Journal of
Peace Research

Journal of Peace Research
1–14
© The Author(s) 2014
Reprints and permission:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/0022343313518940
jpr.sagepub.com
SAGE

The dynamics of cyber conflict between rival antagonists, 2001–11

Brandon Valeriano

School of Social and Political Sciences, University of Glasgow

Ryan C Maness

Department of Political Science, University of Illinois at Chicago

Abstract

Much discussion of the concept of cyberwar, cyber conflict, and the changing dynamic of future security interactions is founded upon the study of what could be, conjured through spectacular flights of the imagination. The goal of this research article is to exhaustively collect information on cyber interactions between rival states in the last decade so that we can delineate the patterns of cyber conflict as reflected by evidence at the international level. The field of cyber security needs a clear return to social science in order to be able to definitively engage the cyber debate with facts, figures, and theory. To that end we provide a dataset of cyber incidents and cyber disputes that spans from 2001 to 2011. Our data include 110 cyber incidents and 45 cyber disputes. Further, we test our theory of cyber conflict which argues that restraint and regionalism should be expected, counter-intuitive to conventional wisdom. We find here that the actual magnitude and pace of cyber disputes among rivals does not match with popular perception; 20 of 126 active rivals engaged in cyber conflict. The interactions that are uncovered are limited in terms of magnitude and frequency suggesting cyber restraint. Further, most of the cyber disputes that are uncovered are regional in tone, defying the unbounded nature of cyberpower. The coming era of cyber conflict may continue to exhibit these patterns despite fears mentioned in the discourse by the media and cyber security professionals.

Keywords

cyber conflict, regionalism, restraint, rivalry

Introduction

In 2011, the United States government declared a cyber attack similar to an act of war, punishable with conventional military means as a form of last resort (Department of Defense, 2011). Cyber engagements directed by one state against another are now considered part of the normal relations range of combat and conflict. The goal of this research is to examine these processes, determine which rival states have been using cyber tactics and where these attacks are directed, and gather information about the severity of the conflicts. What can we learn by examining the cyber relations of rivals and what theories explain international cyber behavior? In particular, we question the reality of this threat. Is it actual or inflated?

Cyber security is clearly an important and pressing question for national security actors. Akin to the shift in strategic operations after 2001 due to terrorism, the rising fear of cyber combat and threats has brought about a reorientation of military affairs (Nye, 2011a). The Department of Defense notes ‘small scale technologies can have an impact disproportionate to their size; potential adversaries do not have to build expensive weapons systems to pose a significant threat to U.S. national security’ (Department of Defense, 2011). This dialogue only suggests that combat is changing and our institutions must rise to meet the challenge. The discourse is that asymmetric combat is real and likely to be realized through cyber conflict. To counter this threat, actors

Corresponding author:
drbvaler@gmail.com

across the globe are promoting a variety of new military organizations and institutions to deal with it.

While it is clear that terrorism is an important concern in terms of scale of operations, locations, and impact, it is less clear whether cyber combat has and will exhibit the same trends. The danger lies in focusing too much on fear of the attack rather than concentrating efforts against actual and demonstrated threats. Preliminary qualitative analysis suggests that, while there is evidence for a plethora of cyber disputes among post-Soviet states, they rarely take the form of serious disruptions to the state of national security (Valeriano & Maness, 2012). In reality, it seems that cyber conflict mimics the dynamics of espionage or economic combat and is not a form of war at all, as zero deaths result from the actions (Rid, 2011).

Here we quantify the number of cyber disputes and incidents experienced by international states in the realm of foreign policy, particularly historical antagonists. We examine the scope, length, and damage inflicted by cyber operations among rival states (Klein, Goertz & Diehl, 2006) from 2001 to 2011 because cyber operations have been added to the arsenal of rival interactions. Our data demonstrate that 20 rival dyads out of 126 engaged in cyber conflict during this period. The average number of cyber incidents among rivals who participate in such behavior is three incidents. The US–Chinese dyad experiences by far the most cyber conflict with 22 observed cyber incidents within five overall cyber disputes. We hope that this research can return the debate on cyber conflict to a more nuanced examination of the threat. Others should be able to use our data to come to their own conclusions. While there is a real danger of cyber combat, one must remain prudent in relation to the actual threat, not the inflated threat presented by the imagination.

What is cyber conflict?

We now live in a digital era in which the speed, interconnectedness, and level of interaction between states and individuals is growing at an exponential rate. This reality brings fear, as the infrastructure we depend on is fragile. Since we depend so much on digital communications, it stands to reason that we are also vulnerable to threats that originate from this realm. The question is to what extent are these fears warranted? How vulnerable is any given country to cyber conflict and what evidence do we have for cyber incidents in the last decade?

First, it is important that we define our terms as they apply to international relations research. Cyberspace has physical elements since it has defined boundaries of mainframes, wires, hard drives, and networks. Therefore, the battlefield where cyber conflict is waged is defined along certain boundaries. Cyberspace is not some abstract concept that has unknowable limits or boundaries; it is divided between the physical layer and syntactic layer (Libicki, 2007). As our ability to store information increases and the speed at which information travels expands, the domains of cyberspace increase.

Nye (2011a: 21) defines cyber warfare as 'hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence'. Many others mirror the same thoughts in their definitions, such as Hersh (2010) who defines cyberwar as the 'penetration of foreign networks for the purpose of disrupting or dismantling those networks, and making them inoperable'. Our concern is that in order to define cyber conflict in the international relations realm, we must understand who uses the tactic, where, how, and for what ends. The Nye definition focuses on violence and leaves out the method of attack. The Hersh definition focuses solely on the dismantling of networks. We therefore 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 short of war and away from the battlefield.[1] We are engaging cyber conflict as an aggressive foreign policy tactic in a developing domain that can also impact other arenas.

There are three areas of cyber conflict, as suggested by Nye (2011b): governments, organizations, and individuals. Government cyber operations cover cyber conflict between government actors and foreign policy decisionmakers. Organizational cyber conflict would typically involve organized non-state actors such as terrorist networks, or hacker groups such as Anonymous. Individual-based cyber conflict would cover rogue actions by lone operators functioning to cause crime, chaos, or general malice.

Going further, cyber security is the term used for a state's defensive (also offensive) capabilities in cyberspace. If a country is able to shut off the internet and the flow of information from coming in or out of its borders, that state is said to have strong cyber defenses (Clarke & Knake, 2010). China, Syria, and Egypt are examples of states with these capabilities. The United States is thought to have great offensive capabilities, which can

[1] We have discarded the use of the term 'cyberwar' where possible because we agree with Rid (2011) that cyberwar is not about actual war where deaths result.

serve as a good defense, as cyber initiators may think twice before attacking the USA for fear of a more severe retaliation. These capabilities must be kept in mind when looking at rivals, as it would be assumed that if a state is endowed with the ability to infiltrate its adversary in cyberspace, it will do so.

It is important to outline which types of cyber strategies are used and the amount of damage they potentially can inflict on international actors. We find the term 'cyber attack' to be misguiding and inappropriate in that it conflates the tactic to sound something akin to a conventional military attack, or that it could conceivably include any sort of probe. We prefer the terms 'cyber incidents' and 'cyber disputes' to the more popular term. Cyber incidents are individual operations launched against a state. Cyber disputes are specific campaigns between two states using cyber tactics during a particular time period and can contain one to several incidents, often including an initial engagement and responses.

To this point, studies about the impact of cyber technologies on foreign relations are purely speculative or based on one or two case studies; no one has yet examined the shape and consequences of cyber operations. As Lynch (2010: 98) puts it, 'a dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States' global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target'. Quotes like these can be problematic in that policy is being suggested without evidence. Rather than suggesting that the nature of combat has changed, we are interested in measuring if, how, and why it has changed.

Cyber disputes in the international system could potentially destroy command and control structures of the military and foreign policy apparatus, wipe out the media communications of a state, destroy financial memory, and wage economic combat; however, all these impacts are purely speculative. The fear that these technologies engender is probably more important than any conjecture a pundit can make. To understand the nature of the threat we must first understand how and where it has been used in the past to grasp its potential impact in the future.

Very few scholars have sought to systematically analyze the evolution of cyber conflict, which is odd since the issue has been in the discourse since Arquilla & Ronfeldt (1993) first examined the topic. Clarke & Knake (2010: xi) suggest the prospect of highly volatile crises increases under the tactic given the speed at which attacks can occur. Choucri (2012) uses a model, based on a configuration of variables, that includes population, resources, and technology that will push states to expand beyond their boundaries. Her work suggests there needs to be a proper configuration in place to propel states towards cyberwar, yet it is unclear what exactly that would be at this point. Others such as Liff (2013) have made strides by discussing the growing frequency and intensity of cyber conflict. Guitton's (2013) perspective is closest to ours in that he notes that European cyber policy tends to be based on threats that have yet to materialize.

Since most military networks are decentralized, offline, or have 'air gaps', the installation and implementation of effective intrusions or infiltrations is a difficult proposition. For example, the Stuxnet worm that hit the Iranian nuclear program had to be planted from the inside with traditional intelligence operatives or through a victimized Iranian employee due to this 'air gap' (Sanger, 2012: 193–196). In terms of conflict operations, the attractiveness of the target in relation to the capability used is a critical equation rarely examined.

Restraint exists in the realm of cyber conflict; some have begun to make this point in various forums. Rid (2011, 2013) argues that cyberwar, in the extreme sense that death will result, has not yet occurred and is unlikely to occur. Likewise, Gartzke (2013) develops the logic for cyberwar being utilized by states as a low-level form of conflict. We contend that cyber conflict is literally the least harmful tactic and easiest option for a state during conflict. Cyber interactions will take a regional tone in that rivals typically are constricted to regional interactions. Next we will further outline our theory of cyber restraint and regionalism as we then move to the empirical study of cyber conflict.

Cyber conflict during rivalry

The benefits of examining the rivalry population rather than interactions between all states are clear and logical. Why focus on all possible dyads when we have exhaustive data on those states most likely to engage in crises, escalated conflicts, and wars (Diehl & Goertz, 2000)? By examining the rivalry population, we should be able to focus on the antagonists experiencing the most as well as the most obvious forms of cyber conflict. Yet, we also allow for the flexibility of adding what might be called cyber rivals who have not exhibited the normal levels of conventional conflict required to be classified as rivals.

The concept of rivalry brings history and patterns of interactions back into the study of political science. To understand why wars or crises develop, one must look at the history of interactions at the military, diplomatic, social, and cultural levels (Valeriano, 2013). Rivalry is defined as longstanding conflict with a persistent enemy (Diehl & Goertz, 2000). It would therefore make sense that cyber conflict would be added to the arsenal of rival interactions and should be investigated under this context.

The next important consideration for rivalry is relative gains or losses. The issue positions of the states engaged in a rivalry are made in relation to the attitude of the other side (Vasquez, 1993). Rivals are in some ways addicted to perpetual conflict because of their singular outlook of targeting the enemy. This spiraling competitive relationship can be a dangerous situation in international affairs due to the buildup of hatreds and tensions over time.

As most rivalry scholars note, there must be some degree of competitiveness, connection between issues, perception of the other as an enemy, and longstanding animosity for a pair of states to be called rivals (Diehl & Goertz, 2000; Thompson, 2001). Cyber operations are a tactic used to gain an advantage either diplomatically or militarily against a target. During a rivalry one would think all options should be on the table, and war and cyber conflict then become viable foreign policy options. It is in this context that the attribution problem in cyber security is minimized because rivals are obvious targets for cyber activity. Scholarship grounded in deterrence theory is where we develop our argument about why cyber conflict is relatively absent among rivals.[2]

Restraint plays a critical role in the cyber realm. Derived from Schelling's analysis that military strength can be used as coercion, deterrence theory heavily influenced post-atomic foreign policy (Schelling, 1966). Instead of risking engagement in direct conflict, great powers developed nuclear arsenals to prevent attack from other states. Jervis (1979, 1989) explains this buildup for deterrence as an extension of diplomacy, where expressions of force are communicated between sides to deter moves rather than using overt force. States are effectively trying to avoid a conflict spiral and a never-ending situation of continuous threats by making severe threats.

As was suggested long ago by Kahn (1960), there are two types of deterrence, immediate and extended. Extended deterrence refers to threats to third parties while immediate threats are related to the state in question. Our theory of restraint in cyber conflict relates back to this original conception of deterrence with modifications. Direct deterrence between two parties often fails. When states try to enhance their security position through threats, alliances, and military buildups, they often fail to provoke the reaction intended – concessions. In fact, they often provoke further conflict and extreme threats (Vasquez, 1993; Hensel & Diehl, 1994). Comprehensive restraint relates to deterrence from spectacular attacks such as nuclear weapons or devastating internet operations focused on power systems and health services. States are restrained from such action through fears of retaliation and escalation of the conflict beyond control.

Immediate deterrence has little relevance to our analysis because threats often invoke the process of the security dilemma, but aspects of comprehensive deterrence endure in our restraint framework. Extending this concept to cyber relations would suggest that restraint does not work at the low level of disputes such as distributed denial of service method (DDoS) incidents or simple vandalism, since there is little to restrain a state from acting at this level. More comprehensive measures, on the other hand, are off the table. It is unlikely that a state would be willing to attack and destroy a power network, social services facility, or government organization such as the Department of Defense due to the fear of retaliation. The dispute then makes little sense since the costs of engagement are potentially devastating and unlimited.

Low-level cyber tactics might be part of what Azar (1972) calls the normal relations range for a rivalry. The surprising finding could be that rivals will tolerate cyber combat operations if they do not cross a line. Cyber conflict is expected to occur and even tolerated, as long as total offensive operations are not conducted. By total offensive operations, we mean direct attacks which might lead to the destruction of the energy infrastructure of a state or infiltrations meant to take control of army units or facilities. These options are off the table for rivals since they will lead directly to war, collateral damage, and economic retaliation. As Nye (2011a) notes, the vulnerabilities evident on the internet make the tactic dangerous to use because a cyber tactic can be easily replicated and sent back to the attacker in kind.

The other factor contributing to restraint is collateral damage. States are now limited in offensive actions due to functional norms of limited harm against civilians. An example of this logic can be inferred from the 2003 US invasion of Iraq. In 2003, Bush Administration officials worried that the effects of cyber combat would not

[2] In the context of cyber conflict, we prefer the term 'restraint' rather than 'deterrence' because conditions of deterrence theory are usually not met in cyber conflict. In deterrence, a threat has to be made known and countered with an equally repressive reaction. This condition is typically not met in cyber security, making the condition of credibility moot in this arena.

be limited to Iraq, but would instead create worldwide financial havoc, spreading across the Middle East to Europe and perhaps to the United States (Markoff & Shanker, 2009). The United States was restrained from launching cyber operations against its rival during outright war, because of the potential fall-out of such operations through the complex networks of interdependence that would extend to civilians. This leads us to Hypotheses 1 and 2 in relation to cyber conflict.

> *H1:* Due to restraint dynamics, the observed rate and number of cyber operations between rivals is likely to be minimal.
>
> *H2:* When cyber operations and incidents do occur, they will be of minimal impact and severity due to restraint dynamics.

Due to the threat of retaliation, potential harm to civilians and the ready possibility of actual direct combat if cyber tactics are utilized at a high level of severity, cyber operations will be limited in the international sphere. We feel that a rate of one dispute per year would be average and more than one a year between rivals would be extreme. When cyber disputes are exhibited, offensive states will choose tactics that are easily hidden and free of direct responsibility. The damage done and intensity will be limited and mainly focused on low-level operations. These hypotheses are directly counter to popular wisdom on the pervasiveness of cyber combat.

In addition to the restraint limitations, we also hypothesize that cyber relations will take a regional tone. The most dangerous enemies will be local, countering the idea that cyber politics will be global, boundless, and unrestricted to conventional domains of kinetic conflict. Examples abound: Russia and Georgia, Pakistan and India, Israel and Iran. We should see the same dynamics at work for cyber rivals. While the suggestion is that cyber wars and conflict can now be inflicted in far-off locations, the reality is likely much different. Since there is restraint at work for cyber conflict, those dyads that do conduct full-scale cyber operations will likely be local rivals due to the salience and immediacy of the rivalry.

Further, states with aims of exerting influence in a particular region may also turn to cyber tactics. Low-level cyber operations constitute a relatively unimportant matter to other states. Small aggressions indicate states expanding their standing and power through these interactions. It is a form of control; states hoping to rise within a regional power hierarchy are likely to leverage any form of capability. States striving for regional strength in relation to their neighboring rivals, such as China, Israel, and India, are the likely cyber conflict culprits. Regional dynamics lead us to hypothesize that states will use cyber capabilities on neighbors rather than global rivals with few exceptions, as we will note.

> *H3:* Cyber incidents and disputes that do occur will likely be limited to regional interactions.

Methodology

The goal is to create a database of all cyber incidents and disputes between countries that is as complete as possible. The US government may have a ready archive of cyber threats and disputes, but this is not available to the public. Instead we rely on our own comprehensive and focused search of both news sources and cyber security reports.

The question remains: is our search comprehensive enough? If a cyber dispute is reported, it likely had enough impact to alter the dynamics of interstate relations. Some operations will be hidden because they point to a specific weakness, but eventually the truth comes out. Many cyber operations committed in the last decade are public knowledge. Generally a source will clue a reporter into the activity and it will be picked up by various media sources. Even Stuxnet and Flame were revealed to the media leading to calls for investigations on the nature of the leaks. Since security network officers are engaged in a practice of making the potential threat known, there is little interest in hiding cyber operations. In addition, the military structures throughout the world are interested in promoting the need to build infrastructure (the cyber industrial complex) to combat cyber actions; therefore they also have little incentive to hide cyber operations. Finally, internet security firms regularly release reports to demonstrate their ability to repel or combat cyber intrusions in order to gather clients. Corporations such as McAfee, Kaspersky, Norton, and Symantec have been very helpful in detailing cyber operations, but of course their information is viewed through a country- and corporation-specific lens.

In the end, it must also be remembered that all prognosticators in the cyber debate are working with limited and selective information. Instead of being deterred in this daunting task of data collection, we move forward, aware that our efforts represent only what is publicly known. We also instituted a lag time for reporting of events, stopping our data collection in 2011 in order to ensure extensive analysis of all incidents and disputes.[3]

[3] Lag times are necessary; for example, Stuxnet was likely initiated sometime in early 2009, started showing up in states' networks in June 2009, and was reported in the media by June 2010.

We note that an active and ongoing coding of cyber events would be unrealistic; time is needed to come to accurate conclusions as to what happens during cyber operations. We concede in advance that there may be possible important missed cyber disputes due to the secrecy of the event and tactic. This dataset is active and will be maintained with additions made as time goes on, but we are confident that at this point we have a quite exhaustive dataset.[4]

Attribution of cyber disputes can be a problematic issue. One of the advantages of a cyber dispute is deniability. In our dataset, states that use information warfare must be fairly explicit and evident. For some cases, attribution is easy; for example, India and Pakistan have been immersed in 'tit-for-tat' cyber incidents for some time and it is fairly clear that actions in this arena are state-sponsored. Likewise, Russia appears to have coordinated its dispute against Georgia and has not denied its part in this operation. If the attribution of a dispute is in serious doubt, we do not code it as a state-based action (Diebert, Rohozinski & Crete-Nishihata, 2012). Anonymous hackers and operatives either working on their own initiative or through off-books enterprises are not coded. We do not take conventional wisdom at its word for operations and instead analyze the history of relations, the intent of the tactic, and the likelihood of government complacency and code disputes from this perspective.

The terminology for our data on cyber operations is important to note. Scholarly and journalistic discourse thus far has had trouble distinguishing smaller, isolated cyber incidents from more extensive and long-term cyber campaigns launched by states. We attempt to bridge this gap and categorize cyber incidents into the larger cyber disputes. For individual cyber conflicts, we use the phrase 'cyber incident'. Incidents such as Shady Rat include thousands of intrusions, but accounting for every single intrusion the operation made is impossible and unwieldy. Therefore, Shady Rat and other multiple-intrusive incidents are coded as just one incident per dyad as long as the goals and perpetrators remain stable. Each cyber incident is directed by one state or on behalf of the state against another state or a state's national security apparatus.

For operations containing a number of incidents that are part of an overall cyber campaign we use the term 'cyber disputes'. For example, incidents such as GhostNet, Shady Rat, the Pentagon Raid, and the F-35 jet plan theft initiated by China against the United States and the US responses of Buckshot Yankee and Cisco Raider are all part of one sustained cyber dispute between the two rivals. Cyber disputes may contain only one incident or dozens. Furthermore, the initiator of the dispute or incident must be from a government or government affiliates in order for an operation to be included in our dataset. Targets may be non-state if they are important to a state's national security. Lockheed Martin, Mitsubishi, large banks, and Boeing are examples of non-state targets relevant to the national security of a state.

To find the relevant news stories and analysis of cyber incidents and disputes between rivals, we enter the search query 'rival A' (e.g. Iran) AND 'rival B' (e.g. Israel) AND 'cyber' OR 'internet attack' OR 'infrastructure attack' OR 'government attack'. The capitalization of the conjunctions is required in the *Google News* search query. What we look for in this search is the date and duration of the incident, who initiated the incident, the foreign policy objective of the initiator (disruption, theft, change the target state's behavior), whether or not a third party was involved in the incident, whether or not there was an official government statement by the initiator about the incident (denial or acceptance), and the method and severity of the incident (see Tables I–IV for more detail). The time period is from 1 January 2001 to 31 December 2011 so that we could get an 11-year sample and also capture the main period of active internet engagement. In most cases sources were corroborated by multiple newspaper articles, blogs, and reports (coming from both think tanks and internet security firms), controlling for source validity and to avoid letting one perspective dictate a data point. Each news story, report, or post utilized is carefully examined to ensure that the proper coding has taken place. Explanations of type and severity of incidents and disputes for our data analysis are explained in Tables I and II.

Before we move forward with our analysis, we must also define and describe the types of cyber weapons available to states. Few understand the internet and even fewer understand the nature of cyber weapons. What tools do states have at their disposal that can do harm to their rivals? Cyber weapons are 'computer codes that are used or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings' (Rid & McBurney, 2012: 6).

[4] It could also be of note that our dataset is biased towards the West since the assumption of media, firm, and institutional openness is a Western assumption. Where possible, we translated foreign language sources either by hand or by machine.

Table I. Cyber methods for incidents and disputes

Type of dispute	*Examples*	*Explanation*
1 Vandalism	Website defacements	SQL injection or cross-scripting to deface websites
2 Denial of service	DDoS, distributed denial of service	Botnets used to effectively shut down websites with high traffic
3 Intrusion	Trapdoors or Trojans, backdoors	Remotely injected software for intrusions and thefts
4 Infiltrations	Logic bombs, worms, viruses, packet sniffers, keystroke logging	Different methods are used to penetrate target networks. Can be remotely used or physically installed
5 APTs	Advanced persistent threats	Precise methods that have specific targets. Move slowly to avoid detection, can be vandalism, DDoS, intrusions, or infiltrations
6 Vandalism and denial of service	Cyber disputes	Combined incidents of vandalism and DDoS
7 Intrusions and infiltrations	Cyber disputes	Combined incidents of intrusions and infiltrations

Table II. Severity scale of cyber operations

Severity type of incident	*Explanation*	*Examples*
Type 1	Minimal damage	State Department website down, probing intrusions
Type 2	Targeted attack on critical infrastructure or military	Financial sector attack, DoD hacked
Type 3	Dramatic effect on a country's specific strategy	Stuxnet, jet plans stolen
Type 4	Dramatic effect on a country	Power grid knocked out, stock market collapse
Type 5	Escalated dramatic effect on a country	Catastrophic effects on country as a direct result of cyber operation

Cyber weapons

Weapons are as Rid (2013: 36) notes, 'instruments of harm'. Cyber weapons obviously vary by type, distinction, usage, and application. We delineate four basic methods (weapons) that cyber conflict initiators have at their disposal. The methods of cyber incidents and disputes we code are comprehensive according to cyber combat tactics and analysis.

Website defacements or vandalism. We begin with the simplest form of cyber weaponry – website defacements or vandalism. Hackers use SQL injection (structured query language) or cross-site scripting (forms of injected code) to deface or destroy victims' web pages (Clarke & Knake, 2010). This form of malice takes over the site for a few hours or days and displays text or pictures that demeans or offends the victim site. The loss of control of a government webpage may be a relatively harmless occurrence, yet the effect of this action on the population can be multiplicative. Generally, these types of attacks have a propaganda element. They also are a form of control, suggesting to the target they lack the capability to control their cyberspace operations.

Table III. Coding for cyber incidents

Interaction type
1 Nuisance (probing, disruption, chaos)
2 Defensive operation (Cisco Raider, Buckshot Yankee)
3 Offensive strike (Ghost Net, Stuxnet)
Target type
1 Private/non-state but important to national security (financial sector, power grid)
2 Government non-military (State Department, government websites)
3 Government military (Department of Defense, Cyber Command)

Distributed denial of service method (DDoS). Next on the list (more sophisticated, but arguably not more severe than vandalism) is the distributed denial of service method (DDoS). These operations flood particular internet sites, servers, or routers with more requests for data than the site can respond to or process (Reveron, 2012). This method effectively shuts down the site thereby preventing access or usage. Government sites important to the functioning of governance are therefore disrupted until the

Table IV. Coding for cyber disputes

Interaction type	
1	Nuisance
2	Defensive operation
3	Offensive strike
4	Nuisance and defensive
5	Nuisance and offensive
6	Defensive and offensive
7	Nuisance, defensive, and offensive
Target type	
1	Private/non-state
2	Government non-military
3	Government military
4	Private and government non-military
5	Private and government military
6	Government non-military and military
7	Private, government non-military, and military
Objectives for initiators	
1	Disruption (take down websites, disrupt online activities)
2	Theft (steal information)
3	Change in behavior (abandon nuclear program, withdraw troops)

flooding is stopped or the hackers disperse. Such attacks are coordinated through 'botnets', or more colorfully, 'zombies', a network of computers that have been forced (or willingly joined, on rare occasions) to operate on the commands of remote users (Clarke & Knake, 2010).

Intrusions. Intrusions, which include Trojans and trapdoors or backdoors, are the third-level of methods used in cyber conflict. These are more targeted and thus can be more severe than defacements and vandalism in regards of longer-term damage. Trapdoors or Trojans are unauthorized software added to a program to allow entry into a victim's network or software program to permit future access to a site once it has been initially attacked (Reveron, 2012). Intrusions need to be added to software, can remain dormant for a long time, and then propagate themselves without notice (Clarke & Knake, 2010).These methods are difficult to detect or repel with firewalls or security software as they are not malicious upon entry into a network. They only become malicious once they become operational.

The purpose of trapdoors (or backdoors) is to steal sensitive information from secured sites. These methods can have destructive effects on a state's national interests. The major difference between Trojans and trapdoors is that trapdoors do not need a human hacker to begin the implementation process, while Trojans do. Trapdoors can be given a pre-dated command as to when to activate without the need for a human being to activate their damaging potential. A recent example of a trapdoor method is the vulnerable chips found in Boeing's 787 onboard computers in 2012.

Infiltrations. Along with some methods of intrusions, infiltrations are the method states can consider an act of war as the US Department of Defense (2011) has declared. Infiltrations and intrusions are not scalar in regards to which one is more severe, but they are generally more sophisticated, more targeted, and thus more severe than defacements or denial of service weapons.[5] Infiltrations are different from intrusions in that different methods are used to penetrate target networks. There are five major methods of infiltrations: logic bombs, viruses, worms, packet sniffers, and keystroke logging (Clarke & Knake, 2010). These five methods are precision attacks that go after specific data or force computers or networks to undertake tasks that they would normally not undertake.

There are five types of infiltrations: (a) logic bombs are programs that cause a system or network to shut down and/or erase all data within that system or network; (b) viruses are programs which need help by a hacker to propagate and can be attached to existing programs in a network or as stand-alone programs. They generally replicate themselves with the intention of corrupting or modifying files; (c) worms are essentially the same as viruses, except they have the ability to propagate themselves; (d) packet sniffers are software designed to capture information flowing across the web; (e) 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 & Knake, 2010: ch. 3).

Advanced persistent threats (APTs) add another layer to the scope of cyber methods and can come in any of the four methods discussed above (Sanger, 2012). Examples of APTs are the Stuxnet worm, the Flame virus, and the Shady Rat infiltrations. According to the cyber security firm Symantec, APTs are different from traditional targeted methods in that they are customized, they move more slowly to avoid detection, their intentions usually are more malicious and advanced and almost certainly come from states, and

[5] It is important to note that this typology is not necessarily an ascending scale, as some Trojans can be more potent than worms.

their targets are much more specific.[6] The level of sophistication is unmatched; there are highly covert and intentional actions behind the operations.

The analysis is confined to rivals because these are the most disputatious members of the international system. Non-state actors are only included in this analysis if they are considered part of a state's national security apparatus, or if the initiators are clearly acting on behalf of their home government.[7] We code these targets as follows: a 1 is coded if the target is non-state, 2 if the target is government but non-military, and 3 if the target is government and military. We also code what we call the objective of the initiator into three broad categories: a 1 is coded if the objective is basic disruption of a state's day-to-day activities; 2 if the objective is to steal sensitive information, plans, or secrets from the target state; and 3 if the initiator is attempting to alter the state's behavior. An example of the latter objective is the USA–Israel cyber dispute with Iran, as the overall objective of this operation is to deter Iran from continuing its nuclear program. This objective is found to be scarce in our data, which indicates that cyber tactics are usually only used to steal or cause minor disruptions on an enemy. Codes for multiple targets or multiple objectives in cyber disputes are presented in Table IV. Cyber activity in the realm of crime, economic sabotage, and general chaos by such groups as Anonymous are beyond the scope of this analysis. We focus on rivals based on spatial consistency (same actors), duration, militarized nature of competition, and linked issues (Klein, Goertz & Diehl, 2006: 335), or by perception (Thompson, 2001).[8] There are 126 active and ongoing dyadic interstate rivals from 2001 to 2011.[9]

Data analysis

The final summary of our data is reported in Table V. Here we list who uses cyber tactics against whom, the number of cyber incidents and cyber disputes a state has been involved in, the highest severity type of a dispute, the highest method used by the state, the highest target type the state has used, and the highest objective of the initiating state. Our list is a serious attempt to represent all publicly acknowledged cyber incidents and disputes between rival states for the years 2001 through 2011.[10]

The most immediate point that can be made about these results is that very few states actually fight cyber battles. This is surprising considering these states are active rivals who have public military disputes with one another often. Perhaps the tactic is under-utilized at this point.

We expect to find a minimal number of incidents and disputes, defined as one incident/dispute per year for each rivalry dyad and we have found even less evidence of cyber methods than this. Our analysis demonstrates that only three dyads experience more than ten incidents and only three dyads experience more than five disputes during the 11-year time frame, suggesting the rate of cyber conflict is low for the total 126 rivalry dyads in our sample. Only 14 (13%) of the 110 recorded incidents get a severity score of 3.

Table VI lists the frequent offenders of cyber combat.[11] The USA and China are at the far end of the scale with several cyber rivalry dyads (six for China, five for the USA) while the other states have few consistent dyadic cyber interactions.[12] The United States and China also

[6] See http://www.symantec.com/threatreport/topic.jsp?aid=industrial_espionage&id=malicious_code_trends.

[7] The attacks originating from Russia were in reaction to decisions made by the governments of Estonia and Georgia, but what remains fuzzy is whether or not the Russian government had direct involvement in the disputes. Diebert, Rohozinski & Crete-Nishihata (2012) argue that the cyber disputes were not government sanctioned while Korns & Kastenberg (2009) take the opposing view and find that the attacks were in tandem with the Russian government's military operations in Georgia.

[8] The cases of Iran and Israel plus India and China were added from the Thompson (2001) data. Estonia and Russia were added due to the notoriety of the case.

[9] Our coding was checked for reliability after the initial data collection effort. The first three coders then switched areas of coverage and checked 10% of another person's coding efforts. Finally, two undergraduate students were given the same information and asked to check 10% of the dataset at random for reliability.

[10] Notable cyber interactions not included in the analysis – Cuckoo's Egg (1988), Morris Worm (1989), the Dutch Hackers incident during Desert Storm (1990), Eligible Receiver (1997), Solar Sunrise (1998), Russian Patriot Hacking, such as during NATO's operation Allied Force (1999), Chinese Patriot Hacking, such as after the NATO bombing of the Chinese Embassy in Belgrade (1999), Moonlight Maze (1999) – because they all took place before the time frame of our analysis.

[11] It is frequently noted that the most prominent cyber actors might also correlate with internet penetration in society. We find the opposite and that there is no correlation between internet usage and cyber offensive actions. Space precludes our inclusion of this table but we find that many of the least active internet societies also tend to use cyber operations. This may be because these states have little to fear in terms of retribution.

[12] Many Chinese cyber disputes, such as Shady Rat and the Byzantine Series, hit multiple targets and not only the United States. However, since we are only focused on rival dyads, the USA–China dyad is the focus of these sophisticated Chinese operations.

Table V. Summary of cyber conflict among rival states (2001–11)

Rival A (number initiated)	*Rival B (number initiated)*	*Cyber incidents*	*Cyber disputes*	*Most severe dispute*	*Highest method type*	*Highest objective*	*Highest target type*
China (20)	USA (2)	22	5	3	6	2	7
Pakistan (7)	India (6)	13	3	3	4	2	3
North Korea (10)	South Korea (1)	11	3	2	6	1	6
Israel (7)	Iran (4)	11	2	3	6	3	5
China (7)	Japan (0)	7	7	3	4	2	3
South Korea (4)	Japan (3)	7	5	2	3	2	4
USA (6)	Iran (1)	7	2	3	6	3	5
China (5)	Taiwan (0)	5	2	2	3	2	2
China (4)	India (0)	4	1	3	6	2	6
Russia (3)	Georgia (1)	4	1	1	5	3	4
Russia (4)	Estonia (0)	4	1	2	2	1	2
Russia (3)	USA (0)	3	3	3	4	1	3
North Korea (3)	USA (0)	3	1	1	5	1	2
China (2)	Vietnam (0)	2	2	2	4	2	2
Lebanon (1)	Israel (1)	2	1	1	4	1	2
North Korea (1)	Japan (0)	1	1	1	2	1	2
India (1)	Bangladesh (0)	1	1	1	3	3	2
Syria (1)	USA (0)	1	1	1	1	1	2
Kuwait (1)	Iraq (0)	1	1	2	4	1	2
China (1)	Philippines (0)	1	1	2	3	2	2

Totals: 110 cyber incidents, 45 cyber disputes
13 Enduring, 4 Proto, 3 Strategic Rivals engage in cyber disputes
Averages: Cyber incident severity: 1.62; Cyber dispute severity: 1.71 (out of 5)
20 out of 126 rival dyads (15.9%) engage in cyber disputes

Table VI. Top ten states by number of rival cyber dyads

State	*Number of cyber dyads*	*Total cyber incidents*	*Total cyber disputes*
China	6	40	29
United States	5	35	12
India	3	18	5
Japan	3	15	13
North Korea	3	15	5
Russia	3	11	5
South Korea	2	18	8
Iran	2	18	4
Israel	2	12	4
Pakistan	1	13	3

have been engaged in 53 cyber incidents and 25 cyber disputes during the duration of our dataset examination. Many of these attacks are with each other, with China being the initiator most of the time.

It is important to note that the burden for all these events often falls on the defender. If the Pentagon's research partners are going to be targeted, these highly sensitive plans should not be located in accessible internet locations in the first place. It is likely that the incident or dispute was not a simple intrusion, but rather a phishing attempt that was surprisingly successful.[13] Stuxnet, while devastating, was conducted by a conventional infiltration of Iranian systems by a spy or unwilling accomplice. These failures should not be blamed on the tactic.

Regionalism appears to play a role in cyber conflict. Figure 1 maps cyber incidents in the Middle East. Blast radii mark the location of the incident, while the lines go back to the initiating state. The vast majority of cyber incidents occur in regional rivalries. Israel and Iran's cyber conflicts continue their push for regional dominance. The only exceptions to cyber conflict's regional tendency in the Middle East include the United States, which has a vested military and economic interest in the same region as all non-regional cyber rivalry dyads. The United States is the global hegemon and is also one of the most 'plugged-in' of all states, making it an attractive target to cyber initiators. In the cyber world, the United States and China represent outliers in their behavior.

[13] Phishing attempts are when hackers use personal pieces of information to acquire and ask for passwords by simple email or other social media interactions.

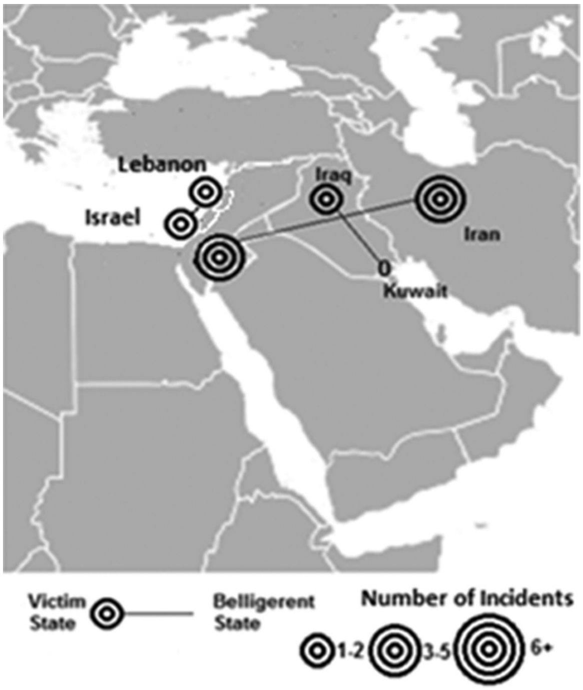

Figure 1. Cyber incidents in the Middle East

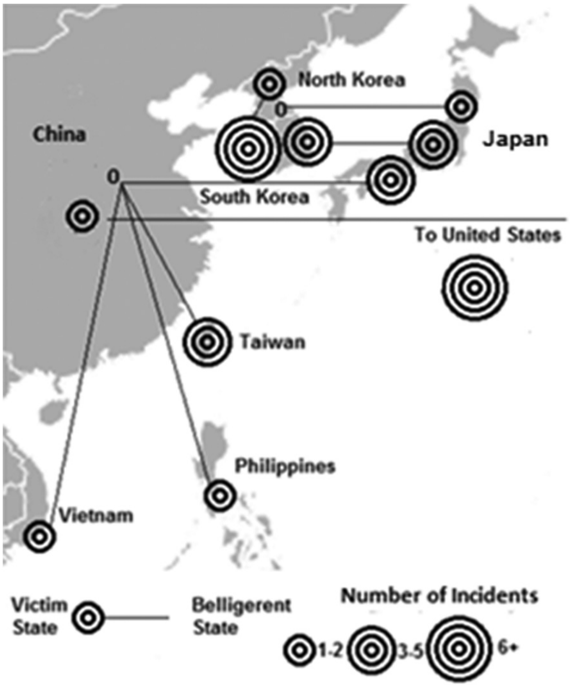

Figure 2. Cyber incidents in East Asia

Hypothesis 3 could be modified to state that minor powers will operate at the regional level, but major powers operate at the global level. The danger is clearly that these operations will shape international norms and make cyber operations permissible.

Cyber conflict also tends to exist in dyads with a major regional power, such as China, Israel, and India. Figure 2 maps cyber incidents in East Asia. China frequently infiltrates its neighbors, including unidirectional cyber tactics on Philippines, Vietnam, and Taiwan. The triad of North Korea, South Korea, and Japan show a continued conflict online. The states engaging in cyber conflict expand their power in non-traditional theaters. The tactics are enough to get rivals' attention, but do not create enough havoc to warrant a militarized response.

Southern Asia provides another theater for cyber conflict. Figure 3 maps Southern Asian cyber conflict. The India–Pakistan dyad features continued cyber conflict with both sides perpetrating defacements. India also exerts its cyber strength on neighboring Bangladesh without response. One-way incidents like this (and from China above) suggest a fear of retaliation or lack of capabilities from the target states.

Although we find strong support for regionalism in this analysis, we cannot overlook the most active cyber dyad in the system that has global implications: the United States and China. The United States and China have been embroiled in 22 cyber incidents within five overall cyber disputes since 2001. China has infiltrated US cyberspace 20 of these 22 times, showing evidence for US restraint from retaliation in what could be interpreted as a gross intrusion upon US sovereignty. The main overall tactic for China when hacking into US mainframes is to steal sensitive or secret information. This alludes to China merely engaging in one of the oldest professions in the world on a new playing field: spying. The recent Mandiant report may have opened a new Pandora's Box in terms of US engagement with China in cyberspace, but the response to this has yet to be observed, at least in the public forum.

Assessment

Even considering our past investigators and theory, we were surprised to find little actual evidence of cyber conflict in the modern era. Why then are there so few rivals engaging in cyber warfare? Furthermore, why are the incidents and disputes limited to mostly defacements or denial of service when it seems that cyber capabilities could inflict more damage to their adversaries?

Based on our analysis, we find our notion of restraint is a better explanation of cyber interactions than any conception of continuous or escalating cyber conflict. States will not risk war with their cyber capabilities because there are clear consequences to any use of these

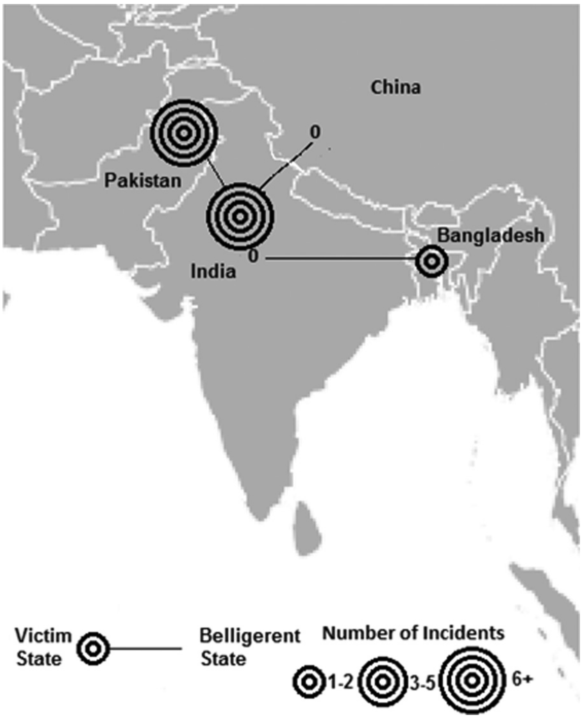

Figure 3. Cyber incidents in South Asia

technologies. States are not reckless, but terrorists and other cyber activists might not be so restrained. The interesting result of the process is that while cyber terrorists will likely proliferate, their ability to do damage will be limited due to the massive resources and conventional intelligence methods needed to make an operation like Stuxnet successful.[14] Stuxnet and Flame could be the harbingers of the future, but in reality it was a collusion of discrete events that worked out for the attacker (Lindsay, 2013). With a will to attack, there must also come a way to attack. With such a high burden on luck and ability, it will be rare to see such important disputes continue in the future.

The recently discovered cyber incidents of Red October and Flame represent the typical outcome of cyber conflict.[15] They are massive cyber operations, but have to date been used for information extraction and espionage purposes. Cyber conflict is in our future, but these events will only be as devastating as the target allows them to be as long as the attacker is restrained by logic, norms, and fear of retaliation. Restraint is clearly in operation for cyber conflict. Constraints can change the behavior of an actor into not doing something it would usually do if left to its own devices. A rival will not blatantly attack its adversary's infrastructure or secret government databases because that state may perceive the attack as it would a physical attack and respond with an equally devastating cyber incident or even with conventional military forces. There is also the fear of collateral damage which remains high for many actors, and this simple limitation may prevent persistent cyber conflict from becoming a reality. Another fear is cyber blowback, as noted by Farwell & Rohozinski (2011), in that tactics could be replicated and targeted back towards the attacker.

The range of relations in the realm of cyberspace has yet to be determined, but it does seem clear that rivals operate as rivals should. They are able to manage their tensions in such a way as to forestall violence yet prolong tensions for long periods of time. Therefore, states have yet to employ widespread damage via cyberspace out of fear of the unknown. They fear the escalation of the rivalry in the absence of a critical event like a territorial invasion. Malicious and damaging cyber tactics seem not to be the norm. The best hope for reducing the possibility of cyber conflict in the future comes from strong institutions capable of managing and restricting cyber-based disputes.

Cyber disputes may not have that ability to spread fear that a conventional, physical attack may demonstrate. Therefore, in order for rivals to win diplomatic and military engagements, an airstrike, naval blockade, or all-out invasion may get the desired outcomes that rivals are looking for instead of a botnet that shuts down the State Department for a day or prevents an ATM from dispensing money for 48 hours. Cyber conflicts, although potentially lethal, do not have the same 'punch' as a physical attack. Future work will explore many topics such as third-party or proxy cyber conflict, the impact of cyber incidents and disputes on conflict and cooperation levels, and the proliferation of cyber norms. For now we have taken a big step forward in returning the debate on cyber tactics to some measure of reality.

Conclusions

We do not doubt that cyber incidents and disputes will increase in the future and will demonstrate a real national security threat to the state. The question we pose asks how serious the threat is. Is it something we should use to promote a reorientation of security strategies? The

[14] As Rid & McBurney (2012: 6) note, cyber weapons may require specific target intelligence and major investments of R&D. Therefore these major operations are likely beyond most (but not all) terrorist organizations.

[15] At this point we have not coded Red October since it is unclear who perpetrated the attack.

purpose of this analysis is to analyze, as best we can, what has already happened and construct realistic future expectations from our findings.

Many governments continue to debate what is commonly known as the 'kill switch' legislation or other sorts of internet restrictions in the name of cyber security. The purpose of these proposed types of laws would give the state the power to shut down the internet in the event of a severe cyber dispute. These types of choices could be detrimental to commerce, privacy, and personal freedom. What is more constructive, we believe, is to create an international institution that mitigates conflict in cyberspace and sets up certain 'cyber norms' of behavior. Energies could be then diverted to stopping cyber threats from terrorists and other non-state actors.

While states should remain vigilant and protective of their interests, there is a point when actions taken in protection of the state actually damage the state. The reduction in commerce, educational and collaborative exchanges, and knowledge is not worth the gains seen through excessive cyber protection strategies. As Mueller (2006: 2) notes in relation to terrorism, 'this process has then led to wasteful, even self-parodic expenditures and policy overreactions, ones that not only very often do more harm and cost more money than anything the terrorists have accomplished, but play into their hands'.

In the end, a state can only steal what its target allows to be stolen in the cyber world. Cyber crime is not persuasive in its ability to control weapons systems, technologies, and research unless the target allows for this unrestricted access across networks. Vigilance is important, but not to the point of the creation of cyber commands and talk of an internet kill switch.

The data we have presented here illustrate that cyber disputes are rare. When they do happen, the impact tends to be minimal. In this analysis, 20 of 126 possible ongoing rivals engage in cyber combat. Of these rival interactions, most fall at the lower end in terms of quantity. In terms of quality, there are very few severe incidents and disputes according to our classification system. While the future may display a period of unrestricted cyber conflict, it is clear that this idea is not the reality; yet.

Interested parties in the future should remain vigilant and monitor actual cyber conflict. Moderation is called for, but this can only be done with real evidence to reduce fears profiteers will place on the cyber world. The future is bright for cyber relations, but only if we allow natural connections to be made to speed the process of globalization and interconnectedness rather than inward-thinking defensive reactions to technological developments.

Replication data

The dataset, codebook, and do-files for the empirical analysis in this article can be found at http://www.prio.no/jpr/datasets and at www.brandonvaleriano.com.

Acknowledgements

We thank James Fielder, Heather Roff-Perkins, Christopher Carmen, and Simon Pratt for comments on the project and thank Sam Bassett and Hugh Vondracek for data collection assistance.

Funding

This research was supported by a grant from the Carnegie Scottish Trust.

References

Arquilla, John & David Ronfeldt (1993) Cyberwar is coming! *Comparative Strategy* 12(2): 141–165.

Azar, Edward E (1972) Conflict escalation and conflict reduction in an international crisis: Suez 1956. *Journal of Conflict Resolution* 16(2): 183–201.

Choucri, Nazli (2012) *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press.

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

Department of Defense (2011) Department of Defense strategy for operating in cyberspace. Report, July (http://www.defense.gov/news/d20110714cyber.pdf).

Diebert, Ronald J; Rafal Rohozinski & Masashi Crete-Nishihata (2012) Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue* 43(1): 3–24.

Diehl, Paul & Gary Goertz (2000) *War and Peace in International Rivalry*. Ann Arbor, MI: University of Michigan Press.

Farwell, James P & Rafal Rohozinski (2011) Stuxnet and the future of cyber war. *Survival* 53(1): 23–40.

Gartzke, Erik (2013) The myth of cyberwar: Bringing war on the internet back down to earth. *International Security* 38(2): 41–73.

Guitton, Clement (2013) Cyber insecurity as a national threat: Overreaction from Germany, France, and the UK? *European Security* 22(1): 21–35.

Hensel, Paul R & Paul F Diehl (1994) It takes two to tango: Nonmilitarized response in interstate disputes. *Journal of Conflict Resolution* 38(3): 479–506.

Hersh, Seymour (2010) The online threat: Should we be worried about cyber war? *New Yorker*, 1 November.

Jervis, Robert (1979) Deterrence theory revisited. *World Politics* 31(2): 289–324.

Jervis, Robert (1989) *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*. Ithaca, NY: Cornell University Press.

Kahn, Herman (1960) *On Thermonuclear War*. Princeton, NJ: Princeton University Press.

Klein, James P; Gary Goertz & Paul F Diehl (2006) The new rivalry dataset: Procedures and patterns. *Journal of Peace Research* 43(3): 331–348.

Korns, Stephen W & Joshua E Kastenberg (2009) Georgia's cyber left hook. *Parameters* 2008–09(Winter) : 60–76.

Libicki, Martin C (2007) *Conquest in Cyberspace*. Cambridge: Cambridge University Press.

Liff, Adam (2013) The proliferation of cyberwarfare and interstate war, redux: Liff responds to Junio. *Journal of Strategic Studies* 36(1): 134–138.

Lindsay, Jon R (2013) Stuxnet and the limits of cyber warfare. *Security Studies* 22(3): 365–404.

Lynch, William J, III (2010) Defending a new domain. *Foreign Affairs* 89(5): 97–108.

Markoff, John & Thom Shanker (2009) Halted '03 Iraq plan illustrates U.S. fear of cyberwar risk. *New York Times*, 1 August.

Mueller, John (2006) *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats and Why We Believe Them*. New York: Free Press.

Nye, Joseph (2011a) Nuclear lessons for cyber security? *Strategic Studies Quarterly* 5(4): 18–38.

Nye, Joseph (2011b) *The Future of Power*. New York: Public Affairs.

Reveron, Derek (2012) An introduction to national security and cyberspace In: Derek Reveron (ed.) *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 3–20.

Rid, Thomas (2011) Cyberwar will not take place. *Journal of Strategic Studies* 35(1): 1–28.

Rid, Thomas (2013) *Cyberwar Will Not Take Place*. London: Hurst.

Rid, Thomas & Peter McBurney (2012) Cyber-weapons. *RUSI Journal* 157(1): 6–13.

Sanger, David E (2012) *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Random House.

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

Thompson, William R (2001) Identifying rivals and rivalries in world politics. *International Studies Quarterly* 45(4): 557–586.

Valeriano, Brandon (2013) *Becoming Rivals: The Process of Interstate Rivalry Development*. London: Routledge.

Valeriano, Brandon & Ryan C Maness (2012) Persistent enemies and cyber security: The future of rivalry in an age of information warfare. In: Derek Reveron (ed.) *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 139–158.

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

BRANDON VALERIANO, b. 1977, PhD in Political Science (Vanderbilt University, 2003); Senior Lecturer in Politics and Global Security, University of Glasgow (2012–); interests include cyber security, rivalry, foreign policy, popular culture and international relations, and international relations theory.

RYAN C MANESS, b. 1975, PhD in Political Science (University of Illinois at Chicago, 2013); Adjunct Assistant Professor of International Relations, University of Illinois at Chicago (2013–); current interests: cyber conflict in international relations, Russian coercive energy policy.