Fighting in Cyberspace:
Complementarity versus substitutability in cyber operations

October 4, 2019

Abstract

When do states fight in cyberspace? Despite a proliferation of anecdote and plausible speculation, researchers and practitioners know relatively little about the characteristics of this emerging conflict domain. In particular, we do not yet know whether cyber operations supplement, or replace, more traditional modes of conflict. Initial research argued that cyber attacks should tend to act as substitutes for other forms of dispute behavior. We assess this logic and conduct of conflict in cyberspace by quantitatively analyzing panel data on cyber versus conventional dispute behavior. Our findings reveal that there is no negative relationship between cyber and conventional conflict, suggesting that the substitution argument completely does not hold. Instead, disruptive cyber operations are mostly used as complements to traditional modes of conflict. Moreover, we demonstrate that strong nations, with advanced technology and abundant resources, are likely to fight opponents on land, sea, air, and space as well as in the cyber domain. The research presented here helps advance our collective understanding of the shape and nature of conflict behavior in an increasingly complex world.

Word count: 174 (abstract); 5,915 (total)

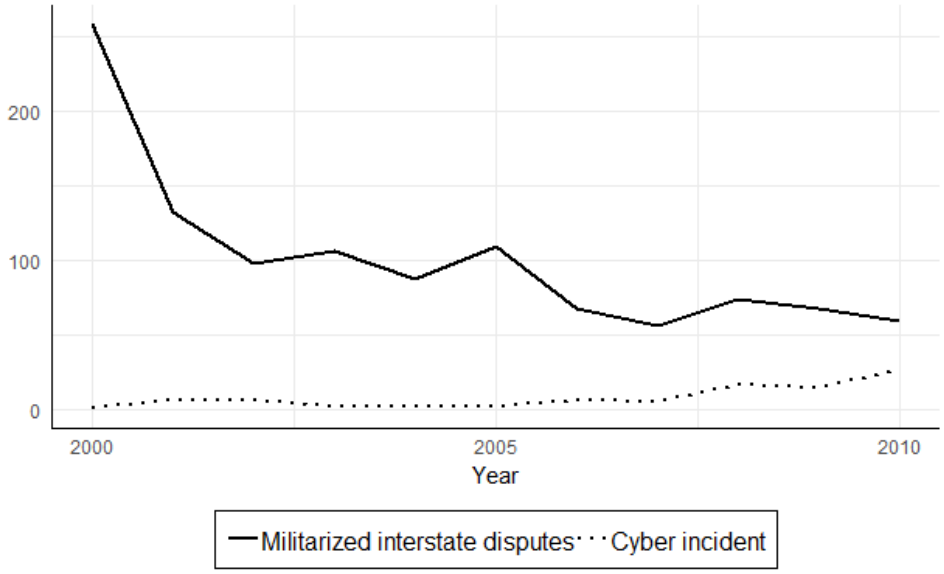
Recent revelation that the United States Cyber Command (USCYBERCOM) had been "dropping cyberbombs" in the fight the against Islamic State furthers concerns that the online environment is rapidly emerging as a major locus of conflict (Sabah, 2016). There is even speculation that warfare in the cyber domain may supplant other, more tangible, forms of dispute behavior. Macro trends in both physical and digital fronts appear to substantiate these perceptions. During the 2000-2010 period, the number of conventional militarized interstate disputes between nations steadily declined whereas the number of aggressive cyber operations[1] slowly increased (Figure 1).[2] Relatively inexpensive in development and use, cyber operations have become a convenient policy tool, allowing governments to obscure attribution and make it difficult to confirm aggressive behavior (Poznansky and Perkoski, 2018). We ask the following questions: *Have nations started using cyber operations instead of conventional modes of conflict to resolve their disputes? If so, should we expect countries to fight primarily or disproportionately in cyberspace?*

Debate has been growing over the role of cyber capabilities in modern warfare. Some scholars view cyber operations as 'weapons of the future' that will play a decisive role in military conflicts (Andres, 2012; Clarke and Knake, 2010; Kello, 2013; McGraw, 2013; Rios, 2009; Schmitt, 1999). Since they can exploit vulnerabilities about which a target may initially be unaware, cyber operations offer the potential to quickly disrupt an opponent's command and control, hinder communication, and create other obstacles to sustaining military operations (Andres, 2012; Clarke and Knake, 2010; Eun and Aßmann, 2014; McGraw, 2013; Rios, 2009; Schmitt, 1999; Sharma, 2010). However, since cyber disruptions tend to be temporary and limited, they may not prove sufficient to coerce targets in all but relatively minor confrontations (Brito and Watkins, 2011; Gartzke, 2013;

[1] *Joint Publication 3 13 Information Operations* (2014, II-9) define "cyber operations" as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."

[2] Figure 1 uses Valeriano, Jensen and Maness 2018's Dyadic Cyber Incident Dataset (DCID) and Militarized Interstate Disputes (MID) data (version 4.2) (Jones, Bremer and Singer, 1996).

Figure 1: PROLIFERATION OF CYBER INCIDENTS AND MILITARIZED DISPUTES, 2000-2010



Junio, 2013; Libicki, 2009; Liff, 2012; Richards, 2014; Rid, 2012; Valeriano and Maness, 2012; Walt, 2010). Because of this, and because conventional capabilities are often required to secure cyber gains, other scholars see cyber operations as complementing, rather than replacing, traditional forms of combat (Gartzke, 2013; Liff, 2012; Valeriano, Jensen and Maness, 2018).

This debate has generated a wealth of policy commentary and a rapidly expanding theoretical literature, but few robust empirical findings (Valeriano and Maness, 2014; Valeriano, Jensen and Maness, 2018). Recently developed datasets on cyber incidents allow researchers to redress previous empirical limitations that have so far impeded quantitative assessment of cyber conflict dynamics. Here, we seek to evaluate the relative merits of the two sides in the "complements versus substitutes" debate. By using two sources of cyber data — Valeriano, Jensen and Maness 2018's Dyadic Cyber Incident Dataset (DCID) and the Council on Foreign Relations' (CFR) Cyber Operations Tracker — plus Version 4.2 of the Militarized Interstate Disputes (MID) dataset, we are able to offer an answer as to whether states fight in cyberspace in addition to, or instead of,

other domains.

We argue that different types of cyber operations have differing levels of salience at different stages of military conflict. Cyber espionage is the most valuable operation prior to the start of a contest, or indeed for preventing conflict from occurring in many instances. Degradation operations can create enough damage on their own that an adversary may not choose to attack, and may not need to be confronted in physical battle, in some instances. Disruptive cyber operations might be best suited for ground campaigns because they focus on undermining an enemy's command and control, making aggression much more difficult. These operations are likely to be particularly fruitful in the midst of a contest; by flooding phones with text messages or calls, for example, these campaigns inundate communications systems, making them unusable for their intended purpose. For these reasons, we expect countries to use disruptive cyber campaigns as a complement for physical fighting.

Our findings confirm this expectation by showing that disruptive cyber operations are mostly used as complementary tools to traditional modes of conflict. Our results also reveal that there is no negative relationship between cyber and conventional conflict, suggesting that the substitution argument completely does not hold. In addition, strong nations, with advanced technology and abundant resources, are more likely to fight opponents on land, sea, air, and space *as well as* in the cyber domain. This finding speaks to Gartzke (2013) who argues that cyberspace is far from an ideal coercive tool for weak actors. Nations with significant resources are much better capable of developing sophisticated cyber "weapons." Moreover, our findings reveal that the decay effect of distance is not much mitigated for cyber — neighboring states continue their territorial disputes using cyber means, alongside conventional operations.[3]

[3]We use "conventional," "kinetic," and "traditional" interchangeably in this paper.

By providing the first global quantitative analysis of cyber and kinetic campaigns, our study sheds light on a theoretical debate focused on the coercive role of cyber operations during conflict and complements existing quantitative and country-specific works on this topic (Borghard and Lonergan, 2017; Brantly, 2016; Gartzke, 2013; Kostyuk and Zhukov, 2019; Lindsay and Gartzke, 2015; Valeriano, Jensen and Maness, 2018). We offer the first disaggregated analysis of the complementarity or substitutability of cyber and conventional "fronts." Unlike Kostyuk and Zhukov (2019) who focus on individual cyber operations and show that there is no overlap between daily cyber and kinetic fronts in the Ukrainian and Syrian conflicts, we show that such an overlap exists at the global level, when one focuses instead on cyber campaigns as the unit of analysis. Finally, our findings have several implications for the shape and nature of future conflicts that increasingly involve operations in the digital domain. While cyber operations seem to be a promising tool for coercion, policymakers should carefully consider the effectiveness of this tool, when not used in conjunction with fighting in other domains.

The paper proceeds as follows. Section 1 briefly reviews the recent literature on the relationship between cyber and conventional military operations, and discusses the debate over complementarity or substitution of these operations. Section 2 introduces respective datasets on cyber and conventional conflict. Sections 3 and 4 present our empirical strategy and summarize the paper's empirical findings. Section 5 offers a discussion of the broader significance of these results and provides concluding remarks.

1 The Theory and Practice of Modern Conflict

During the last two decades, countries have been using cyber operations to coerce their adversaries independently from, and jointly with physical, conventional operations. An example of the former includes the infamous 2007 Estonian attacks when "an entire

country has been targeted on almost every digital front all at once...[and] a government itself fought back" (Davis, 2007). Examples of the latter include the digital dimensions of the conflicts in Georgia (2008) and Ukraine (2014-ongoing). While the role of cyber operations differs among these three conflicts, they share a common perpetrator. Why did Russia use cyber attacks as its primary tool in its dispute with Estonia in 2007, but used its military in addition to cyber operations to invade Georgia one year later?[4] More generally, *what determines when an initiator uses cyber operations as a complement to, instead of a substitute for, conventional tools of conflict?*

1.1 Advantages and Disadvantages of Cyber and Kinetic Operations

To better understand the logic of complements and substitutes in conducting warfare in multiple potential domains, let us first examine the advantages and disadvantages of using different implements of coercion (conventional versus cyber) to compel adversaries and resolve disputes. Compared with physical force, the low production and execution cost of cyber operations (COs) and their availability for purchase, increases their appeal (Bellovin, Landau and Lin, 2017; Gartzke, 2013). A lower cost, however, does not necessarily equate with effectiveness, which is a strong function of the target's characteristics. Unlike kinetic forms of warfare, a minor change in a target can make a cyber "weapon"[5] ineffective, while attacking two similar targets might require development of a new code or necessitate significant changes to existing code. Bombs do not necessarily need to be redesigned each time they are used. It is much easier to serialize the production of conventional weapons than of cyber weapons. Indeed, unlike explo-

[4] For a more focused answer to the reasons Russia varied its kinetic operations while maintaining cyber attacks as a near constant in its military operations, see Gannon, Gartzke and Lindsay (2017).

[5] A "Cyber weapon" is "a software-based IT artifact or tool that can cause destructive, damaging, or degrading effects on the system or network against which it is directed...Cyber weapons can be instantiated in hardware as well" (Bellovin, Landau and Lin, 2017, 60).

sives, once code has been reverse-engineered, it can be used by the target against the originator or the code, or against third parties (Bellovin, Landau and Lin, 2017, 65).

This low projected cost of cyber operations may give the inaccurate impression that these operations can give weaker states leverage over conventionally superior adversaries (Liff, 2012). Because weak actors might be afraid of confronting strong adversaries in more direct (i.e. "kinetic") physical combat, cyber substitutes are nominally an attractive option over other types of conflict. In reality, however, developing sophisticated cyber resources requires significant time and energy (Ablon and Bogart, 2017; Gartzke, 2013). The offense in cyberspace must be tailored for each target, since in most instances entry and exploitation are unique. Moreover, since it is often unknown what types of targets the government or military will seek to attack in the future, establishing access paths over the widest possible scope of potential targets is a necessary component of cyber offense.[6] This drives up the cost of developing cyber-offensive capabilities in addition to the costs of studying how a target functions and behaves. As a result, it is doubtful that weak nations will be able to develop the organizational and technical capacity necessary to launch sustainable, high-quality cyber operations against multiple targets in a stronger state (Liff, 2012, 425). Only states that already have significant resources can afford to invest in this costly planning/production process (Gartzke, 2013).

Moreover, scholars have questioned the effectiveness of cyber operations in achieving a coercive effect (Borghard and Lonergan, 2017; Lindsay and Gartzke, 2015; Valeriano and Maness, 2014, 2015; Valeriano, Jensen and Maness, 2018). Successful coercion requires that punishment be both anticipated and avoidable by accommodation (Schelling, 1966) — two criteria that are difficult to meet in cyberspace. First, COs are most effective when unanticipated. The effectiveness of COs depreciates quickly after

[6]For details related to the pre-planning of attacks, see Gartzke, Libicki and Lindsay (2019).

first use, which creates incentives for "zero-day" surprise attacks before the target recognizes and fixes a vulnerability (Axelrod and Iliev, 2014). The second, "avoidability" condition is potentially even more problematic. Due to attribution problems and uncertainty over an attacker's identity, targets may question whether an adversary can credibly commit to ceasing its attacks (Carr, 2011; Kugler, 2009; Tsagourias, 2012). Targets may also see compliance as unnecessary in order to prevent further damage. Due to uncertainty over the damage caused by attacks, some attacks will go undiscovered. When detected, cyber attacks expose vulnerabilities that administrators can repair, hardening the system from future attack.

Despite the limited ability of COs to operate as coercive mechanisms, the secrecy of COs and the cyber attribution challenge make this form of aggression an attractive option for governments and non-state actors. They allow leaders to deny any responsibility for damaging, invasive or compromising operations and, as a result, the leaders face a low chance of retaliation by the target, as well as lowering their risks at home (audience costs), compared with traditional coercive tools. When this cost-willingness threshold is low, states may use cyber as a substitute for other forms of aggression.

Technical advances have made it possible to attribute the origin of COs to the actual machine that was used to execute a given operation. These advances and specific features of COs have significantly reduced uncertainty around cyber attribution. Some of these features, which include the motive of the attacker and the type of operations, are often unique for each country. For instance, China's main interest lies in obtaining "proprietary information, such as research and development data...[and]... intelligence access to sensitive communications, from senior government officials to Chinese political dissidents" (Geers et al., 2014, 6). Until recently the Asian-Pacific region was home to "high-frequency, brute-force" operations whereas attacks coming from Russia and East-

ern Europe are "more technically advanced and highly effective at evading detection" (Geers et al., 2014, 3). Such advancements that help to resolve concerns about cyber attribution raise a further question. How much longer will states be able to use cyber operations instead of conventional tools to resolve their disputes?

In addition to cost and secrecy, the distance between nations is another important variable that may affect a country's decision to use COs as a complement to, or substitute for, other forms of conflict. In particular, distance generally tends to reduce dispute propensity (and intensity). Scholarly works on conventional conflicts demonstrate that contiguity (Boulding, 1962; Bremer, 1992; Diehl, 1985; Hensel et al., 2000; Senese, 2005) and claims over territory (Hensel et al., 2000; Huth, 2009; Vasquez, 1995, 2001, 2009) are among the most robust and substantively important explanations of conflict between rivals. Rival countries that share borders and have sufficient motivation to fight one another in a conventional dispute might also use COs as a complementary tool. The decay effect of distance might be mitigated for cyber, given that the loss is naturally smaller. Specifically, when rivalries are distant from each other, they may be more likely to use cyberspace as a means to signal resolve during increased tensions (Valeriano and Maness, 2014, 2015). But distance can still influence willingness to fight; states that are far removed should be less motivated to confront one another in any domain.

This example highlights two additional factors that might affect a nation's willingness to fight in cyberspace. First is the presence of a dispute between the two nations, giving a state a reason to use cyber and/or conventional tools. Second is Internet dependence. In order to use cyber operations as a tool, both the attacker and the target should have some level of technological sophistication. Specifically, states with higher Internet usage may be more willing to attack others and also more attractive as targets to others.

1.2 Effectiveness of Different Types of Cyber Operations in Combat

But different cyber operations play different functions that determine how important they are for ground combat. For instance, while ongoing espionage operations are important during combat, they are mostly valuable prior to the onset of a contest. This is especially the case for cyber espionage that requires significant time and resources to establish an access path to a target's facilities. For instance, many cyber espionage campaigns started a few years prior to the start of the Ukrainian conflict. Some examples include *Snake*, cyber espionage against Ukrainian computer systems that dates back to 2006 (*Snake campaign and cyber espionage toolkit*, 2014), the BlackEnergy trojan used for espionage starting in 2010 (Labs, 2014), and *Operation Potao Express*, a target espionage campaign launched in 2011 against the Ukrainian government and military (Lipovsky and Cherepanov, 2015). While some espionage operations continued during the conflict (e.g., Armageddon), many of them stopped — some due to their diminishing value and some due to the fact they had been discovered (Kostyuk and Zhukov, 2019).

While important in combat, degradation cyber operations, designed to "sabotage the enemy target's networks, operations, or systems" (Valeriano, Jensen and Maness, 2018), can create enough damage on their own and achieve a country's desired goal. For instance, the well-known joint Israeli-U.S. *Stuxnet* operation, aimed to slow Iran's development of its nuclear weapons by ruining its nuclear centrifuges, was used as a substitute for other more drastic measures, including diverting Israel from bombing Iran. It requires significant time and resources to design these quite effective but dangerous tools because, if not carefully planned, they can cause devastating second-order effects. To avoid such effects, Stuxnet, for instance, was designed to specifically target the Iranian nuclear facility, and even though it spread out to other facilities, it did not

cause other damage.

Unlike degradation cyber operations, disruption cyber operations might be the most suited for use alongside ground combat because they focus on disrupting enemy command and control. Defined as "low-cost, low-payoff irritants that probe an adversary's resolve and signal intent," these operations include website defacements, distributed denial of service attacks (DDoS) used against websites and phones, among others (Valeriano, Jensen and Maness, 2018). They are particularly effective during combat because by flooding phones with text messages or calls, for instance, these campaigns inundate communications systems, making them unusable. For these reasons, we expect countries to use disruption cyber campaigns to complement their physical fighting.

The question of whether cyber is a complement or substitute to traditional forms of warfare has deep implications for the theory and practice of national security. Yet public and academic debates on this topic have unfolded largely in the absence of rigorous empirical evidence. Part of the challenge lies in the novelty of this phenomenon—use of cyber operations as a tool of coercion is a relatively new phenomenon. Our study attempts to bridge these two areas of research. We pursue this goal by studying the direction and magnitude of the relationship between cyber incidents and conventional disputes in the short decade for which evidence is available, 2000-2010. If countries tend to use cyber as a complement, then there should be a positive relationship between conventional conflict and cyber operations. If states instead use cyber as a substitute, then we should see a negative relationship between conventional and cyber operations. As discussed, we expect states to mostly incorporate disruptive cyber campaigns as integral tools of modern combat, rather than as a replacement for older forms of war.

2 Data

We analyze several datasets to assess the empirical validity of our hypotheses on complementarity/substitution of cyber and conventional conflict. Below we briefly describe key details of these datasets and discuss their relevance to this study.

2.1 Cyber Operations

Our dependent variable—*cyber campaigns*—takes the value of 1 when a country has been conducting a cyber campaign and 0 when a country has not been conducting a cyber campaign during the period under study. To evaluate relationships between such campaigns, we use Valeriano, Jensen and Maness (2018)'s Dyadic Cyber Incident Dataset (DCID) (Version 1.5) and the Council on Foreign Relations' (CFR) Cyber Operations Tracker. It is important to note that both datasets focus on cyber campaigns or incidents, defined as an accumulation of individual cyber attacks or operations to achieve a strategically important goal. For instance, both datasets code cyber attacks against Estonia that lasted for about three weeks in 2007 as one incident. Not without limitation, this approach has its benefits. First, it ensures that the cyber campaign data suffers less from reporting bias than data on individual cyber attacks. While an individual attack might be unreported or undiscovered, it is much more difficult not to notice a full-scale cyber campaign. This is especially the case when a significant amount of time has passed since the start of a campaign — between nine and nineteen years for the 2000-2010 period. Second, a cyber attack rarely occurs as an isolated effort; generally a series of attacks occur together. By focusing on campaigns instead of individual attacks, we can study how strategically important the overall effort in the cyber domain is to the larger national objectives.

Dyadic Cyber Incident Dataset (DCID). Valeriano, Jensen and Maness (2018)'s Dyadic Cyber Incident Dataset (DCID) (Version 1.5) contains information on 115 cyber incidents that took place between 2000 and 2010. During this period, 11 nations conducted cyber campaigns against 18 other nations, resulting in 23 unique dyads. The U.S.-China dyad had the largest number of cyber incidents (27), followed by the India-Pakistan dyad (10), and then by the Iran-Israel (9) and Russia-Georgia (9) dyads.

Because certain actions in cyberspace are easier to track, we also consider different types of cyber operations, in addition to the presence or absence of cyber campaigns, as our dependent variables. Following the Valeriano, Jensen and Maness (2018) typology, we focus on two types of cyber campaigns – *degradation* (17 instances), *disruption* (44 instances), and *espionage* (54 instances).[7] According to this typology, espionage should be the least observable, followed by *disruption* operations — "low-cost, low-payoff irritants that probe an adversary's resolve and signal intent, [such as] website defacements and distributed denial of service (DDoS)" — and *degradation* operations — "operations designed to sabotage the enemy target's networks, operations, or systems" (Valeriano, Jensen and Maness, 2018). We use DCID as our main dataset for measuring cyber operations.

Council on Foreign Relations' (CFR) Cyber Operations Tracker. We use the Council on Foreign Relation's data to run our robustness checks. Last updated in July 2018, this original dataset[8] contains information on 262 events that include cyber operations

[7] Valeriano, Jensen and Maness (2018) distinguish four types of incidents — *disruption*, *short-term espionage*, *long-term espionage*, and *degradation*. We combine *short-term espionage* and *long-term espionage* into one category — *espionage*. We explain how we create our final dataset in the section below.

[8] Source: https://www.cfr.org/interactive/cyber-operations#CyberOperations

against adversarial nations and dissidents at home, indictments, etc. The bulk of these cases, however, either involve or are between non-state actors, an area that is not currently the focus of our analysis. By limiting the sample of cases to those where one nation-state targeted another nation-state, we are left with seventy-seven cases during the 2000-2010 period. Six nations are reported to have conducted cyber campaigns against 28 other nations in these data, resulting in 35 unique dyads. There are 69 espionage campaigns, 6 disruption campaigns, and 2 degradation campaigns. The significant limitation of these data serves as a hard test for our analysis. If the results hold for this limited sample of observations, they should also hold for the larger (unobserved) population of state-sponsored cyber operations. The observed sample contains the most overt uses of cyber conflict, disproportionately those involving disruption or other acts most often said by some observers to be substitutes for traditional modes of warfare.

2.2 Conventional Operations

To measure the presence of a dispute or a rivalry between countries, we use Militarized Interstate Disputes (MID) data, which measures the presence of a militarized interstate dispute between two nations (CONVENTIONAL) (Maoz, 2005). The latest version (version 4.2) of this dataset runs until 2010, with 400 unique dyads, initiated by 130 nation-states against 130 nation-states.

2.3 A Dataset of Cyber and Conventional Military Operations

Before introducing our methods and results, we present a brief overview of how we constructed the final dataset used in our analysis. To ensure we do not focus only on positive cases in which either a cyber or conventional event took place, we first use all dyads in DCID cyber and conventional datasets to construct a universal set of dyads. We

thus ensure that each dyad occurred in each year in our cyber and conventional datasets. This created a large number of instances where neither cyber nor conventional conflict events took place in a given year. As a result, our final dataset contains 322 unique dyads in which either a cyber or conventional tool was used to resolve a dispute during the 2000-2010 period, making a total of 3,542 observations. After removing duplicate dyad-years from this dataset, we find that an attacker used a cyber campaign against a target in 81 cases and failed to do so against a target in 3,461 cases. In 17 cases, an attacker conducted a cyber disruption campaign against a target and they did not use cyber disruption against a target in 3,525 cases. In 53 cases, an attacker was found to pursue cyber espionage against a target and they did not use cyber espionage against a target in 3,489 cases. In 11 cases, an attacker pursued a cyber degradation campaign against a target and did not use cyber degradation against a target in 3,531 cases. In 843 cases, an attacker initiated a conventional operation against a target and did not use conventional operations against a target in 2,699 cases.

While this approach allows us to record so-called *negative* cases of cyber and/or conventional incidents, it does not address situations in which an incident has not been reported in these data. While this is less of a problem for the cases of conventional attacks, it is a significant issue for cyber campaigns. Regrettably, we cannot capture events that remain unknown. However, we can speculate about patterns of unobserved behavior. Given that cyber events tend to be under-reported, let us examine how the direction of bias in the cyber events data affects our results. Under-reported data on cyber operations might make us reach a "false negative" conclusion, resulting in a Type II error. To guard against this, our approach poses a "hard test" for our claims. Events are more likely to be under-reported if they are more difficult to observe. To the degree that cyber campaigns substitute for conventional conflict behavior, they will be highlighted, both

by their intensity and the lack of other, potentially obscuring behavior. Note, for example, the prominence of by the US-Israeli attack on Iran's nuclear enrichment centrifuges (Stuxnet) and the attack by North Korea on Sony Pictures, two cases that have featured prominently in arguments about the changing face of war. Smaller or less overt forms of cyber attack (i.e. espionage) are more likely to be missed by observers and also more likely to serve as complements to conventional conflict. Similarly, cyber attacks that coincide with other forms of warfare may be obscured in the fog of conventional battle.

If despite under-reporting, we find statistically significant results, it is perhaps reasonable to conclude that a stronger relationship would also be statistically significant. Specifically, we demonstrate that disruptive cyber operations are positively statistically related to physical campaigns, serving as complements to kinetic forms of warfare (Section 4). Thus, while acknowledging some of the (many) limitations involved, we nevertheless proceed, in the belief that initial steps are a useful step in cumulative research.

3 Empirical Strategy

We use *generalized estimating equations (GEE)* to address correlation between measures over time and to evaluate the relationship between conventional and cyber campaigns.

$$logit(P(Y_{ijt} = 1)) = \beta_0 + \beta_1 CONVENTIONAL_{ijt} + GX_{ijt} + \beta_2 Y_{ijt-1}. \quad (1)$$

In Equation 1, Y_{ijt} is a dummy variable, which stands for whether an initiator i (SIDEA) uses cyber operations against a target j (SIDEB) in a given year t; CONVENTIONAL$_{ijt}$ is a dummy variable, which stands for whether an initiator i (SIDEA) uses conventional conflict tools against a target j (SIDEB) in a given year t; $X_{ijt} = \left[x_{1ijt}, \ldots, x_{kijt}\right]'$ is a matrix of k exogenous variables, and G is a five-dimensional vector of coefficients. We

do not include country-fixed effects into our model because (1) GEE corrects for dyad effects and (2) many of our independent variables are either time-invariant or change very slowly over time. To account for time, we lag our dependent variable (Y_{ijt-1}).

In the first four models, we estimate the likelihood that a country uses conventional tools with each individual type of a cyber campaign—ESPIONAGE, DISRUPTION, DEGRADATION—and uses these conventional tools with all types of cyber campaigns (CYBER_ALL) (Figure 2). Since different types of cyber campaigns influence each other, we use a multivariate dependent variable (CYBER VALUE) for our last model (Figure 3). Our exogenous variables include the percentage of an attacker's/target's Internet users weighted by each country's total population (INTERNET_USERS_A/T (LOG)), the distance between two countries (CAP_DISTANCE (LOG)), the level of an attacker's national material capability (CINC (LOG)),[9] and a measure of the expressed difference of interests between states, a crude indicator of nations' possible willingness to fight (AFFINITY).

To take into account the possibility that nations with high Internet usage might be more attractive as targets, or might be more likely to attack others through the medium of cyberspace, we control for *technology*, measured as the number of Internet users weighted by the total population in each of the two respective countries (INTERNET_USERS_A/T (LOG)).[10] We obtain a measure of Internet usage from the World Bank. We control for the *distance* between two countries in a dyad to address the possibility that countries that share borders are more likely to use conventional weapons whereas those that are further away may be more likely to use cyber means. We measure distance using the distance between their two capitals in miles (CAP_DISTANCE (LOG)).[11] We measure the level of *national capabilities*, using Singer, Bremer and Stuckey (1972)'s Composite Index

[9] To address the data skewness, we use a logarithmic transformation of all variables.

[10] As our robustness checks, we consider GDP per capita as our measure of *technology* (Section 4.2.)

[11] As our robustness checks, we consider two other measures of *distance* (Section 4.2.)

of National Capability (CINC) score (version 5.0). This helps to address the possibility that substituting cyber capabilities may be more attractive than other types of conflict for weak (or unresolved) actors, relative to their opponents. Lastly, to account for a nation's potential willingness to fight, we use the dyadic *affinity* score (AFFINITY) from Voeten, Strezhnev and Bailey (2017)'s United Nations General Assembly Voting data.[12]

4 Results and Robustness Checks

4.1 Generalized Estimating Equations

Results from the generalized linear models, where we use each type of cyber operations iteratively as our dependent variable, are presented in Figure 2. To ensure our results are more readily interpretable, we standardize our continuous explanatory variables — AFFINITY, CAP_DISTANCE (LOG), CINC (LOG), and INT_USERS_A/T (LOG).

As these findings reveal, only disruptive cyber campaigns are likely to be used to complement fighting on the ground. This is not surprising given the short-term impact of these operations, which are often meant to disrupt an enemy's command and control. These results also show that degradation cyber operations, which are designed to sabotage a target's networks, operations, or systems, are used independently from traditional military campaigns, most likely because these operations are rare[13] and "loud" campaigns can create enough damage on their own. Lastly and not surprisingly, cyber espionage campaigns tend to take place independently from conventional operations, considering that most of these campaigns occur prior to start of conventional conflicts.

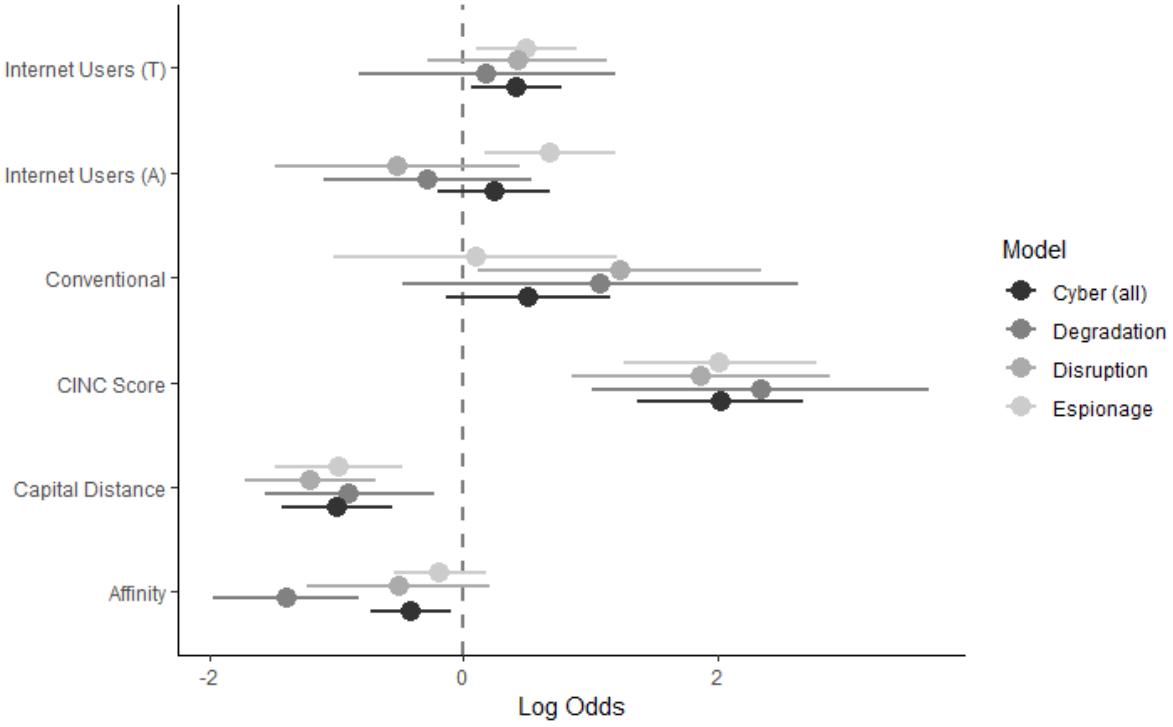
In addition to the complementarity of cyber disruption campaigns to other modes

[12] As our robustness checks, we use the dyadic *agree* score from Voeten, Strezhnev and Bailey (2017)'s United Nations General Assembly Voting data as our measure of *affinity* (Section 4.2.)

[13] There are only 14 degradation campaign in the dataset of 2,870 cyber campaigns.

of conflict, we also demonstrate the effect of other variables on a nation's propensity to attack over the Internet. Specifically, the fewer interests that two countries share (AFFINITY), the more likely the initiator is to use any type of cyber campaign (Model 1) or degradation cyber campaign against the target (Model 2). With a decrease in the physical distance between national capitals (CAP_DISTANCE) and an increase in a state's level of national capabilities (CINC), an initiator is more likely to use cyber campaigns against the target. Lastly, the higher the Internet reliance of an initiator and target (INT_USERS_A/T), the more likely an initiator is to conduct cyber espionage against a target.

Figure 2: USE OF CYBER CAMPAIGNS FOR CONVENTIONAL DISPUTES: RESULTS FROM GENERALIZED ESTIMATING EQUATIONS (GEE) MODELS



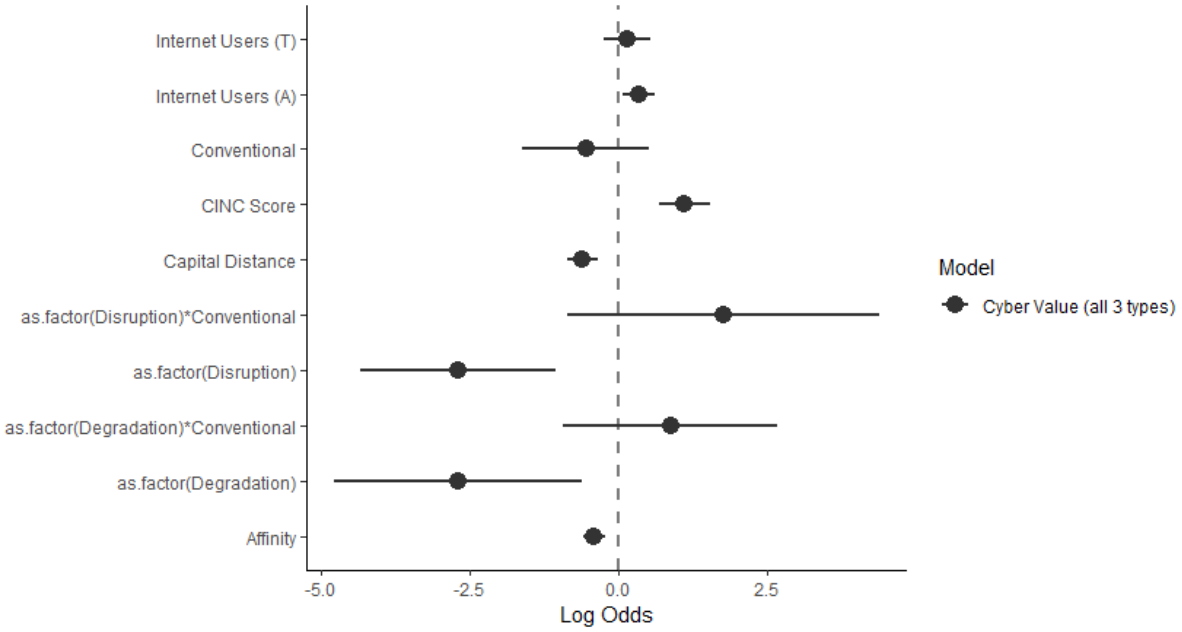
To investigate how cyber and conventional operations influence each other, we ran

multivariate GEE models. Specifically, we "stretched" our dataframe and created one long dependent variable (CYBER VALUE) that contains all types of cyber campaigns (ESPIONAGE, DISRUPTION, DEGRADATION).[14] We use GEE logistic regression to regress all of the DVs on their lagged values and other relevant covariates. In addition to including lags for all cyber campaigns (DEGRADATION _LAG, DISRUPTION_LAG, and ESPIONAGE_LAG), we also considered the effect of each type of cyber campaign (DEGRADATION (as factor), DISRUPTION (as factor), and ESPIONAGE (as factor)) on the likelihood of any type of a cyber campaign, and the interaction effect between each type of cyber campaign and conventional operations on the likelihood that any type of cyber campaign.

Figure 3 displays these results. In a manner similar to the results above, cyber operations are unlikely to be used as a complementary tool to conventional campaigns. Interestingly, disruption and degradation cyber campaigns are unlikely to be used with another type of cyber operation. Our findings further confirm that with an increase in dissimilarity of interests (AFFINITY), a decrease in the distance between the two capitals (CAP_DISTANCE), and an increase in the initiator's level of national capabilities (CINC), the initiator is more likely to use any cyber means necessary to coerce its adversary.

[14]We omit CYBER from this model because of collinearity of a composite variable with its components.

Figure 3: USE OF CYBER CAMPAIGNS FOR CONVENTIONAL DISPUTES: RESULTS FROM MULTIVARIATE GENERALIZED ESTIMATING EQUATIONS (GEE) MODELS



4.2 Robustness Checks

In addition to the analyses already presented, we conducted the following five sets of robustness checks:

1. We use monthly data for our analysis (Models 7-12 of Table 1 and Section 3.1 of the Online Appendix).

2. We use a different measure for *affinity*. Instead of the AFFINITY score that ranges from "-1" (least similar interests) to "1" (most similar interests), we use a *voting similarity index* (AGREE) that ranges between 0 and 1 (Models 13-17 of Table 1 and Section 3.2 of the Online Appendix).

3. We use different measures for *distance*. Instead of CAP_DISTANCE (LOG), we use

a dummy variable to identify whether the two countries are located in the same geographical region (SREGION) (Models 18, 20-23 of Table 1 and Section 3.3 of the Online Appendix) and a dummy for CONTIGUITY indicating whether states share a land border or are separated by less than 150 miles of water (Stinnett et al., 2002) (Models 24-26 of Table 1 and Section 3.3 of the Online Appendix).

4. We use a different measure for *technology*. Instead of INTERNET_USERS_A/T (LOG), we use a state's GDP per capita (GDP_PERCAPITA_A/T (LOG)) (Model 19, 27-30 of Table 1 and Section 3.4 of the Online Appendix).

5. We use the Council on Foreign Relations' (CFR) Cyber Operations Tracker as our source of cyber operations (Models 31-33 of Table 1 and Section 3.5 of the Online Appendix).[15]

Table 1 summarizes our main results and robustness checks for all types of cyber campaigns. The results confirm the complementarity of disruption cyber campaigns with conventional military operations — if a country fights its enemy on the ground, it is likely that it will also use disruption cyber campaigns to affect the enemy's command and control. In addition, with a decrease in an attacker's national capabilities, an increase in the distance between the two nations, and a decrease in the target's Internet reliance,[16] the attacker is less likely to use cyber campaigns against the target.

[15] We have not included the results for the degradation cyber campaigns using the CFR data due to the perfect separation issue because there are only two degradation campaigns in the CFR data. Because of this, we also did not include the results for the multivariate GEE model using the CFR data.

[16] The result for a target's Internet reliance is not robust across all the models.

Table 1: MAIN RESULTS & ROBUSTNESS CHECKS: ALL TYPES OF CYBER CAMPAIGNS

Model ID	*Results Type*	*Attack Type*	*MIDs*	*Affinity*	*Distance*	*CINC Score*	*Technology*	
							Attacker	*Target*
1	Cyber (all)	Main		−	−	+		+
2	Degradation	Main		−	−	+		
3	Disruption	Main	+		−	+		
4	Espionage	Main			−	+	+	+
5	Cyber (ext.)	Main		N/A	N/A	N/A	N/A	N/A
6	Cyber (ext.)	Main		−	−	+		+^
7	Cyber (all)	Monthly		−	−	+	+	+
8	Degradation	Monthly		−	−^	+		
9	Disruption	Monthly	+		−	+		+
10	Espionage	Monthly			−	+	+	+
11	Cyber (ext.)	Monthly		N/A	N/A	N/A	N/A	N/A
12	Cyber (ext.)	Monthly		−	−	+	+	+
13	Cyber (all)	"Affinity"		−	−	+		+
14	Degradation	"Affinity"		−	−	+		
15	Disruption	"Affinity"	+		−	+		
16	Espionage	"Affinity"			−	+	+	+
17	Cyber (ext.)	"Affinity"		−	−	+		+^
18	Cyber (ext.)	"Distance"		−	−	+		
19	Cyber (ext.)	"Technology"		−	−	+		
20	Cyber (all)	"Distance"	+^	−	−	+		+
21	Degradation	"Distance"		−	−	+		
22	Disruption	"Distance"	+	−	−	+		
23	Espionage	"Distance"		−	−	+	+	+
24	Cyber (all)	"Distance"	+	−^		+		+
25	Disruption	"Distance"	+			+		+^
26	Espionage	"Distance"				+	+	
27	Cyber (all)	"Technology"		+	−	+		
28	Degradation	"Technology"	+^	−		+^		
29	Disruption	"Technology"	+^	−^	−	+		+
30	Espionage	"Technology"		−	−	+		
31	Cyber (all)	CFR data			−	+	+	+
32	Disruption	CFR data	+^	−	−	+		+
33	Espionage	CFR data				+	+^	+

***Cyber (ext.)**: Cyber Value (extended); **N/A:** not applicable; ^ - 10% statistical significance*

5 Discussion and Implications

Much remains to be done in assessing the impact of new forms of conflict on war and peace. We have only modestly increased available knowledge, at best. Still, it may be helpful to begin to think about how better to answer questions of considerable salience and consequence. Our efforts here can perhaps serve as a useful point of departure.

We asked a basic question about the nature of new modes of conflict: Do they substitute for or complement existing forms of military aggression? We have provided an answer, which while tentative is also unequivocal and large in substantive terms: disruptive cyber operations are much more likely to be associated with existing forms of conflict than they are to be exercised in isolation. Cyber disruption is generally not a substitute for conventional (kinetic) forms of military violence. Further, the decline in militarized conflict identified in recent decades cannot be explained simply by the rise of disruptive "cyberwar." Much to the contrary, the dependence of disruptive cyber operations on conventional conflict behavior to motivate and prove fruitful in both military and political terms means that the decline in kinetic forms of warfare has occurred *despite* the increasing availability of new modes of warfare (cyber operations).

This is not the case for espionage and degradation campaigns. Our results show that these campaigns tend to be used in isolation. Considering that cyber espionage tends to start years prior to the possibility of active conflict, one way to check the robustness of our findings would be to run the analysis using (1) recoded datasets that merge the objectives of espionage campaigns with specific military actions and/or (2) a time window prior to the start of military action that associates an espionage campaign with this military action. While degradation operations are used independently from military violence, further research must show whether these results continue to hold, considering the recent move to publicly attributing cyber operations.

In addition to the complementarity of cyber and other modes of conflict, we also demonstrated an effect of other variables on the propensity of nations to attack one another over the internet. Distance mutes the propensity of nations to engage in cyber conflict. Given the ease with which the cyber domain transits physical space, we suspect that this is a reflection of the decline in motivation among actors, rather than a loss of

capacity. Capable states and states with a high dependency on the Internet are also more likely to be associated with cyber conflict. In the latter instance, the propensity is greatest for targets. We also found that these relationships persist, despite taking into account the interdependencies of key variables over time and space.

These findings have deep implications for the theory and practice of national security. By providing the first global quantitative analysis of cyber and kinetic campaigns, our study sheds light on a theoretical debate focused around a coercive role of cyber operations during conflict (Borghard and Lonergan, 2017; Brantly, 2016; Gartzke, 2013; Kostyuk and Zhukov, 2019; Lindsay and Gartzke, 2015; Valeriano, Jensen and Maness, 2018). It complements quantitative and country-specific works on this topic. Unlike Kostyuk and Zhukov (2019) who, by focusing on individual cyber operations, demonstrated that there is no overlap between daily cyber and kinetic fronts in the Ukrainian and Syrian conflicts, we show that such overlaps exist globally when one focuses on a cyber campaign as a unit of analysis. While further research is needed to assess the dynamics of cyber and conventional operations, this finding shows that media, public and decision-makers tend to overestimate the role cyber operations play in modern conflict. As more nations have been using information campaigns to complement war "on the ground," future research should investigate the role this new tool plays in kinetic conflicts.

Future research will also help determine whether our initial findings are correct. There is every possibility that the many constraints imposed by circumstances, data limitations (both in time and space) and even our estimation decisions could later be found to condition our findings. We look forward to improvements in data coverage—temporal, spatial and in terms of missing data—that might allow researchers to more authoritatively assess the nature of cooperation and contestation the cyber domain. Nev-

ertheless, it is useful to provide the best answers one can provide at the current time, given these limitations. At the very least, our findings must cast considerable doubt on the rising perception that cyber conflict is a substitute for conventional forms of conflict behavior. The evidence at present emphatically states otherwise. We hope that this finding in itself is valuable, thought-provoking and helps clarify perceptions of cyber conflict among policy makers and the general public.

References

Ablon, Lillian and Andy Bogart. 2017. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. Rand Corporation.

Andres, Richard. 2012. "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence." *Trans. Array Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Derek S. Reveron. 1st ed. Washington DC: Georgetown University Press* .

Axelrod, Robert and Rumen Iliev. 2014. "Timing of cyber conflict." *Proceedings of the National Academy of Sciences* 111(4):1298–1303.

Bellovin, Steven M, Susan Landau and Herbert S Lin. 2017. "Limiting the undesired impact of cyber weapons: technical requirements and policy implications." *Journal of Cybersecurity* 3(1):59–68.

Borghard, Erica D and Shawn W Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26(3):452–481.

Boulding, Kenneth E. 1962. "Conflict and defense: A general theory.".

Brantly, Aaron Franklin. 2016. *The Decision to Attack: Military and Intelligence Cyber Decision-making*. University of Georgia Press.

Bremer, Stuart A. 1992. "Dangerous dyads: Conditions affecting the likelihood of interstate war, 1816-1965." *Journal of Conflict Resolution* 36(2):309–341.

Brito, Jerry and Tate Watkins. 2011. "Loving the Cyber Bomb-The Dangers of Threat Inflation in Cybersecurity Policy." *Harv. Nat'l Sec. J.* 3:39.

Carr, Jeffrey. 2011. *Inside cyber warfare: Mapping the cyber underworld*. O'Reilly Media, Inc.

Clarke, Richard A and Robert K Knake. 2010. "Cyber War: The Next Threat to National Security and What to Do About It.".

Davis, Joshua. 2007. "Hackers take down the most wired country in europe." *Wired Magazine* 15(9):15–09.

Diehl, Paul F. 1985. "Contiguity and military escalation in major power rivalries, 1816-1980." *The Journal of Politics* 47(4):1203–1211.

Eun, Yong-Soo and Judith Sita Aßmann. 2014. "Cyberwar: Taking Stock of Security and Warfare in the Digital Age." *International Studies Perspectives* .

Gannon, Andres, Erik Gartzke and Jon Lindsay. 2017. "After Deterrence: Explaining Conflict Short of War.".

Gartzke, Erik. 2013. "The myth of cyberwar: bringing war in cyberspace back down to Earth." *International Security* 38(2):41–73.

Geers, Kenneth, Darien Kindlund, Ned Moran and Rob Rachwald. 2014. World War C: Understanding nation-state motives behind today's advanced cyber attacks. Technical report Technical report, FireEye.

Hensel, Paul R et al. 2000. "Territory: Theory and evidence on geography and conflict." *What do we know about war* pp. 57–84.

Huth, Paul K. 2009. *Standing your ground: Territorial disputes and international conflict*. University of Michigan Press.

Joint Publication 3 13 Information Operations. 2014.

Jones, Daniel M, Stuart A Bremer and J David Singer. 1996. "Militarized interstate disputes, 1816–1992: Rationale, coding rules, and empirical patterns." *Conflict Management and Peace Science* 15(2):163–213.

Junio, Timothy J. 2013. "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate." *Journal of Strategic Studies* 36(1):125–133.

Kello, Lucas. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38(2):7–40.

Kostyuk, Nadiya and Yuri M Zhukov. 2019. "Invisible digital front: Can cyber attacks shape battlefield events?" *Journal of Conflict Resolution* 63(2):317–347.

Kugler, Richard L. 2009. "Deterrence of cyber attacks." *Cyberpower and National Security* pp. 309–340.

Labs, F-Secure. 2014. Blackenergy & Quedagh. Technical report F-Secure.

Libicki, Martin C. 2009. *Cyberdeterrence and cyberwar*. Rand Corporation.

Liff, Adam P. 2012. "Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war." *Journal of Strategic Studies* 35(3):401–428.

Lindsay, Jon R and Erik Gartzke. 2015. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." *Typescript, University of California, San Diego* .

Lipovsky, Robert and Anton Cherepanov. 2015. Operation Potao Express: Analysis of a cyber-espionage toolkit. Technical report ESET.
URL: *http://www.welivesecurity.com/wp-content/uploads/2015/07/Operation-Potao-Express_final_v2.pdf*

Maoz, Zeev. 2005. "Dyadic Militarized Interstate Disputes Dataset Version 2.0." *UC Davis)* .

McGraw, Gary. 2013. "Cyber War is Inevitable (Unless We Build Security In)." *Journal of Strategic Studies* 36(1):109–119.

Poznansky, Michael and Evan Perkoski. 2018. "Rethinking Secrecy in Cyberspace: The

Politics of Voluntary Attribution." *Journal of Global Security Studies* .

Richards, Julian. 2014. *Cyber-war: The Anatomy of the Global Security Threat*. Palgrave Macmillan.

Rid, Thomas. 2012. "Cyber war will not take place." *Journal of Strategic Studies* 35(1):5–32.

Rios, Billy K. 2009. "Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack." *The Virtual Battlefield: Perspectives on Cyber Warfare* 3:143.

Sabah, Daily. 2016. "Cyber bombs being used to destroy Daesh: US defense chief.".

Schelling, Thomas C. 1966. "Arms and influence." *New Haven: Yale* .

Schmitt, Michael N. 1999. "Computer network attack and the use of force in international law: thoughts on a normative framework." *Columbia Journal of Transnational Law* 37:1998–99.

Senese, Paul D. 2005. "Territory, contiguity, and international conflict: Assessing a new joint explanation." *American Journal of Political Science* 49(4):769–779.

Sharma, Amit. 2010. "Cyber Wars: A Paradigm Shift from Means to Ends." *Strategic Analysis* 34(1):62–73.

Singer, J David, Stuart Bremer and John Stuckey. 1972. "Capability distribution, uncertainty, and major power war, 1820-1965." *Peace, war, and numbers* 19:48.

Snake campaign and cyber espionage toolkit. 2014. Technical report BAE Systems.

Stinnett, Douglas M, Jaroslav Tir, Paul F Diehl, Philip Schafer and Charles Gochman. 2002. "The correlates of war (cow) project direct contiguity data, version 3.0." *Conflict Management and Peace Science* 19(2):59–67.

Tsagourias, Nicholas. 2012. "Cyber attacks, self-defence and the problem of attribution." *Journal of conflict and security law* p. krs019.

Valeriano, Brandon, Benjamin Jensen and Ryan C Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press.

Valeriano, Brandon and Ryan C Maness. 2014. "The dynamics of cyber conflict between rival antagonists, 2001–11." *Journal of Peace Research* 51(3):347–360.

Valeriano, Brandon and Ryan C Maness. 2015. "Cyber Hype versus Cyber Reality: Restraint and Norms in Cyber Conflict.".

Valeriano, Brandon and Ryan Maness. 2012. "The fog of cyberwar: why the threat does not live up to the hype." *Foreign Affairs* .

Vasquez, John A. 1995. "Why do neighbors fight? Proximity, interaction, or territoriality." *Journal of Peace Research* 32(3):277–293.

Vasquez, John A. 2001. "Mapping the probability of war and analyzing the possibility of peace: The role of territorial disputes." *Conflict Management and Peace Science* 18(2):145–173.

Vasquez, John A. 2009. *The war puzzle revisited*. Vol. 110 Cambridge University Press.

Voeten, Erik, Anton Strezhnev and Michael Bailey. 2017. "United Nations General Assembly Voting Data.".
URL: *http://hdl.handle.net/1902.1/12379*

Walt, Stephen M. 2010. "Is the Cyber Threat Overblown?" *Foreign Policy* 30.

Online Appendix

Fighting in Cyberspace:

Complementarity versus substitutability in cyber operations

Nadiya Kostyuk*and Erik A. Gartzke†

July 21, 2019

Contents

*Doctoral Candidate, University of Michigan, Ann Arbor, nadiya@umich.edu; http://www-personal.umich.edu/ nadiya/index.html

†Professor of Political Science and Director of the Center for Peace and Security Studies (cPASS), University of California, San Diego, egartzke@ucsd.edu.

1 Summary Statistics and Correlation Plots

Figure 1 depicts the correlation plot and Table 1 shows the summary statistics for main dependent and explanatory variables.

Figure 1: Correlation Plot

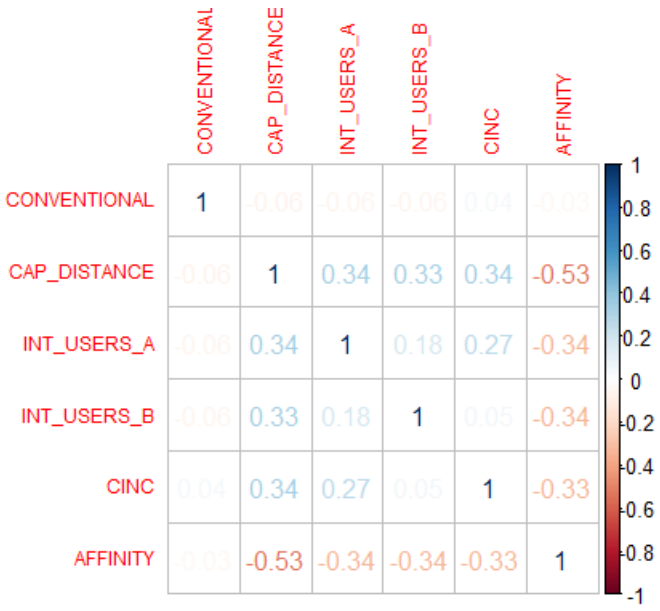


Table 1: Summary Statistics

	Cyber	Disruption	Espionage	Degradation	Convent.	Cap Distance	Internet Users	CINC Score	Affinity
Minimum	0.000	0.000	0.000	0.000	0.000	118	0.0	0.0000	-1.000
Median	0.000	0.000	0.000	0.000	0.000	1560	6.2	0.0041	0.944
Mean	0.023	0.005	0.015	0.003	0.227	2992	18.1	0.0208	0.654
Maximum	1.000	1.000	1.000	1.000	1.000	16375	93.4	0.2082	1.000

2 Main Results

2.1 Results from Generalized Estimating Equation (GEE) Models

In the first four models, we estimate the likelihood that a country uses conventional tools with each individual type of cyber campaign—Espionage, Disruption, Degradation—and uses these conventional tools with all types of cyber tools (Cyber_All) (Table 2). To make our results easy to interpret, we standardize our continuous explanatory variables — Affinity, Cap_Distance (log), Int_Users_A/T (log), CINC (log).

As our findings reveal, only disruption cyber campaigns are likely to be used to complement fighting on the ground. This is not surprising given the short-term impact of these operations, which are often meant to disrupt an enemy's command and control. These results also show that

degradation cyber operations, which are designed to sabotage a target's networks, operations, or systems, are used independently from traditional military campaigns, most likely because these operations are rare[1] and "loud" campaigns can create enough damage on their own. Lastly and not surprisingly, cyber espionage campaigns tend to take place independently from conventional operations, considering that most of these campaigns take place prior to start of conflicts.

In addition to the complementarity of cyber disruption campaigns and other modes of conflict, we also demonstrate that other variables effect a nation's propensity to attack over the Internet. Specifically, the fewer interests that two countries share (AFFINITY), the more likely the initiator is to use any type of cyber campaign (Model 1) or degradation cyber campaigns against the target (Model 2). With a decrease in the physical distance between the capitals of two nations (CAP_DISTANCE) and an increase in a state's level of national capabilities (CINC), an initiator is more likely to use cyber campaigns against the target. Lastly, the higher the Internet reliance of an initiator and target, the more likely the initiator is to execute cyber espionage against the target (INT_USERS_A/T).

Table 2: USE OF CYBER CAMPAIGNS FOR CONVENTIONAL DISPUTES: RESULTS FROM GENERALIZED ESTIMATING EQUATION (GEE) MODELS

	Dependent Variables			
	Cyber (All)	*Degradation*	*Disruption*	*Espionage*
	Model 1	*Model 2*	*Model 3*	*Model 4*
CONVENTIONAL	0.52	1.08	1.23^{*}	0.10
	(0.33)	(0.79)	(0.57)	(0.57)
AFFINITY	-0.41^{*}	-1.39^{***}	-0.51	-0.19
	(0.16)	(0.29)	(0.37)	(0.18)
CAP_DISTANCE (LOG)	-1.00^{***}	-0.90^{**}	-1.20^{***}	-0.98^{***}
	(0.22)	(0.34)	(0.26)	(0.26)
CINC (LOG)	2.03^{***}	2.34^{***}	1.86^{***}	2.02^{***}
	(0.33)	(0.68)	(0.52)	(0.39)
INT_USERS_A (LOG)	0.24	-0.28	-0.51	0.68^{**}
	(0.23)	(0.42)	(0.49)	(0.26)
INT_USERS_T (LOG)	0.42^{*}	0.18	0.43	0.50^{*}
	(0.18)	(0.51)	(0.36)	(0.20)
CYBER_ALL_LAG	4.21^{***}			
	(0.58)			
DEGRADATION_LAG		5.36^{***}		
		(1.02)		
DISRUPTION_LAG			2.28	
			(1.50)	
ESPIONAGE_LAG				5.00^{***}
				(0.55)
Number of clusters	316	316	316	316
Maximum cluster size	10	10	10	10
Number of observations	2,870	2,870	2,870	2,870

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{\wedge}p < 0.1$

[1] There are only 14 degradation campaign in the dataset of 2,870 cyber campaigns.

2.2 Results from Multivariate Generalized Estimating Equation (GEE) Models

Since different types of cyber campaigns influence each other, we use a multivariate dependent variable (CYBER_VALUE) in our last model. Specifically, we "stretched" our dataframe and created one long dependent variable (CYBER VALUE) that contains all cyber variables (ESPIONAGE, DISRUPTION, DEGRADATION).[2] In addition to including lags of all types of cyber campaigns (DEGRADATION _LAG, DISRUPTION_LAG, and ESPIONAGE_LAG), we also considered the effect of each type of cyber campaign (DEGRADATION (as factor), DISRUPTION (as factor), and ESPIONAGE (as factor)) on the likelihood that any type of a cyber campaign is taking place, and the interaction effect between each type of cyber campaign and conventional operations on the likelihood that any type of a cyber campaign is taking place.

Table 3 presents the results. In a manner similar to the results above, cyber operations are unlikely to be used as a complementary tool to conventional campaigns. Interestingly, disruption and degradation campaigns are unlikely to be used with any type of cyber operation. Our findings further confirm that with an increase in dissimilarity of interests (AFFINITY), a decrease in the distance between the two capitals (CAP_DISTANCE), and an increase in the initiator's level of national capabilities (CINC), the initiator is more likely to use any cyber means necessary to coerce its adversary.

[2] We did not include CYBER in this model because it is a composite variable that consists of ESPIONAGE, DISRUPTION, DEGRADATION.

Table 3: Use of Cyber Campaigns for Conventional Disputes: Results from Multivariate GEE Models

	Dependent Variables	
	Cyber Value (All 3 types) *Model 5*	*Cyber Value (All 3 types)* *Model 6*
Conventional	0.07	-0.09
	(0.44)	(0.46)
Disruption (as factor)	-2.31^{***}	-2.42^{***}
	(0.63)	(0.66)
Degradation (as factor)	-2.12^{*}	-2.22^{*}
	(0.85)	(0.88)
Espionage_Lag	5.08^{***}	3.45^{***}
	(0.34)	(0.40)
Disruption_Lag	3.20^{*}	2.09^{*}
	(0.86)	(0.99)
Degradation_Lag	5.00^{***}	3.30^{***}
	(0.38)	(0.48)
Disruption (as factor)*Conventional	1.58	$1.70^{\wedge}$
	(1.02)	(1.02)
Degradation (as factor)*Conventional	0.64	0.76
	(0.84)	(0.83)
Affinity		-0.42^{**}
		(0.16)
Cap_Distance (log)		-0.95^{***}
		(0.17)
CINC (log)		1.75^{***}
		(0.30)
Internet_Users_A (log)		0.15
		(0.26)
Internet_Users_T (log)		$0.29^{\wedge}$
		(0.16)
Number of clusters	316	316
Maximum cluster size	30	30
Number of observations	8,610	8,610

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{\wedge}p < 0.1$

3 Robustness Checks

In addition to the analyses already presented, we conduct the following five sets of robustness checks:

1. We use monthly data for our analysis (Section 3.1).
2. We use a different measure for *affinity*. Instead of the Affinity score that ranges from "-1" (least similar interests) to "1" (most similar interests), we use a *voting similarity index* (Agree) that ranges between 0 and 1 (Section 3.2).
3. We use different measures for *distance*. Instead of Cap_Distance (log), we use a dummy variable to identify whether the two countries are located in the same geographical region (Sregion) and a dummy for Contiguity indicating whether states share a land border or are separated by less than 150 miles of water (Stinnett et al., 2002) (Section 3.3).
4. We use a different measure for *technology*. Instead of Internet_Users_A/T (log), we use a state's GDP per capita (GDP_PerCapita_A/T (log)) (Section 3.4).

5. We use the Council on Foreign Relations' (CFR) Cyber Operations Tracker as our source of cyber operations (Section 3.5).

Table 4 summarizes our main results and robustness checks for all types of cyber campaigns. The results confirm the complementarity of disruption cyber campaigns with conventional military operations — if a country fights its enemy on the ground, it is likely that it will also use disruption cyber campaigns to affect the enemy's command and control. In addition, with a decrease in an attacker's national capabilities, an increase in the distance between the two nations, and a decrease in the target's Internet reliance,[3] the attacker is less likely to use cyber campaigns against the target.

Table 4: Main Results & Robustness checks: All Types of Cyber Campaigns

Model ID	*Results Type*	*Attack Type*	*MIDs*	*Affinity*	*Distance*	*CINC Score*	*Technology*	
							Attacker	*Target*
1	Cyber (all)	Main		–	–	+		+
2	Degradation	Main		–	–	+		
3	Disruption	Main	+		–	+		
4	Espionage	Main			–	+	+	+
5	Cyber (ext.)	Main		N/A	N/A	N/A	N/A	N/A
6	Cyber (ext.)	Main		–	–	+		+ ^
7	Cyber (all)	Monthly		–	–	+	+	+
8	Degradation	Monthly		–	–^	+		
9	Disruption	Monthly	+		–	+		+
10	Espionage	Monthly			–	+	+	+
11	Cyber (ext.)	Monthly		N/A	N/A	N/A	N/A	N/A
12	Cyber (ext.)	Monthly		–	–	+	+	+
13	Cyber (all)	"Affinity"		–	–	+		+
14	Degradation	"Affinity"		–	–	+		
15	Disruption	"Affinity"	+		–	+		
16	Espionage	"Affinity"			–	+	+	+
17	Cyber (ext.)	"Affinity"		–	–	+		+ ^
18	Cyber (ext.)	"Distance"		–	–	+		
19	Cyber (ext.)	"Technology"		–	–	+		
20	Cyber (all)	"Distance"	+ ^	–	–	+		+
21	Degradation	"Distance"		–	–	+		
22	Disruption	"Distance"	+	–	–	+		
23	Espionage	"Distance"		–	–	+	+	+
24	Cyber (all)	"Distance"	+	– ^		+		+
25	Disruption	"Distance"	+			+		+ ^
26	Espionage	"Distance"				+	+	
27	Cyber (all)	"Technology"		+	–	+		
28	Degradation	"Technology"	+ ^	–		+ ^		
29	Disruption	"Technology"	+ ^	– ^	–	+		+
30	Espionage	"Technology"		–	–	+		
31	Cyber (all)	CFR data			–	+	+	+
32	Disruption	CFR data	+ ^	–	–	+		+
33	Espionage	CFR data				+	+ ^	+

***Cyber (ext.)**: Cyber Value (extended); **N/A**: not applicable; ^ - 10% statistical significance*

3.1 Monthly Data

In this section, we use monthly data for our analysis. Table 5 and 6 present results.

[3] The result for a target's Internet reliance is not robust across all the models.

Table 5: Robustness Checks: GEE Models Using Monthly Data

	Dependent Variables			
	Cyber (All)	*Degradation*	*Disruption*	*Espionage*
	Model 7	*Model 8*	*Model 9*	*Model 10*
Conventional	0.26	-0.54	1.75**	0.20
	(0.41)	(1.38)	(0.59)	(0.47)
Affinity	−0.31*	−1.22***	-0.45	-0.23
	(0.15)	(0.27)	(0.33)	(0.17)
Cap_Distance (log)	−0.87***	−0.71^	−0.77***	−0.92***
	(0.21)	(0.40)	(0.22)	(0.23)
CINC (Log)	1.71***	2.25***	1.72***	1.68***
	(0.29)	(0.51)	(0.45)	(0.33)
Int_Users_A (log)	0.71***	-0.02	-0.04	0.80***
	(0.19)	(0.41)	(0.44)	(0.24)
Int_Users_T (log)	0.50**	0.24	0.71**	0.60**
	(0.16)	(0.29)	(0.28)	(0.21)
Cyber_All_Lag	8.22***			
	(0.52)			
Degradation_Lag		9.16***		
		(0.64)		
Disruption_Lag			4.82***	
			(1.08)	
Espionage_Lag				9.67***
				(0.54)
Number of clusters	291	291	291	291
Maximum cluster size	131	131	131	131
Number of observations	34,526	34,526	34,526	34,526

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{\wedge}p < 0.1$

Table 6: Robustness Checks: Multivariate GEE Models Using Monthly Data

Dependent Variables		
	Cyber Value (All 3 types) Model 11	*Cyber Value (All 3 types) Model 12*
Conventional	-0.06	0.02
	(0.62)	(0.67)
Disruption (as factor)	−4.91***	−5.00***
	(0.84)	(0.87)
Degradation (as factor)	−2.97*	−3.04*
	(1.20)	(1.25)
Espionage_Lag	8.09***	6.80***
	(0.56)	(0.55)
Disruption_Lag	5.92***	4.84***
	(0.66)	(0.64)
Degradation_Lag	8.06***	6.73***
	(0.52)	(0.57)
Disruption (as factor)*Conventional	2.26	2.42
	(1.60)	(1.60)
Degradation (as factor)*Conventional	-0.32	-0.17
	(1.63)	(1.61)
Affinity		−0.29**
		(0.10)
Cap_Distance (log)		−0.73***
		(0.15)
CINC (log)		1.08***
		(0.26)
Internet_Users_A (log)		0.37*
		(0.18)
Internet_Users_T (log)		0.18*
		(0.09)
Number of clusters	291	291
Maximum cluster size	393	393
Number of observations	103,578	103,578

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{\wedge}p < 0.1$

3.2 Alternative Measure of "Affinity"

We use a different measure for *affinity*. Instead of the Affinity score that ranges from "-1" (least similar interests) to "1" (most similar interests), we use a *voting similarity index* (Agree) that ranges between 0 and 1 (Tables 7 and 8 (Model 17)).

Table 7: Robustness Checks: GEE Models Using an Alternative "Affinity" Measure

	Dependent Variables			
	Cyber (All)	*Degradation*	*Disruption*	*Espionage*
	Model 13	*Model 14*	*Model 15*	*Model 16*
Conventional	0.52	1.08	1.23^{*}	0.10
	(0.33)	(0.79)	(0.57)	(0.57)
Agree	-0.41^{*}	-1.39^{***}	-0.51	-0.19
	(0.16)	(0.29)	(0.37)	(0.18)
Cap_Distance (log)	-1.00^{***}	-0.90^{**}	-1.20^{***}	-0.98^{***}
	(0.22)	(0.34)	(0.26)	(0.26)
CINC (Log)	2.03^{***}	2.34^{***}	1.86^{***}	2.02^{***}
	(0.33)	(0.68)	(0.52)	(0.39)
Int_Users_A (log)	0.24	-0.28	-0.51	0.68^{**}
	(0.23)	(0.42)	(0.49)	(0.26)
Int_Users_T (log)	0.42^{*}	0.18	0.43	0.50^{*}
	(0.18)	(0.51)	(0.36)	(0.20)
Cyber_All_Lag	4.21^{***}			
	(0.58)			
Degradation_Lag		5.36^{***}		
		(1.02)		
Disruption_Lag			2.28	
			(1.50)	
Espionage_Lag				5.00^{***}
				(0.55)
Number of clusters	316	316	316	316
Maximum cluster size	10	10	10	10
Number of observations	2,870	2,870	2,870	2,870

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{\wedge}p < 0.1$

Table 8: Robustness Checks: Multivariate GEE Models Using Alternative Measures

Dependent Variables			
	Cyber Value (All 3 types) Model 17	*Cyber Value (All 3 types) Model 18*	*Cyber Value (All 3 types) Model 19*
Conventional	-0.09	0.00	0.02
	(0.46)	(0.43)	(0.52)
Disruption (as factor)	-2.42^{***}	-2.44^{***}	-2.31^{**}
	(0.66)	(0.66)	(0.73)
Degradation (as factor)	-2.22^{*}	-2.23^{*}	-2.31^{*}
	(0.88)	(0.89)	(1.03)
Espionage_Lag	3.45^{***}	3.16^{***}	3.52^{***}
	(0.40)	(0.40)	(0.47)
Disruption_Lag	2.09^{*}	1.84^{*}	1.99
	(0.99)	(0.69)	(1.31)
Degradation_Lag	3.30^{***}	3.33^{***}	3.13^{***}
	(0.48)	(0.5)	(0.84)
Disruption (as factor)*Conventional	$1.70^{\wedge}$	1.69	1.73
	(1.02)	(1.03)	(1.15)
Degradation (as factor)*Conventional	0.76	0.72	0.01
	(0.83)	(0.83)	(1.31)
Agree	-0.42^{**}		
	(0.16)		
Affinity		-0.71^{***}	-0.53^{***}
		(0.15)	(0.14)
Cap_Distance (log)	-0.95^{***}		-1.20^{***}
	(0.17)		(0.25)
Same Region		2.65^{***}	
		(0.37)	
CINC (log)	1.75^{***}	1.48^{***}	2.16^{***}
	(0.30)	(0.23)	(0.37)
Internet_Users_A (log)	0.15	0.20	
	(0.26)	(0.30)	
Internet_Users_T (log)	$0.29^{\wedge}$	0.27	
	(0.16)	(0.17)	
GDP_PerCapita_A (log)			-0.11
			(0.13)
GDP_PerCapita_T (log)			0.10
			(0.16)
Number of clusters	316	316	298
Maximum cluster size	30	30	30
Number of observations	8,610	8,610	7,398

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{\wedge}p < 0.1$

3.3 Alternative Measures of "Distance"

We use different measures for *distance*. Instead of Cap_Distance (log), we use a dummy variable to identify whether the two countries are located in the same geographical region (Sregion) (Tables 9 and 8 (Model 18)) and a dummy for Contiguity indicating whether states share a land border or are separated by less than 150 miles of water (Stinnett et al., 2002) (Tables 10 and 8 (Model 19)). We have not included the results for the degradation cyber campaigns with the Contiguity measure of distance due to the perfect separation issue between Contiguity and Degradation. Because of this, we also did not include the results for the multivariate GEE model with the Contiguity measure of distance.

Table 9: Robustness Checks: GEE Models Using an Alternative "Distance" Measure (Same Region)

	Dependent Variables			
	Cyber (All)	*Degradation*	*Disruption*	*Espionage*
	Model 20	*Model 21*	*Model 22*	*Model 23*
Conventional	$0.63^{\wedge}$	1.31	1.61^{**}	0.09
	(0.33)	(0.92)	(0.50)	(0.56)
Affinity	-0.79^{***}	-2.29^{***}	-0.87^{**}	-0.65^{***}
	(0.16)	(0.64)	(0.40)	(0.17)
Same Region	3.12^{***}	4.47^{*}	3.84^{***}	3.38^{***}
	(0.53)	(1.82)	(1.11)	(0.60)
CINC (Log)	1.86^{***}	3.04^{***}	1.54^{**}	1.90^{***}
	(0.27)	(0.77)	(0.50)	(0.35)
Int_Users_A (log)	0.35	-0.36	-0.56	0.82^{**}
	(0.26)	(0.45)	(0.52)	(0.30)
Int_Users_T (log)	0.40^{*}	0.15	0.43	0.45^{*}
	(0.19)	(0.46)	(0.37)	(0.22)
Cyber_All_Lag	3.96^{***}			
	(0.54)			
Degradation_Lag		5.54^{***}		
		(0.97)		
Disruption_Lag			$1.99^{\wedge}$	
			(1.15)	
Espionage_Lag				4.68^{***}
				(0.56)
Number of clusters	316	316	316	316
Maximum cluster size	10	10	10	10
Number of observations	2870	2870	2870	2870

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{\wedge}p < 0.1$

Table 10: Robustness Checks: GEE Models Using an Alternative "Distance" Measure (Contiguity)

	Dependent Variables		
	Cyber (All)	*Disruption*	*Espionage*
	Model 24	*Model 25*	*Model 26*
Conventional	1.08**	1.96**	0.73
	(0.35)	(0.74)	(0.48)
Affinity	−0.23^	-0.22	-0.16
	(0.12)	(0.33)	(0.11)
Contiguity	0.42	0.94	0.47
	(0.47)	(1.27)	(0.72)
CINC (Log)	1.58***	1.41*	1.68***
	(0.29)	(0.66)	(0.36)
Int_Users_A (log)	0.19	-0.58	0.75**
	(0.25)	(0.43)	(0.28)
Int_Users_T (log)	0.54*	0.71^	0.41
	(0.23)	(0.37)	(0.26)
Cyber_All_Lag	3.93***		
	(0.76)		
Disruption_Lag		1.75	
		(1.78)	
Espionage_Lag			5.36***
			(0.77)
Number of clusters	219	219	219
Maximum cluster size	10	10	10
Number of observations	1,970	1,970	1,970

***$p < 0.001$, **$p < 0.01$, *$p < 0.05$, ^$p < 0.1$

3.4 Alternative Measure of "Technology"

We use a different measure for *technology*. Instead of Internet_Users_A/T (log), we use a state's GDP per capita (GDP_PerCapita_A/T (log)) (Tables 11 and 8).

Table 11: Robustness Checks: GEE Models Using an Alternative "Technology" Measure

	Dependent Variables			
	Cyber (All)	*Degradation*	*Disruption*	*Espionage*
	Model 27	*Model 28*	*Model 29*	*Model 30*
Conventional	0.52	2.01^	1.37^	0.04
	(0.36)	(1.11)	(0.81)	(0.67)
Affinity	0.52***	−1.46**	−0.43^	−0.45**
	(0.14)	(0.52)	(0.25)	(0.14)
Cap_Distance (log)	−1.26***	-0.75	−1.59**	−1.16***
	(0.29)	(0.53)	(0.49)	(0.33)
CINC (Log)	2.46***	2.00^	2.35***	2.44***
	(0.37)	(1.09)	(0.65)	(0.41)
GDP_PerCapita_A (log)	-0.13	0.69	-0.24	-0.06
	(0.16)	(0.60)	(0.18)	(0.27)
GDP_PerCapita_T (log)	-0.09	1.02	−0.55***	-0.06
	(0.19)	(0.85)	(0.16)	(0.22)
Cyber_All_Lag	4.16***			
	(0.71)			
Degradation_Lag		6.80***		
		(1.89)		
Disruption_Lag			2.02	
			(1.74)	
Espionage_Lag				5.20***
				(0.66)
Number of clusters	298	298	298	298
Maximum cluster size	10	10	10	10
Number of observations	2,466	2,466	2,466	2,466

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{\wedge}p < 0.1$

3.5 Alternative Data of Cyber Operations: Council on Foreign Relations' Cyber Operations Tracker

We use the Council on Foreign Relations' (CFR) Cyber Operations Tracker as our source of cyber operations (Table 12). We have not included the results for the degradation cyber campaigns using the CFR data due to the perfect separation issue.[4] Because of this, we also did not include the results for the multivariate GEE model using the CFR data.

[4] There are only 2 degradation campaigns in the CFR data.

Table 12: Robustness Checks: Council on Foreign Relations' Cyber Operations Tracker

	Dependent Variables		
	Cyber (All)	*Disruption*	*Espionage*
	Model 31	*Model 32*	*Model 33*
Conventional	0.16	1.38^	-0.28
	(0.39)	(0.82)	(0.60)
Affinity	-0.17	-0.78^{*}	0.01
	(0.20)	(0.34)	(0.24)
Capital Distance	-0.45^{*}	-1.68^{**}	-0.22
	(0.18)	(0.51)	(0.16)
CINC (Log)	2.20^{***}	2.19^{***}	2.50^{***}
	(0.51)	(0.51)	(0.54)
Int_Users_A (log)	0.48^{*}	0.33	0.53^
	(0.24)	(0.51)	(0.31)
Int_Users_T (log)	0.48^{***}	0.84^{**}	0.75^{***}
	(0.17)	(0.32)	(0.18)
Cyber_All_Lag	2.24^{***}		
	(0.43)		
Disruption_Lag		-38.26^{***}	
		(0.90)	
Espionage_Lag			2.14^{***}
			(0.42)
Number of clusters	333	333	333
Maximum cluster size	11	11	11
Number of observations	3,326	3,326	3,326

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{\wedge}p < 0.1$

References

Stinnett, Douglas M, Jaroslav Tir, Paul F Diehl, Philip Schafer and Charles Gochman. 2002. "The correlates of war (cow) project direct contiguity data, version 3.0." *Conflict Management and Peace Science* 19(2):59–67.