H-**Diplo** | **ISSF**

Roundtable, Volume XI, No. 7 (2016)

A production of H-Diplo with the journals *Security Studies*, *International Security*, *Journal of Strategic Studies*, and the International Studies Association's Security Studies Section (ISSS).

issforum.org

H-Diplo/ISSF Editors: **Thomas Maddux and Diane Labrosse**
H-Diplo/ISSF Roundtable and Web/Production Editor: **George Fujii**
Commissioned by **Thomas Maddux**

Brandon Valeriano and Ryan Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System.* New York: Oxford University Press, 2016. ISBN: 9780190204792 (hardcover, $29.95).

Published on **5 December 2016**

Shortlink: tiny.cc/ISSF-Roundtable-9-7
Permalink: http://issforum.org/roundtables/9-7-cyber
PDF URL: http://issforum.org/ISSF/PDF/ISSF-Roundtable-9-7.pdf

Contents

Introduction by Nazli Choucri, Massachusetts Institute of Technology

It is great pleasure to write an introduction to this roundtable on *Cyber War Versus Cyber Realities* by Brandon Valeriano and Ryan Maness. This is an important book, one of the very few that addresses the new cyber age from a theoretical as well as an empirical perspective. The reviews are written by notable scholars who are well versed on relevant substance, theory, and methods. Each brings an important perspective to bear on the challenges at hand. And each provides important critiques in highly constructive terms. This book is also somewhat controversial in its purpose as well as its theoretical views, analysis, and execution.

Joe Burton addresses the matter of purpose in the opening paragraph of his review that states: "In *Cyber War versus Cyber Realities*, Brandon Valeriano and Ryan C. Maness seek to dispel some of the fear and hyperbole that surround cyber-attacks, arguing that the cyber threat has too often been overhyped. The book makes a valuable contribution to a still underdeveloped literature on cyber security and pushes back against a rising tide of mischaracterization, overstatement, and outright fearmongering about recent cyber disputes." And further along he asks: "Are the authors right? Is cyber war being overhyped….?"

The three reviews of *Cyber War Versus Cyber Realities* converge on three basic points, if not more. First is a unanimous appreciation by the reviewers of the value of this effort and the contributions it makes to the nascent literature on cyber security and cyber conflict. Jon Lindsay writes: "Valeriano and Maness have done real service to the field by taking cyber hyperbole down a notch and highlighting the need for better theory about and empirical evaluation of cyber conflict and that "skepticism of alarmist cyber hype need not lead to premature dismissal of real conceptual and practical challenges." Paul Diehl puts it a bit differently when he states that "What is unique about Valeriano and Maness's book, and what makes it path-breaking even though far from definitive, is that it is the first to provide both theory and empirical evidence to bear on the subject. In doing so it is likely to direct all serious research on the subject in the immediate and medium term." While there is no need to summarize the key points or results at this point, it is important to signal that they generally run against the conventional wisdom among cyber observers and analysts. Highlighting a "theory of cyber restraint" is an important addition to our theoretical perspectives.

The second point of convergence among the reviewers involves matters of theory. Each of the reviewers acknowledges the challenges at hand, and the difficulties of addressing them. But there is not always agreement among them about the precise nature of the theoretical dilemma. For example, Lindsay notes that Valeriano and Maness "… repeatedly argue that actors fear military retaliation for extreme attacks, but this point appears inconsistent with their skepticism about deterrence." Diehl states that the "… authors do a fine job of debunking the idea that deterrence theory can account for the empirical patterns of the relatively few (more on that below) and limited cyber-attacks thus far." And Burton provides a note of reconciliation by observing correctly the "still underdeveloped literature on cyber security." Especially underdeveloped, in this context, are propositions about the impact of cybersecurity in the overall calculus of national security.

And third is a general agreement about the methodological rigor of this effort, while at the same time signaling some potentially important limitations. Lindsay writes that "the empirical section is the most novel part of the book. It provides some evidence to back up claims about how states in enduring rivalries show some restraint in their publicly reported cyber interactions." But then he turns to a serious critique, namely the "restriction of cyber events to rival state dyads." This data collection practice is one of the most developed, an important legacy of twentieth-century methodology. But this may well be a case where a twentieth-century method for capturing international interactions is particularly unsuitable for the twenty-first century.

Today the 'real' and the 'virtual' are increasingly interconnected. The state remains the dominant entity as in traditional world politics, but a wide range of non-state actors are especially salient in the cyber domain, often more important that the state system itself. By focusing on rival dyads, the authors are likely to 'lose' much of the dynamics shaping the nature of the cyber conflict itself.

A large and growing market has grown around reporting about cyber incidents, instruments, and so forth. It is an ecosystem that transcends the state system and has created a new source of value for sellers and buyers of that type of information. We do not know if we should consider this matter simply as 'noise' or if we should try to mine this market for information of potential value for our understanding of inter-state cyber conflicts. Even if we decide that we should do so, we will be confronted with the immense challenge of standardization of metrics and measures. The dyadic data is what we have. And we must adjust our inferences accordingly.

This last point is especially relevant given that, as Lindsay reminds us, a "data collection cutoff is inevitable and necessary for any research endeavor. The authors' dataset ends at 2011, but the world of cybersecurity moves fast." Here is another key feature of twenty-first century 'realities' that has to be managed by scholars of international relations. The speed of cyber interactions and communication could not even have been envisaged during much of the twentieth century. We generally use time as an implicit variable for organizing data, reporting on events, or signaling periodicities, for example, but time *per se* is seldom the focus of theory or methods.

It is important to stress that the three reviews are important essays in their own right, all notable contributions to an emerging literature on twenty-first century world politics.

Participants:

Brandon Valeriano (Ph.D. Vanderbilt University) is a Reader at Cardiff University in the School of Law and Politics. Valeriano has published dozens of articles in such outlets as the *Journal of Politics*, *International Studies Quarterly, Journal of Peace Research, and International Studies Review*. His two most recent books are *Cyber War versus Cyber Reality* at Oxford University Press (2015) and *Russian Coercive Diplomacy* at Palgrave (2015) with two *Foreign Affairs* pieces summarizing the works entitled "The Coming Cyberpeace" and "Paper Tiger Putin." Ongoing research explores cyber coercion, external threats and video games, and arms races and repression in cyberspace. Valeriano has written opinion and popular media pieces for such outlets as the *Washington Post*, *Slate*, *Foreign Affairs*, *Business Insider*, and the *Conversation*.

Ryan C. Maness (Ph.D. University of Illinois, Chicago) is a research fellow of security and resilience studies in the Department of Political Science at Northeastern University. Ongoing research includes international cyber conflict and security, cyber coercion, issues of post-Soviet space, Russian foreign policy, American foreign policy, conflict-cooperation dynamics between states using events data, and regional security and energy politics. Maness has published peer-reviewed articles in *Journal of Peace Research*, *Armed Forces and Society*, and *Journal of Slavic Military Studies*, as well as in *Foreign Affairs*. He has recently completed two books, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press, 2015) and *Russia's Coercive Diplomacy: Cyber, Energy and Maritime Power* (Palgrave Macmillan, 2015). His main focus is the continuation of an empirical cyber incident and dispute dataset and Russian energy policies in post-Soviet space. His new book project uses content analysis to study the concept of state coercion in cyberspace.

Nazli Choucri, Professor of Political Science at MIT, works on different aspects of international relations, most notably on sources and consequences of international conflict and violence. Professor Choucri is the architect and Director of the *Global System for Sustainable Development* (GSSD), an interactive multi-lingual knowledge and networking system on sustainability and its complexity. She served as Principal Investigator of the MIT-Harvard project on *Explorations in Cyber International Relations*, a multi-year multidisciplinary collaboration. She is Editor of the MIT Press Series on *Global Environmental Accord* and, formerly, General Editor of the *International Political Science Review*. For many years she served as the Associate Director of MIT's Technology and Development Program. She has authored eleven books, including *Cyberpolitics in International Relations* (MIT Press) and over 120 articles.

Joe Burton is a lecturer in International Relations and International Security. He has a Ph.D. and Master of International Studies degree from the University of Otago and an undergraduate degree in International Relations from the University of Wales, Aberystwyth. Burton's doctoral research was on the NATO alliance. His research is currently focused on U.S. foreign policy, contemporary security issues, such as cyber security and energy security, and how states, non-state actors, international organisations and alliances are adapting to deal with new strategic challenges. He has published several reviews and articles in journals such as *Political Science* and *New Zealand International Review* and is co-editor of *More Power to the People? Public Participation in Foreign Policy* (London: Palgrave Macmillan 2011.

Paul F. Diehl is Associate Provost and Ashbel Smith Professor of Political Science at the University of Texas-Dallas. Previously, he was Henning Larsen Professor of Political Science at the University of Illinois at Urbana-Champaign. He served as President of the International Studies Association for the 2015-2016 term. His areas of expertise include the causes of war, UN peacekeeping, and international law. His most recent book is the co-authored *The Puzzle of Peace: The Evolution of Peace in the International System* (Oxford University Press, 2016).

Jon R. Lindsay is Assistant Professor of Digital Media and Global Affairs at the University of Toronto Munk School of Global Affairs. He is the author of China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (Oxford University Press, 2015), with Tai Ming Cheung and Derek Reveron, and his articles on cybersecurity and military innovation have appeared in *International Security*, *Security Studies*, *Journal of Strategic Studies,* and *Technology and Culture*. His current research includes a book on the impact of information technology on military power and a multi-institutional project on cross-domain deterrence. He holds a Ph.D. in political science from the Massachusetts Institute of Technology and an M.S. in computer science from Stanford University, and he has served in the U.S. Navy with operational assignments in Europe, Latin America, and the Middle East.

Review by Joe Burton, Victoria University[1]

In *Cyber War versus Cyber Realities*, Brandon Valeriano and Ryan C. Maness seek to dispel some of the fear and hyperbole that surround cyber attacks, arguing that the cyber threat has too often been overhyped. The book makes a valuable contribution to a still underdeveloped literature on cyber security and pushes back against a rising tide of mischaracterization, overstatement, and outright fearmongering about recent cyber disputes. Phrases like those used by former U.S. Defense Secretary Leon Panetta to describe a possible "cyber Pearl Harbor"[2] against the United States, elevated claims that computer viruses could be used as 'weapons of mass disruption,' and fears that terrorist groups and nation-states could use cyber attacks to cripple critical infrastructure seem to have become commonplace in the discourse around cyber security, and the authors warn us to be wary of the effects of this kind of securitization.

In this respect, the book adds to a body of scholarship that questions the actual impact of contemporary security threats, including John Mueller's *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats and Why We Believe Them*, which analyzes the exaggeration of the terrorism threat in the post-9/11 era; the article by Thomas Rid, "Cyber War Will Not Take Place," and the book by Rid with the same title, which argue that cyber war will not take place because cyber attacks are never in-and-of-themselves acts of violence; and Mary O'Connell's article, "Cyber Security without Cyber War," where she warns of the militarization of cyber security discourse and the negative impact that might have in developing effective responses to cyber security issues.[3] *Cyber War versus Cyber Realities* comes at an important historiographical juncture too, with considerable academic backlash against claims that social media was instrumental in the events of the Arab Spring, and in the aftermath of the Edward Snowden affair, which has revealed a massive accumulation of power over the Internet by national security agencies, arguably because of overwrought fears about terrorism. Indeed, the authors are part of a growing group of academics who are cyber skeptics and who question the role of information and communication technologies in international relations. This skepticism is welcome when considering the impact of new technologies on long-established patterns of international behavior.

This book takes a meticulous, quantitative approach to puncture some of the hype, using an extensive data set to analyze cyber incidents involving rival 'dyads' (pairs of states) over a ten-year period between 2001 and 2011. One of the central claims of the book is that the use of malicious cyber attacks by rival states does not normally alter the propensity for those states to cooperate with each other. In other words, cyber attacks do not often fundamentally harm relations between states and rarely lead to serious repercussions. States will

[1] This review was previously published on H-Diplo in a slightly different form in April 2016. Please see http://www.h-net.org/reviews/showpdf.php?id=44981

[2] Quoted in Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.", *New York Times*, 11 October 2012, available: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0, accessed 3 December 2016.

[3] John Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats and Why We Believe Them* (New York: Free Press, 2006); Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35:1 (2012): 5-32; Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013); and Mary O'Connell, "Cyber Security without Cyber War," *Journal of Conflict & Security Law* 17:2 (2012): 187-209. DOI: https://doi.org/10.1093/jcsl/krs017.

continue to cooperate even as they are targeted by the other state by cyber attacks. This finding appears to be borne out by recent events. Despite massive Chinese cyber espionage against the United States, for example, the two countries continue to cooperate in many areas in which they have core and shared interests. The September 2015 meeting between Presidents Barack Obama and Xi Jinping in Washington, D.C. led to an agreement to reign in criminal organizations using the Internet for cyber crime, even while both countries continue to subvert and survey each other's digital networks for political and military gain.

Perhaps the most important contribution of the book to cyber security debates is the discussion of how states appear to show considerable restraint in their use of cyber tools against each other, and this is corroborated by a useful analysis of a number of high-profile cyber attacks. The Russia-based attacks against Estonia in 2007, which the authors characterize as an exercise in cyber harassment rather than cyber war, led to a pattern of de-escalation by North Atlantic Treaty Organization (NATO) officials. Russia, too, they claim, exercised considerable restraint in using cyber means to respond to what was perceived to be a serious political insult (the removal of the Bronze Soldier, a monument to the Soviet 'liberation' of Estonia) and could have used much more forceful foreign policy instruments, including more damaging cyber attacks, conventional military means, or even energy disruptions. Restraint dynamics were also in evidence when cyber attacks were used, probably by Iran, against the oil company Saudi Aramco in 2012—the 'Shamoon' virus, which wiped thirty thousand hard drives. In that case, the Saudi government reacted by doing next to nothing and the attack had a negligible impact on already tense Iran-Saudi relations.

Why do states appear to exercise restraint in cyber interactions? First, the authors claim that there is a degree of cyber interdependence between rival states, particularly as the ability to attribute cyber attacks to specific actors has improved. Some degree of malicious cyber actions are also expected to occur by states and will be tolerated as part of the regular business of international relations, especially if they do not cross certain thresholds (at the most extreme end involving a loss of life). What the authors call "total cyber operations" remain off the table, as they are likely to lead to more serious consequences, including the destruction of infrastructure, significant collateral damage, significant economic losses, and even war. Cyber weapons can also be reverse engineered in a way that conventional weapons cannot, and this contributes to restraint around their deployment. Possible harm to civilians through collateral damage tilts the balance toward restraint dynamics in cyber conflicts and emerging norms of behavior in cyberspace also add to restraint between rival states in the cyber security sphere. Implicit in the argument of the authors is that cyber norms have already emerged, and can be seen in U.S. reluctance to use cyber attacks in Iraq in 2003 and in Libya in 2011. A further restraint dynamic relates to how cyber attacks might have the unintended consequence of dragging third parties into a conflict, a type of cyber 'entrapment,' a concept first established by realist alliance scholars, and now applied to the cyber sphere. Finally, the fear that cyber attacks could lead to a conventional response by states also creates a degree of restraint. Again, this seems to be a highly relevant observation. The U.S. government has explicitly acknowledged that all options are on the table in response to cyber attacks, including the use of conventional military force. NATO's cyber doctrine for the defense of its members takes the same position.[4]

The book also advances debates about international relations theory and cyber security, and the authors are critical of how realist notions of deterrence may create a tendency to develop offensive cyber capabilities so as

[4] For a detailed discussion see Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," *Defence Studies* 15:4 (2015): 297-319. DOI: http://dx.doi.org/10.1080/14702436.2015.1108108.

to be able to retaliate against cyber attacks, thereby fueling the sort of militarized approach to cyber security that the book is so critical of. The authors' observation is that cyber conflicts are more usefully seen as socially constructed, and linked to regional and geopolitical struggles. Cyberspace is often conceived of as a global network and one that defies boundaries—the ultimate transnational threat. But evidence to date suggests that most cyber disputes are intertwined with prior social and historical interaction between nation-states. Cyberspace may be a virtual realm in one sense, but it is also built on cables, servers, computer hardware, and digital infrastructure that is located in a still territorial, bordered world. Stuxnet, for example, was a symptom of decades of tensions between Iran, the United States, and Israel. It cannot be separated from a well-established pattern of destructive, antagonistic relations. The Bronze Soldier case is another illustrative example. The use of cyber attacks by Russian-based hackers was a response to a set of broader political and historical tensions with Estonia that stemmed from World War Two and beyond. The authors' placement of the empirical discussion and case studies within this constructivist framework fills at least some of the vacuum that exists in theoretical discussions of cyber security.

Are the authors right? Is cyber war being overhyped and, if this is the case, why? If it is, moreover, what impact is this having on the development of cyber security policy? Certainly there appears to be a massive industry built up around cyber security, which is looking to profit from people's fears about cyber intrusions. President Dwight Eisenhower's prophetic warning of the emergence of a military industrial complex does not seem fantastical in the context of the billions of dollars being awarded by the U.S. government for the safeguarding of digital infrastructure and the intrusive role that agencies like the National Security Agency have taken in cyberspace. Just as with the threat from terrorism in the post-9/11 environment, an excessively military response to cyber attacks, combined with a failure to develop a wide range of civil and criminal mechanisms, may lead to less effective policy. It may even, as the authors contend, endanger the stability of the international system, deny society the positive effects of the Internet, and corrupt the way the Internet itself operates. One hopes that these claims also turn out to be an exaggeration of what is possible if the Internet continues to be exploited by states for narrow self-interest.

If anything remains under-examined in the discussion of what constitutes cyber war it is the way cyberspace is interacting with other domains of warfare to give states an advantage on the twenty-first-century battlefield. The 2008 Russia-Georgia war is a case in point, where cyber attacks gave advancing Russian forces a significant tactical advantage. Cyber attacks are being used not only in land warfare but also against drones, in the naval domain, and even against space-based satellite systems. In this respect, cyberspace is emerging as an influential fifth domain of warfare. The fact that national militaries across the globe are investing heavily in this area of operations is not so easily explained away by the overhyping argument. Cyber attacks could also be seen as part of evolving patterns of information warfare used by both states and non-state actors to control the information environment. This is a potentially useful conception of cyber warfare that sits outside the approach utilized by the authors in this book and appears to be in evidence in Russia's use of hybrid warfare tactics in Ukraine, which have included cyber attacks against the Ukrainian government. Overall, however, the book is an essential contribution to the cyber security literature, and one that substantially advances the debate about the impact of cyber war as a term of reference and an empirical reality.

Review by Paul F. Diehl, University of Texas-Dallas

International-affairs scholarship and policy analysis is prone to faddish pursuits, often at the behest of contemporary events or purportedly new or rediscovered phenomena. The romance with environmental security concerns beginning in the early 1990s is illustrative. The idea that environmental changes would prompt resource shortages and other deleterious consequences that in turn would produce violent conflict was a novel notion at the time (this was prior to most of the climate-change debate). Early commentary on the matter was filled with unsubstantiated anecdotes, dire predictions, "using the future as evidence"[1]and little hard data. Initial studies[2] were enormously influential, but were later heavily criticized and in retrospect appear to have been misleading if not incorrect.

The possibility of so-called 'cyber wars' is a more recent phenomenon, but has generated the same kind of alarmist rhetoric and unsubstantiated assessments. What is unique about Valeriano and Maness's book, and what makes it path-breaking even though far from definitive, is that it is the first to provide both theory and empirical evidence to bear on the subject. In doing so it is likely to direct all serious research on the subject in the immediate and medium term.

This essay focuses on some limitations in the theory and data associated with the authors' arguments about cyber conflict. This should not, however, obscure the many strong contributions that are found in the work. First, Chapter 2 is a step forward in conceptualization, clarifying and moving beyond the overused term 'cyber war.' The better term 'cyber conflict' used by the authors is a more encompassing and yet clearer conceptualization. Later chapters that detail some of the cyber conflict incidents, such as Stuxnet, are good primers for non-experts and stand in stark contrast to superficial media coverage. Chapter 8 applies 'just war theory' to cyber conflict to derive a series of guidelines (see 201) for 'cyber justice.' The authors present a convincing, although perhaps idealistic, set of standards against which one should evaluate actions in cyber space.

Despite the book's many merits, there are a number of concerns on theory and data that undermine the credibility of the arguments made. Let us begin with the theoretical argument. The authors do a fine job of debunking the idea that deterrence theory can account for the empirical patterns of the relatively few (more on that below) and limited cyber attacks thus far. Deterrence does not work in the cyber context because of collateral damage, blowback, and other factors. That leaves room for an alternative explanation and the authors present a theory of restraint based on many of the same elements about cyber conflict that made deterrence unsuitable as an explanation.

The theory of cyber restraint is inherently narrow in a number of ways, often by the authors' own admissions. The theory (and subsequent) empirics in Chapters 3 and 4 are based on state-state interactions (Chapter 7 does address non-state actors). Even more restrictive, these are confined to 'rivalries,' long-standing militarized competitions between the same pairs of states such as India-Pakistan and Israel and her neighbors.

[1] Nils Petter Gleditsch, "Armed Conflict and The Environment: A Critique of the Literature," *Journal of Peace Research* 35:3 (1998): 381-400. DOI: https://doi.org/10.1177/0022343398035003007.

[2] Thomas Homer-Dixon, "Environmental Scarcities and Violent Conflict: Evidence from Cases," *International Security* 19:1(1994): 5-40.

One could criticize the authors for ignoring other contexts or rivalries (e.g., economic rivalries that might use cyber attacks for espionage), and indeed we do not know how frequently cyber conflict occurs in those settings. Rather, it seems appropriate to examine the theoretical argument only in the context to which it purports to apply, recognizing that other explanations might be needed for different situations.

How does cyber conflict fit into the context of rivalries? The authors argue that cyber attacks might stem from several motivations in a rivalry, involving strategies of cyber terrorism and cyber espionage. Most of these seem to come from a *realpolitik* orientation and several do not seem to map well with the goals and dynamics of certain rivalries. The authors argue that "the main reasons that a state would support cyber terrorism is to seek to equalize capabilities with a rival or to punish a rival sufficiently to produce a change in the target's behavior" (70). Taking the capability motivation first, the authors suggest state-sponsored terrorism is part of 'balancing' behavior. Cyber actions, according to the authors, might involve stealing technology (which is more espionage than terrorism), presumably by the weaker side. The tactic might also be used by the stronger state in order to arrest the development of a rising challenger. Both of these suggest that long term processes can be facilitated by cyber attacks. It is conceivable that massive, successful attacks might work toward those goals, but this does not make sense in the context of the theory here that is based on restraints and limited attacks. If the authors are correct in arguing that such attacks will be relatively infrequent and less severe, and I think they are, then such attacks are not likely to affect the capability distribution to any meaningful degree. The authors refer to this motivation as "misguided" (71) but this seems to be because of the risk of war from capability equality rather than the failure of the balancing strategy from cyber attacks.

A corollary to this argument is that cyber terrorism can serve as a tool in proxy battles (71), especially by weaker countries. There are a number of underdeveloped issues including connections between principal and agent in the attacking state. Some of the choice of tactic is purportedly designed to "hide goals and motivations" (71), but that makes it very difficult to distinguish incidents that are state-sponsored or directed from those attacks by hackers and other non-state actors.

The second motivation is for states to impose pain on rivals. This comes from an expectation that rivals are primarily concerned with "relative gains and losses" (52). Nevertheless, not all rivalries are the same. William Thompson and his colleagues[3] make a distinction between "positional" and "spatial" rivalries.[4] The former are those in which the states battle for stature or influence globally or in a regional context. Among such enemies (e.g., U.S.-China), imposing costs on a rival makes sense, particularly if there is great animosity between them.

Spatial rivalries are a different matter. These are primarily fought over territorial control (e.g., Ethiopia-Somalia). Spatial rivals occupy the same region; this makes sense as states do not often have disputes over borders and other territories that are of great distance from the homeland. The authors note (99, Table 4.10)

[3] Michael Colaresi, William Thompson, and Karen Rasler, *Strategic Rivalries in World Politics: Position, Space and Conflict Escalation* (Cambridge: Cambridge University Press, 2008).

[4] *Ibid* also reference "ideological rivalries" that contend over competing belief systems – these are likely to resemble positional competitions with respect to the desire to punish or inflict pain on an enemy. They are also less common than positional or spatial rivalries.

that three-fourths of cyber rivals are regional and almost all of these have territorial disagreements. How do cyber attacks assist states in territorial disputes? There is not a clear explanation in this work. It might be that such attacks can gain information about the opponent's military capability, strategy, and positioning vis-à-vis defending or potentially seizing the territory in question. Nevertheless, the motivation to inflict pain on a rival does not seem as purposive in this context as it might for positional rivalries. Attacking a rivalry with cyber tools also does not seem to get a rival any closer to acquiring a given territory; it is even less clear how a status quo state profits by a cyber attack against a rival claimant. For such rivalries, cyber conflict cannot be something that achieves what conventional military action might (71). Perhaps the limited utility of cyber conflict in territorial rivalries explains its limited use better than the authors' theory of restraint. That most rivalries are regionally-based and most have some territorial component[5] seems to indicate that regionalism is better understood as a fact of rivalry than a theoretically significant component of cyber conflict (65-70).

The same limited utility is evident in rivalry actions that seek to change a regime or remove a leader from power in an enemy state (66). There might be some reasons to use cyber attacks in rivalries, but they are unlikely to achieve the goals that are at the heart of the rivalry. Can one really believe that Gaza cyber attacks by Palestinians (66) against the Israeli leadership were designed for or would actually have removed that leadership? The argument on discrediting leadership is more believable, but still less likely to achieve the policy change that would be desired by the attackers.

More compelling as a motivation for cyber attacks is a rival's use of the tactic for espionage and related intelligence purposes. The goal there is to "steal, harass, or make known the ability to penetrate networks" (68). The first two are plausible, but the latter makes little sense for the same reason that deterrence does not operate: penetrating a network is likely only useful once, as the target will take adaptive actions to prevent recurrence. A useful line of inquiry might have been to focus on why and how cyber espionage could be a better tool for gathering information than conventional spying methods. Instead, the authors discuss how cyber espionage might contribute to "balancing" behaviors or to impose economic costs on a rival (69). This does not seem to comport with the term 'espionage' and does not necessarily explain why the attacks are limited; the analysis here appears to begin with restraint as an assumption (68) rather than an explanation for behavior.

One of the elements lacking in the theory is a consideration of dynamics and cyber defense. The explanation for limited attacks is almost entirely from the supply side. Yet states spend an enormous amount of money on protecting infrastructure from cyber attacks, and some of these efforts may prevent attacks from occurring or discourage some from trying. These will not show in the data (see more below).

Beyond theoretical concerns with rivalries, this work is likely to come under the greatest criticism in terms of its empirical base. The authors start with 126 rival pairs of states in which cyber conflict might occur. To identify cyber incidents, they used "the *Google News* search engine and also [combed] through reports, books, and testimonies of cyber incidents" (82). Over the period 2000-2011, the authors identify 111 "cyber incidents" and 45 "cyber disputes," which are aggregations of related incidents (231), within twenty rival pairs of states. Companies and organizations regularly claim thousands upon thousands of hacking and other cyber attack events every day. One study of U.S. companies alone found 160 *successful* cyber attacks per week in

[5] Gary Goertz, Paul F. Diehl, and Alexandru Balas, *The Puzzle of Peace: The Evolution of Peace in the International System* (Oxford: Oxford University Press, 2016).

2014.[6] Even though this book only examines state-state incidents, could there really be only just over 100 of these in a ten year period?!

The authors are innovative and meticulous in designing and implementing coding schemes for the incidents and there is not much to criticize after they have the list of incidents. Nevertheless, there are serious doubts that the authors have identified all or even most of the state-state cyber attacks. Ensuring that the list of incidents is accurate and complete is not only important for the validity of the conclusions derived from the statistical analyses, but more importantly for the theoretical argument, which depends on there being only a limited number of incidents. The authors are not unaware of this issue, but they seem to dismiss its importance: "We are confident that we have included in our data the most significant and the great majority of cyber actions that were capable of damaging relations between states" (82). They then go on to offer a number of caveats and then conclude with the justification, one has some merit, to be fair, that "it is the most comprehensive source of data and has been vetted by many investigators since 2011" (83).

The authors admit that the data only include what is "publicly known" (83). What is likely to be missing and how serious are such omissions? One could speculate that errors of omission are merely random ones and therefore the 111 incidents undercount actual incidents but are nevertheless a representative sample. This addresses issues with statistical inferences, but it does not alleviate concerns with overall incident frequency. It is also unlikely. There is little reason to suspect that those incidents that publicly reported have the same profile as incidents writ large. There are several possibilities to suggest that the number of reported incidents is much less than actual ones.

We do not know for sure how many attempts at cyber attacks have occurred and even secret intelligence documents could miss undetected attempts. One might first guess that only attempts that are of a certain magnitude receive public attention or are revealed by sources to the public. This goes beyond the threshold of "capable of damaging relations between states" referenced above. If this is true, it is less detrimental to the authors' arguments in that it supports the contention that cyber attacks will be limited; that is, the missing cases are all low-level ones and their inclusion doesn't change the argument about restraint. More seriously is the likelihood that only attacks with some measure of success get reported. There might be numerous incidents that are repelled because of problems with the attack or the effectiveness of ever evolving cyber defense (see point above). The ratio of successful attacks to attempts in the private sector is suggestive of this. In addition, public source material, especially that derived from news outlets and publications, has a Western orientation or bias. That is, it is much more likely to report incidents of China attacking the U.S. (less so the reverse) than incidents involving minor powers on other continents; this is an inherent problem for any data set, not merely on cyber conflict.

When all is said and done, the authors do not know how bad their problems with case identification are and frankly neither do its critics. Is there a better way of data collection? There probably is not, at least from open sources. This fact indicates that there is not necessarily some flaw in the authors' collection efforts, but neither does it allay the concerns that have been raised above.

[6] Riley Walters, "Cyber Attacks on U.S. Companies in 2014," Heritage Foundation Issue Brief No. 4289, 27 October 2014, http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014, accessed on 18 February 2016.

Cyber conflict is a fascinating new topic and it calls for good, systematic research based on theory to understand it. Valeriano and Maness have made an impressive first effort in this direction. Future research will hopefully refine their theoretical formulations and move beyond the narrow orientation on state rivals. Progress in establishing a valid data base, however, is a more daunting task and scholars and policymakers might need to rely on case studies rather than large N assessments.

Review by Jon Lindsay, University of Toronto

Popular discussion of computer network security has long been dominated by technical analysis, media sensationalism, and alarming warnings from public officials about digital Pearl Harbors. A handful of university press titles by international-relations scholars offer a more measured and often skeptical perspective.[1] Brandon Valeriano and Ryan Maness provide a noteworthy addition to this emerging academic counterpoint to the conventional wisdom. Whereas most assessments of cyber threats rely on a few qualitative case studies and deductive argumentation, the authors provide the first multi-method empirical approach.

Cyber War versus Cyber Realities aims to tamp down a "fear based process of threat construction" (2) and raise the level of scholarly rigor in the debate about the impact of computer security on international security. These are laudable ambitions, and the book ably highlights a number of desiderata for any rigorous study of this understudied topic. First, the authors wade into an important policy debate and seek to identify the assumptions and opportunities for scholarship therein. Policy relevance is refreshing in a discipline that too often eschews it. Second, the book does not take the word of technologists for granted. Just because something can happen does not mean it will. Third, in looking beyond the technology, the authors inquire into the political economic incentives actors may have or lack to employ serious attacks. Fourth, the authors aim to develop a deductive theory on the utility of cyber war and use it to infer testable hypotheses about the distribution of conflict behavior in cyberspace. Fifth, the authors employ a multi-method empirical strategy to test their ideas, using an original dataset of international cyber conflict between rival states and qualitative studies of recent cases (the 2007 denial of service attacks in Estonia, the 2010 Stuxnet attack in Iran, and the 2012 Iranian retaliation on the oil company Saudi Aramco). Finally, Valeriano and Maness seek to ground their findings in a normative framework, cautioning against over-militarizing cyberspace and advocating for efforts to improve 'cyber hygiene' in organizations of all kinds. Scholarship that delivered on all of these goals would do much to improve the quality of debate about cybersecurity.

Valeriano and Maness do an important service to the field in elevating the conversation about cyber threats, yet their analysis also raises some questions that deserve closer scrutiny and should spur further research. They offer an unwieldy theory of "cyber restraint" in Chapter 3 that combines or conflates a number of different mechanisms (see 61-64) that may or may not account for the non-use of cyber weapons. Some of these claims appear to be specific to the technology. For example, they claim that malware use creates a proliferation or blowback risk if other actors repurpose the code, and they also claim that malware exploits, once revealed, are likely to be patched by the defender. Yet if malware is easy to patch, why is it a proliferation risk? Other claims are not specific to information technology but concern the use of force of any type, e.g., the idea that twenty-first century actors are invested in globalization and thus seek not to destabilize the system (63). The authors repeatedly argue that actors fear military retaliation for extreme attacks, but this point appears inconsistent with their skepticism about deterrence (e.g., 54-61). It is unclear why 'restraint' is an alternative to 'deterrence' when several of the mechanisms the authors highlight are rooted in concerns about denying

[1] These include, *inter alia*, Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001); Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007); Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge, 2008); Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013); Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (Lincoln: Potomac Books, 2015).

effects, suffering punishment, or otherwise expecting the costs of action to outweigh the benefits, which are the building blocks of deterrence theory.

There is no discussion of whether these different mechanisms are mutually exclusive and collectively exhaustive for 'restraint,' whether some might operate more strongly than others or only under particular conditions, whether they might be in tension under other conditions, or whether they should fail altogether under some circumstances. Some of the assumptions they leverage are contested in the international-relations literature, notably the claim that globalization and interdependence reduce conflict propensity.[2] Others are rooted in quite different realist or social constructivist paradigms. For instance, they assert that "cyber actions are a sacred taboo that must not be violated" (63), but provide little evidence that cyber actors are worried about public opinion or moral opprobrium about the specifically cyber nature of the means of attack—indeed, many actors may believe that nonlethal and sanitary cyber effects are preferable to kinetic destruction on both moral and consequentialist grounds. The notion of a cyber taboo may be explained by the operational challenges of cyber attack or by strategic disincentives, but the authors lump all of these together in their theory. Future work remains to be done in more precisely specifying and testing the fine grained mechanisms driving or restraining various types of cyber conflict.

The empirical section is the most novel part of the book. It provides some evidence to back up claims about how states in enduring rivalries show some restraint in their publicly reported cyber interactions. The regionalism of attacks, except for those involving the U.S., is a particularly interesting finding given the rhetoric about the globalization of cyberwar. It is plausible, even likely, that new data sources will back up their findings of many low intensity cyber operations and few of great consequence. Yet the authors might have exercised some more 'restraint' in their claims drawn from these data. Their dataset of media reporting from 2001-2011 includes episodes of both espionage and attack, coded at different level of intensity. It would be surprising if targeted espionage, financial crime, hacktivist protest, and military cyberwarfare were all governed by the same incentives and constraints, so why should they all be in the same dataset? This conflation is especially problematic for espionage, which tends to be self-hiding, and thus we should not expect the most sophisticated and successful operations to emerge on the public radar. A state might enjoy considerable advantages through hacking that might never come to light in the open media. We would know far less about the extent of U.S. National Security Agency cyber exploitation without the 2013 Snowden leaks. (Incidentally, Edward Snowden receives no mention in the book apart from "revelations of the NSA's activities" on page215. This is not an artifact of publication date since the authors include citations to 2014 sources. Snowden very much changed the public debate about the art of the possible and the extent of the actual in cyber operations.)

Furthermore, the restriction of cyber events to rival state dyads excludes many important interactions between states and their populations or anarchists and their states. China's aggressive information control strategy

[2] John J. Mearsheimer, "The False Promise of International Institutions," *International Security* 19:3 (1994): 5-49; Robert O. Keohane and Lisa L. Martin, "The Promise of Institutionalist Theory," *International Security* 20:1 (1995): 39-51; Kristin M. Lord, *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security, Democracy, or Peace* (Albany: State University of New York Press, 2007).

includes digital disruption and physical arrests of dissidents identified as online threats.[3] Also excluded is potentially consequential battlefield use of cyber operations (for intelligence exploitation of insurgents as well as manipulative information operations to shape combat outcomes) which, according to anecdotal reporting, appear to have been considerable force multipliers for U.S. Special Operations in Iraq and Afghanistan.[4] It is understandable that these irregular uses would be excluded in the authors' research design for rival dyads, yet they should be more forthcoming about the limited ability of their empirical strategy to test the generality of the theory.

A data collection cutoff is inevitable and necessary for any research endeavor. The authors' dataset ends at 2011, but the world of cybersecurity moves fast and some of the most interesting developments have occurred after 2011. The Stuxnet family has expanded to include Flame, Gauss, Duqu, and Equation, revealing a lot of sophisticated U.S. functionality in the field. Chinese penetration of the U.S. Office of Personnel Management has raised questions about whether some espionage is simply too broad or too damaging to be tolerated in the same way as in the past. In addition to Stuxnet, disruptive attacks now include North Korea's wiping of Sony networks in 2014, a mysterious outage at a German steel mill in 2014, a massive Chinese denial of service attack against dissidents leveraging U.S.-based cloud infrastructure in 2015, and the sophisticated Black Energy outage in Ukraine in late 2015. All of these events exhibit some degree of 'restraint' under one or another of the explanations offered by Valeriano and Maness, to be sure. Yet these events also suggest, to many observers, a worrisome trend of increasing use and perhaps a weakening of a 'taboo' that probably never existed. At the same time, innovation in the global information economy continues unabated, with developments in mobile computing and the internet of things that were unimagined in 2011, raising questions about whether any cyber-specific aspects of their theory are sensitive to such technological changes. Many productive information technology innovations seem to be occurring in tandem with the supposed militarization of cyberspace, so it is entirely possible that 'securitization' is actually reinforcing efficient economic and social exchange, not undermining cyberspace as the authors fear. Again, more fine-grained conditional theory and more careful identification of empirical variables is needed to provide a satisfactory explanation for the distribution of cyber conflict.

The study of war and especially major war is always a study of rare events. Lots of military capability exists that is used only rarely, or is most useful when it is not being used. There has never been a thermonuclear war, and yet scholars and policymakers have found much of strategic, political, and organizational interest to study. Moreover, theoretical precision about all the nuclear wars never fought—why some force structures are more destabilizing than others and what net assessment tells us about the prospects of crisis bargaining—has arguably played an important role in ensuring that the chance of nuclear war remains low. Valeriano and Maness are on firm ground in arguing that low-level cyber attacks are part of the normal repertoire of strained relations between international rivals, or in pointing to restraint in historical events, but they offer little comment on the conditions under which cyber weapons might constitute or catalyze a more dangerous escalation. One need only look back to CANOPY WING, an alleged U.S. electronic warfare program aimed

[3] Ronald Deibert et al., eds., *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics* (Cambridge: MIT Press, 2012).

[4] Shane Harris, *@War: The Rise of the Military-Internet Complex* (Boston: Houghton Mifflin Harcourt, 2014).

at Soviet nuclear command and control in the later Cold War, to appreciate the disruptive potential of modern cyber methods in some scenarios.[5]

Valeriano and Maness frame their approach as "a clear middle path" of "cyber moderation" between the extremes of hyped-up cyber revolution and "cyber skepticism" that there will be no cyberwar in the future; in this *via media*, "Cyber conflict will occur, but the conflicts themselves will be trivial, will not result in a change in behavior in the target, and will largely be regional cyber incidents connected to traditional international issues at stake" (40). Later they assert that "cyber operations overall tend to be futile" (219). The reader might be forgiven for believing that Valeriano and Maness are firmly in the skeptics' camp. The question is whether their dismissal of official concerns in capitals around the world as militarism and hype is warranted or premature. An empirical study of airpower before WWII would have found an absence of evidence of airpower's ability to damage industrial economies and might reasonably have concluded that aviation would be limited to a signaling, observation, and transportation role. There is already enough evidence to support a prediction that cyber means will play an important role supporting any future military operation in a major war (which is rare for reasons that have little to do with cyberspace, but nonetheless is worrisome for the health of many things other than cyberspace). We simply do not know at present what a cyber-intensive military conflict would look like, just as we really do not know, thank goodness, how a thermonuclear war would unfold. There is a place for theory, models, and experiments that take seriously the potential for serious cyber operations.

Valeriano and Maness have done real service to the field by taking cyber hyperbole down a notch and highlighting the need for better theory about and empirical evaluation of cyber conflict, even if they will not have the last word on the topic. It is to be hoped that more scholars will add to the promising beginnings of this literature. Rightful skepticism of alarmist cyber hype need not lead to premature dismissal of real conceptual and practical challenges. Cyber conflict has the potential to highlight new puzzles in political theory and wicked problems in public policy.

[5] Benjamin B. Fischer, "CANOPY WING: The U.S. War Plan That Gave the East Germans Goose Bumps," *International Journal of Intelligence and CounterIntelligence* 27:3 (September 2014). DOI: http://dx.doi.org/10.1080/08850607.2014.900290.

Author's Response by Brandon Valeriano, Cardiff University and Marine Corps University, and Ryan C. Maness, Northeastern University

What Have We Done? More on Cyber Realities

We embarked on the project that eventually resulted in *Cyber War versus Cyber Realities* back in 2010 because there was a clear gap in the field between the discourse on the future of war and empirical evaluations of the domain of cyberspace. Our book was the first step in our project to alleviate this gap and push the field in a new direction. We thank the reviewers for their evaluation of our efforts. Seeing our work laid out in such a way is flattering and makes the mammoth effort of this research appear to be worthwhile. Here we offer a few notes of context, respond to a few concerns by the forum members, and note where our future research is headed.

The Rivalry Context and Beyond

Valeriano's first field of focus was on rivalry, so the natural question we began with was how modern rivals would engage on the technological battlefield. If anyone would utilize cyber capabilities, it surely would be rivals who would do anything and everything to harm their enemy.[1] It seemed at the time to be a simple conjecture, but information was sparse and our initial case studies on the Russo-Georgian and the Iranian-U.S. dyad brought more questions than answers, which is why we embarked an effort to quantitatively analyze the content of cyber conflict interactions.[2]

As many might know, constructing a dataset is an enormously difficult proposition that more often than not leads directly to failure. Our effort has been difficult but fruitful; our data collection stopped in 2011 once we submitted our article the "Dynamics of Cyber Conflict" for review in early 2012.[3] Since then we have expanded the data to include all rival cases up to 2014 with a greater focus on outcomes. We continue to build on this data and now are in the process of applying for the funding required to collect data on all states, non-state actors, and also to utilize data-scrapping methods to ensure reliability and comprehensive coverage in our continued data collection efforts.

The Utility of Cyber Security Incident and Dispute Data

All data is a work in progress and we recognize this. We have been particularly careful to provide an open data source with very specific coding rules in order to share our efforts with the field. As of yet, we do not know of any significant missed incidents and would have loved to have found evidence of more incidents that we

[1] Brandon Valeriano. *Becoming Rivals: The Process of Interstate Rivalry Development* (New York: Routledge, 2013).

[2] Brandon Valeriano and Ryan C. Maness, "Persistent Enemies and Cyber Security: The Future of Rivalry in an Age of Information Warfare" in Derek Reveron's *Cyberspace and National Security: Threats, Opportunity and Power in a Virtual World*, (Washington, D.C.: Georgetown University Press, 2012): 139-158.

[3] Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011", *Journal of Peace Research* 51:3 (2014): 347-360. DOI: https://doi.org/10.1177/0022343313518940.

could have coded, but we did not. As Paul Diehl notes, a U.S. company might suspect 160 successful cyber-attacks per week, and the U.S. government has noted millions of attempts each day, but these claims do not stand up to empirical verification and include noise that is prevalent in cyber security claims. Automated processes often seek to exploit loopholes and vulnerabilities, thousands of users each day search for weaknesses in defenses in order to discover zero-day exploits and claim bug bounties, but these actions are beyond the scope of our analysis because we are only considering actual attacks launched by state-based actors seeking to alter the foreign policy landscape (at this point).

To be clear, for the book, we code all rival state-initiated cyber incidents and disputes from the years 2001-2011. State attribution must be verified by at least two sources verified by government statements, policy reports, internet security firm reports, or white papers from software security firms. Variables coded include cyber method (Vandalism. DDoS, Intrusions, Infiltrations); interaction type (nuisances, defensive counters, offensive strikes); Target type (private sector, government non-military, government military); severity (based on an ordinal scale); damage type (direct and immediate, direct and delayed, indirect and immediate, indirect and delayed); and initiator objective (disruption, espionage, coercion).[4] Each cyber incident could involve thousands, even millions of bombardments and last for hours, days, or even weeks. A cyber dispute may contain anywhere from one to numerous cyber incidents and take place during a continuous time period. Differing from Jon Lindsay's assessment, we do not code financial crime, hacktivist protests, or espionage unless these are state-based actions launched in the context of a rivalry.

We think Diehl hits the nail on the head most when he says "we over count success" since this is the reality of most data collection efforts. For something to be witnessed in cyber security, the opposition must try to do something and be recognized for their attempt. Failure in the sense that no one notices the action in the first place is beyond the scope of our analysis since we are examining the impact of cyber actions. If nothing actually happens, then what can we measure, but more importantly does the target even know and alter its behavior?

The question we are focused on now is the efficacy of cyber actions. We do not only count successful actions that result from cyber action, as our data is more a function of observable impacts and success in action is a variable to be examined. This is the heart of our new work on cyber coercion where we now seek to examine the success or failure of cyber actions, suggesting that coercive attempts often fail but espionage and disruption events manage to make impacts.[5] This would answer Diehl's question about how cyber actions help in territorial disputes. They do not, and since espionage and disruption might not be useful for such disputes, we only note that the context of cyber actions often occurs under the cloud of traditional foreign policy disputes, suggesting that the conflict only continues a new domain. This is often because it is a sign of expressing protest or dismay but not necessarily seeking to change the situation. Thus effectiveness of cyber actions is a question to be examined.

Deihl's concern with our large-N cyber security research is a bit surprising for those coming from the conflict processes community where he has been a leading light in the Correlates of War community. This is the

[4] For more detailed explanations of variables, see our codebook at http://drryanmaness.wix.com/irprof.

[5] Benjamin Jensen, Ryan C. Maness, and Brandon Valeriano, "Cyber Victory: The Efficacy of Cyber Coercion," Working Paper, 2016.

heart of our work (rightly dedicated to J. David Singer) since single case studies are problematic in that scholars can estimate large effects on what might be outliers or minor incidents. That the Stuxnet virus has become the World War I of the cyber security community has not escaped notice. Everyone has a different estimation and evaluation of Stuxnet, yet this is only one case and we need more information to make judgements on such an important issue. Diehl is right to note that we need more of a conception of the defense and we will build towards this in creating a dataset of cyber capabilities that includes offensive, defensive, and societal conceptions of cyber security. We continue to build our data and hope that others will join us on this journey that is far from complete.

Did we get all the data and include all the cases? For now, we note that we just have a sample of the rivalry population but this is the population of the most interest since these are the most dangerous dyads. We therefore believe that we have a representative sample of the important events in the cyber security landscape and will continue to build on this data as time goes on, expanding to non-rivals and non-state actors alike. We have been very clear from the start that this is the data on which our book is based. We do not overestimate our claims, as Lindsay's review seems to suggest we do.

Lindsay does fault us for failing to include the Edward Snowden revelations of 2013, noting they changed the cyber security debate dramatically. To us this is an empirical question that requires us to analyze the data. That we have 2014 citations does not mean that we could have updated the data for a 2015 release date. The reality is that we submitted the first version of this manuscript in 2013 and were allowed to revise the draft by mid-2014 (there was an eight-month turnaround time for publication) but this revision did not extend to a new version of the data because creating data is an extensive effort that requires verification and reliability checks. We are in the process now of releasing data that extends to 2014 for all rival states, but this effort took us quite a few more years and is not something that can be done on the spur of the moment. Certainly the Snowden releases did add a few data points for our more recent work, but in the context of rivalry relations this was just more of the same in regards to competition between China and the United States. The more worrisome issue of cyber espionage between friends and non-rivals alike will require a more comprehensive data update as well as new theoretical work.

Theorizing about Cyber Restraint

We disagree with Lindsay on the nature of cyber deterrence. The term does not fit the landscape of cyber actions, as Sean Lawson and many others note, with a term like cross domain deterrence being more appropriate as Jon Lindsay and Erik Gartzke use in some of their developing but as of yet unpublished research.[6] For us, cyber deterrence is problematic in that it suggests single-domain responses, forgets the foundation of deterrence is on defensive actions and survival – conditions often absent in cyber security, and becomes infinitely more complicated when threats are often not communicated because action implies disclosing abilities, not to mention the attribution issue.[7]

[6] Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology and Politics* 10:1 (2013): 86-103. DOI: http://dx.doi.org/10.1080/19331681.2012.759059.

[7] Martin C. Libicki, *Cyberdeterrence and Cyberwar.* (Washington: RAND Corporation, 2009).

For these reasons we moved towards articulating the concept of cyber restraint as the condition that operations in the domain. This is an inductive theory, building from our earlier book chapter in 2012, not a deductive theory with assumptions, as Lindsay suggests. We make no assumptions but only dissect the reasons restraint might be in operation. These reasons need empirical investigation and we clearly could not investigate them all at this time.[8] We do want to make clear we see no inherent contradiction in the idea that the use of cyber weapons will be limited because of the one-shot nature of the weapons. For us the danger is not with proliferation, as Lindsay inaccurately suggests, since this would be an oxymoron if we are talking about zero day exploits, but rather that attack options will be limited once exploits are made known. Nor is the fear of retaliation inconsistent with restraint. We are discussing the empirical outcome of restraint versus the fear based projections made in the abstract. That there can be a difference between what is observed and what is feared is appropriate. Restraint is not acting based on fear of the unknown, whereas deterrence invokes fear of the known to prevent action.

We believe the term restraint is accurate of the current cyber era when we consider the great caution that states have utilized in using cyber weapons. Diehl and Lindsay both point out that restraint is limited when the target is non-state actors. But, as we discuss, this term only applies to state-versus-state conflict, and not necessarily to the actions of proxies or terrorists, so actions like the U.S.-versus-insurgents in Afghanistan would require a new theoretical lens. Concerning non-state initiators, restraint may be especially absent yet the capabilities of such actors are dwarfed by states. We agree with Diehl that balancing behavior in cyberspace will not actually succeed, but it still does motivate the action of weaker actors when they consider cyber tactics to equalize with the enemy and we intend to look at capability distribution questions as our work continues. We do agree with Lindsay that more theoretical work needs to be done on the mechanisms restraining cyber action and see great hope in the work now being done by scholars looking at such questions, in addition to scholars examining what my predict cyber action.

Are We Right?

As Joe Burton points out, the central question is whether we are right. For now, we believe that we have accurately captured the emerging dynamics of the cyber domain as it stands. We do not, as Lindsay suggests we should, speculate on the nature of escalation in cyberspace because we are focused on empirical evaluations and find little evidence of cyber escalation or spillover conflicts as argued in the chapter 4 of the book. Furthermore, preliminary analysis of the updated dataset that covers 2000-2014 has seen a relative rise in cyber espionage and disruption campaigns and a reduction in the use of targeted cyber weapons, implying that states are learning about the utility of cyber actions as well as restraining themselves out of fear of escalation.

Cyber operations in Russia's annexation of Crimea are an important case for many in the field since they exhibit the limited use of cyber options, as digital means were generally used for disruption of communications and the manipulation of information but there was no outright cyber combat, which

[8] The deductive component of cyber restraint, to be clear, is the normative elements of ethics and concern for collateral damage which would require a different research design to investigate. The field clearly needs more investigative work on the beliefs of decision-makers as they are confronted with cyber-attack options.

suggests that cyber conflict is not the harbinger of future warfare.[9] If Russia (a bull masked as a bear in the international system) is restrained and limited in its actions, what can we say about the future of cyber warfare?[10] Surely computers will be part of all future conflict, but computer-aided network violence and malice is a much different thing than computers causing physical destruction and becoming weapons of harms.

We are now interested in many developing questions focused on three areas 1) extending our data outside the rivalry domain to all states and non-state actors to understand how different contexts influence action 2) the impact and reaction to cyber threats and conflict in the population and society, and 3) the utility of cyber force and power. All these questions motivate our future explorations and suggest that *Cyber War versus Cyber Realities* is only a small part in a larger whole that is the cyber security field as it connects with the fields of Conflict Processes, Strategic, and Security Studies.

Our turn towards evidence and context in cyber security is important, but we hope that many more come after to develop new and novel descriptions of this domain utilizing evidence, discourse analysis, and advanced scientific techniques; and move us away from the hyperbole that often characterizes discussions of cyber security issues.

[9] Kenneth Geers, Editor, *Cyberwar in Perspective: Russian Aggression against Ukraine.* CCD COE, 2015.

[10] Ryan C. Maness and Brandon Valeriano, *Russia's Coercive Diplomacy: Energy, Cyber and Maritime Policy as New Sources of Power* (London: Palgrave Macmillan, 2015).