of them experienced a cyber

incident. The mean for *ln(Distance)* indicates that this logged variable is evenly distributed. The low mean for *Share of GDP*, *Share of Personnel*, *Share of Expenditure*, *Share of EnCon*, and *Share of PEC* indicates that a majority of the dyadic rivalries involve a much weaker state. The two most notable cases are with *Share of Expenditure* and *Share of PEC*: 41% of the observations for *Share of Expenditure* is less than 0.1 and 50% of the observations for *Share of PEC* is less than 0.1. The mean of *NATO* indicates there are twice as many dyadic rivalries that do not include a state who holds membership in NATO.

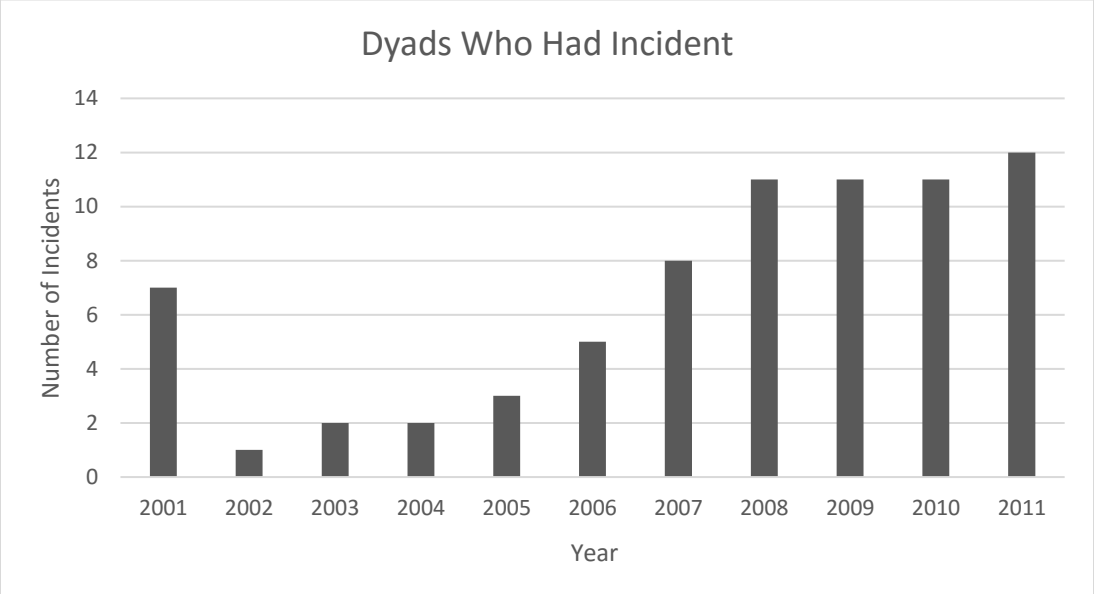

Figure 1 Dyads who had incident

Figure 1 is not intended to show the number of cyber incidents, but rather how many dyadic rivals experienced a cyber incident in a given year. This graph illustrates that the trend of dyadic rivals experiencing a cyber incident has been increasing since 2002.

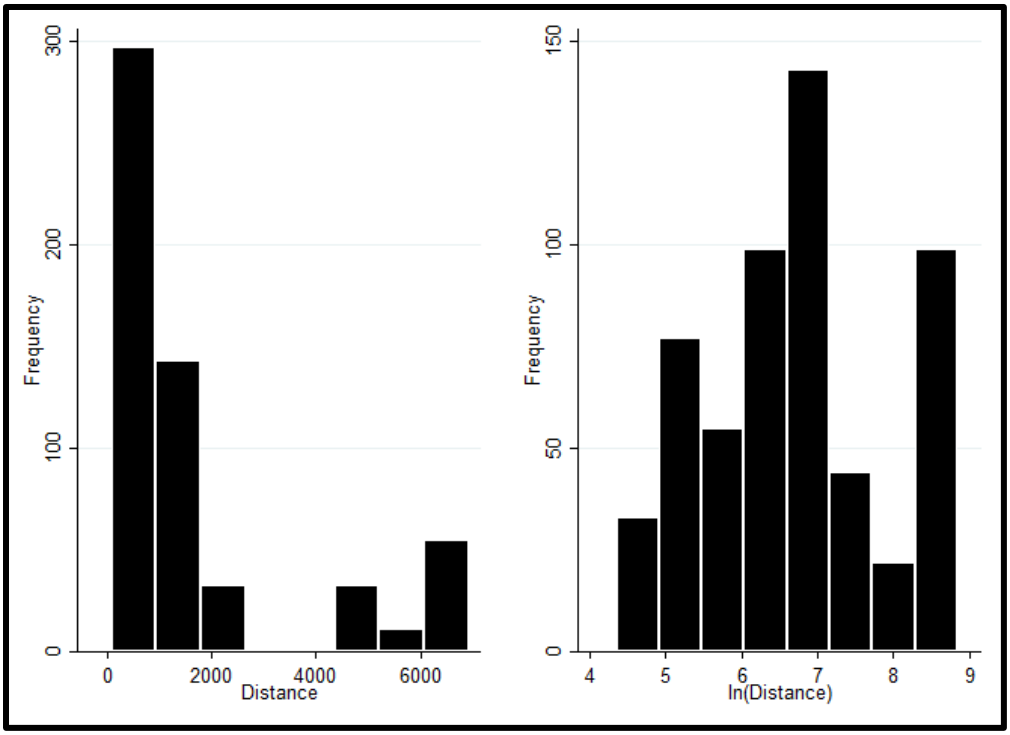

Figure 2: Distance Histiogram

Figure 2 is a histogram which displays the frequency of occurrences. The bar chart on the left shows the frequencies of the raw distance between state capitals while the right shows the frequencies of the natural log of the distance between capitals. When the natural log is taken, the data becomes approximately normally distributed.

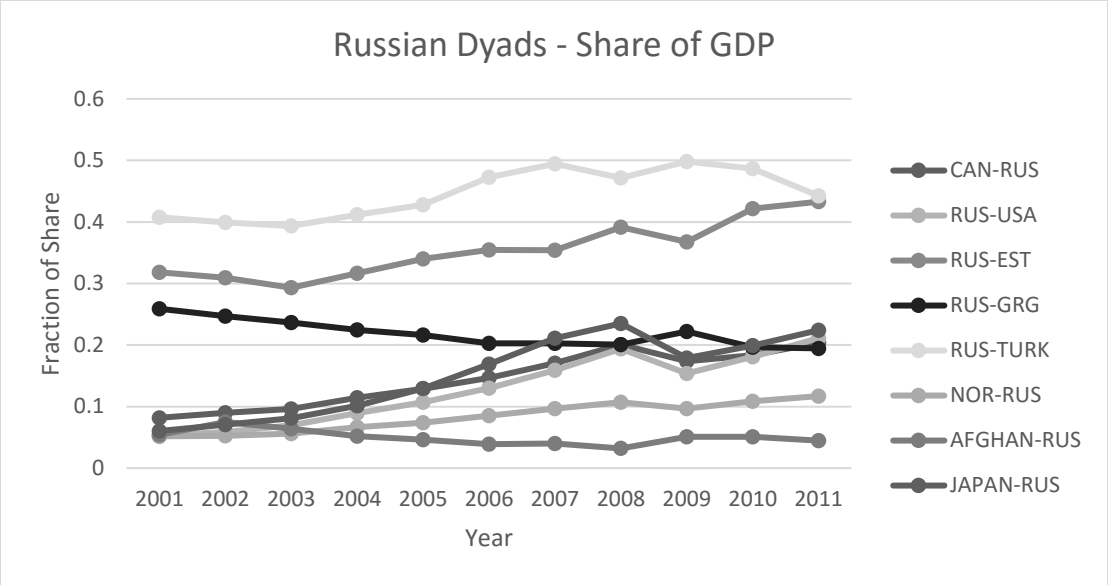

Figure 3: Share of GDP between Russian Dyads

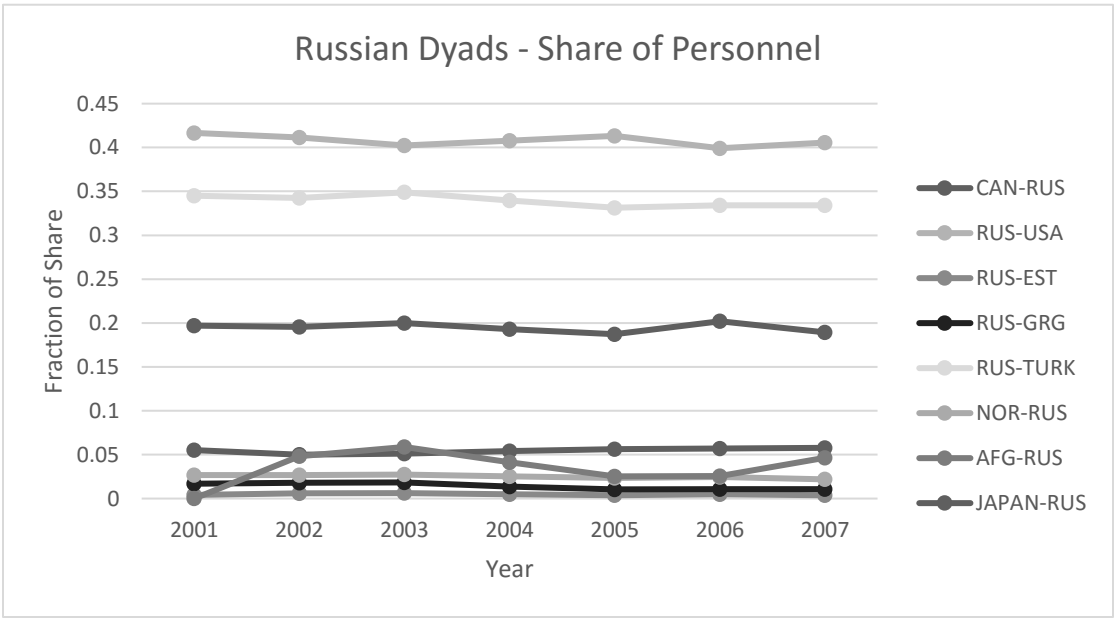

Figure 4: Share of Personnel between Russian Dyads

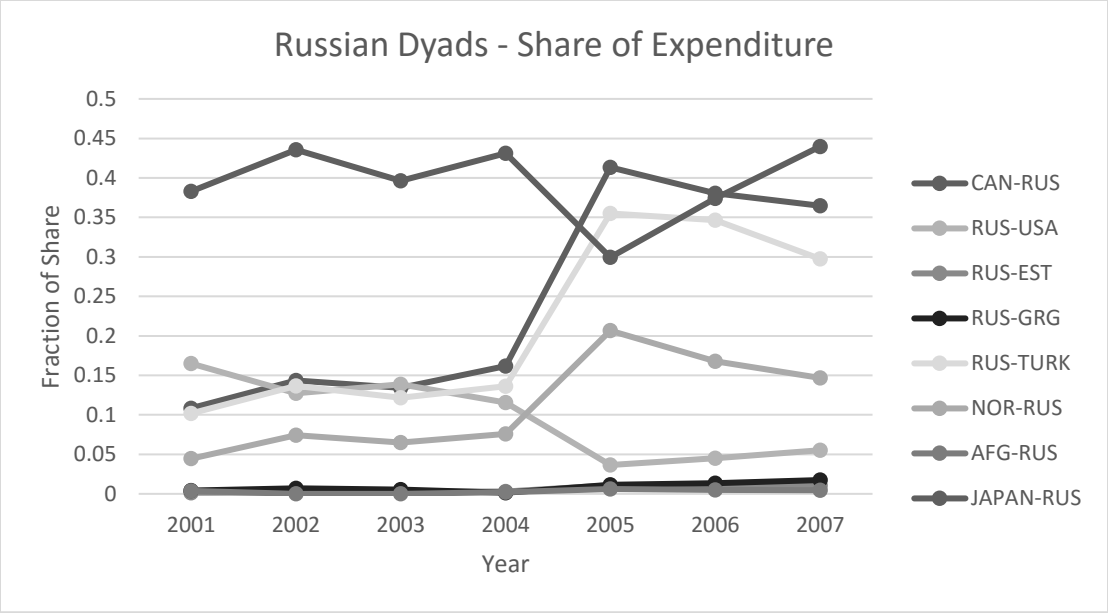

Figure 5: Share of Expenditure between Russian Dyads

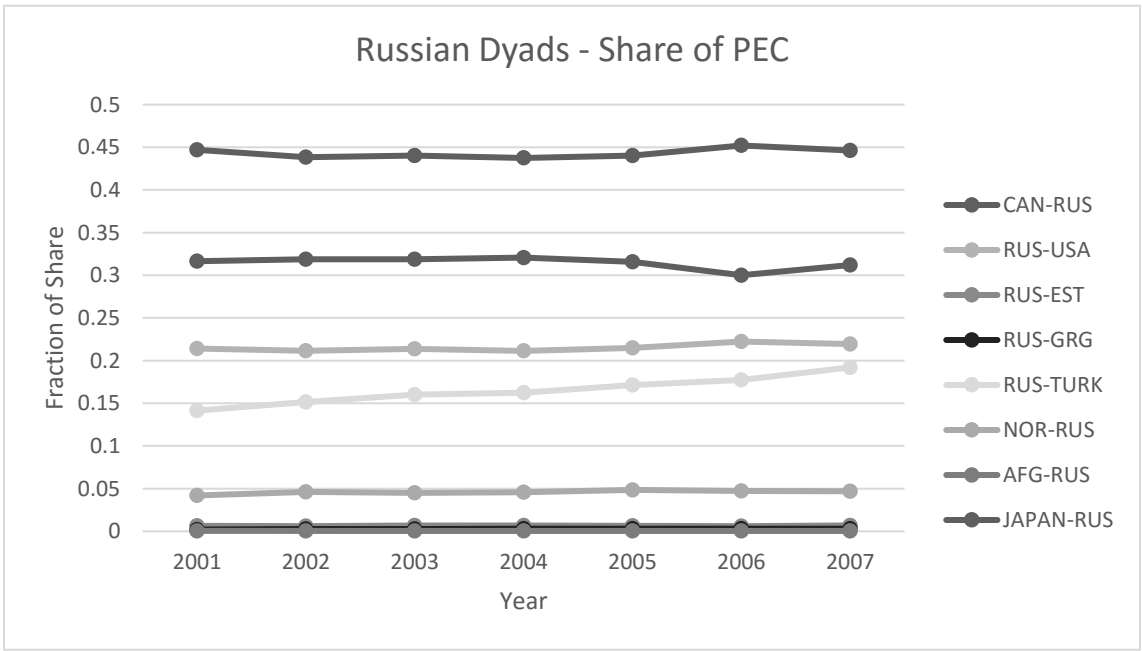

Figure 6: Share of PEC between Russian Dyads

For Figures 3 through Figure 6, I look at the Share of GDP, Share of Personnel, Share of Expenditures, and Share of PEC for the dyadic rivals including Russia. In Figure

3, Estonia and Georgia both have a higher share of GDP with Russia, but when looking at Figure 5 their share of military expenditure is very small when compared with Russia, as is their share of military personnel (Figure 4). In Figure 5, I observe some interesting patterns. Dyads including Estonia, Georgia, and Afghanistan were relatively stable and the weaker state's share was extremely low. Norway, Turkey, and Canada seem to follow the same trend over the years, but at different shares of expenditure. All three stay relatively stable from 2001 to 2004, but in 2005 they significantly increase before steadily decreasing again. I found it surprising that from 2001 to 2007, Russia's share of military expenditure decreases.

Models

In order to test the validity of my hypotheses, I performed a logistical regression analysis on several models since my dependent variable is a binary-level variable and my data is panel data (cross-sectional and time-series). For Hypothesis 1, I used *ln(Distance)*, *Share of Personnel*, and *Share of Expenditure* as independent variables. For Hypothesis 2, I use the same independent variables as in Hypothesis 1, but also using *Member in NATO* as a control variable. To run all of my models, I used STATA v14 with robust commands which are used to detect influential variables and adjusts the "estimates that take into account some of the flaws in the data itself." (UCLA Institute for Digital Research and Education 2014) I ran several different models using a Logistic Regression, or logit, with my *Incident* variable always as the dependent variable. In addition, I ran several different models to ensure robustness and to check if my variables are conditional upon each other for significance:

H1-1: $\text{Incident} = \beta_1 \text{Share of Personnel}_i + \beta_2 \ln(\text{Distance})_i + \alpha + \varepsilon$
H1-2: $\text{Incident} = \beta_1 \text{Share of Personnel}_i + \beta_2 \ln(\text{Distance})_i + \alpha + \varepsilon$

H1-3: Incident = β_1Share of Personnel$_i$ + β_2Share of Expenditure$_i$ + β_3 ln(Distance)$_i$ + α + ε

Hypothesis 1 (H1) is meant to analyze whether or not the share of military strength impacts the likelihood of the occurrence of a cyber incident.

H2-1: Incident = β_1Share of GDP$_i$ + $\beta_2$ln(Distance)$_i$ + β_3NATO$_i$ + α + ε
H2-2: Incident = β_1Share of Personnel$_i$ + $\beta_2$ln(Distance)$_i$ + β_3NATO$_i$ + α + ε
H2-3: Incident = β_1Share of Expenditure$_i$ + $\beta_2$ln(Distance)$_i$ + β_3NATO$_i$ + α + ε
H2-4: Incident = β_1Share of Personnel$_i$ + β_2Share of Expenditure$_i$ + $\beta_3$ln(Distance)$_i$ + β_4NATO$_i$ + α + ε
H2-5: Incident = β_1Share of GDP$_i$ + β_2Share of Personnel$_i$ + β_4NATO$_i$ + α + ε
H2-6: Incident = β_1Share of GDP$_i$ + β_2Share of Expenditure$_i$ + β_4NATO$_i$ + α + ε
H2-7: Incident = β_1Share of GDP$_i$ + β_2Share of Personnel$_i$ + β_3Share of Expenditure$_i$ + $\beta_4$ln(Distance)$_i$ + β_5NATO$_i$ + α + ε
H2-8: Incident = β_1Share of GDP$_i$ + β_2Share of Personnel$_i$ + β_3Share of Expenditure$_i$ + β_4NATO$_i$ + α + ε

Hypothesis 2 (H2) is similar to Hypothesis 1, but includes *Share of GDP* and *NATO* variables. H2 analyzes how a state's strength controlling for membership in NATO affects the probability of the occurrence of a cyber incident. Because I include more variables I have a greater number of possible models than is seen in H1. In H2-8 I removed *ln(Distance)* to see the impact it had on the other variables involved.

Results and Analysis

Table 2 through 4 present the results for all of my models. Models H1-1 through H1-3 concern Hypothesis #1 and H2-1 through H2-8 concern Hypothesis #2. Across all models, except H2-8, ln(Distance) has a positive and statistically significant effect on the probability of occurrence of a cyber incident.

The χ^2 Test for all of the models, except H2-8, is less than 0.05 which rejects the null hypothesis, that none of the coefficients in my model are equal to zero. The Wald χ^2 for all of the models are greater than 3.841 and allows me to reject the null hypothesis,

meaning that the independent variables significantly explain variation in the dependent variable.

Table 2: Results for Hypothesis 1 Models

	H1-1	**H1-2**	**H1-3**
Share of Personnel	.732		1.281
	(1.119)		(1.361)
Share of Expenditure		2.502*	2.135
		(1.313)	(1.476)
ln(Distance)	.425**	.587**	.587**
	(.151)	(.188)	(.187)
N	354	309	301
Pseudo-R^2	0.0341	0.0621	0.064
Wald-χ^2	8.7	10.08	9.95
Prob > χ^2	0.0129	0.0065	0.019

Aside from *ln(Distance)*, the only other variable that has a positive and statistically significant effect on the probability of occurrence of a cyber incident is *Share of Expenditure* (H1-2). While scholars such as Valeriano and Maness argue for regionalism playing a significant role in the use of cyber operations. My data shows that as distance increases the likelihood increases, which would suggest that when a state lacks the capability or refuses to use conventional military forces against a rival they will resort to the use of cyber operations instead. From this I conclude that the share of military expenditure and the logged distance between the two states increases and the probability of a cyber incident increases. The lack of capability gives support towards the argument from Breen and Geltzer who conclude that strong states also employ asymmetric warfare

in order "to achieve dramatic results against weaker opponents" (Breen and Geltzer, 2011: 52). With these results I would reject my first hypothesis, but note that it is rejected because the *Share of Personnel* is insignificant. I conclude that while *Share of Expenditure* is significant, it doesn't sufficiently reflect the strength or accurately depict the capabilities shared between the dyadic rivals.

Table 3: Results for Hypothesis 2 Models

	H2-1	**H2-2**	**H2-3**	**H2-4**
Share of GDP	-2.685*			
	(1.159)			
Share of Personnel		1.625		2.261
		(1.421)		(1.657)
Share of Expenditure			1.895	1.131
			(1.219)	(1.481)
ln(Distance)	0.628***	0.802***	0.759***	0.830***
	(0.16)	(0.242)	(0.212)	(0.241)
NATO	-1.431***	-1.449*	-0.844*	-1.126*
	(0.334)	(0.572)	(0.452)	(0.543)
N	572	354	309	301
Pseudo-R^2	0.0894	0.0687	0.0753	0.084
Wald-χ^2	38.66	13.3	13.36	12.35
Prob > χ^2	0.000	0.004	0.0039	0.0149

Table 4: Results for Hypothesis 2 Models

	H2-5	H2-6	H2-7	H2-8
Share of GDP	-2.31 (1.643)	-2.559 (1.809)	-3.424 (1.883)	-5.801** (2.178)
Share of Personnel	1.978 (1.464)		3.139 (1.761)	3.751* (1.687)
Share of Expenditure		1.977 (1.239)	1.143 (1.482)	1.066 (1.609)
ln(Distance)	0.6958** (0.241)	0.5748** (0.217)	0.633** (0.229)	
NATO	-1.642* (0.654)	-0.901* (0.469)	-1.339 (0.644)	-0.442 (0.439)
N	354	309	301	280
Pseudo-R^2	0.0795	0.0872	0.1045	0.0815
Wald-χ^2	12.28	13.95	12	8.1
Prob > χ^2	0.0154	0.0075	0.0348	0.0882

In H2-1, *Share of GDP* and *NATO* has a negative and statistically significant effect while *ln(Distance)* has a positive and statistically significant effect on the probability of occurrence of a cyber incident. *Share of GDP*, *Share of Personnel*, and *Share of Expenditure* in models H2-2 through H2-7 are not statistically significant. When I remove *ln(Distance)* in H2-8, *Share of GDP* has a negative and statistically significant effect and *Share of Personnel* has a positive and statistically significant effect on the probability of occurrence of a cyber incident.

In the models for Hypothesis 2, I found it surprising that membership in NATO reduced the probability of a cyber incident as it ran contrary to my hypothesis. It was also

interesting to note that when removing *ln(Distance)* from the model, *Share of GDP* and *Share of Personnel* become statistically significant; model H2-8. When controlling for other variables, 6 of the 8 H2 models show that my *NATO* variable is statistically significance, but has a negative impact on the occurrence of a cyber incident which is a rejection of my second hypothesis. From the data and previous literature, I can see that states are hesitant to employ cyberwarfare, but particularly when one of the rivals is a member of NATO. When *NATO* is involved cyber capabilities can be pooled and used to retaliate against the aggressor.

The constancy of *ln(Distance)* and the several significant "share" variables coincides with Bennett (1996) who states that rivals "will commit substantial resources (military, economic, or diplomatic) toward opposing each other." Cyber operations can assist a state in opposing each other. As an example of a lasting issue, unresolved between two rivals, would be Estonia and Russia where Russia is accused of performing a DDoS attack against Estonia in 2007, which was thought to be in response to the Estonian government removing pro-Russian statues from public view (Clarke and Knake 2010). The cyber incidents involving Russia are supported by the results of the data and serves as a great case study. Rivalries involving the United States are outliers as my data suggests that membership in NATO reduces the probability of a cyber incident, but does not prevent it from happening. China has also been a leading employer of cyberwarfare, but has employed more cyberespionage than any other type of cyberwarfare particularly against the United States of America. (Breen and Geltzer 2011) China's use has assisted it both militarily and economically, one such example occurs when China is accused of stealing the designs of the F-35 and using it in their J-31 (Weisgerber 2015). It assists the China

militarily by advancing their military capabilities to rival the United States who is seen as the sole global power since the fall of the Soviet Union. It assists them economically as it costs very little to hack and saves funds spent on research and development.

Table 5: Predicted Probability Table

	Variable	**Δ in X**	**Δ in pr(Y)**	**% Δ**
H1-1	ln(Distance)	Mean +1 SD	0.1	65.7
H1-2	Share of Expenditure ln(Distance)	Mean +1 SD Mean +1 SD	0.071 0.156	45.9 100.8
H1-3	ln(Distance)	Mean +1 SD	0.16	100.8
H2-1	Share of GDP ln(Distance) NATO	Mean +1 SD Mean +1 SD 0 → 1	-0.076 0.249 -0.272	33.9 111.1 76.1
H2-2	ln(Distance) NATO	Mean +1 SD 0 → 1	0.211 -0.163	159.2 76.5
H2-3	ln(Distance) NATO	Mean +1 SD 0 → 1	0.214 -0.109	146.3 57
H2-4	ln(Distance) NATO	Mean +1 SD 0 → 1	0.245 -0.142	167.9 67.6
H2-5	ln(Distance) NATO	Mean +1 SD 0 → 1	0.16 -0.172	128.6 80.6
H2-6	ln(Distance) NATO	Mean +1 SD 0 → 1	0.144 -0.117	98 59.4
H2-7	ln(Distance)	Mean +1 SD	0.159	112.1
H2-8	Share of GDP Share of Personnel	Mean +1 SD Mean +1 SD	0.087 0.114	59.2 77.5

Table 5 presents the predicted probability of cyber incidents for statistically significant variables in each of the models presented in Table 2 through Table 4. For the

continuous variables, the baseline probability is calculated with all variables held at their mean value. The change in the probability is calculated by taking the difference between the baseline probability and the probability when the variable is increased by one standard deviation with all other variables still held at their mean value. For my binary independent variable (NATO), the baseline probability is calculated with NATO valued at zero and all other variables at their mean. The change in the probability is calculated by taking the difference between the baseline probability and the probability when NATO is valued at 1 with all other variables still at their mean value.

The most notable percentage changes in Table 5 are found with *ln(Distance)* in models H2-1 through H2-7. The other variables in all of the models had percentage changes that ranged from 29.8% to 80%, but ln(Distance) in the H2 models had percentage change range from 98% to 167.9%. You also see this large percentage change in models H1-2 and H1-3, but in the rest of the models the percentage change is far lower. These results lead me to believe that when controlling for military strength (expenditure or personnel) and membership in NATO, *ln(Distance)* causes the predicted probability to greatly increase. These results seem contrary to some previous literature that suggest that closer proximity caused an increase in the likelihood of a cyber incident, but my data suggests that as distance increases between dyadic rivals that a cyber incident is more likely to occur than with dyadic rivalries that are closer to each other. Figure 7 demonstrates the contribution of distance to the change in the probability of an incident. This graph holds all values at their mean or modes (for binary variables), and employs model H2-6.

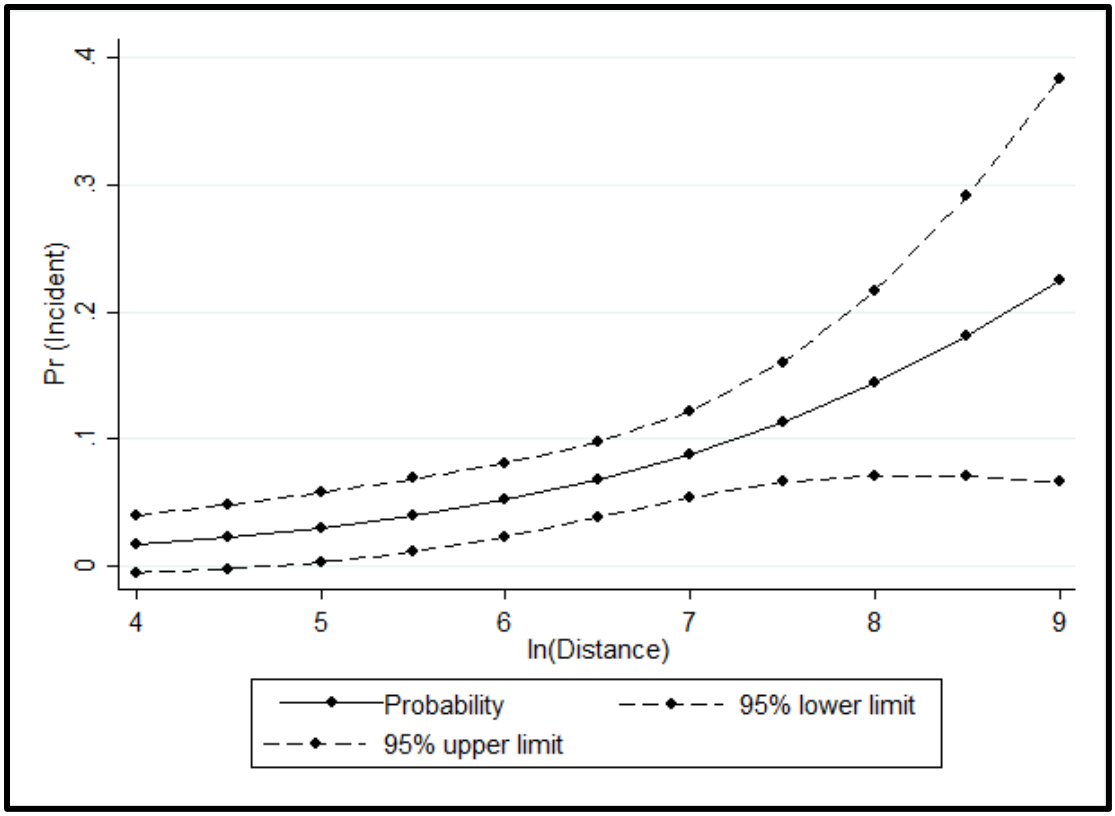

Figure 7: Confidence Intervals for Distance

However, there are some problems that limit the usefulness of logistical regression models since reducing data or observations down to a binary or dichotomous level loses a lot of information in comparison to other measurement levels. This may cause the importance of the impact of the independent variables to be misestimated. In STATA, I ran a correlation matrix to check for multicollinearity in my models; I also ran several models to avoid multicollinearity. I employed robust standard errors in my estimation to correct for heteroskedasticity across dyads. Although I have a large sample size, I do face problems with missing data as the data gathered from the Correlates of War Project only went from 2001 to 2007, and from the World Bank I was missing data from some countries like Taiwan. Another issue with my dataset lies with my dependent variable. The data was collected by Valeriano and Maness who used open source (Google News) to collect the

data. It is possible that the data collected is extremely limited by what is reported by the various governments and news agencies. For reasons of classification, pride, and/or fear, there may be more cyber incidents that have occurred that have not yet been reported.

CHAPTER FIVE: CASE STUDY

The Russo-Georgian War of 2008 is the most well-known use of cyber operations between two states and serves to illustrate the data results. This war occurred between Georgia, Russia, and separatists from South Ossetia and Abkhazia concerning two provinces attempting to break away and establish their own country (CNN 2013). This war took place in August of 2008, but followed a turbulent period of military posturing. Prior to this war, cyber operations came in the form of cyber espionage, cybercrimes, and petty cyber incidents used against military and government networks or computers. In this cyber incident Russia used a variety of methods of cyber operations against Georgia which prevented and reduced the Georgian government's ability to communicate to its own citizenry, to the various institutions of the state, and to the international community. (Cyber Committee 2012; Hollis 2011). Although Russia denies using cyber operations in conjunction with its invasion, it is noted that cyber incidents happened to coincide almost simultaneously with the Russian military movements and bombings.

The relations between Russia and Georgia had been turbulent with Russia having a history of interfering with the domestic affairs of Georgia. Throughout the 19th century Russia slowly annexed Georgia, but after the Russian revolution in 1918 Georgia declared its independence (Cornell 2001). Over the next couple of years, the Georgians experienced conflicts with the Ossetians who were often poor, landless peasants. The Ossetians were supported by the Bolsheviks (Souleimanov 2013) and monarchal style of government. In

1921, the Soviets invaded Georgia where they installed a Soviet government. As the Soviet Union began to decline Georgian nationalism arose and the Soviet government of Georgia dissolved the South Ossetian Autonomous Region that was established by the Soviet Union (Saparov 2014). On April 9, 1991, Georgia became the first non-Baltic state to declare its independence from the Soviet Union. Even after the fall of the Soviet Union, the Russians supported the Ossetians in a conflict that lasted until June of 1992 (Cornell 2001).

Tensions did not improve over the years, but even with occasional outbursts, the situation in South Ossetia remained stable. After the rise of Putin, Russia started issuing passports to the residents of Abkhazia and South Ossetia without Georgia's permission in 2002. In 2003 a pro-Western government was installed in Georgia and relations began to deteriorate. In 2004, Saakashvili, the new Georgian President, aimed to restore order to Ossetia and Abkhazia. Saakashvili also sought to join NATO (BBC 2008) which only intensified the rivalry as Russia saw such moves by Georgia as a security threat (Evans 2008). In 2012, General Yuri Baluyevsky admitted that the Russo-Georgian War was premeditated to force a regime change preventing Georgia from joining NATO, and not a response to Georgian aggression. In 2006, Georgia deported four Russians accused of espionage and Russia responded by persecuting ethnic Georgians living within the Russian Federation (Van Herpen 2014).

By 2008, open conflict started between the Ossetian separatists and Georgia. Russia, continuing their support of the separatists, issued a decree recognizing Abkhazia and South Ossetia as states independent of Georgia on April 16, 2008. A few days later a Russian jet shot down a Georgian unmanned aerial vehicle (UAV). Based on the UAV footage, Georgia accused Russia of amassing troops in Abkhazia to which Russia accused

Georgia of planning to invade Abkhazia, promising to retaliate against any Georgian aggression. At the end of May, Russia began repairs on a railway from Russia into Abkhazia that would later be used to transport Russian soldiers during the war in August (BBC 2008). Throughout July, attacks occurred between the separatists and Georgians resulting in several deaths (Antidze 2008). In this month, Russia and Georgia both performed military exercises, but even after the training concluded the Russians kept their troops along the Georgian border (Cornell, Popjanevski, and Nilsson 2008; Cyber Committee 2012). During these training maneuvers, Russian cyber operations targeted Georgian computers and networks as a test run for the cyber operations used during the war in August (Cyber Committee 2012). In August, indirect fire attacks were exchanged between the two sides during the nights of the first week. In response to the movement of Georgian artillery towards South Ossetia on August 7, Russia launched land, sea, and air operations against Georgia (Financial Times 2008; Hollis 2011). It was preceding and during these Russian operations that Georgian websites were hacked causing transportation, communication, financial, and government websites to be inaccessible (Hollis 2011).

In sum, this example illustrates how cyber operations are employed by a strong state against a weaker rival. This also lends support to the arguments of Rasler and Thompson (2000) who argue that dyadic rivalries will be involved with conflicts over spatial (territorial) issues and positional issues. While this conflict would be considered a spatial conflict, I would argue that Georgia's desire to join NATO also brought in a positional issue to the conflict. My data infers that membership in NATO decreases the likelihood that a cyber incident would occur, which could help explain why Russia

employed both cyber and physical military operations against Georgia: to attack a rival before it joins NATO and has the military support of powerful allies, and to remove its pro-Western and pro-NATO government for one that is more conducive to the will of Russia.

CHAPTER SIX: CONCLUSION

In this thesis I have discussed factors that may influence the probability of a cyber incident occurring between dyadic rivals. A logistical regression analysis was performed on a dataset that tested 52 dyads over 11-years against 7 independent variables that were intended to provide evidence for these two hypotheses. The 52 dyads include 20 dyads who experienced a cyber incident and 32 dyads that had not. My results show that there isn't any consistency from model to model that supports all of my hypotheses. My first hypothesis argues that the weaker state within a rivalry would employ cyber operations against a stronger rival. However, my data infers that it is not only weak states that employ cyber operations resulting in my first hypothesis being rejected. My second hypothesis argued that when controlling for membership in NATO, the likelihood of cyber incidents increases, but my data, however, shows that NATO has a negative relationship with the occurrence of cyber incidents and my second hypothesis is rejected.

Based on the results there are two important trends and observations I wish to highlight: 1) the share of military personnel, military expenditure, and energy consumption is not enough to explain cyber incident trends, and 2) the logged distance and membership in NATO was consistently significant and explained variations in the occurrence of a cyber incident. With the first trend, the lack of significance may be caused by the small amount of data currently available for analysis. As more data becomes available and more incidents occur, this first trend can be verified. With the second trend, I conclude that as distance

increases between dyadic rivals the probability of a cyber incident increases which goes against the previous scholarship that argued the theory of regionalism.

Clearly from the results, additional research is needed. One fix may come as a result of the publication of more data from the Correlates of War Project. In future research I may include a variable that indicates if one, or both, of the dyads possess nuclear technology and/or nuclear weapons. I could also replace my dependent variable with one that shows the number of cyber incidents between dyadic rivals in a given year. A third alternative variable to include in my models would be one that indicated the differences in culture or ethnicity to see if ethnic rivalries influences dyadic rivalries. Many scholars have made comparisons between nuclear weapons and cyberwarfare, but I would be looking at it from the point of view that nuclear states will be more likely to employ cyberwarfare because they fear retaliation less than if they used a nuclear weapon against a rival (Pytlak 2014).

States will increasingly have to address issues surrounding cyberspace. The fear of retaliation or vulnerability will always be present as some argue that cyber defensive capabilities will never overtake cyber offensive capabilities as the latter is constantly transforming and evolving while the former is constantly playing "catch up." Even with this pessimistic outlook, states will still need to develop regulations and international laws to deal with cyber incidents, particularly since the severity and number of cyber incidents are increasing over the years. In the past, most cyber incidents involved petty harassment rather than causing any damage, but recent events have demonstrated cyber incidents are targeting critical infrastructure as seen with Ukraine. On December 23, 2015, the Prykarpattyaoblenergo control center in Western Ukraine was hacked and the substation was taken offline. To further hinder any recovery operations, the hackers sabotaged the

operator workstations by changing their passwords and shutting down the back-up power supplies that would have kept the substation up and running (Zetter 2016). This incident is the first one known to cause a blackout and serves not only as another cyber incident attributed to Russia when it is in open conflict with one of its rivals, but also as one of the examples of the growing trend of cyber incident against a dyadic rival.

REFERENCES

"2008 Georgia Russia Conflict Fast Facts." 2013. *CNN*. Last Accessed on May 16th, 2016. http://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/.

Antidze, Margarita. 2008. "Georgia plans operation to free detained soldiers." July 8. http://www.reuters.com/article/idUSL08676780 (May 16, 2016).

Arreguín-Toft, Ivan. 2001. "How the Weak Win Wars: A Theory of Asymmetric Conflict." *Inernational Security* 26, 93-128.

Bennett, D. Scott. 1996. "Security, Bargaining, and the End of Interstate Rivalry." *International Studies Quarterly* 40, 157-184.

Breen, Michael, and Joshua Geltzer. 2011. "Asymmetric Strategies as Strategies of the Strong." *Parameters*: 41-55.

Caplan, Nathalie. 2013. "Cyber War: the Challenge to National Security." *Global Security Studies* 4: 93-115.

Clarke, Richard, and Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins Book

Cornell, Svante E. 2001. *Small Nations and Great Powers: A Study of Ethnopolitical Conflict in the Caucasus*. UK: Curzon Press.

Cornell, Svante E., Johanna Popjanevski, and Niklas Nilsson. 2008. "Russia's War in Georgia: Causes and Implications for Georgia and the World." *Central Asia-Caucasus Institute & Silk Road Studies Program* (August).

Correlates of War Project. *Direct Contiguity Data, 1816-2006*. Version 3.1.

Correlates of War Project. 2014. National Material Capabilities Data Documentation. Version 4.0

"Countdown in the Caucasus: Seven days that brought Russia and Georgia to war." 2008. *Financial Times*. Last Accessed May 16th, 2016. www.ft.com/intl/cms/s/0/af25400a-739d-11dd-8a66-0000779fd18c.html#axzz48rTz72rH.

Cyber Committee. 2012. "The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict." *Armed Forces Communications and Electronics Association*.

"Data: GDP Per Capita." *World Bank*. Last Accessed April 11th, 2016. http://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

"Energy Statistics Yearbook." 2015. Last Accessed April 11th, 2016. *United Nations*. http://unstats.un.org/unsd/energy/.

Evans, Michael. 2008. "Vladimir Putin tells summit he wants security and friendship." April 5. from http://www.timesonline.co.uk/tol/news/world/article3681609.ece (May 16, 2016).

Geller, Daniel S. 1993. "Power Differentials and War in Rival Dyads." *International Studies Quarterly* 37 (June): 173-93.

Hansen, Lene, and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53: 1155-1175.

Hollis, D. 2011. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal* 7 (January).

Lewis, James A. 2002. "Assessing the Risks of Cyber Terrorism, Cyber War, and Other Cyber Threats." *Center for Strategic and International Studies* (December).

Pytlak, Allison. 2014. "Why Do States Use Cyber Weapons? An Empirical Analysis of State-sponsored Cyber Interactions and Rival Dynamics, 2011-2011" Master's Thesis. City University New York.

"Q&A: Conflict in Georgia." 2008. *BBC*. Last Accessed May 16th, 2016. http://news.bbc.co.uk/2/hi/europe/7549736.stm.

Rasler, Karen, and William R. Thompson. 2000. "Explaining Rivalry Escalation to War: Space, Position, and Contiguity in the Major Power Subsystem." *International Studies Quarterly* 44 (September): 503-530.

Saparov, Arsène. 2014. *From Conflict to Autonomy in the Caucasus: The Soviet Union and the Making of Abkhazia, South Ossetia and Nagorno Karabakh*. New York: Routledge.

Souleimanov, Emil. 2013. *Understanding Ethnopolitical Conflict: Karabakh, South Ossetia, and Abkhazia Wars Reconsidered*. New York: St. Martin's Press.

"Stata Data Analysis Examples Robust Regression." *UCLA Institute for Digital Research and Education*. Last Accessed on December 10th, 2014. http://www.ats.ucla.edu/stat/stata/dae/rreg.htm.

Valeriano, Brandon. 2013. *Becoming Rivals: The Process of Interstate Rivalry Development*. New York: Routledge.

Valeriano, Brandon, and Ryan C. Maness. 2014. "The Dynamics of Cyber Conflict Between Rival Antagonists." *Journal of Peace Research* 51: 347-360.

Van Herpen, Marcel H. 2014. *Putin's Wars: The Rise of Russia's New Imperialism*. Lanham: Rowman & Littlefield.

Vasquez, John. 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 (December): 531-558.

Weisgerber, Marcus. 2015. "China's Copycat Jet Raises Questions About F-35." September 23. http://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/ (April 27, 2016)

Zetter, Kim. 2016. "Everything We Know About Ukraine's Power Plant Hack." January 20. http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ (April 27, 2016)

APPENDIX A

List of Dyadic Rivals

Iran-USA
Russia-Canada
Belize-Guatemala
Honduras-Nicaragua
Colombia-Nicaragua
Colombia-Venezuela
Guyana-Suriname
Greece-Turkey
Cyprus-Turkey
Russia-USA
Russia-Estonia
Russia-Georgia
Russia-Turkey
Armenia-Azerbaijan
Armenia-Turkey
Russia-Norway
Guinea-Sierra Leone
Liberia-Guinea
Liberia-Sierra Leone
Congo-Uganda
Burundi-Tanzania
Rwanda-Uganda
Sudan-Uganda
Iran-Turkey
Iraq-USA
Iraq-UK
Iraq-Turkey
Iraq-Saudi Arabia
Syria-USA
Lebanon-Israel
Israel-Syria
Kuwait-Iraq
Afghanistan-USA
Afghanistan-Russia
Afghanistan-Tajikistan
Afghanistan-Uzbekistan
Afghanistan-Pakistan
China-USA
China-Taiwan
China-Japan
China-Vietnam
China-Philippines
North Korea-USA
North Korea-South Korea
North Korea-Japan
Israel-Iran
South Korea-Japan
Japan-Russia
India-Pakistan
India-Bangladesh
Congo-Rwanda
China-India

APPENDIX B

Concerning the Predicted Probability Table

For model H1-1, the predicted probability of a cyber incident increases from a baseline probability of a cyber incident is 0.153 to a probability of 0.253, a 65.7% change. The baseline probability of a cyber incident for model H1-2 is 0.155. The predicted probability of a cyber incident increases for MILEXSHARE to 0.226, a 45.9% change. The predicted probability of a cyber incident increases for LOGDISTANCE to 0.311, a 100.8% change. For model H1-3, the predicted probability of a cyber incident increases from a baseline probability of a cyber incident that is 0.159 to a probability of 0.319, a 100.8% change.

The baseline probability of a cyber incident for model H2-1 is 0.224 for the continuous variables and 0.358 for the binary variable. The predicted probability of a cyber incident decreases for Share of GDP to 0.148, a 33.9% change, and increases for ln(Distance) to .473, a 111.1% change, at one standard deviation above the mean for both variables. The predicted probability of a cyber incident increases for NATO to .085, a 76.1% change when one, or both, of the states in the dyad are members of NATO. The baseline probability of a cyber incident for model H2-2 is 0.132 for the continuous variable and 0.213 for the binary variable. The predicted probability of a cyber incident increases for ln(Distance) to 0.343, a 159.2% change, at one standard deviation above the mean. The predicted probability of a cyber incident decreases for NATO to 0.049, a 76.5% change. The baseline probability of a cyber incident for model H2-3 is 0.146 for the continuous variable and 0.192 for the binary variable. The predicted probability of a cyber incident increases for ln(Distance) to 0.36, a 146.3% change, at one standard deviation above the mean. The predicted probability of a cyber incident decreases for NATO to 0.082, a 57% change. The baseline probability of a cyber incident for model H2-4 is 0.146 for the

continuous variable and 0.211 for the binary variable. The predicted probability of a cyber incident increases for ln(Distance) to 0.391, a 167.9% change. The predicted probability of a cyber incident decreases for NATO to 0.068, a 67.6% change. For model H2-5, the baseline probability of a cyber incident for the continuous variable is 0.125 and for the binary variable is 0.213. The predicted probability of a cyber incident increases for ln(Distance) to 0.285, a 128.6% change. The predicted probability of a cyber incident decreases for NATO to 0.041, an 80.6% change. The baseline probability of a cyber incident for model H2-6 is 0.147 for continuous variable and 0.197 for the binary variable. The predicted probability of a cyber incident increases for ln(Distance) to 0.291, a 98% change. The predicted probability of a cyber incident decreases for NATO to 0.08, a 59.4% change. For model H2-7, the predicted probability of a cyber incident increases from a baseline probability of a cyber incident that is 0.142 to a probability of 0.302, a 112.1% change. The baseline probability of a cyber incident for model H2-8 is 0.147. The predicted probability of a cyber incident increases for Share of GDP to 0.059, a 59.2% change. The predicted probability of a cyber incident increases for Share of Personnel to 0.261, a 77.5% change.