How We Stopped Worrying about Cyber Doom and Started Collecting Data

Valeriano, Brandon; Maness, Ryan C.

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Valeriano, B., & Maness, R. C. (2018). How We Stopped Worrying about Cyber Doom and Started Collecting Data. *Politics and Governance*, *6*(2), 49-60. https://doi.org/10.17645/pag.v6i2.1368

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 49–60
DOI: 10.17645/pag.v6i2.1368

Article

How We Stopped Worrying about Cyber Doom and Started Collecting Data

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

[1] Donald Bren Chair of Armed Politics, Marine Corps University, Quantico, VA 22134, USA; E-Mail: drbvaler@gmail.com
[2] Defense Analysis Department, Naval Postgraduate School, Monterey, CA 93943, USA; E-Mail: rmaness@nps.edu

* Corresponding author

Submitted: 17 January 2017 | Accepted: 12 March 2018 | Published: 11 June 2018

Abstract
Moderate and measured takes on cyber security threats are swamped by the recent flood of research and policy positions in the cyber research field offering hyperbolic perspectives based on limited observations. This skewed perspective suggests constant cyber disasters that are confronting humanity constantly. The general tone of the debate argues that cyber war is already upon us and our future will only witness more cyber doom. However, these hyperbolic perspectives are being countered by empirical investigations that produce the opposite of what is to be expected. It is generally observed that limited cyber engagements throughout the geopolitical system are the dominant form of interaction. Our task here is to offer a different path forward. We first posit what can be known about cyber security interactions with data as well as what cannot. Where is the water's edge in cyber security research? We then examine the known works in the field that utilize data and evidence to examine cyber security processes. Finally, we conclude with an offering of what types of studies need to be done in the future to move the field forward, away from the prognostication and generalizations so typical in the discourse in this constantly changing and growing field.

Keywords
cyber conflict; cyber security; cyber strategy; data collection; quantitative methods

Issue
This article is part of the issue "Global Cybersecurity: New Directions in Theory and Methods", edited by Tim Stevens (King's College London, UK).

1. The Challenge of Cyber Security Threat Data

Beginning in 2014, various news organizations began reporting on a particular cyber security firm, Norse Corporation, and their active cyber threat map (Walker, 2015). *Mashable* noted in 2016 that "the global cyber war is raging on, and this mesmerizing map shows just how serious it has become" (Gallucci, 2016). The map is dynamic, colorful, and gets the point across quickly, a criterion for any decent visualization of data. As late of August 2017, the Defense Intelligence Agency (DIA) tweeted out a link and photo of the threat maps suggesting it represented ongoing cyber-attacks (DIA, 2017). Yet this map is not a very clear representation of any real threats that nation-states face on a daily basis.

Unfortunately, the Norse cyber threat map does not represent active threat data, but attacks, likely by bots, on preset honeypots. Honeypots are a method of providing data on fake targets to either distract the opposition from the real targets or to deter an aggressor from attacking in the first place (Gartzke & Lindsay, 2015). While sometimes a useful method to gather threat intelligence if presented a sleight of hand for an attractive target, honeypots as reported in popular discourse are not exactly an accurate representation of the cyber threat landscape. In this case, the goal was to demonstrate the ability to track global attacks to gain interest in the company and promote its capabilities.

Nearly all active threat maps either present data tracking honeypots and various bot networks that are de-

void of human agency, simply presenting what is in fact fake data. Active representation of the threat landscape is the goal, but the reality is that the picture of the cyber security threat landscape we currently have is incomplete, misleading, or outright fake.

High profile data breaches have been consuming media narratives for at least a decade. With each act of cyber disruption or espionage, pundits as well as government officials and several academics declare that cyberwarfare is upon us, is the future of warfare, and it is only a matter of time before a "Cyber Pearl Harbor" wreaks havoc on the American homeland (Gurdus, 2016). With this new revolution in military affairs, the battlefield, according to some, is forever changed and the next big war could very well be a cyberwar (Clarke & Knake, 2010; Kello, 2013). Politicians, pundits, and practitioners have jumped on this doomsday narrative and have promoted cyber arms races, offensive advantage, and deterrence strategies to stay one step ahead of would be adversaries in order to prevent them from infiltrating networks out of fear of massive retaliation. These revolutionists point to acts such as Stuxnet, Shamoon, Sony, and the Office of Personal Management (OPM) hack as the new norm of conflict between states, and that the US is losing ground with every tolerated cyber-attack on American networks.

This illustration points out the need for reliable collected data on cyber incidents between entities to challenge threat inflation. Empirical evidence and inferences with data from the academic community can help serve policy makers in constructing policies that help in developing proper normative behavior from states.

The challenge of collecting cyber security data runs right up against the difficult reality of collecting information on active threat interactions in real time. The process is difficult, complicated, and prone to error, but not impossible. Researchers need to be clear that there is an imperative to collect data on all forms of conflict and no domain presents easy opportunities for data collection. Scholars and activists alike are still trying to sort through casualty data in Syria (Black, 2016). Human Rights Watch (2017) data is likely prone to reporting bias reflected by an increased interest in human rights abuses through time.

The impediment for cyber security can be considered even more challenging. While interest in cyber security interactions is increasing, bringing with it elevated reporting of cyber breaches, there remains a greater problem. In a domain thought to be mostly secret, how do you collect data on what most of the population assumes is uncollectable and mainly classified? Why even seek to overcome this challenge, given the high degree of difficulty? In this article, we will review why the need to collect data on cyber security interactions, how the process can be conducted and is not only possible but happening, highlight ongoing attempts to empirically assess the cyber security complex.

2. The Need for Cyber Security Data

Moderate and measured takes on cyber security issues that intersect with policy and international relations issues can be out of place amongst the recent flood of research and policy positions in the cyber conflict and security field. The general tone of the debate suggests that cyber war is here, it is our present, and it will be our future. One gets millions of hits if "Cyber Pearl Harbor" is Googled (Lawson & Middleton, 2016). The basic assumption is that our future military, diplomatic, and economic history will involve the use of computers as the main avenue of attack and defense because these technologies are not only transformative, but also cheap and easy.

Cyber strategies and tactics are like any other technological development. At first, new technologies suggest immense possibilities and promise to give states an edge, yet the reality is that technological advances rarely change the face of the battlefield, either in the diplomatic, economic, or military realm. New technologies can be used to defeat specific threats or defenses, such as the tank helping break the stalemate of the trenches in World War I; but are often limited in other contexts. Tanks need to be supported by infantry and logistical teams constantly supplying fuel or towing the machines, limiting their effectiveness and reach. cyber strategies will be no different, and they will be just another important piece in the arsenal but not game-changing on their own.

Claims of revolutionary importance are easy to make, and persuasive given certain examples, but there are always countering examples. Vasquez (1991) makes the case that nuclear weapons were not responsible for the long peace during the Cold War, rather the lack of direct territorial disputes between rivals limited devastating war. The important point is that no one example or story tells the complete picture, and for that we need evidence and data to support much of the theory and practice.

Data-focused research can make an important and lasting statement. By looking at the complete landscape of interactions, we can leverage a different view of the evidence and data. No longer does one attack stand out, but the total picture emerges and in cyber security it is a picture of a restrained international system developing a norm against the use of cyber weaponry (Valeriano & Maness, 2015).

We do offer one key caveat. Our focus is mainly on nation-state interactions because they are discussed as the most devastating and dangerous. In reality, collecting data on cyber-crime or digital attacks of civil society is just as important, but ignored in the field. We hope refocus the debate a bit here and help scholars rethink the domain regarding the nation-state seeking to move towards a more holistic view of cyber security as an everyday security issue. By moving beyond the dramatic examples of Stuxnet and the Sony Hack, we can expand the range of possibilities but also expose the limitations inherent in new technologies. These caveats are critical when theorizing about the future use of cyber weaponry.

3. Reality Is a Social Construction

There have been many challenges to the utility of data in international relations. Hedley Bull (1966) long ago argued that data-based analysis was tortuous and inelegant. He also maintained that nothing in data-based examination goes beyond what can be deduced using conventional wisdom. J. David Singer (1969) challenged this presentation as being naïve about the utility and purpose of data. There is a limitation on our ability to understand the world without taking a total snapshot of interactions to make predictions, understand patterns, and examine how outliers may alter our perceptions of interactions. Data can illuminate counterintuitive patterns not readily apparent to the qualitative observer.

Insights from postmodern and critical scholars are imperative to our task. If reality is basically what we make of it (Berger & Luckmann, 1991), what happens when the perspective we construct to deal with nascent threats is divorced from reality? While data and evidence will never be value free, an insight offered by critical theory, it also offers a more nuanced approach to the issue than selecting the obvious cases for examination and extrapolating from outliers. We must start somewhere; the postmodern project is a reaction to the behavioral turn in the social sciences. The cyber security field has to yet to even start its behavioral moment but seems to have started with the suggestion that collecting data is impossible (Kello, 2013).

As Vasquez (1998, p. 218) points out, language and conceptual frameworks are prone to self-fulfilling prophecies. If we allow the language we use to construct how we view security challenges, we likely will miss key developments in the field. Social science is not value-free, but this does not mean that it must be data-free in order to reflect the true state of nature. Language without the consideration of data and evidence will often be empty and akin to Norse's threat map, which is an imperfect and often a misrepresented vision of reality.

Using social science methods can improve the practice of cyber security. "Science is not simply a useful tool, but a practice that creates a mode of life that consciously destroys other ways of thinking and living" (Vasquez, 1998, p. 219). Without encouraging the perspective that data adds to the cyber security debate, we might accept observations as truth when in fact they merely reflect a skewed sample that is not reflective of actual patterns and practice. To encourage better behavior in cyberspace, to stop gross abuses, and to predict future events, we must move beyond biased and constrained samples offered by observational logic that cannot move beyond description and theoretical logic.

For Vasquez (1998), "good" empirical theories should be accurate, falsifiable, have explanatory power, be progressive, be consistent with what is known in other areas, yet also be parsimonious. Theories must pass reasonable tests of fact first. The process of progress inherent in a social science enterprise starts with the collection and analysis of data. Once data is collected, positions and theories can be challenged and falsified in light of evidence. We then can move towards explaining the past, present and future based on the data processes that we observe now.

The key addition of Lakatos (1970) is that for a theory to be progressive, it must obtain more empirical content than the prior theory and generate new and interesting questions. Without a foundation of theory, data and logic, we have no bias on which to proceed with knowledge based inquiries. Cyber security theory is empty without a firm foundation of fact that then pushes us to explore new directions.

Of course, data is always biased by the unit collecting the data and interpreting the evidence. However, this is also a strength of data, others can come along and use it for their own ends and expand upon the original intent of the data to build different perspectives. The basic point is that we need to stop engaging important policy questions through prognostication that would be more suitable on a 2am television advertisement. Political scientists and policymakers should not be fortune tellers who make guesses about the future without reference to what we already know. We have evidence from the recent past and emerging contemporary situation, so we must use it to engage critical policy questions.

4. What We Can and Cannot Know from Data

It is thought that most cyber strategies and events are secret, but this is not entirely true. Much of what happens in cyberspace is the definition of overt—by interacting with external networks, threat actors make their presence known. Attackers may try to mask their origins, but language traits, common techniques and malware, and motive as well as historical context can give us a great deal of information about who is attacking whom. For example, near the beginning of the 2018 Winter Olympic Games in Pyeong Chang, South Korea, the International Olympic Committee (IOC) was hacked and subsequently stolen emails from the organization were released to the public (Matsakis, 2018). Forensic analysis attributes this operation to the Russian Federation, which was the primary culprit from the beginning, as the country had been banned from competition for the games for a massive doping scandal that Moscow vehemently denies guilt to this day. Feeling cheated, the APT 28 Russian hacking group FancyBear, the same group responsible for attacking Democratic Party networks during the 2016 US presidential election, enacted their revenge in the digital realm.

Covert action is "the effort of one government to influence politics, opinions, and events in another state through means that are not attributable to the sponsoring state" (Anderson, 1998, p. 423). Yet in cyber security, the attribution problem is often overstated, what is beyond our ability is constructing real-time data that can be used to charge culprits in the act based on domestic le-

gal standards. Observing malicious cyber behavior is possible but delineating responsibly in a legal sense is quite difficult. Measuring ongoing infiltrations, unknown zero-day threats, and attempts at access that fail are difficult if not impossible to observe. Once an operation achieves a certain level of access, inserts malware into the target, and seeks to coerce the opposition, there are clear observable patterns that can be documented.

In short, there is much we can know about the cyber security domain that can be gleamed from observations. Operating in this landscape as if the threats cannot be known, monitored, and predicted betrays the great advances we have made in doing exactly this. What we cannot do is watch ongoing operations as they occur. This is mainly because organizations might not know they are violated till after this happens, as was the case for the OPM hack (Koerner, 2016). Cyber security companies might operate at a level where they promise a great deal of information, but this is likely to be a promise that cannot be kept. There is clearly a great utility in cyber security data, but we must temper expectations and excitement with collaborative analysis and sobered expectations of the utility of these data-based efforts.

In the cyber security field, we witness all sorts of interactions that can be processed into data. Incidents and events, malware and its spread, vulnerabilities, and social media interactions are all critical elements of the cyber security discourse and represent collectable data samples. Yet, the majority of the cyber security field seems to reject the idea that data collection is possible. This is perplexing in the face of calls to reform the vulnerabilities equities process (VEP), or the process by which threats are communicated by the government to private industry (Newman, 2017). Cyber security data is clearly observable and a part of the news cycle for cyber interactions, but it is generally removed from the political, policy, and military discourse.

Unfortunately, some critics and skeptics believe that collecting data on a subject is synonymous with perfect information about a topic. Data producers have never claimed that their data was complete, total, or absent of bias. These attributes are common for all data enterprises. In the social science world, all data collection enterprises will be incomplete or inaccurate in some way. This does not mean that data projects should be scrapped, but that those who use these projects should understand the limits and possibilities inherent in data collection enterprises.

It must also be made clear that are we are generally speaking of cyber security interactions are they pertain to state-based action. Extending this data-based architecture to criminal interactions would require different theories, data collection methods, and processes. Future efforts should seek to move beyond the state towards examining non-state behavior including criminal interactions.

We can only observe what actually happens rather than what was intended to happen, this is one reason to focus on states where malicious action is to be expected and even admitted at times. It is not exactly an interstate crisis if one state tries to attack another state in cyberspace and fails to be noticed. This is an unobserved process, a tree falling in the woods with no one to witness the fall so to speak. Can there really be a coercive impact if one node in the interaction does not even know there was an interaction?

Scholars must be prepared to go to war with the data we have, not the data we wish we had. There are inherent limitations in the data collection process that make data problematic for many reasons but gathering a wide snapshot of interactions is clearly preferable to observing a single interaction and extrapolating from that data point. That is not data analysis but an exercise in guesswork that has no place in the academic or policy enterprise.

5. Other Data-Focused Efforts in Cyber Security so Far

The Department of Homeland Security (DHS) now has an incident reporting feature (DHS, 2018a) and ongoing efforts to collect data (DHS, 2018b). Without this step, we are operating in known environment needlessly wearing a blindfold. Hopefully this will allow the US to become an open and transparent leader for cyber security data, but this also leaves out the rest of the world in terms of sampling, making it a problem to generate a global sample enabled by the targets.

The United Kingdom's National Cyber Security Strategy proposes data driven solutions to the problem but these efforts are typically clouded by a disagreement on methods and evaluation standards rather that starting first with active threat information collection (UK Government, 2016). The US Office of the Director of National Intelligence (ODNI) office offers a standard of evaluation hoping to generate what they deem as a "Cyber Esperanto" method of data evaluation and coding but fails to articulate a standard by which incidents would be collected (Ackerman, 2017). Generally, the focus on evaluating the phases of attacks rather than starting with a macro sweep of the field.

It is strange that the cyber security domain has restricted itself from understanding the basic contours of the conflict dynamics through the analysis of empirical events. To not take this step is a self-defeating strategy that betrays our standard operating procedures in other military and political domains. The first step is to always understand the behavior of the key threat actors in a domain, however in the cyber security field we seem to think that the adversary is inherently unknowable and without a past, this is an unhelpful conjecture. The first step always seems to develop risk management methods to minimize damage without seeking to understand the goals and past actions of the attacker in the first place.

In academia, Healey and Grindal (2013) make clear strides early on to seek to revive the idea of a disciplinary history of cyber conflict and examine as many cases as

possible. Another excellent example is Lindsay's (2015) listing of prominent Chinese cyber espionage cases. The problem is that these examples of macro-case studies are few and far between. With the exception of Karatzogianni (2012) and Middleton (2017), most studies focus on a few prominent cases like Stuxnet, Shamoon, and Sony, at the expense of the typical behavior and strategies that rival countries exhibit in cyberspace.

The plethora of new emerging data sources of information is heartening, but also reinforces key points we make in *Cyber War Versus Cyber Realities* (Valeriano & Maness, 2015). We have observed restraint in cyber interactions. Escalation is rare (Valeriano, Jensen, & Maness, 2018), and most disputes piggyback on previously known foreign policy conflicts and crises that are well established, often connected to territorial disputes. Schneider (2017) demonstrates that even in the context of wargame scenarios, escalation is rare.

Examining the data on cyber incidents, Pytlak and Mitchell (2016) are able to point out that rivalry intensity does not predict which rivals will engage in cyber conflict. Instead the best predictor is the presence of nuclear weapons. While the possibility of escalation in the context of nuclear weapons is troubling, we also know that empirically, nuclear states can push their negotiations to the edge of war and draw back (Beardsley & Asal, 2009). Mauslein (2014) also demonstrates empirically that rival states are less likely to engage in cyber conflict due to escalation risks which counters the early idea that rival states would be primary testing ground for cyber disputes (Valeriano & Maness, 2012).

Understanding the impact of cyber confrontations appears to be the next key challenge. In an examination of 1,841 cyber events from 2013 to 2016 in Ukraine, Kostyuk and Zhukov (2017) demonstrate that cyber actions had no discernible impact on battlefield events. Narrowing down on fighting between 2014 and 2015, the authors find no escalatory patterns in the cyber data, but conventional attacks do result in corresponding reprisals. While this study represents a small selection of battlefield events in Ukraine, there does appear to be a pattern emerging. Evidence from a case study on Syria finds many of the same patterns as in the Ukraine case. Valeriano et al. (2018) produce a macro level view of the impact of cyber strategies suggesting that only 5% of the 192 incidents coded produce a describe change in behavior in the target. What is more important is that these events demonstrate no clear escalatory pattern. Cyber strategies, even intensely invasive ones that seek to degrade networks and systems, neither appear to compel the adversary nor do they produce the escalation risks often hypothesized by scholars such as Buchanan (2016).

The Axelrod and Iliev (2014) formal model is another useful examination of the utility of cyber conflict. They note that actors with a high degree of stealth have a lower likelihood of utilizing a cyber weapon because the utility of the weapon does not decline through time (it is unlikely to be discovered). They also note that gain is a key consideration, a state will only use a cyber weapon if there is a gain to be made. The studies by Valeriano et al. (2018) and Kostyuk and Zhukov (2017) suggest that gains are rare therefore the Axelrod and Iliev (2014) formal model would predict a low instance of cyber conflict when the consideration of effects and gains are added.

A novel investigation produced by Lawson and Middleton (2016) might be a useful example for future scholars looking to collect data on threat perceptions and securitization policies. By examining the threat construction of the term "Cyber Pearl Harbor", the authors are able to delineate the history of the term's use and the key referent objects. They find that 45% of the time, the term is used to describe threats to civilian infrastructure. The authors also demonstrate that the term is only used to discuss actual events 33% of the time with majority of frames being used to discuss imagined or non-actual threats.

6. Expanding Cyber Security Data

Our team has been coding cyber incident data since 2010 and serves as a unique example of how the process of collecting cyber security data and evidence can be done. Our first peer reviewed published work appeared in 2014 in *Journal of Peace Research* (Valeriano & Maness, 2014). In this article we note that cyber conflict is much more restrained than generally understood by popular discourse. Threat inflation is ripe in cyber security, and the real use of cyber tools seems to be to enhance the power of strong states.

The data that Valeriano and Maness (2014, 2015) have built challenges the cyber revolution perspective and does so with the tools of social science, and is a necessary turn given the general tone of the debate. We first determine that a viable data collection method in light of limited resources was to focus on states that are committed interstate rivals (Diehl & Goertz, 2001). This allows us to focus on those actors with an intense history of recent hostilities that should be the most likely users of cyber technology on the battlefield (Maness & Valeriano, 2018).

In our research (Maness & Valeriano, 2016; Maness, Valeriano, & Jensen, 2017; Valeriano & Maness, 2014, 2015), we have been able to marshal a massive amount of evidence that is useful in dissecting the actual trends on the cyber battlefield in a geopolitical context. We demonstrate that while cyber-attacks are increasing in frequency, they are limited in severity, are directly connected to traditional territorial disagreements, and mostly take the shape of espionage and low-level disruptive campaigns rather than outright warfare.

Given this data-based perspective, we question the dynamics of the cyber security debate and offer a countering theory where states are restrained from using more malicious cyber actions due to the limited nature of the weapons, the possibly of blowback, the connection between the digital world and civilian infrastructure, and

the reality that any cyber weapon launched can be replicated and used right back against the attacker. Given all of these perspectives gleamed from the data, we must moderate our views about the transformation that is offered by cyber strategists who stress a more revolutionist tone (Lango, 2016).

Social science clearly matters for contemporary technological policy debates. Absent rigorous methods, much of what is in the field is basically guesswork. Our work really owes an intellectual debt to J. David Singer, who started the effort to quantify war at the University of Michigan with the Correlates of War (COW) project (Small & Singer, 1982). Our project builds on this methodology and uses many of the same coding strategies. We recognize that data is a work in progress and seek to build more and more knowledge through subsequent updates. By gathering the full picture, we can gain the perspective that really matters in these emerging policy debates regarding the cyber battlefield.

The problem with collecting data where it does not exist already are centered around the difficulties that come with starting such an endeavor in the first place. Often it has been claimed that it would be impossible to collect cyber conflict data, as such data would present a skewed picture of the scope of the field. Yet the imagined impossibility of collecting data should never be the barrier in starting such an undertaking, and the only real barrier should be the literal impossibility of collecting such information.

In the process of collecting data on these state-based cyber events, we found that official leaks to the media have been helpful, but more importantly for the cyber security field was the obvious impetus by cyber security firms to demonstrate their ability to identify attacks and release reports forensically accounting for the process behind the attacks. This sort of information was exactly what we were looking for and it continues to be available to this day as the ultimate calling card demonstrating skills and expertise, but also as a source of information in our investigation. We are prudent and recognize that there have been other efforts at empirically-focused cyber security research. We welcome all and every effort since it will allow for the field to seek the overall goal for the accumulation of knowledge around cyber security practices.

Subsequent work in our book *Cyber War Versus Cyber Realities* reinforced these points and added case studies to support our empirical findings. Our next book, *Cyber Strategy*, includes cyber incident data from 2000 to 2014 between rival states. Our cut point is 2014 because the majority of the coding effort was done in 2016 and we are firm in belief that while cyber incidents can be coded, one needs to wait at least a year to make sure the sources, actors, and targets are confidently known.

The main addition in our work is a consideration of the efficacy of cyber actions. Simply, do they work? To that end we have now coded concessions and targets in the data. We also altered the severity coding to account for a wider scale of events. All cyber incidents in the Dyadic Cyber Incident and Dispute (DCID) are dyadic and the countries must be considered rivals, which are states with recent past animosities with each other. For the coding of the variables for all pairs of states added to the dataset (non-state actors or entities can be targets but not initiators as long as they critical to state-based systems, or if the original hack escalates into an international incident in the non-cyber domain), the initiation must come from a government or there must be evidence that an incident or dispute was government sanctioned.

For the target state, the object must be a government entity, either military or non-military; or a private entity that is part of the target state's national security apparatus (power grids, defense contractors, and security companies), an important media organization (fourth estate), or a critical corporation. Third parties are noted and coded as an additional variable in the data.

We are also now including information on cyber strategies, breaking this down into a four-point typology that is mutually exclusive and logically exhaustive.

1. *Disruptions:* which include taking down websites, disrupting online activities, and are usually low cost, low pain incidents such as vandalism or DDoS techniques;

2. *Short-Term Espionage:* gains access that enables a state to leverage critical information for an immediate advantage example; an example being the Russian theft of DNC emails and publicly releasing them in a disinformation campaign during the 2016 US presidential election;

3. *Long-Term Espionage:* seeks to manipulate the decision-calculus of the opposition far into the future through leveraging information gathered during cyber operations to enhance credibility and capability, an example being China's theft of Lockheed Martin's F-35 plans;

4. *Degrade:* attempt physical degradation of a targets' capabilities. Example: US' Stuxnet against Iran; create chaos in a country to invoke a foreign policy response.

The most active dyad in the international system is China and the US. The majority of these incidents between the world's two most powerful states are espionage campaigns. China sees itself as the rising power that is far behind its status quo counterpart, and this could explain the disproportional balance in initiations between the two states (Lindsay, 2015). Most US-initiated attacks against China are counterespionage degradation campaigns to raise the costs of future espionage by China so that they slow or stop these malicious attacks on American intellectual property and government information. US–China cyber relations came to a head as a result of the OPM hack discovery in 2015, where China successfully stole the personal and sensitive information of over 20 million federal employees and contractors. This led to a high-level meeting between Obama and Chinese President Xi Jingping dur-

ing the latter's state visit in September 2015, where the two agreed to halt intellectual property theft from each other. It has been reported that China has drastically reduced its cyber espionage on the US as a result of this agreement, which was a diplomatic victory for the Obama Administration where escalation and arms races have been avoided (FireEye, 2017). It remains to be seen whether this behavior will hold with the new Trump Administration, whose early rhetoric with Beijing has been more bombastic.

The more recent cyber menace for the US has been Russia, where the former Cold War foe has successfully socially engineered attacks on political networks, including the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC), as well as Hillary Clinton's presidential campaign manager John Podesta's email account. The information stolen from these accounts was then strategically released to WikiLeaks (ODNI, 2017), which could have changed enough minds in crucial swing states and possibly was the deciding factor in the victory of Donald Trump in the 2016 US presidential election. The Obama Administration has responded with economic sanctions on high-level Kremlin operatives and has expelled a few dozen diplomats from the US. However, it remains to be seen if the Trump Administration will continue to hold the Russians to account for these acts of espionage and information warfare.

Yet these data breaches could have been easily prevented with basic cyber hygiene practices for those with access to the networks, and the political espionage conducted by Russia is not outside the acceptable behaviors for spy agencies. The blame could easily lie with the Democratic Party for being so vulnerable to outside attack. Before promoting offensive posturing and escalatory retaliatory action, the US needs to get its networks better defended society-wide, and cyber hygiene policies to prevent such easy attacks such as the Russian election hacks would be a good first start. If the US is considering going toe to toe with its cyber adversaries, the defenses of its large attack surface and vulnerable networks need to be shored up significantly.

Dyads not involving the US are overwhelmingly regional rivals, suggesting that adversarial relationships between these states have been ongoing for years (Vasquez, 1993). Rivals who have been managing these relationships for a long time have developed normal relations (Azar, 1972) and given that most of these cyber incidents and disputes launched against each other are disruptions or espionage, the probability that cyber conflict between regional rivals will lead to escalatory tensions remains low.

Breaking down the macro evidence of Valeriano et al. (2018), Table 1 below shows that 87% of all cyber incidents between rival states are either disruptions or espionage. Victims of these acts of cyber malice have not responded in an escalatory fashion in the majority of cases (Maness et al., 2017), indicating that responses have either been proportional via conventional foreign policy tactics, such as targeted economic sanctions, or diplomatic outreach to promote better behavioral patterns have been successful. Evidence for policies of restraint as the future of governance of the international cyber realm are demonstrated, strengthening these modes of behavior for all states in the international system, as championed by the UN's Group of Government Experts (GGE), should be the primary goals of the government of the US and its NATO and EU allies.

Table 1. Cyber incidents by coercive objective.

Coercive Objective	Number (%)
Disruption	70 (36%)
Espionage	97 (51%)
Degradation	25 (13%)
Total	192 (100%)

US deterrence proponents such as former Director of National Intelligence James Clapper have posited that cyber-attacks will get worse "until such times as we create both the substance and psychology of deterrence" (Jones, 2015). This is assuming that cyber incidents will not only grow in number but also in severity, where escalation will be the future if deterrence mechanisms cannot be put into place. This would require developing sophisticated cyber weapons, communicating these capabilities to potential adversaries in the cyber realm, and being willing to follow through with action that may harm civilians, lead to escalatory retaliation, and provide enemies with digital technologies they did not have before the attack. Yet this type of thinking is an enduring one as more high-profile data breaches, usually espionage campaigns or disruptive information operations and rarely physical degradations (Valeriano et al., 2018) continue to proliferate and be misconstrued in popular narratives (Lawson, 2013).

According to the data, offensive posturing and digital arms races that the US may set into motion as policy could be self-defeating policies (Craig & Valeriano, 2016). There are normative modes of behavior from states that have been observable since the turn of the century based on collected empirical data that suggest that cyberspace can be governed from a less escalatory strategy, where restraint mechanisms can be built upon if the US and its transatlantic allies continue to push for stabilizing norms. The question that remains at the time of this writing is whether or not the Trump Administration will continue this process or turn toward the more dangerous deterrent strategy.

Scholars who have looked at past dynamics of cyber conflicts find that there is evidence for restraint from states. Reveron (2012) acknowledges that states have great capabilities in terms of inflicting damage on one another, yet this does not mean that they will. Espionage and disruptions seem to be the majority of state-based

actions, and more coercive degrading techniques such as Stuxnet or Shamoon are exceptions to the rule according to Valeriano et al. (2018). The need for weaponized retaliatory responses and initiating policies that promote this behavior may therefore be premature at this point, according to available evidence.

The key point is the evidence is critical to evaluate the domain. How can policy decisions be made without considering the shape and scope of the environment? Some scholars paint a vastly different picture than those in the discourse and this is spurred on by a careful analysis of empirical evidence.

7. Important Components of any Dataset

Many groups have produced lists of cyber events, the most prominent might be Hackmageddon (2018). The key aspect to understand is that making a list of cyber events is not enough to produce social science inferences or data analyses. So much more is required. The Council on Foreign Relations (CFR) cyber operations tracker covers cyber incidents from the years 2005–2017 (CFR, 2018). It includes incidents that are "suspected" to have state sponsorship plus non-state action. This is a problem for datasets of this kind, as laying blame on a state or group for cyber actions has enormous geopolitical implications. Throwing suspected state-sponsored incidents in with verifiable ones is problematic coding and raises the possibility of retractions at a later date.

For the variable coded as affiliation, which attempts to attribute the group responsible for the cyber incident, 105 cells of this variable are left blank. Furthermore, 37 of these cells either begin with the phrases "believed to be" or "possibly", indicating further uncertainty of who just might be responsible for the cyber incident. This translates to the coders having 74% of their coded incidents being uncertain that the culprit had been a state actor.

In the DCID, we wait at least one calendar year to pass before we begin to code a year. Right now, our latest, version, 1.1 covers all dyadic cyber incidents between rival states from 2000–2014. We are in the process of coding version 1.5, which will include state-initiated incidents from the years 2000–2016. Both collect government initiated cyber action between rival states from the years 2000–2014, which are extracted from the Klein, Goertz and Diehl (2006) dataset on enduring rivals as well as Thompson's (2001) strategic rivalry dataset. Coding efforts are mirrored after the COW project that records conventional conflict dynamics since the Napoleonic Wars (Jones, Bremer, & Singer, 1996). Several variables are coded based on typologies, methods, target types, coercive objectives, and severity levels. Events are coded into cyber incidents and disputes. Incidents are individual events that can last a matter of hours, days, or weeks, depending on method and have specific objectives. The Stuxnet worm is classified as a cyber incident. Disputes are larger campaigns that can contain multiple incidents and are part of a larger strategy. The Olympic Games dispute which contains Stuxnet but also espionage incidents such as Duqu and Flame.

Many cyber incidents can take months to find the proper attribution, especially covert espionage incidents. The analogy of the iceberg is often made with the idea that much what we know about cyber interactions falls below the surface. Instead we argue that at some point, the iceberg flips over and we are able to get a representative sample of the dynamics of all cyber actions. What is unknown is important, but it is also unknowable. For an incident to make it in the DCID, we must have at least two verifiable sources that have given enough confidence to place the blame on a state actor. Sources include government intelligence reports and cyber security forensic reports.

We must be clear that datasets need some things in common to make them useable to the wider community. Every effort to produce a trusted source of cyber security information should contain clear coding rules, independent variables, compatibility with other coding efforts, and reliability checks. Clear coding rules are critical for any social science effort. How does an outside observer know what is coded in the dataset? What is included and what is left out? This is associated with the condition of replication. Can someone come behind your effort and produce something similar? Clear instructions are critical in order to ensure the progression of knowledge, building and reproducing prior work is critical in seek to confirm knowledge.

A dataset cannot simply be a list of events, that is just a list. Independent variables are critical for any data source. This should include location information, characteristics of the unit of observation, issues such as linkages to other events, damage and severity, and a host of other factors that make up what might be a traditional dataset that can be used for analysis. If there is just a list of events, this is just a single variable that would then need to be merged into another source.

The next clear requirement is the compatibility with prior efforts. The whole purpose of data collection efforts being clear and replicable is to ensure that knowledge is moving forward based on some sort of basic consensus. Others should be able to build on your work and push things forward. The data should be compatible with other sources, our cyber events coded in the DCID dataset has country codes, dates, and other events that can be linked and merged to other data efforts. This effort is based on the Correlates of War project (Jones et al., 1996), a long-standing data collection effort and can be fit in with other data research done in the International Relations field. Avoiding trying to reinvent the wheel and respecting the efforts of those that have come before is critical in moving forward towards shared wisdom.

Finally, reliability is likely the most critical aspect of any dataset. Is it reliable in that we are sure that it was coded correctly, absent of as much bias as possible, and others should be able to take the coding rules and agree

with the basic judgements made? Our DCID data was independently checked by three other hired coders at both rounds of data coding. Version 1.1 of the DCID also had a group of 15 military officers go through all the coding of the more subjective elements to ensure that our coding of success, impact, and actors was reliable and could withstand basic measures of intercoder reliability and acceptance of judgement calls made on borderline cases.

Salehyan (2015) has a useful review of the things needed to produce data in the conflict studies field. There are a host of other issues we have not even begun to mention such as source bias, source inclusion, scalability, information extraction, and the challenges of analysis. One such challenge rarely admitted in cyber security is the problem of selection effects (Fearon, 2002). If we are only taking a sample, such as state-based actions reported by the press, or in our case, only actions between rivals, we are only coding a selection of the wider possible universe of cases. This constraint is critical in understanding the implications of the possible analysis done on the data. Selecting which cyber incidents to be examined, whether state-based, cybercrime, or cyber activism, is a critical judgement call that one must make to facilitate analysis, and the coders must be clear about these choices and their implications.

8. Data Investigations of the Future, What Comes Next?

Social science investigations into cyber security interactions are rare to this point. There is much that needs to be done before we can suggest that the field has a strong grasp of cyber security interactions. Instead, speculation substitutes for detailed understanding and this is of limited value given the importance of cyber security challenges. Rigorous surveys of cyber security interactions are rare. While it seems clear that the public and elites regards cyber threats as prime challenges to the security of the state (Stares, 2017), it is unclear just what context is given to the respondents and what background they are operating under when making sweeping judgements about the security challenges states face.

Embedding experiments within surveys is a potential avenue for future research. Kreps and Schneider (2017) demonstrate that public respondents are unlikely to advocate for escalation even under hypothetical situations. Experiments into human behavior in response to cyber security threats is also critical. Utilizing biological samples of stress, a series of studies seem to suggest that the population regards cyber security threats on par with conventional terror threats (Gross, Canetti, & Vashdi, 2016). Cyber security challenges result in elevated stress levels (Gross et al., 2017). What is unclear is if this is an outlier tied to the sample country, Israel, and what conditions might bring down elevated threat frameworks.

Repression is another key area to study in the future. The expectation is that the future of cyber combat will be state on state violence when in reality we observe much more state on individual cyber violence than would be expected (Valeriano, 2016). The challenge is collecting data on cyber repressive events which are akin to human rights violations. Some have made strides examining individual state repressive incidents (Gohdes, 2015), while others have demonstrated that states experiencing DDoS attacks are also likely the victims of internal repression (Asal et al., 2016).

Future datasets will need to expand to investigate non-state actors and internally repressive cyber incidents. We believe this is the critical future of cyber security investigations. Investigating the macro data inherent in cyber processes can help us understand much more about the domain than the conjecture that seems to dominate the field. All these efforts are a work in progress but working in conjunction with other scholars and avoiding duplication is the only way to move forward.

9. Conclusion

Establishing knowledge about the cyber security domain is critical because it is recognized as a Tier 1 security threat. The potential implications of a cyber security disasters and the strategic logic behind the cyber threats makes the utilization of cyber weapons a possible method of interstate competition. The challenge is to understand how much of this perspective is based on threat inflation and how realistic any of these conjectures is in relation to reality.

By undertaking data exploration efforts, we can seek progress forward on critical security questions. There is appears to be a consensus in the field that there is evident restraint in cyberspace despite the potential for conflict. This consensus is supported by the Council of Foreign Relations incident data which locates only 191 incidents from 2005–2017. The DCID data, which is restricted to only rival states, locates 192 incidents from 2000–2014 (Maness et al., 2017). Other supporting investigations find similar limited engagements utilizing cyber methods to alter state to state relationships.

States are the most cyber-capable actors in the international system (Nye, 2011), therefore collecting data on cyber actions enacted by state actors has been our starting point. The next step in our research program is to begin collection of data on non-state actors, which is a much larger universe of cases, but not impossible to collect data and infer implications of the dynamics of cybercrime, cyber terrorism, and cyber hackitivism. Our same methods and procedures, we posit, will uncover these unknowns in the social science realm of cyber conflict and security research.

This is not to say that data is the only way forward in cyber security. Rigorous case study logic that establishes critical casual actions is welcome. Examining wargames and responses in combat scenarios is also important. Formal modeling would be useful in deducing behavioral options and the constraints imposed by institutions. The cyber security field is ripe for more social science-based in-

vestigations, but these must include the direct collaboration of social scientists who have experience in coding data, practitioners who experience the events first hand, and policy-makers who seek to transform the data into actionable events.

Acknowledgments

Thoughts and prayers for the Chicago Bears. We thank our dogs, the US Marine Corps, the US Navy, and Donald Bren. We do not thank Star Wars, Netflix, and Amazon for being too distracting.

Conflict of Interests

The authors declare no conflict of interests.

References

Ackerman, R. (2017, August 1). Creating a common language of cybersecurity. *AFCEA*. Retrieved from https://www.afcea.org/content/creating-common-language-cybersecurity

Anderson, E. (1998). The security dilemma and covert action: The Truman years. *International Journal of Intelligence and CounterIntelligence*, *11*(4), 403–427.

Asal, V., Mauslein, J., Murdie, A., Young, J., Cousins, K., & Bronk, C. (2016). Repression, education, and politically motivated cyberattacks. *Journal of Global Security Studies*, *1*(3), 235–247.

Axelrod, R., & Iliev, R. (2014). Timing of cyber conflict. *Proceedings of the National Academy of Sciences*, *111*(4), 1298–1303.

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

Beardsley, K., & Asal, V. (2009). Nuclear weapons as shields. *Conflict Management and Peace Science*, *26*(3), 235–255.

Berger, P., & Luckmann, T. (1991). *The social construction of reality: A treatise in the sociology of knowledge*. London: Penguin.

Black, I. (2016, February 10). Report on Syria conflict finds 11.5% of population killed or injured. *The Guardian*. Retrieved from https://www.theguardian.com/world/2016/feb/11/report-on-syria-conflict-finds-115-of-population-killed-or-injured

Buchanan, B. (2016). *The cybersecurity dilemma*. New York, NY: Oxford University Press.

Bull, H. (1966). International theory: The case for a classical approach. *World Politics*, *18*(3), 361–377.

Council on Foreign Relations. (2018). *Cyber operations tracker*. Retrieved from https://www.cfr.org/interactive/cyber-operations

Clarke, R., & Knake, R. (2010). *Cyber war: The next threat to National Security and what to do about it*. New York, NY: Harper Collins.

Craig, A., & Valeriano, B. (2016). Conceptualising cyber arms races. In *Cyber conflict (CyCon), 2016 8th international conference on cyber conflict* (pp. 141–158). Piscataway, NJ: IEEE.

Department of Homeland Security. (2018a). *Report cyber incidents*. Retrieved from https://www.dhs.gov/how-do-i/report-cyber-incidents

Department of Homeland Security. (2018b). *Cyber incident data and analysis working group white papers*. Retrieved from https://www.dhs.gov/publication/cyber-incident-data-and-analysis-working-group-white-papers

Defense Intelligence Agency. (2017, August 14). *Cyber attacks going on right now* [Tweet]. Retrieved from https://twitter.com/DefenseIntel/status/897106479546851329

Diehl, P., & Goertz, G. (2001). *War and peace in international rivalry*. Ann Arbor, MI: University of Michigan Press.

Fearon, J. (2002). Selection effects and deterrence. *International Interactions*, *28*(1), 5–29.

Fireeye. (2017). *Red line drawn: China recalculates its use of cyber espionage*. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf

Gallucci, N. (2016, October 21). This mesmerizing map shows what cyberattacks look like. *Mashable*. Retrieved from: http://mashable.com/2016/10/21/norse-map-global-hacking-problem/#isxCIop4N8q3

Gartzke, E., & Lindsay, J. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348.

Gohdes, A. (2015). Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research*, *52*(3), 352–367.

Gross, M., Canetti, D., & Vashdi, D. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists*, *72*(5), 284–291.

Gross, M., Canetti, D., & Vashdi, D. (2017). Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*, *3*(1), 49–58.

Gurdus, E. (2016, December 15). We're headed for a "cyber Pearl Harbor", says Adm James Stavridis. *CNBC*. Retrieved from http://www.cnbc.com/2016/12/15/were-headed-at-a-cyber-pearl-harbor-says-adm-james-stavridis.html

Hackmageddon. (2018). *Cyber attacks statistics*. Retrieved from http://www.hackmageddon.com/category/security/cyber-attacks-statistics

Healey, J., & Grindal, K. (Eds.). (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Washington, DC: Cyber Conflict Studies Association.

Human Rights Watch. (2017). Syria: Events of 2016 (*World Report 2017*). Retrieved from https://www.hrw.org/world-report/2017/country-chapters/syria

Jones, D., Bremer, S., & Singer, J. D. (1996). Militarized interstate disputes, 1816–1992: Rationale, coding rules, and empirical patterns. *Conflict Management*

and Peace Science, *15*(2), 163–215.

Jones, S. (2015, July 29). Cyber insecurity: West eyes Dr. Strangelove tactics in cyber wars. *Financial Times*. Retrieved from http://www.ft.com/cms/s/0/2d23d4c8-35d2-11e5-b05b-b01debd57852.html?siteedition=intl&utm_content=buffere8653&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#axzz3h6sRmLBL

Karatzogianni, A. (2012). Cyberconflict and the future of warfare. In H. Gardner & O. Kobtzeff (Eds), *The Ashgate research companion to war. Origins and prevention* (pp. 491–504). Burlington, VT: Ashgate.

Kello, L. (2013). The meaning of the cyber revolution: Perils in theory and statecraft. *International Security*, *38*(2), 7–40.

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

Koerner, B. (2016, October 23). Inside the cyberattack that shocked the US Government. *Wired*. Retrieved from https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government

Kostyuk, N., & Zhukov, Y. (2017). Invisible digital front: Can cyber attacks shape battlefield events? *Journal of Conflict Resolution*. doi:10.1177/0022002717737138

Kreps, S., & Schneider, J. (2017, December). *Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics*. Paper presented at Emerging Technologies and Strategic Stability Conference, Stanford University, Stanford, CA.

Lakatos, I. (1970). Criticism and the growth of knowledge. In I. Lakatos & A. Musgrave (Eds.), *Proceedings of the international colloquium in the philosophy of science, London, 1965, volume 4*. Cambridge: Cambridge University Press.

Lango, H. (2016). Competing academic approaches to cyber security. In K. Friis & J. Ringsmose (Eds.). *Conflict in cyberspace* (pp. 7–26). New York, NY: Routledge.

Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*, *10*(1), 86–103.

Lawson, S., & Middleton, M. (2016, September). Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991–2016. Paper presented at Legal and Policy Dimensions of Cybersecurity, George Washington University, Washington, DC.

Lindsay, J. (2015). Introduction: China and cybersecurity: controversy and context. In J. R. Lindsay, T. M. Cheung, & D. S. Reveron (Eds.), *China and cybersecurity: Espionage, strategy, and politics in the digital domain* (pp. 1–28). New York, NY: Oxford University Press.

Maness, R., & Valeriano, B. (2018). International cyber conflict and national security. In D. Reveron, N. Gvosdev, & J. Cloud (Eds.), *Oxford handbook on US national security* (pp. 139–158). New York, NY: Oxford University Press.

Maness, R., & Valeriano, B. (2016). The impact of cyber conflict on international interactions. *Armed Forces and Society*, *42*(2), 301–323.

Maness, R., Valeriano, B., & Jensen, B. (2017). *The dyadic cyber incident and dispute dataset, version 1.1*. Retrieved from https://drryanmaness.wixsite.com/cyberconflcit/cyber-conflict-dataset

Matsakis, L. (2018, January 10). Hack brief: Russian hackers release apparent IOC emails in wake of Olympics ban. *Wired*. Retrieved from https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails

Mauslein, J. (2014). *Three essays on international cyber threats: Target nation characteristics, international rivalry, and asymmetric information exchange*. (Doctoral dissertation). Kansas State University, Kansas, USA.

Middleton, B. (2017). *A history of cyber security attacks: 1980 to present*. Boca Raton, FL: CRC Press.

Newman, l. (2017, November 15). Feds explain their software bug stash-but don't erase concerns. *Wired*. Retrieved from https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns

Nye, J. (2011). *The future of power*. New York, NY: Public Affairs.

Office of the Director of National Intelligence. (2017, January 6). *Assessing Russian activities and intentions in recent US elections*. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

Pytlak, A., & Mitchell, G. (2016). Power, rivalry and cyber conflict. In K. Friis & J. Ringsmose (Eds.), *Conflict in cyber space: Theoretical, strategic and legal perspectives* (pp. 65–82). New York, NY: Routledge.

Reveron, D. (2012). An introduction to national security and cyberspace. In D. Reveron (Eds), *Cyberspace and national security: Threats, opportunities, and power in a virtual world* (pp. 3–20). Washington, DC: Georgetown University Press.

Salehyan, I. (2015). Best practices in the collection of conflict data. *Journal of Peace Research*, *52*(1), 105–109.

Schneider, J. (2017). *The information revolution and international stability: A multi-article exploration of computing, cyber, and incentives for conflict*. (Doctoral dissertation). The George Washington University, Washington, DC, USA.

Singer, J. D. (1969). The incomplete theorist: Insight without evidence. In K. Knor (Ed.), *Contending approaches to international politics* (pp. 62–86). Princeton; NJ: Princeton University Press.

Small, M., & Singer, J. D. (1982). *Resort to arms: International and civil wars, 1816–1980*. Thousand Oaks, CA: SAGE.

Stares, P. B. (2017). Preventative priorities survey: 2018. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/report/preventive-priorities-survey-2018

?utm_medium=partner&utm_source=atlantic_global&utm_campaign=pps&utm_content=12101

Thompson, W. (2001). Identifying rivals and rivalries in world politics. *International Studies Quarterly*, *45*(4), 557–587.

UK Government. (2016). *National cyber security strategy 2016 to 2021*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Valeriano, B. (2016). Closing the Internet up: The rise of cyber repression. *Council on Foreign Relations Net Politics*. Retrieved from https://www.cfr.org/blog/closing-internet-rise-cyber-repression

Valeriano, B., & Maness, R. (2012). Persistent enemies and cyber security: The future of rivalry in an age of information warfare. In D. Reveron (Ed.), *Cyberspace and national security: Threats, opportunity and power in a virtual world* (pp. 139–158). Washington DC: Georgetown University Press.

Valeriano, B., & Maness, R. (2014). The dynamics of cyber conflict between rival antagonists, 2001–2011. *Journal of Peace Research*, *51*(3), 347–360.

Valeriano, B., & Maness, R. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. New York, NY: Oxford University Press.

Valeriano, B., Jensen, B., & Maness, R. (2018). *Cyber strategy: The changing character of cyber power and coercion*. New York, NY: Oxford University Press.

Vasquez, J. (1991). The deterrence myth: Nuclear weapons and the prevention of nuclear war. In C. Kegley (Ed.), *The long postwar peace* (pp. 205–223). New York, NY: HarperCollins.

Vasquez, J. (1993). *The war puzzle*. Cambridge: Cambridge University Press.

Vasquez, J. (1998). *The power of power politics*. Cambridge: Cambridge University Press.

Walker, L. (2015, July 12). Real time cyber-attack map shows scope of global cyber war. *Newsweek*. Retrieved from http://www.newsweek.com/real-time-cyber-attack-map-shows-scope-global-cyber-war-352886

About the Authors

Brandon Valeriano is the Donald Bren Chair of Armed Conflict at the Marine Corps University. He has published five books and dozens of articles. His two most recent books are *Cyber War versus Cyber Reality* (2015) and *Cyber Strategy* (2018), both with Oxford University Press. Ongoing research explores cyber coercion, biological examinations of cyber threat, repression in cyberspace, and the influence of video games on foreign policy outlooks.

Ryan C. Maness is an assistant professor of Cyber Conflict and Security in the Defense Analysis Department at the Naval Postgraduate School. His current research explores cyber strategy and coercive effects and how the tactic fits within overall military strategies for various countries. His specific focus is Russia's use of cyber and disinformation tactics in foreign policy as well as military strategy. His research is based on the collection of cyber events through quantitative methods and is currently constructing a cyber incidents dataset that will not only encompass state actors, but non-state actors as well.