*Original Manuscript*

Armed Forces & Society
1-23

DOI: 10.1177/0095327X15572997
afs.sagepub.com
SAGE

# The Impact of Cyber Conflict on International Interactions

**Ryan C. Maness[1] and Brandon Valeriano[2]**

## Abstract

Analysts suggest that the rise of the cyber domain of combat has led to a revolution in military affairs and have greatly changed how society interacts with the Internet. The structure and content of interactions on the battlefield have supposedly changed in light of this development. In the rush to note the changing face of conflict, few scholars have actually examined the impact of cyber conflict on foreign policy relationships. Here we use weekly events data to examine exactly what happens between countries when cyber conflict is utilized as a foreign policy choice. Using a previously constructed data set of cyber actions, we measure conflict and cooperation after a cyber operation to understand the true impact of this new way to arm a state and society. We find that only one method of cyber malice, denial of service, and one tactical goal, seeking a change in behavior in the opposing side, impacts conflict–cooperation dynamics between states.

## Keywords

cyber conflict, foreign policy, events data

[1] Northeastern University, Boston, MA, USA
[2] University of Glasgow, Glasgow, UK

**Corresponding Author:**
Ryan C. Maness, Northeastern University, Department of Political Science, 360 Huntington Ave, Boston, MA 02115, USA.
Email: r.maness@neu.edu

## Introduction

Pundits have dubbed cyber conflicts "cool wars" because of the technology involved.[1] It is said that these conflicts reflect the changing dynamics of state-to-state interactions in the post–Cold War world. States are not willing and able to interact in an outright violent manner, but must restrain their actions below typical thresholds of conflict which makes these conflicts not cold or hot, but cool. The argument is that the structure, content, and location of interactions on the military battlefield have changed in light of these developments. Yet beyond the media and potential hype, what are the actual responses from states when breached in the digital realm? Few have endeavored to investigate the consequences of these actions, thus the goal of this article is move beyond the rhetoric and investigate the impact of cyber tactics on foreign policy interactions.

Some would estimate the cyber threat is pressing and important. US President Barack Obama has declared that the "cyberthreat is one of the most serious economic and national security challenges we face as a nation."[2] Former US Defense Secretary Leon Panetta goes further, "I believe that it is very possible the next Pearl Harbor could be a cyber attack ... [that] would have one hell of an impact on the United States of America. That is something we have to worry about and protect against."[3] Clark and Knake (32) frame the cyber debate as transformational, stating, "there is a credible possibility that such conflict [cyber] may have the potential to change the world military balance and thereby fundamentally alter political and economic relations."[4] The question we have is what is the reality of this threat and prospect? The hope for this research is to return the debate on cyber conflict to a more nuanced approach based on empirical evidence. Data and analysis allow us to make more accurate policy choices based on the current state of relations.

Valeriano and Maness note that although cyber conflict is proliferating, the level of severity in cyber incidents remains minimal.[5] Using the data set of cyber incidents developed by Valeriano and Maness, we measure the level of conflict and cooperation observed after a cyber incident and dispute to understand the true impact of this new tactic on foreign policy dynamics.[6] This article is one of the first attempts to quantify the impact of cyber actions. We attempt to motivate the community to explore the empirical impact of cyber actions that connects to the reality of the context, rather than the speculation rampant in the discourse.

We propose a theory of cyber restraint based on intentions, noting the constraints on cyber actors and their available responses. The fundamental question we ask is does cyber conflict raise the level of conflict interactions between states, or is there different conflict–cooperation dynamics based on the type and severity of the cyber incident or dispute?

Based on our results, we find that only one method of cyber malice, distributed denial of service (DDoS), affects conflict–cooperation dynamics between states. The effect is a souring of relations between pairs of states when DDoS tactics are utilized as a foreign policy tool. We also find that regional powers and dyads containing the

United States have important conflict–cooperation effects when cyber incidents are involved. The latter effects are all negative, except for one pair of states, the United States and China. When China uses cyber conflict directed toward the United States, the United States will respond with diplomacy and try to improve relations with the rising power. These results challenge the typical conventional wisdom proposed by pundits and academics suggesting that cyber interactions are a revolutionary new way of conducting interstate interactions.[7]

## Cyber Conflict and International Relations Scholarship

This project represents a view of international cyber conflict through the lens of the international relations field. The arena is cyber conflict among states or directed toward states in the realm of foreign policy. We cannot speak about the nature of cybercrime, but only about the nature of international interactions between states and their affiliates because there is a history, source, and method to analyzing these events that feed directly into the nature of cyber conflict between international competitors.

It does seem clear that the term cyber war is overwrought and descriptive of a process that has yet to occur. Rid is correct to point out that cyber war is not happening, allowing us to argue that the processes developing in cyberspace is something a bit different from traditional warfare.[8] Cyber is a tactic, not a form of complete warfare. It is a tool in the arsenal of diplomacy and international interactions just as other forms of threats are in the toolbox of a state's arsenal of power.[9] As Dunn-Cavelty notes, the cyber threat thus far is inflated yet a popular tool for politicians, policy makers, and defense contractors in contemporary discourse.[10]

We define cyber conflict as the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities. For us, cyber conflict is a foreign policy tool used by states or individuals against states.[11]

In 2011, the USs government declared a cyber incident similar to an act of war, punishable with conventional military means.[12] This is a significant step, because it allows the response to a nonphysical malicious incident in cyberspace to be in the physical, kinetic form. Conflict then shifts from cyberspace to conventional forms. Rarely have we seen nonphysical threats become the source of physical counter threats.[13] It cannot be argued that cyber operations are not causing a shift in the way foreign policy is made; our contention is that this shift might be problematic in light of evidence.[14]

In addition to cyber decision-making processes that shift how organizations and groups may respond to threats, we see cyber actions becoming part of the normal process of international relations threat construction. Cyber operations, cybercrime, and other forms of cyber activities directed by one state against another are now considered part of the normal relations range of combat and conflict.[15] It is now acceptable to respond to an incident in one domain, cyberspace, through another domain,

the physical and conventional layer, thus these responses become the norm in international relations. The barriers between the hypothetical and the abstract have broken down due to the fears of the costs the cyber world imposes in the physical world. As Clarke and Knake (xiii) argue, "cyber war may actually increase the likelihood of the more traditional combat with explosives, bullets, and missiles."[16] The domains have blended together and transformed into a new potential path to conflict.

Clarke and Knake (32) frame the cyber debate as transformational, stating, "there is a credible possibility that such conflict [cyber] may have the potential to change the world military balance and thereby fundamentally alter political and economic relations."[17] Further, even academics are making similar claims; Kello (32) declares that "The cyber domain is a perfect breeding ground for political disorder and strategic instability. Six factors contribute to instrumental instability: offense dominance, attribution difficulties, technological volatility, poor strategic depth, and escalatory ambiguity."[18] The question we have is what is the reality of this threat and prospect? We aim to return the debate on cyber conflict to a more nuanced approach based on empirics substantiating the actual dangers of cyber combat. While there is a real danger of cyber combat, one must remain prudent in relation to the actual threat, and not the inflated threat presented by the imagination. Data and analysis allow us to make more accurate policy choices as to how to react, based on the current state of relations.

## Cyber Restraint and Intent

Understanding the past and current uses of cyber power and reactions to the tactic can help us explain and predict future uses and responses to the tactic. With a focus on offensive cyber operations and the inflated nature of mythical cyber threats, we seem to have misdirected the application of the technology in the policy sphere.[19] Instead of a revolution in military affairs, cyber tactics just seem to have refocused the state on external threats. By focusing on the external threats, and not the actual reaction to the cyber actions, as a community we fail to provide proper analysis of the true conduct of cyber foreign policy interactions.

Cybersecurity is the framework for state defense against any potential malicious cyber incidents entering its borders and networks through digital channels. Choucri gives a more broad definition and refers to cybersecurity as "a state's ability to protect itself and its institutions against threats, espionage, sabotage, crime and fraud, identity theft, and other destructive e-interactions and e-transactions."[20] The often used term "cyber attack," used liberally by media pundits and academics alike, is a loaded term and can lead to inflated connotations of what is actually going on in terms of interactions in cyberspace between states. Therefore, the preferred term "cyber incidents" is used throughout this article, in place of the more hyperbolic and nebulous "cyber attack" term.

This article focuses on the impact of cyber events on the conflict and cooperation dynamics between rival states. Do cyber incidents influence and lead to more

conflictual relations? Do cyber incidents defy conventions and lead to positive sanctions rather than negative sanctions? We cannot really answer these questions until one takes a macro view of the situation and examines the entire picture of cyber interactions through time.

In general, it would be thought that during a rivalry, a situation of constant and historic animosity, a state will do all it can to harm the other side. In some instances, it will do almost anything, even wound itself, as long as the other side is hurt more.[21] Rivals participate in zero sum games of status. If a rival state uses a cyber operation to harm its enemy, the likely response will be characterized by further conflictual relations. Yet, our theory is based on the idea of restraint limiting cyber options because this is a different domain.

We have elaborated on a theory of cyber restraint elsewhere, but it would be useful to briefly review this process as it has an impact on our ultimate perspective that guides action in this study.[22] Cyber actions are difficult to undertake because by nature the weapon is reproducible. This makes it unlikely that any cyber option utilized will not be released to all, thus making the weapon now free to anyone who would wish to utilize it. Because of this factor, blowback is highly likely, and with the very same method used at the onset. Added to this is the fact that cyber weapons are costly to develop and not at all cheap or easy to use as some seem to think. These three factors, the reproducibility, blowback, and costly nature of the weapons, make it likely that states will be restrained in using cyber options.

The question that remains is if one side is attacked with a cyber weapon, what is the likelihood of response? Given our theory of restraint, we predict minimal reactions. Here restraint combined with the limited strategic impact of cyber activities, as suggested by Gartzke, produces the foreign policy outcomes we observe.[23] There is limited strategic value on cyber operations and states are often restrained from initiating massive and retaliatory cyber operations once attacked. There is also the consideration of collateral damage, even if attacked first, the danger of collateral damage using cyber options will limit the hand of responding state, effectively producing a cyber "straight jacket".

> **Hypothesis 1:** *Cyber incidents will not lead to conflictual foreign policy responses between rival states due to the dynamics of restraint.*

Cyber actions have not escalated in severity through time, as demonstrated by our past research.[24] Stuxnet was the most famous and drastic cyber action so far, yet analysis of the event demonstrates little impact.[25] If anything, cyber operations typically represent probes and faints to harass an enemy and demonstrate capabilities. States are capable of so much more in cyberspace, yet they seem to hold back from unleashing their full cyber capabilities. Norms and taboos also reinforce this process and are critical because cyber weapons are not controllable and manageable, as the makers of Stuxnet found when it escaped into civilian sectors.

International cyber interactions are determined by the issue that draws states into conflict. Most rival interactions in cyberspace will have a regional context connected to the issue of territorial considerations or disputes, as most rivalries start due to territorial concerns.[26] These disputes may institute a culture of antagonism. Vasquez and Valeriano find that the modal category for war is territorial issues.[27] To locate the source of cyber incidents and disputes, territorial considerations are often at the heart of the issue.

Therefore, we argue that the one arena where states will not be restrained is in foreign policy contestations in regional subsystems. Generally provoked and dominated by territorial disputes, actors in a regional system must display power and capability in order to deter their local enemies from taking advantage of the targeted state. To stay on top of the regional hierarchy and protect the homeland, regional powers will demonstrate cyber capabilities in order to protect their positional status, something we find evidence for in prior work.[28] Therefore, regional actors are more likely to respond to cyber incidents with conflictual interactions. This should also be particularly true since most regional rivals contain territorial disputes and these disputes are particularly dangerous for escalation and cooperative relations.[29]

> **Hypothesis 2:** *Cyber incidents between regional rivals will lead to negative foreign policy responses*

Thus considering the intent of a cyber action is an important task, and we argue that cyber actors will likely be restrained in their cyber interactions and this trend will only be muted when regional rivals interact. Another factor that might lead to negative foreign policy interactions is the nature of the cyber incident. Coercive behavior in cyberspace typically fails to achieve the desired ends. When Russia infiltrated Estonia in 2007, the reaction by Estonia was not to move closer to the Russian sphere of influence, but to fully commit to the West.[30] When a state tries to use cyber tactics to change behavior, the targeted state will likely respond in a negative fashion.

In addition to coercion, spectacularly public cyber incidents using methods that are difficult to conceal from a population, like DDoS methods are also likely to engender a response. A targeted state cannot afford to look weak and fail to respond to such actions that seek to make a demonstration of capability. Other cyber tactics, such as espionage and nuisances, are less likely to exhibit reactions because they can be concealed and the targeted state is unlikely to pursue escalatory reactions, given the potential for cyber escalation.

> **Hypothesis 3:** *Intending to motivate a change in behavior through demonstration cyber incidents such as DDoS methods is likely to provoke a negative foreign policy response.*

In order to test our hypotheses, we must utilize an events history research design to compare the impact of cyber actions with the level of conflict and cooperation

between states. This is the only feasible way to understand the impact of cyber incidents on the foreign policy dynamics between states at the macro level.

## The Events Data Method and History

Events-based data methodology was once the past and now seems to be the future of empirical analysis in international politics. Events data measure any interaction, from the smallest diplomatic exchange to the invasion of a country, between two states over time. The advantage is the movement away from yearly interactions to weekly or monthly units, painting a finer and more detailed picture of totality of relations between entities. Data are compiled by combing media sources and coding them into the appropriate categories.

Events data were intended to measure the conflict and cooperation relationship between states. Here we find the use of an events data methodology appropriate and necessary to investigate cyber interactions. Events data have been used more frequently in recent years by scholars due to the work of Goldstein.[31] Goldstein creates a conflict–cooperation scale out of the 63 nominal events in World Events Interaction Survey (WEIS). As Conflict and Peace Data Bank's coding ended in 1978, over the years, it has been used more sparsely. WEIS has been continued into the 1980s and the fact that WEIS has 63 event types as well as verb-based actions, listed in Figure 1, means that WEIS interval level coding could help us uncover some useful relationships in the cyber realm. Goldstein uses a −10 to 10 conflict–cooperation scale with decimals to measure the intensity of individual events. The −10 score indicates the most conflictual relationship between a pair of states, which is a military attack, and 10 is the most cooperative relationship, which is state merger. Goldstein's work and his scale is now used in contemporary events data sets, such as Schrodt's Kansas Events Dataset and King and Lowe's Integrated Data for Events Analysis, that are machine assisted and use a variety of worldwide news sources.[32]

It must be noted that we chose a custom-built conflict–cooperation outcome as our dependent variable for this analysis. We are not interested in the events coded, but the most stable research question of positive and negative sentiment between countries at the aggregate level. Events data might be unable to capture an accurate account of protests, or cyber incidents for that matter, but it can capture conflict and cooperation, which is needed to measure reactions from states after a cyber incident. Since no scholar has uncovered the foreign policy dynamics of cyber actions between states, it is pertinent to this study to include both conflict and cooperation scores to be able to test for significance for both simultaneously.

We create an events data set that compiles conflict–cooperation scores between dyads that also use cyber tactics as a foreign policy tool from the years 2001 to 2011. Scores from this data set, in the style of Goldstein's scale, serve as the dependent variable of our analysis. Our independent variables cover all cyber conflict among rival states, and with these measures, we can uncover the impact of cyber incidents on the foreign policy relations between states.[33]

| | |
|---|---|
| −10.0 Military attack; clash; assault | −0.1 Explicit decline to comment |
| −9.2 Seize position or possessions | −0.1 Request action; call for |
| −8.7 Nonmilitary destruction/injury | 0.0 Explain or state policy; state future position |
| −8.3 Noninjury destructive action | 0.1 Ask for information |
| −7.6 Armed force mobilization, exercise, display; military buildup | 0.6 Surrender, yield to order, submit to arrest |
| −7.0 Break diplomatic relations | 0.6 Yield position, retreat, and evacuate |
| −7.0 Threat with force specified | 1.0 Meet with; send note |
| −6.9 Ultimatum; threat with negative sanction and time limit | 1.2 Entreat; plead; appeal to; beg |
| −5.8 Threat with specific negative nonmilitary sanction | 1.5 Offer proposal |
| −5.6 Reduce or cutoff aid or assistance; act to punish/deprive | 1.8 Express regret; apologize |
| −5.2 Nonmilitary demonstration, walk out on | 1.9 Visit; go to |
| −5.0 Order person or personnel out of country | 1.9 Release and/or return persons or property |
| −4.9 Expel organization or group | 2.0 Admit wrongdoing; apologize, retract statement |
| −4.9 Issue order or command, insist, demand compliance | 2.5 Give state invitation |
| −4.4 Threat without specific negative sanction stated | 2.8 Assure; reassure |
| −4.4 Detain or arrest person(s) | 2.8 Receive visit; host |
| −4.1 Reduce routine international activity; recall officials | 2.9 Suspend sanctions; end punishment; call truce |
| −4.0 Refuse; oppose; refuse to allow | 3.0 Agree to future action or procedure, to meet or to negotiate |
| −4.0 Turn down proposal; reject protest, demand, and threat | 3.4 Ask for policy assistance |
| −3.8 Halt negotiation | 3.4 Ask for material assistance |
| −3.4 Denounce, denigrate, and abuse | 3.4 Praise, hail, applaud, and extend condolences |
| −3.0 Give warning | 3.6 Endorse other's policy or position; give verbal support |
| −2.4 Issue formal complaint or protest | 4.5 Promise other future support |
| −2.2 Charge, criticize, blame, and disapprove | 4.5 Promise own policy support |
| −2.2 Cancel or postpone planned event | 5.2 Promise material support |
| −1.9 Make complaint (not formal) | 5.4 Grant privilege; diplomatic recognition; de facto relations |
| −1.1 Grant asylum | 6.5 Give other assistance |
| −1.1 Deny an attributed policy, action, role, or position | 6.5 Make substantive agreement |
| −0.9 Deny an accusation | 7.4 Extend economic aid; give, buy, sell, loan, and borrow |
| −0.2 Comment on situation | 8.3 Extend military assistance |
| −0.1 Urge or suggest action or policy | |

*Source:* Goldstein (1992): 376-77.

**Figure 1.** Goldstein's (1992) Interval Conflict–Cooperation Scale.

## Research Design

The data on cyber incidents have been compiled by Valeriano and Maness.[34] The data set, the Dyadic Cyber Incident and Dispute Dataset (DCID), covers the years 2001 to 2011 and records all rival state-to-state cyber incidents. In all, 111 cyber incidents included in the eleven-year period are contained in the data set. Only events that can be attributable to states are recorded. Nonstate third-party entities such as Anonymous or the Syrian Electronic Army are not included; only state-based, government-sanctioned cyber events are coded.[35] Targets must also be state-based or can be a private network that is important to a state's national security. Boeing, Google, and Lockheed Martin are examples of this.[36]

DCID captures twenty dyads that have engaged in cyber conflict since 2001. These are the only dyads of possible states that have used cyberspace as a strategic tool during this time period.[37] We delineate these pairs of states into separate directed dyadic groups and as the analysis is over a period of time, the most appropriate technique is using generalized least squared (GLS) and ordinary least squared (OLS) panel data regressions. Panel data are used to observe the behavior of different entities across time and can also account for spatial correlations, and we find that accounting for both temporal and spatial correlation are required for this analysis. Our entities are dyads, and we look at effects of events for these pairs of states to get an overall analysis of foreign policy interactions. For our purposes, we measure the effects of cyber incidents on the conflict–cooperation scores for all dyads that have chosen to use cyber techniques as a foreign policy tool. There are two models that can be used to uncover these effects using panel data: random effects and fixed effects. GLS random effects models assume that the variation across our dyads is random and uncorrelated with the independent variables in our model.[38] However, we find that running an OLS fixed effects model is also warranted, as different conflict cooperation dynamics can be exhibited through time. Rival relationships go through ebbs and flows, and fixed effects account for different temporal correlations.[39] As we are also interested in the separate effects of cyber conflict on conflict and cooperation between states, we run a fixed effects model that treats each separate dyad as a dummy variable on the others. Both models for panel data are therefore run. Random effects are run to get an overall picture of cyber conflict on conflict cooperation on the entire population, and fixed effects are run to uncover the individual and unique effects on cyber conflict for each dyad in the data set.

The unit of analysis for our events data is dyadic week. Our time period analyzed is 2001–2011. Each event for each dyad within a week is given a Goldstein interval score, and the cumulative score of the conflictual or cooperative relationship for that dyad for each week is the dependent variable.[40] The more negative the cumulative weekly score, the more conflictual the relationship for the pair of states, and the more positive the cumulative score, the more cooperative the relationship. The Goldstein scale is an appropriate tool for this analysis as the independent variables,

cyber incidents, are rare events as there are only 111 cyber incidents with over 13,000 data points over a ten-year time span.[41] The dyads are also directed, accounting for observations where one side is the initiator and then the receiver in an active dyad resulting in forty groups.[42] As we are using panel regression techniques, separating pairs of states into directed dyads is crucial to get accurate results of the relationship between cyber conflict and foreign policy interactions.

Our independent variables are compiled from the DCID data set.[43] The main explanatory variables are cyber incidents. These variables, as well as every other independent variable used, are dichotomous where "1" is coded if cyber conflict is present, "0" if not. These variables are also directed, therefore, when a country initiates cyber conflict against its rival, it is matched with a Goldstein score-based foreign policy response, which is the directed dependent variable from the target state.[44] The assumption is that a directed cyber incident against a country initiates a conflict–cooperation dynamic (or a foreign policy response) from the targeted state. The cyber incident is lagged one week before the conflict–cooperation response. Each typology (interaction, method, target, initiator objective, and severity level) explained below is run separately from the others so as to avoid covariation in the results.

Cyber incidents are individual events that target a country for a matter of hours, days, or weeks that are coded as one per dyadic week. There are three types of cyber interactions for incidents: nuisances, defensive operations, and offensive strikes (Table 1). Along with a macro analysis of all cyber incidents, we also run several separate panel regressions that code each incident by type, target, method, initiator objective, and severity. If any of these incidents are present in each separate panel regression, we code the type, target, method, initiator objective, or severity as "1," "0" otherwise. Table 1 also lists the possible targets of a cyber incident. As we focus exclusively on government to government interactions, nonstate actors are only included in the data if they are considered part of a state's national security apparatus. Targets are private, government but nonmilitary, or government and military. Incidents are coded based on the objective of the initiator: disruptions are basic disruptions of a state's day-to-day activities; espionage is when the objective is to steal sensitive information, plans, or secrets from the target state; and change in behavior is when the initiator is attempting to alter the target state's behavior.

Cyber incidents are also coded by method. Methods are the ways in which initiators are able to access the networks of their rivals. Vandalism is the process of injecting code into a website that defaces that site. Denial of service methods are the coordinated flooding of particular websites or networks by activating multiple remotely controlled computers to bring down the target. Intrusions are methods used to remotely and quietly access a network and potentially steal information. Finally, infiltrations are cyber methods that can do the most potential harm. These include viruses, worms, logic bombs, and keystroke logging.[45] Targets such as power grids and defense networks can be the targets of infiltrations and can cause widespread panic and confusion. Advanced persistent threats are the most sophisticated form

**Table 1.** Types of Cyber Incidents.

| | |
|---|---|
| Interaction type | |
| 1 | Nuisance |
| 2 | Defensive operation |
| 3 | Offensive strike |
| Target type | |
| 1 | Private/nonstate but important to national security |
| 2 | Government nonmilitary |
| 3 | Government/military |
| Objectives for initiators | |
| 1 | Disruption |
| 2 | Espionage |
| 3 | Change in behavior |
| Method type | |
| 1 | Vandalism (website defacements) |
| 2 | Denial of Service (DDoS, distributed denial of service) |
| 3 | Intrusion (Trapdoors or Trojans, Backdoors) |
| 4 | Infiltrations (Malware) |
| 5 | Advanced Persistent Threats (APTs, Precision malware that targets specific secure information) |
| Severity type | |
| 1 | Minimal damage |
| 2 | Targeted attack on critical infrastructure or military |
| 3 | Dramatic effect on a country's specific strategy |
| 4 | Dramatic effect on a country |
| 5 | Escalated dramatic effect on a country |

of cyber tactic. This specific method can be in either intrusion or infiltration form, and target specific parts of networks that other methods cannot. Table 1 also lists the possible methods used for cyber incidents.

Our last cluster of explanatory variables in Table 1 measures the severity of cyber operations. This scale is ascending where "1" is the least harmful and "5" is the most severe. Our data collection thus far has only found that the most severe incidents to date are only in the "3" severity range.[46]

Our control variables are added to each regression that is ran with each of the explanatory variables. Time-series and panel regressions are controlled for trending, which holds constant the level of conflict and cooperation over time so that the impact of each cyber incident has the same relative reaction from states. As our dependent variables are all other forms of foreign policy interactions, such as economic sanctions or armed military conflict, the lagged regressions control for these outcomes.[47] The level of conflict and cooperation is controlled for the previous week so that the impact of a cyber incident is also controlled. The "Major Power" variable is coded as "1" if there is a major power in the dyad, "0" otherwise.[48] The "Same Region" variable encompasses the effects of region and captures the prediction of the second

**Table 2.** Random Effects Panel Regression: Total Cyber Incidents.

| | Coefficient | *SE* | z-score | *p* Value | 95 percent low | 95 percent high |
|---|---|---|---|---|---|---|
| Cyber incident | 0.264 | 0.614 | 0.43 | .667 | −0.939 | 1.467 |
| Major power | 1.246 | 0.980 | 1.27 | .203 | −0.673 | 3.166 |
| Region | −1.743 | 1.433 | −1.22 | .224 | −4.552 | 1.066 |
| Constant | 0.433 | 1.494 | 0.29 | .773 | −2.496 | 3.362 |

*Note:* $N = 13{,}449$, Wald $\chi^2 = 4.67$, $p > \chi^2 = .198$.

**Table 3.** Random Effects Panel Regression: Cyber Incidents by Type.

| | Coefficient | *SE* | z-score | *p* Value | 95 Percentage low | 95 Percentage high |
|---|---|---|---|---|---|---|
| Nuisance | −3.438 | 1.923 | −1.79 | .074* | −7.208 | 0.331 |
| Defensive | 1.420 | 1.390 | 1.02 | .307 | −1.304 | 4.143 |
| Offensive | 0.381 | 0.712 | 0.53 | .593 | −1.016 | 1.777 |
| Major power | 1.218 | 0.984 | 1.24 | .216 | −0.711 | 3.148 |
| Region | −1.703 | 1.452 | −1.17 | .241 | −4.549 | 1.142 |
| Constant | 0.427 | 1.510 | 0.28 | .777 | −2.532 | 3.387 |

*Note:* $N = 13{,}449$, Wald $\chi^2 = 9.01$, $p > \chi^2 = .109$.
*$p < .10$.

hypothesis; a "1" is coded if the two countries in the dyad also lie in the same region, "0" otherwise. Our regions include East Asia, South Asia, post–Soviet space, the Middle East, Europe, and the Americas. The results of our random and fixed effects models for cyber incidents are presented in the following section.

## Data Analysis

Tables 2 and 3 present the findings of the random effects model for cyber incidents. Overall, cyber incidents and their types do not have statistically significant effects on foreign policy interactions if examined according to interaction types. We fail to reject the null hypothesis, which means that cyber incidents have no effect on the foreign policy responses between states, given the data at hand. Rivals are still using other foreign policy tactics besides cyber to harm each other, and it seems clear cyber conflict has yet to significantly affect foreign policy interactions on the balance. One exception is the cyber incidents coded as nuisances, which are statistically significant at the 93 percent confidence level. This does not meet the conventional two-tailed level of statistical significance, which is the 95 percent confidence level; however, these results do warrant mentioning. These low-level vandalism or DDoS type campaigns are sometimes public and widespread, which could explain why there is a negative response from states.

**Table 4.** Random Effects Panel Regression: Cyber Incidents by Method.

| | Coefficient | *SE* | *z*-score | *p* Value | 95 Percentage low | 95 Percentage high |
|---|---|---|---|---|---|---|
| Vandalism | 0.941 | 1.49 | 0.70 | .485 | −1.701 | 3.583 |
| DDoS | −11.427*** | 2.482 | −4.60 | .000 | −16.292 | −6.563 |
| Intrusions | 0.818 | 1.136 | 0.62 | .534 | −1.759 | 3.394 |
| Infiltration | 0.880 | 0.978 | 0.90 | .368 | −1.036 | 2.796 |
| APTs | −0.103 | 1.131 | −0.09 | .927 | −2.320 | 2.113 |
| Major Power | 1.340 | 0.992 | 1.35 | .177 | −0.605 | 3.285 |
| Region | −1.658 | 1.471 | −1.13 | .260 | −4.541 | 1.224 |
| Constant | 0.254 | 1.527 | 0.17 | .868 | −2.740 | 3.248 |

*Note:* APT = advanced persistent threat. $N = 13{,}449$, Wald $\chi^2 = 27.35$, $p > \chi^2 = .0003$.
***$p < .001$.

Table 4 shows the random effects results of the different methods of cyber conflict states have used against each other from 2001 to 2011. Again, cyber methods as incidents do not have statistically significant effects on foreign policy interactions; thus, there is no evidence that there is any relationship between these variables, except for one particular method. Interestingly, it is the DDoS method that has statistically significant negative effects on conflict cooperation dynamics between rival states. This is surprising due to the low level of severity as well as the usual short durations of denial of service methods. So why are there negative reactions by rival states for DDoS methods, which are low-level cyber tactics?

The outcomes of DDoS methods may be the reason behind the negative foreign policy responses from target states, which allows us to fail to falsify the third hypothesis. The main goal for states that launch DDoS incidents is to shut down websites and cause havoc, which can effectively disrupt the daily lives of many people. This disruption may be trivial, yet it is still a nuisance. When a bank website is shut down, thousands of customers cannot conduct online transactions. When a government website is not working, citizens cannot access the government services they are seeking. Yet, the actual effect of these cyber incidents is trivial, yet the importance can be found in the perceptions and fears associated with these incidents that are amplified. DDoS methods, therefore, have a psychological effect on populations which leads to conflictual responses by the targeted state. Although rather benign in terms of long-term damage, denial of service methods evoke strong and negative reactions.

Table 5 shows the random effects panel regressions. There is no statistically significant effect when it comes to the nature of the target on which the initiator launches a cyber incident. This shows that is not the target type that evokes foreign policy responses from rival states.

Tables 6 and 7 display the random effects results of cyber incidents coded for the intentions of the initiators as well as severity levels. The effects of these coded explanatory variables are insignificant, except for when the initiator's intent is to

**Table 5.** Random Effects Panel Regression: Cyber Incidents by Target.

| | Coefficient | *SE* | z-score | *p* Value | 95 Percentage low | 95 Percentage high |
|---|---|---|---|---|---|---|
| Private | 1.812 | 1.638 | 1.11 | 0.269 | −1.399 | 5.022 |
| Government nonmilitary | 0.673 | 0.750 | 0.90 | 0.370 | −0.798 | 2.144 |
| Government military | −0.819 | 0.946 | −0.87 | 0.387 | −2.672 | 1.035 |
| Major power | 1.237 | 0.976 | 1.27 | 0.205 | −0.677 | 3.150 |
| Region | −1.762 | 1.419 | −1.24 | 0.215 | −4.544 | 1.020 |
| Constant | 0.458 | 1.483 | 0.31 | 0.758 | −2.450 | 3.365 |

*Note:* $N = 13{,}449$, Wald $\chi^2 = 7.68$, $p > \chi^2 = .1745$.

**Table 6.** Random Effects Panel Regression: Cyber Incidents by Initiator Objective.

| | Coefficient | *SE* | z-score | *p* Value | 95 Percentage Low | 95 Percentage High |
|---|---|---|---|---|---|---|
| Disruptions | 0.474 | 0.731 | 0.65 | .517 | −0.959 | 1.907 |
| Theft/Espionage | 1.118 | 0.792 | 1.41 | .159 | −0.436 | 2.672 |
| Behavioral Change | −4.127*** | 1.155 | −3.57 | .000 | −6.390 | −1.864 |
| Major Power | 1.418 | 0.965 | 1.47 | .142 | −0.474 | 3.309 |
| Region | −1.684 | 1.349 | −1.25 | .212 | −4.329 | 0.960 |
| Constant | 0.301 | 1.437 | 0.21 | .834 | −2.516 | 3.118 |

*Note:* $N = 13{,}449$, Wald $\chi^2 = 21.27$, $p > \chi^2 = .0007$.
***$p < .001$.

**Table 7.** Random Effects Panel Regression: Cyber Incidents by Severity Level.

| | Coefficient | *SE* | z-score | *p* Value | 95 Percentage low | 95 Percentage high |
|---|---|---|---|---|---|---|
| Severity 1 | −0.794 | 0.723 | −1.10 | .273 | −2.212 | 0.624 |
| Severity 2 | 0.677 | 0.949 | 0.71 | .475 | −1.183 | 2.537 |
| Severity 3 | 0.342 | 0.918 | 0.37 | .709 | −1.457 | 2.141 |
| Major power | 1.181 | 0.982 | 1.20 | .229 | −0.743 | 3.105 |
| Region | −1.629 | 1.409 | −1.16 | .248 | −4.391 | 1.132 |
| Constant | 0.467 | 1.487 | 0.31 | .754 | −2.447 | 3.381 |

*Note:* $N = 13{,}449$, Wald $\chi^2 = 7.09$, $p > \chi^2 = .2143$.

change the behavior of the target state. Attempting to force a state to do something it otherwise would not do in a coercive manner will usually evoke a negative response. Whether the tactic is diplomatic, military, or even in cyberspace, states do not like being told what to do, and how to conduct their foreign policy.

The findings on cyber incidents using the fixed effects panel data method uncover the individual directed dyadic effects of these events on foreign policy interactions. Table 8 shows the results of our fixed effects method and shows that overall cyber incidents as well as major powers in a dyad do not have any statistically significant effects on foreign policy interactions. However, the regional variable produces negative and statistically significant results. Regional rivals engage in low-level cyber incidents to exert power without escalating into more complicated and dangerous conflicts. Cyber incidents are a way to burn the other side using "botnets" instead of bullets.[49]

Most interesting for the findings in this controlled-group analysis are the statistically significant responses from the United States after it is the victim of a cyber incident. With the exception of China, the United States responds negatively and coercively to all of its rivals if it is the victim of cyber conflict. When the United States is the victim of cyber conflict originating from China, this evokes cooperative responses from the American foreign policy regime. It must be noted that these are public reactions captured by the events data dependent variables. Behind closed doors, therefore, the US reaction to intrusions by China in its secure networks could be quite different. Regardless, our focus on public events and the results seem counterintuitive due to all of the publically negative reports from cybersecurity firms about Chinese aggression in cyberspace.

The three most powerful cyber states, the United States, Russia, and China have been in talks about norms in cyberspace.[50] This is where the more cooperative scores between the United States and China are most likely being generated. However, since 2011, relations between the United States and Russia have been steadily spiraling downward, and domestic actions by the US Congress and Department of Justice have led to the indictment of five People's Liberation Army members with charges of espionage and theft.[51] The progress made on the development of cyber norms as well as the cordial responses from the United States when the victim of Chinese cyber malice, therefore, may be a thing of the past.

Enemies of the United States also react negatively to American incursions in cyberspace. Syria, North Korea, and Iran all evoke negative and statistically significant foreign policy responses when their networks are breached. The most famous incidents in this cluster of dyads are the ones inflicted on Iran by the United States and Israel and include Flame (2009), Stuxnet (2010), Duqu (2011), and Gauss (2011). Interestingly, it seems that most of the blame for these incidents falls with the United States within Iran, as the conflict–cooperation effects of Israeli incursions do not show an impact.

The last groups of dyads that have statistically significant reactions to cyber incidents are regional. Israel–Lebanon, China–India, and India–China all produce negative foreign policy reactions to cyber incidents. One state, Japan, reacts to cyber incidents with more cooperative interactions with their regional rivals. When South Korea and China send the botnets to Japan, the Japanese governments will respond with an olive branch. It seems that Japan does not want to escalate cyber conflict with its growing East Asian competitors.

**Table 8.** Fixed Effects Panel Regression: Cyber Incidents with Directed Dyadic Dummies.

| | Coefficient | *SE* | *t*-score | *p* Value | 95 Percentage Low | 95 Percentage High |
|---|---|---|---|---|---|---|
| Cyber incident | 0.145 | 0.620 | 0.23 | .816 | −1.072 | 1.361 |
| Major power | −0.110 | 1.241 | −.09 | .929 | −2.543 | 2.322 |
| Same region | −8.704** | 2.904 | −3.00 | .003 | −14.398 | −3.011 |
| United States–Iran | −10.159*** | 1.002 | −10.14 | .000 | −12.123 | −8.196 |
| United States–Syria | −10.686*** | 1.128 | −9.47 | .000 | −12.899 | −8.475 |
| United States–China | 3.229** | 1.060 | 3.05 | .002 | 1.151 | 5.308 |
| United States–North Korea | −4.703*** | 1.038 | −4.53 | .000 | −6.737 | −2.668 |
| United States–Russia | −2.689** | 0.983 | −2.74 | .006 | −4.615 | −0.762 |
| Iran–United States | −9.070*** | 1.052 | −8.62 | .000 | −11.131 | −7.008 |
| Syria–United States | −6.712*** | 1.205 | −5.57 | .000 | −9.073 | −4.351 |
| China–United States | 0.329 | 0.990 | 0.33 | .740 | −1.612 | 2.269 |
| North Korea–United States | −6.438*** | 1.056 | −6.10 | .000 | −8.508 | −4.368 |
| Russia–Georgia | 1.140 | 3.028 | .038 | .707 | −4.795 | 7.075 |
| Estonia–Russia | 2.667 | 3.527 | 0.76 | .450 | −4.246 | 9.578 |
| Georgia–Russia | 0.455 | 3.015 | 0.15 | .880 | −5.456 | 6.366 |
| Iran–Israel | −0.690 | 3.301 | −0.21 | .834 | −7.161 | 5.781 |
| Iraq–Kuwait | 1.959 | 3.511 | 0.56 | .577 | −4.923 | 8.841 |
| Lebanon–Israel | −6.082 | 3.300 | −1.84 | .065 | −12.551 | 0.387 |
| Israel–Iran | 0.053 | 3.298 | 0.02 | .987 | −6.412 | 6.519 |
| Israel–Lebanon | −15.125*** | 3.300 | −4.58 | .000 | −21.594 | −8.656 |
| Kuwait–Iraq | 3.115 | 3.561 | 0.87 | .382 | −3.864 | 10.095 |
| China–Taiwan | 4.039 | 2.956 | 1.37 | .172 | −1.756 | 9.834 |
| China–Japan | 3.737 | 2.931 | 1.28 | .202 | −2.008 | 9.481 |
| China–India | −3.341* | 1.460 | −2.29 | .022 | −6.202 | −0.480 |
| China–Vietnam | 4.298 | 3.431 | 1.25 | .210 | −2.427 | 11.022 |
| China–Philippines | 2.291 | 3.536 | 0.83 | .409 | −4.010 | 9.851 |
| Taiwan–China | 4.399 | 2.935 | 1.50 | .134 | −1.354 | 10.152 |
| North Korea–South Korea | 1.384 | 3.183 | 0.43 | .664 | −4.854 | 7.623 |
| North Korea–Japan | 3.633 | 3.026 | 1.20 | .230 | −2.299 | 9.565 |
| South Korea–Japan | 4.359 | 2.982 | 1.46 | .144 | −1.486 | 10.204 |
| Japan–China | 6.222* | 2.919 | 2.13 | .033 | 0.501 | 11.943 |
| Japan–North Korea | 3.471 | 2.982 | 1.16 | .244 | −2.373 | 9.316 |
| Japan–South Korea | 6.313* | 3.000 | 2.11 | .035 | 0.441 | 12.185 |
| India–China | −3.996** | 1.398 | −2.86 | .004 | −6.735 | −1.258 |
| India–Pakistan | 3.369 | 3.182 | 1.06 | .290 | −2.868 | 9.607 |
| India–Bangladesh | 1.356 | 3.420 | 0.40 | .692 | −5.348 | 8.060 |
| Pakistan–India | 3.659 | 3.180 | 1.15 | .250 | −2.575 | 9.893 |
| Bangladesh–India | 3.378 | 3.430 | 0.98 | .325 | −3.345 | 10.100 |
| Vietnam–China | 2.483 | 3.360 | 0.74 | .460 | −4.103 | 9.070 |

*(continued)*

**Table 8.** (continued)

| | Coefficient | *SE* | *t*-score | *p* Value | 95 Percentage Low | 95 Percentage High |
|---|---|---|---|---|---|---|
| Philippines–China | 2.788 | 3.238 | 0.86 | .389 | −3.558 | 9.135 |
| Constant | 6.315*** | 1.425 | 4.43 | .000 | 3.521 | 9.109 |

*Note:* $N = 13{,}449$, $F = 19.9$, $p > F = .0000$, Root MSE = 17.60, Adjusted $R^2 = .053$.
***$p < .001$.
**$p < .01$.
*$p < .05$, Dyads Dropped: Russia–United States, Russia–Estonia.

## Assessment

Overall, we demonstrate that for most cyber incidents, there is little evidence to argue that these tactics have a significant impact of foreign policy or military interactions, except in certain circumstances, at least so far. We therefore are able to falsify the first hypothesis of this analysis. Only certain types of incidents, DDoS, have specific and negative repercussions in states, allowing us to fail to falsify the third hypothesis. This is likely because DDoS events are so public and have collateral damage impacts in the daily lives of the citizens in the targeted states are impacted. Looking at intentions, we find that only incidents that intend to change the behavior in the target have dramatic and negative impacts on the conflict and cooperation levels between states.

DDoS methods in cyberspace, above all, have a psychological as well as a widespread effect on society. These incidents do not have the capabilities to do the amount of lasting damage the likes of intrusions and infiltrations; however, they are the only incidents that evoke negative responses from their victims. Examples of DDoS incidents include the ones launched against Estonia and Georgia by Russia in 2007 and 2008, respectively; on July 4, 2009, denial of service incidents against the United States and South Korea by North Korea; and most incidents between South Korea and Japan over the 10 years in our analysis. We assert that because these types of cyber tactics infiltrate the public domain, grievances toward the government for disruption of daily life are widespread and the foreign policy apparatuses for states are forced to respond in an assertive manner. If this cyber method is the only one to evoke a response between states, how dangerous is the current state of conflict in cyberspace?

We find evidence that incidents launched by states where the main intention is to coerce the target state to change its policy or behavior also evokes significant and negative reactions. Stuxnet, Flame, Duqu in the Olympic Games dispute between the United States and Iran as well as Israel and Iran are examples of these types of incidents. India's warning to Bangladesh to get its terrorist problem under control in March 2010 is another. These types of incidents seem to be launched when the level of relations between rivals is already sour. India was still reeling from the 2008

Mumbai terrorist attacks, later traced to Islamist fundamentalist groups in Pakistan. A stern warning given in cyberspace is an interesting foreign policy choice and signals a change in tactics.

Looking at regional interactions and specific dyads in the sample, attacks at the regional level tend to have a negative impact on cooperation levels. Therefore, the second hypothesis fails to be falsified. These incidents generally engender negative feelings and repercussions. The interactions between many regional actors are characterized by negative levels of cooperation after the cyber incident.

Evidence suggests that states rarely do use cyber tactics and when they do use the tactics, the responses rarely invoke a reaction. We need to examine the issue of escalation more in the future, but for now, we suggest that most cyber actions are done to demonstrate capabilities at the regional level or to harass a rival when they have an exposed weakness. When we look at cyber actions between states, we find little evidence the context of international interactions has changed.

## Conclusion

Most cyber incidents are allowed to occur without any significant response from the victim. In fact, incidents between great powers like the United States and China actually result in positive relations rather than further degenerative interactions. The reason for this is likely because cyber incidents fall below the normal range of operations. They generally are silent and focused methods meant to not upset the delicate balance of relations between competing rival states. When China infiltrates the United States, the United States responds diplomatically without further cyber operations. The future could be different, but for now, powers have learned to manage relationships even during constant and harmful cyber operations. We believe that the United States is restraining itself from reacting in a negative manner with China so as not to escalate cyber conflict to the doomsday levels many pundits and academics say is inevitable.

The trend that defies these patterns is DDoS methods. This is likely because DDoS are the most public of cyber methods and hold psychological weight that governments are forced to respond when infiltrated in cyberspace. While being low on the severity scale, they are like fireworks that go off in the night. In a digitally connected society, everyone sees them and the state may then be forced to react. The good thing is that these reactions fall short of the level of war and outright conventional violence. If these types of cyber incidents are not managed in the future, they could lead to further devastating counter cyber incidents. For now, states seem to be happy to respond with protests and then turn the other cheek.

The only cyber incidents that consistently evoke negative foreign policy responses are those that attempt to change state behavior.[52] Like all forms of diplomatic coercion, states do not like being told what to do by others, especially when the coercion is a matter of national security to the target state. Iran's motives to achieve weapons-grade uranium enrichment are, in its eyes, to protect itself. Any

state trying to alter this goal will be met with escalatory and coercive tit-for-tat behavior.

Thus far, these types of cyber operations are limited, but allowing them to become part of a state's foreign policy arsenal could lead to escalation and actual cyberwar, where casualties become a real possibility. The 2007 cyber dispute between Russia and Estonia brought the issue of cyberwar to the forefront of international relations discussions in governments, media, and academia. However, the dispute that started it all did not evoke any significant response from the target state. We often find this dynamic at work in our macro sample, giving us hope that the future era of cyber combat can be effectively managed. We are much more positive about the possibility of cyber cooperation and cyber peace than most other scholars and believe the data warrants these conclusions. Most states seem to be restrained in their actions in cyberspace. These findings bode well for the future of cyber international interactions and question the nature of shifting doctrines in military organizations.

## Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

## Notes

1. David Rothkopf, "The Cool War," *Foreign Policy*, February 20, 2013, accessed July 3, 2014, http://www.foreignpolicy.com/articles/2013/02/20/the_cool_war_china_cyberwar?page=full.
2. The White House, "Foreign Policy: Cybersecurity," *The White House*, accessed August 5, 2014, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity.
3. Karne Parrish, "Panetta Warns of Cyber Threat Growing Quickly," *Department of Defense News*, February 6, 2013, accessed August 4, 2014, http://www.defense.gov/news/newsarticle.aspx?id=119214.
4. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Harper Collins, 2010), 32.
5. Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," *Journal of Peace Research* 51, 3 (2014): 347-60.
6. Valeraino and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," 2014.
7. Clarke and Knake, *Cyber War*, 2010; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, 2 (2013): 7-40; Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, Inc., 2010).

8. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, 1 (2011): 5-32; Thomas Rid, *Cyber War Will Not Take Place* (London, UK: Hurst & Company, 2013).
9. Martin C. Libicki, *Conquest in Cyberspace* (Cambridge, UK: Cambridge University Press, 2007).
10. Miriam Dunn-Cavelty, *Cyber-security and Threat Politics: US Efforts to Secure the Information Age* (New York, NY: Routledge, 2008).
11. Although the research design easily could extend to this level, if the data were available.
12. Thomas Barlow, "China ups Ante in Cyber Warfare," *The Australian*, May 31, 2013, accessed July 6, 2014, http://www.theaustralian.com.au/national-affairs/opinion/friendly-china-ups-ante-in-cyber-warfare/story-e6frgd0x-1226654075003; White House, "Foreign Policy: Cybersecurity," 2014; Michael Schmitt, "The Tallinn Manual on the International Law Applicable to Cyber Warfare," *NATO Cooperative Cyber Defence Center for Excellence*, accessed May 31, 2013, http://www.ccdcoe.org/249.html.
13. Brandon Valeriano and Ryan C. Maness, *Cyber Hype Versus Cyber Reality: Restraint and Norms in Cyber Conflict* (Oxford, UK: Oxford University Press, in press).
14. Erik Gartzke, "The Myth of Cyberwar: Bringing War on the Internet back down to Earth," *International Security* 38, 2 (2013): 41-73; Clement Guitton, "Cyber Insecurity as a National Threat: Overreaction from Germany, France, and the UK?" *European Security* 22, 1 (2013): 21-35, doi:10.1080/09662839.2012.749864; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, 3 (2013): 365-404.
15. The term "normal relations range" is coined by Edward Azar in his 1972 article. Edward E. Azar, "Conflict Escalation and Conflict Reduction in an International Crisis, Suez 1956," *Journal of Conflict Resolution* 16, 2 (1972): 183-201; Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," 2014.
16. Clarke and Knake, *Cyber War*, 2010.
17. Ibid.
18. Kello, "The Meaning of the Cyber Revolution," 2013. The suggestion is that since the offense is thought to dominate in this domain, this makes defense complicated, creates incentives for increasing capacity and thus increasing volatility, which then increases opportunities for escalation.
19. Dunn-Cavelty, *Cyber-security and Threat Politics*, 2008.
20. Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: MIT Press, 2012), 43.
21. Valeriano and Maness, *Cyber Hype Versus Cyber Reality*, in press.
22. Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," 2014.
23. Gartzke, "The Myth of Cyberwar," 2013.
24. Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," 2014.
25. Valeriano and Maness, *Cyber Hype Versus Cyber Reality*, in press; Lindsay, "Stuxnet and the Limits of Cyber Warfare," 2013; Stuxnet was the cyber incident that disrupted

the centrifuges of the Iranian uranium enrichment program. Estimates on how long this set back Iran's nuclear weapons program range from a few months to five years.

26. John Vasquez and Christopher S. Leskiw, "The Origins and War-proneness of International Rivalries," *Annual Review of Political Scence* 4 (2001): 295-316.
27. John A. Vasquez and Brandon Valeriano, "Classification of Interstate Wars," *Journal of Politics* 72, 2 (2010): 292-309.
28. Author citation, Chapter 4.
29. John Vasquez, *The War Puzzle* (Cambridge, UK: Cambridge University Press, 1993).
30. Known as the "Bronze Soldier" dispute, this cyber operation happened when the Estonian government moved a Soviet-era grave marker from the central square of Tallinn to a more remote location. The result of this move was a series of vandalism and DDoS incidents that affected the Estonian government and private sector for approximately two weeks.
31. Joshua S. Goldstein, "A Conflict-cooperation Scale for WEIS Events Data," *Journal of Conflict Resolution* 36, 2 (1992): 369-85.
32. Philip A. Schrodt, "Event Data in Foreign Policy Analysis," in *Foreign Policy Analysis: Continuity and Change in Its Second Generation*, ed. Laura Neack, Patrick J. Haney, and Jeanne A. K. Hey (New York: Prentice Hall, 1993); Gary King and Will Lowe, "An Automated Information Extraction Tool for International Conflict Data with Performance as Good as Human Coders: A Rare Events Evaluation Design," *International Organization* 57, 3 (2003): 617-42.
33. Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," 2014.
34. Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," 2014. Data set available at drryanmaness.wix.com/irprof.
35. Organizations that initiate these types of attacks have no clear origin and many times have multiple political agendas, and as we are interested in the state-level dynamics of cyber conflict, these types of cyber incidents would not be a useful addition to the DCID nor our events data set.
36. The DCID data set (Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," 2014) acknowledges the fact that attribution can be problematic, as deniability is easy for states. States that use cyber tactics against their rivals must be fairly explicit, and if attribution cannot be found, it is not included in the data set. A state must acknowledge its part or forensics from cyber security companies must show evidence of state involvement; therefore, this is a comprehensive list of cyber incidents and disputes that fits best for our model.
37. James P. Klein, Gary Goertz, and Paul F. Diehl, "The New Rivalry Dataset: Procedures and Patterns," *Journal of Peace Research* 43, 3 (2006): 331-48; William R. Thompson, "Identifying Rivals and Rivalries in World Politics," *International Studies Quarterly* 45, 4 (2001): 557-86.
38. A Hausman test was run to see whether or not random or fixed effects would be the better fit for our data and model. It was found that random effects were the better fit, however; we also ran the fixed effects model to parse out the individual effects of each dyad.

Random effects are useful if it is believed that differences across dyads have some influence on the dependent variable. This type of panel regression accounts for spatial correlations. For this analysis, we assume that the differences in the nature of cyber conflict for each dyad will have an influence on our conflict–cooperation scores, as the nature of each rivalry is different. The intensity and relations range for each rival that uses cyber tactics as a foreign policy tool are not the same, therefore the random effects model is appropriate for the analysis.

39. This model assumes that each dyad has its own individual characteristics that may influence the independent variables, and this accounts for the variety of standard errors that each dyad will produce. Something within each dyad may affect the independent or dependent variables, producing different standard error scores, and must be controlled. Another assumption of fixed effects is that each dyad is different and thus the error term and constant of each dyad should not be correlated with the other dyads. Finally, the fixed effects approach for panel regression controls for trending and minimize any unit root issues that might arise.
40. Goldstein, "A Conflict-cooperation Scale for WEIS Events Data," 1992.
41. With forty directed dyads over a ten-year time span, the amount of data points would be around 20,000. However, as not all dyads have interactions all of the time periods, several weeks were dropped in the analysis, making the data point count 13,449.
42. Scott Bennett and Allan Stam, "Research Design and Estimator Choices in the Analysis of Interstate Dyads When Decisions Matter," *Journal of Conflict Resolution* 44, 5 (2000): 653-85.
43. Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," 2014.
44. Bennett and Stam, "Research Design and Estimator Choices in the Analysis of Interstate Dyads When Decisions Matter," 2000.
45. Logic bombs are programs that cause a system or network to shut down and/or erase all data within that system or network. Viruses are programs that need help by a hacker to propagate and can be attached to existing programs in a network or act as stand-alone programs. They generally replicate themselves with the intention of corrupting or modifying files. Worms are essentially the same as viruses, except they have the ability to propagate themselves. Packet sniffers are software designed to capture information flowing across the web. Keystroke logging is the process of tracking the keys being used on a computer so that the input can be replicated in order for a hacker to infiltrate secure parts of a network (Clarke and Knake, *Cyber War*, chapter 3).
46. This is not to suggest that cyber variables are the only factors that impact the dependent variable, only that these are the variables we are interested in at this point in time.
47. Adding independent variables such as economic sanctions and militarized disputes would lead to a problem of collinearity, as these types of disputes are possible dependent variables. Furthermore, the current data sets that encompass militarized disputes and economic sanctions are not updated to the point that they would be able to be included throughout the entire time span of this analysis. The dependent variables are the one week

lagged Goldstein score-based foreign policy responses from the target states after being the victim of a cyber incident, toward the initiating states.

48. J. David Singer, "The 'Correlates of War' Project: Interim Report and Rationale," *World Politics* 24, 2 (1972): 243-70.
49. Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," 2014.
50. Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," 2014. The Track II dialogues, the Sunnylands Summit, and talks within the UN Security Council and General Assembly are all examples of inroads to norms in cyberspace among the major powers.
51. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," *Justice.gov*, May 19, 2014, accessed August 4, 2014, http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.
52. See Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," 2014, drryanmaness.wix.com/irprof and cyberconflictdata.com.

## Author Biographies

**Ryan C. Maness** (PhD University of Illinois at Chicago, 2013) is a visiting fellow of Security and Resilience Studies at the Northeastern University, Boston, MA. His main research interests focus on the use of events data as a tool of uncovering foreign policy interactions between states. His focus right now is with Russian foreign policy and its use of cyber as a new form of power projection. He has two forthcoming books with Valeriano, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* with Oxford University Press, and *Russia's Coercive Diplomacy: Cyber, Energy and Maritime Policy as New Forms of Power* with Palgrave Macmillan.

**Brandon Valeriano** (PhD Vanderbilt University, 2003) is a senior lecturer in Global Security at the University of Glasgow in the School of Social and Political Sciences. His main research interests include investigations of the causes of conflict and peace. His focus right now is in cybersecurity and the intersection between gaming and international relations.