Beyond Hyperbole: The Evolving Subdiscipline of Cyber Conflict Studies

Dr. Aaron F. Brantly

Hardly a day goes by without a cyber-related news story coming across the wires, yet the International Relations (IR) subdiscipline of cyber conflict studies has yet to meaningfully impact a wider discourse. This article examines the impact of five recent scholarly works on the evolution of this subdiscipline that, while quite popular within the general population, remains largely ignored by the broader International Relations (IR) scholarly community. The article dissects the strengths and weaknesses of these works and their place in the evolving literature by a generation of scholars who are moving debates beyond hyperbole. By highlighting cyber conflict studies to date, this roadmap hopefully will help to advance the study of cyberspace within the IR cyber community.

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven: Yale University Press. 2017. 319 pp., $35 Hardcover (ISBN: 978-0300220230).

Buchanan, Ben. *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations*. New York: Oxford University Press. 2017. 290 pp., $35.62 Paperback (ISBN: 978-0190665012).

Valeriano, Brandon, Jensen, Benjamin M., & Maness, Ryan C. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press. 2018. 305 pp., $34.95 Hardcover (ISBN: 978-0190618094).

Mandel, Robert. Optimizing *Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks*. Washington, DC: Georgetown University Press. 2017. 289 pp., $64.95 Hardcover (ISBN: 978-1626164123).

Perkovich, George, & Levite, Ariel E. *Understanding Cyber Conflict: 14 Analogies*. Washington, DC: Georgetown University Press. 2017. 310 pp. $89.14 Hardcover (ISBN: 978-1626164970).

The sky is falling, or so it seems when watching the nightly news, newspapers, or many social media pundits. Cyber conflict appears to spell doom and gloom, and little can be done. The bits, bytes, and interwoven networks once jokingly (or not) referred to as "tubes" and meant to liberate and usher in a new era for humanity seemingly are now being turned against us in new and vicious forms of conflict.[1] Ironically, academia has been partially complicit in the hyperbole engulfing contemporary conversations on cyber conflict. The subdiscipline within security studies focusing on cyber security and conflict

Dr. Aaron F. Brantly is an Assistant Professor of Political Science at Virginia Tech (PhD, University of Georgia, 2012; MPP, American University, 2008). Dr. Brantly is the director of the Tech4Humanity Lab at Virginia Tech. His research focuses on national security policy issues in cyberspace including big data, terrorism, intelligence, decision-making and human rights. He is the author or editor of four books *The Decision to Attack: Military and Intelligence Cyber Decision-making, US National Cybersecurity: International Politics, Concepts and Organization,* and *Cybersecurity: Politics, Governance and Conflict in Cyberspace and The Cyber Deterrence Problem.*

has been advancing rapidly in recent years. The field has progressed substantially from the days when John Arquilla and David Rondfelt penned their work *In Athena's Camp:Preparing for Conflict in the Information Age in 1997*.[2] Since then the number of Internet-connected devices has grown exponentially, with Internet users now exceeding 50% of the global population. The last two decades have seen a bevy of new works addressing the growing concerns surrounding what is now ubiquitously, albeit unhelpfully, termed "cyberspace."

Over this time frame, the technical and organizational realities of cyberspace have changed dramatically. The US elevated cyber to warfighting domain status, and the associated force structure is now an independent combatant command headed by a 4-star general. Concurrently, the US has worked with NATO to establish cyber capabilities (a) in Tallinn, Estonia in response to Russian aggression against this small NATO member in 2007, and more recently (b) at an operations center in Brussels. Many, if not all, advanced countries are now developing cyber capabilities across their military, intelligence, and civilian sectors. The last two decades have also witnessed the theft of billions of dollars of intellectual property by state-sponsored hackers and cyber-attacks to manipulate elections, degrade nuclear facilities in Iran and North Korea, attack dams and industrial steel production, and briefly take power grids offline, to highlight some of the many of incidents that have taken place.

The rigor and depth of cyber conflict research is growing, yet there remains much hyperbole and lack of technical understanding. It is into this gap that the authors reviewed in this article attempt to delineate the mechanisms of conflict within cyberspace. Much discussion and scholarly work on cyber conflict is new, but much began far earlier.[3] Substantial research on cyber issues occurred well before 1984, when William Gibson coined "cyber" as it is commonly known today. Scholars such as Norbert Weiner established early radical

concepts of what the future of human-machine interaction would look like and actively used the word "cyber."[4] Wiener, along with John von Neumann, who invented modern computer architecture, were far ahead of their time in foreseeing the power and potential impact of computers on society, preceding even the Internet and its rise to global prominence. The rapid changes transpiring since the Cold War's end have prompted a global communications and information transmission substrate[5] that cuts across nearly every attribute of human existence. Chris Demchak and Peter Dombrowski define this substrate as a socio-technical system upon which modern world order is built.[6] The value and significance of cyberspace is difficult to assess and its full impact on international politics is obscured by its deep penetration into everyday life.

The importance of cyberspace to world order has been long debated. Among works that have greatly impacted the study of cyber conflict were those by Martin Libicki, an economist, who established an informed approach in a series of RAND-produced reports for the U.S. Air Force, including *Conquest in Cyberspace: National Security and Information Warfare,*[7] and *Cyberdeterrence and Cyberwar*.[8] Beyond Libicki, scholars such as Greg Rattray, Franklin Kramer, Stuart Starr, and Larry Wentz produced detailed analyses and edited volumes that confirmed why cyber conflict studies are critical to military audiences.[9] Myriam Dunn Cavelty extended the field to critical studies in her dynamic 2009 volume C*yber-security and Threat Politics.*[10] This flurry of early activity was measured in tone and sought to build a field based on informed study, without hyperbole.

Yet it was a 2010 book by former White House official Richard Clark and Robert Knake that catapulted the debate forward.[11] This book was aggressive, hyperbolic, and caused substantial ripples within the national security establishment. Yet, the rhetoric inspired substantial backlash within academia and spurred scholars such as Thomas Rid and Erik Gartzke to pen articles seeking to orient, both linguistically and theoretically, the impact of cyber conflict within the broader IR canon.[12] These works inspired the first set of conceptual volumes on cybersecurity, including the first two data-driven analyses of state behavior in cyberspace, by Brandon Valeriano & Ryan Maness,[13] and your author (Aaron Brantly).[14] They also inspired the first major analyses on cyber conflict cases by Jason Healey.[15] Combined, the literature up until the works discussed here sought to address arguments within a developing IR/security studies framework.

This is the historical backdrop for authors writing today, who face the challenge of establishing the relevance of their works to the broader discipline of IR, and, in particular, security studies. They also must address the challenges evident within the existing cyber conflict literature. These works must also capture the fine line between understating and hyperbolizing the importance of cyber conflict to security studies. Because cyber security and conflict issues often are poorly understood, authors sometimes are tempted to make claims based on public statements by government officials whose understanding of the nuanced realities of cyberspace, at best, is marginal. These claims, in contrast to these made about nuclear weapons

in an earlier era can, and often do, exceed reality. This article attempts to highlight how new works on cybersecurity can build upon existing literature and theory and add new concepts to the fields of IR and security studies without hyperbole. This analysis of the impact and effectiveness of arguments in advancing the evolving subdiscipline concludes by identifying three tracks in which works on cyber security and conflict fall.

Works examined below were chosen because they address the importance of theory to the evolving discipline of cybersecurity and conflict studies within a broader security studies subdiscipline. They offer five approaches to the study of cyber conflict, providing a cross-sectional view of a developing field of inquiry. Each offers a means of conceptualizing analytical leverage of a subdiscipline in constant flux. Some works attempt to build upon the past, while others appear wholly disconnected from existing literature. The central premise of this article is that, irrespective of the theoretical approach, new works that emerge from a core heuristic and expand knowledge within a novel domain of interaction via auxiliary hypotheses will better illuminate the security challenges of cyberspace, and also its broader security concepts. This does not mean that works that do not address theory are not valuable; they are, but their value added is derived through elevation of the discussion within the scholarly community, or the cataloging cases through informed commentary. Each work examines the challenges arising in cyberspace via a differing theoretical or methodological lens, each encompasses current relevant concerns, and each emphasizes state actions in cyberspace.

LEAVING THEORY BEHIND AND ELEVATING DISCUSSIONS

Lucas Kello in his 2017 book, *The Virtual Weapon: The International Order*, builds on his 2013 piece in *International Security*, with a discussion of the significance of conflict arising within cyberspace.[16] He provides robust examples of the many challenges associated with cyberspace and focuses on problems caused by particular state actors such as Russia and China while touching upon more complex issues surrounding policy, law, strategy, and tactics of offensive and defensive behavior. Kello begins his analysis aiming to establish a unifying theory around cyber conflict. He attempts to do this by robustly pushing back at critics of the subfield and advancing a distinct framework that elevates the position of cyber security and conflict. His approach is controversial and positions cyber security and conflict as something fundamentally distinct from conventional IR paradigms.

Kello diverges from more conventional theoretical approaches at the outset when he strikes swiftly against conventional IR theories: "Skeptics invoke that unfailing servant of intellectual reactionism in the field of international security studies: Carl von Clausewitz."[17] He then accurately argues that security studies have a substantial bias towards physical over virtual interactions.[18] Kello then turns to the hyperbole that dominates the balance of his book by comparing nuclear weapons and virtual ones. He writes:

> Some observers regard the advent of cyberspace as the greatest transformation in security affairs since the invention of nuclear arms. For all the symbolic enormity of the explosions over Japan in 1945, this comparison is wrong: it inflates the relative significance of the atomic bomb.
>
> ...both were driven by new technology and both were consequential in their own times. But the transforming potential of the cyber revolution is on a scale much deeper and broader than that of its older technological cousin.[19]

Kello's work is important to the literature on cyber conflict. Yet, by continuously trying to elevate the importance and value of cyber conflict above that of more conventional security paradigms he segregates his claims from the rigorous theoretical and conceptual works predating his analysis. When he writes "information is no longer just a source of power; it has become force itself,"[20] he hypes the centrality of cyberspace's role in international conflict so much that it negates the relative importance of other forms of conflict preceding it. The value of his work comes in his robust, provocative analysis of concepts such as deterrence, power, and state versus nonstate responsibilities. Each of these issues in isolation is of immense value and should serve to elevate the role of cyberspace within the broader security studies field without negating the more conventional security challenges. The framing of *The Virtual Weapon* makes it controversial. A more measured approach to conventional security challenges and the existing literatures would have made his point about the importance of cyber conflict. In contrast to Kello's claims, cyber conflict does not displace, but rather adds confusion and contention to, a security-challenged world.

Hyperbole aside, in many ways Kello accomplishes his goal: he contentiously elevates the value of cyber conflict, so much so that he questions whether IR scholars can even grasp the intricacies, nuances, and enormity of cyber conflict using conventional IR paradigms such as realism and liberalism. And while he correctly concludes that "[h]umans will be able to define many of its [cyberspace's] chief properties but without controlling or even grasping the security implications of its applications in society,"[21] His rejection of existing theoretical paradigms, and, instead, branching out with no grounding in pre-existing theory, adheres neither to a Lakatosian knowledge building approach of extending outward from a central core, nor to the rigors of Popperian analysis, which would require fully falsifying claims he ignores. He builds a case for developing a unified theory of cyber conflict within its own distinct ontological framework ungrounded in and unconstrained by prior international relations theories.

ROOTING IN A PARSIMONIOUS CORE

Where Kello's analysis seems almost deliberately hyperbolic and contentious, Ben Buchanan is measured and constructive. Buchanan's 2017 *The Cybersecurity Dilemma* arguably is one of the best theoretical works within the cyber conflict studies subfield and one that will impact the field in much the same way as Thomas Rid's *Cyber War Will Not Take Place*,[22] forcing the

subdiscipline to be more linguistically precise.[23] Buchanan's work meticulously covers many confounding aspects of state actions in cyberspace. His analysis of state perceptions interacting in a domain of uncertainty and obfuscation challenges readers to join him in pondering the complexities of conflict in a new way. His examination of the perspectives of cyber offense and defense as seen through the lens of the intruder and the defender, deftly examines what he refers to as a "paradox" in cyberspace. The argument and scope of *The Cybersecurity Dilemma* is narrowly focused and buttressed by substantial case analyses and anecdotes from historical intelligence and cyber incidents, thereby establishing it as a critical contribution. Rather than attempting to survey the entire field of cyber conflict writ large, or make grandiose claims about its importance, Buchanan allows the case analyses and mechanisms of state interaction to speak for themselves. In contrast to Kello, he builds deliberately on prior work to expand core theoretical debates on the security dilemma to encompass concerns about cyber conflict.

States use cyberspace to achieve advantages over one another. To do this they must seek out targets within cyberspace through a slow deliberate process in most instances. In building the logic for how states develop offensive capabilities against one another in cyberspace, Buchanan counters the fact that cyberspace events occur more rapidly than kinetic events and explains why the perception of speed arises disregards the deliberate and often painstaking efforts to identify relevant targets, penetrate them, and achieve persistent presence. He then connects this seemingly offensive behavior to the logic of defense by forward presence, a topic now highlighted in the 2018 U.S. Department of Defense Cyber Strategy which states:

> The Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions.[24]

Buchanan anticipated US activities while highlighting how such behaviors further the mutual fear and mistrust between nations in a manner similar to Robert Jervis.[25] By going into adversaries' networks for defensive purposes, Buchanan notes that state defensive behaviors look remarkably offensive. He also draws out informational challenges such as attribution that give rise to the security dilemma.

By slowly, deliberately, and painstakingly building the case for a security dilemma in cyberspace, Buchanan is able to demonstrate why cyberspace is so important to international politics. He leverages this constrained approach to push back against common concepts in cyberspace, such as offense dominance.[26] He ties concepts of cyber conflict to conventional conflict where the analogies work well and by identifying areas where the logic of comparison fails. Specifically, he highlights the complexities of action in a domain where so much occurs behind the scenes. His final conclusion explores the likelihood that conflict and discord will continue within cyberspace as a function of the dilemma he builds, without implying anything beyond the scope of the existing data. Thus, he delineates the mechanics of a narrow, yet vital, set of attributes of conflict in cyberspace, and thereby provides a robust theoretical foundation

for future qualitative and quantitative analysis.

Buchanan's reticence to prognosticate on the potential severity of interactions in cyberspace allows the work to stand on its own merits and strengthens its argument without the rampant speculation of so many different works that came before. *The Cybersecurity Dilemma*'s constrained scope offers a model for how IR research on cyber conflict can be tied to the broader field, with a discipline that avoids addressing speculation as to a wider range of cyber challenges. His efforts have been mirrored in similar analyses such as Lonergan and Borghard's "The Logic of Coercion in Cyberspace."[27] Disciplined focus on one theory or issue at a time, allows these works to link cyber conflict and security to the broader security studies literature without artificially separating it as a new and fundamentally isolated from the rest of the discipline. The acceptance of existing ontologies, and the expansion of the core to encompass and explain novel phenomena, also avoids the pitfalls of hyperbole and groups the theory in tested, if not always entirely accurate, theories that predating cyberspace.

AN EXPANSIVE THEORETICAL APPROACH

Less parsimonious, but equally detailed, is the robust analysis of deterrence in cyberspace by Robert Mandel, in his 2017 book, *Optimizing Cyberdeterrence*, which leans more toward hyperbole than Buchanan's *The Cybersecurity Dilemma* but undertakes to analyze deterrence in cyberspace within the existing theoretical constraints of the broader discipline. In particular, Mandel builds his argument for tailored deterrence strategies in cyberspace by highlighting the weaknesses of targets to prevent, mitigate, and respond to cyber-attackers.[28] Mandel's analysis is detailed, yet broad in scope, examining a variety of means to engage in deterrence both within a domain and across domains. Mandel offers a more nuanced and likely more successful approach than those cyber deterrence scholars who urge only one option. He generally views cyber as requiring "broad inclusive deterrence,"[29] which contrasts with scholars such as Scott Jasper who seek out technical solutions (active deterrence),[30] normative forms of deterrence,[31] or other novel strategies such as entanglement.[32] Mandel analyzes deterrence less in conventional security paradigms offered by other scholars, but he does address many core concerns about cyber deterrence shared by these scholars.[33]

To explain why multiple deterrent options are needed, Mandel examines many reasons why deterrence in cyberspace is so difficult. In particular he identifies six key attributes: low perceived cyber defender credibility, high perceived cyber defender hypocrisy, high cyber attacker punishment resiliency, high cyber attacker obstacle adaptability, high cyber attacker operational secrecy, and low professed cyber attacker. These categories go beyond more constrained analyses associated with conventional deterrence literature, applying a logic more tailored to deter specific cyberspace threats. This deliberate choice is often criticized within the broader IR and security studies fields but is largely aligned with studies on nuclear deterrence. While such studies are robust in isolation, they often suffer from a loss of credibility due to failure to

consider escalatory behaviors that lead up to nuclear weapon use. Similarly, cyber deterrence viewed separately from the broader security implications of state interactions is problematic, as it often unduly prioritizes cyber conflict and attacks over more conventional solutions. Mandel avoids this by grounding his approach in case analyses that establish a concrete need for cyber-specific deterrence strategies.

One area where Mandel's work makes substantial headway in relation to deterrence is in a levels-of-analysis examination in Chapter 3. Whereas most conventional works on deterrence assume supremacy of the state,[34] Mandel takes special notice of those areas impacted by cyber-attacks that exist both below and above the nation-state.[35] He addresses often overlooked issues of capacity to deter that are missed in more conventional conversations on deterrence that are critically important in cyberspace. We obviously want to deter cyber adversaries, but how do we change bureaucracies, incentives, and public and private relationships to make deterrence viable? When discussing nuclear or even conventional kinetic deterrence, rarely are bureaucratic inertia or incentives to understand or implement new solutions considered. The organization of deterrence for kinetic options are established with clear hierarchies, and structured to facilitate or maximize deterrence. Cyberspace pervades all of government, private and civilian life, and infrastructures. Organizational understanding and capacities to deter, or the willingness to build in mechanisms, radically differ from conventional security studies models. Understanding these differences poses challenges to states seeking to deter. At the basic level they undermine the logic of deterrence and otherwise obfuscate successful deterrence strategies.

In concluding his analysis Mandel writes: [The] Cyberthreat does not exist in a vacuum, so responses should be formulated and implemented "in the context of larger global security affairs," explicitly connected to broader individual, local, national, regional and global security policies affecting both state and human security.[36]

This is good advice. Mandel's work throughout provides a robust assortment of case analyses framing the need for new, optimized deterrence strategies. He aptly frames the problem and hints at solutions, but does not prescribe them. His overall objective is not to provide a deterrence strategy, but rather, to set the stage for future scholars to build on his nuance in seeking out novel solutions, at the same time challenging decision-makers to implement concrete steps to secure cyberspace. Mandel essentially outlines the core heuristic and paves the way for subsequent scholars to expand upon his findings with novel auxiliary hypotheses.

MOVING BEYOND THEORY TO ANALOGICAL REASONING

Analysis in the first three works is rooted in theory and cases studies. Each work seeks to build a theory, whether broad and encompassing, as in the case of Kello, or narrow and focused by Buchanan. These efforts seek to tie cyber conflict to conventional security studies paradigms or leave them behind entirely. Cyberspace is and remains a socio-technical domain, replete with complex state and sub-state interactions. Use of cyberspace for conflict, for those

unfamiliar with its more advanced intricacies, can seem pedantic, even overwrought. To highlight the effects of cyber conflict in more conventional security studies it helps to reframe the arguments and use reasoning between two disparate albeit connected concepts. George Perkovich and Ariel E. Levite, in their edited volume *Understanding Cyber Conflict*, compiled a cohort of authors to leverage the power of analogy to generate frameworks for understanding the evolving subfield of cyber conflict within IR. Their work is thought-provoking and well organized. It helps provide a foundation for the expansion of theories outward from core heuristics by contextualizing complex interactions in cyberspace.

The use of analogy is not meant to elucidate a profound theory of how cyber conflict functions or how to achieve better deterrence in cyberspace. Instead, the 14 analogies presented attempt to link cyber conflict concepts directly to their conventional security studies counterparts. Each analogy, written by different authors, establishes a conceptual reference point for non-cyber conflict scholars. In the first, Michael Warner ties the form and function of cyber conflict to intelligence and in so doing highlights some of the many ways cyber conflict learns from and derives much of its applicability from intelligence.[37] Perhaps most importantly, Warner is able to tone down at the outset any potential hyperbole by noting:

> Both (intelligence and cyber) are inherently fragile and provocative. While neither is necessarily dangerously destabilizing in international relations, we must learn to perform cyberspace operations as we learned to perform intelligence activities - that is, with professional skill, with strict compliance with the law, and with careful oversight and accountability.[38]

Warner is joined in toning down hyperbole by retired LtGen Robert E. Schmiddle, Jr., USMC, Michael Sulmeyer, and Ben Buchannan in the second analogy, which compares nonlethal weapons and cyber capabilities carefully delineating the characteristics of cyber capabilities as different from nonlethal weapons,[39] thereby providing a robust starting point for plural analysis, not only on the use of such capabilities as acceptable in times of war and peace, but also in their material function. Questions raised on the reversibility, minimization of collateral damage, and deterrent attributes of the capabilities establish firm ground for future debates on the utility of cyber capabilities. The authors create parallels between a variety of nonlethal weapon systems and the actual use of cyber capabilities. This analogy permits rigorous conversations on severity and implications for use of cyber capabilities without resorting to exaggerated hypotheticals. Specifically, framing cyber capabilities as such also highlights their unique characteristics without equating them to the lethality of conventional kinetic weapons. Moreover, the discussion examines the concepts of attacking persons versus attacking materiel. By identifying that death by cyberattack has not yet transpired, the authors are able to focus on the true impact of cyber capabilities, i.e.: the destruction, denial, and degradation of systems. Constraining the scope of forecasts via analogy is important, and aligns studies of cyber conflict with security studies rather than science fiction.

One of the most interesting chapters examines the systematic utilization of cyber conflict by the Russian Federation in a variety of scenarios ranging from Estonia and Georgia to Ukraine.[40] Blank's analysis extends the breadth of impact of conventional cyber conflict outward to include the historically relevant forms of information and electronic warfare. While not an analogy, the case analysis does provide context in which cyber conflict is relevant to current security challenges. This chapter contrasts substantially with the chapter that follows, by John Arquilla, which examines the preventive nature of cyber conflict through multiple historical cases dating back to Thucydides and up to the DPRK and the use of Stuxnet against Iran.[41] The focused scope of Blank's chapter allows for the effects of specific cyber operations to be drawn out. Arquilla's sweeping comparisons are intellectually stimulating, but less effective in highlighting the true impact of cyber capabilities, if only because many of the effects are less than certain. Arquilla wisely hedges his assessment by characterizing cyber as a potential preventive measure, rather than declaring it a new weapon of critical importance in state conflict prevention.

In the contrast between these two chapters we see many of the fundamental challenges arising within the cyber conflict studies subdiscipline. Efforts to extend the logic of digital and virtual weapons, while highly relevant and of strategic and perhaps tactical value in one instance, are in others overextended and lack analytic leverage. Reining in the impulse to overvalue cyber conflict or capabilities helps to more accurately captures the true impact of cyberspace. As stated by Francis Gavin, "There is danger in focusing on technology to the exclusion of underlying political factors."[42] The chapters in this volume, provide a diversity of cases and analogies relevant security and conflict issues; each one caveats the arguments without hyperbole. Whether leveraging concepts of economic warfare,[43] Pearl Harbor,[44] air defense constructs,[45] or even nuclear technologies,[46] the scope, while detailed, does not exalt cyber conflict beyond reality.

This work establishes contours and grounds the domain's realities in a way that allows future scholars to apply theory. It stands as a key resource for those interested in studying cyberspace. The analogies within the volume help define the core ontologies of the field establish its foundations. While not driven by theory, they inform scholarship on an often-misunderstood technical domain.

PIECING THE PUZZLE: TESTING THE CORE

Because all things cyber, digital, Internet of Things, quantum, crypto, or whatever the buzzword, are often confusing to non-technical specialists, constructing theories based on reality can be challenging. One such challenge is the dearth of readily available public data on state interactions in cyberspace. Such data that is usable and relevant to cyber conflict scholars is often plagued by inaccuracies or derived from media reporting and hearsay, which has led to an abundance of case study-based works. Case studies are extremely valuable but are often obscure macro-level trends explainable by IR theories. Several projects are underway to operationalize cyber conflict data across all instances[47] and within specific conflicts such as Ukraine.[48] These studies will further add a data driven understanding of cyber conflict.

Brandon Valeriano, Benjamin Jensen, and Ryan Maness build upon previous efforts in their first work *Cyber War Versus Cyber Realities*[49] by continuing to develop a robust dataset of state cyber incidents in their new work *Cyber Strategy: The Evolving Character of Power and Coercion*,[50] and set the bar for data-driven analysis within the subfield. They use data to parse out many of the theoretical concepts developed by Buchanan, Kello, and Mandel, and analogies highlighted in Perkovich and Levite. Their analyses are robust and address the limits of coercive power within cyberspace. More importantly, they add quantitative rigor to a field too often dominated by conjecture and "Chicken Littles" that claim the sky is falling. By building a dataset and testing hypotheses, they rein in debate and challenge the subfield to build a more systematized foundation. This book is unique in tying cyber conflict literature directly to that of more conventional security studies. Equally important, the authors define their hypotheses at the outset and provide a consequential set of testable concepts around which they build arguments and engage in quantitative analysis.

By rigorously tying concepts of security studies to cyber conflict in their first several chapters, Valeriano et al., are able to use analytical/conceptual weight of their intellectual forebearers to carve out a niche for cyber conflict. When examining such conflict across the spectrum of espionage, and other disruptive and degrading activities, the authors found "cyber operations produce *only limited concessions*" (emphasis in original).[51] Diving deeper, their analysis found cyber espionage and disruption provided degradation but within the context of traditional powers, limited coercive impact.[52] Moreover, they identified the US as the primary coercive actor producing 89% of incidents of cyber degradation.[53] Beyond the limited scope of cyber to coerce, they also find there are "unique forms of coercion;" however, these are often combined with more traditional instruments of state power extending beyond cyberspace. Valeriano et al. rightly assess: "Cyber Coercion adds another vector for pressuring an adversary to change their behavior, but it must be evaluated in its proper geopolitical context."[54] They add:

> The more we study the impact of cyber actions, the more we find that those actions that do achieve a desired change in behavior in the target are rare, marginal in comparative impact, and costly in terms of giving up techniques to the adversary.[55]

Beyond the quantitative rigor, one of the more useful attributes of their analysis is a robust assessment of the effectiveness of various forms of coercion in cyberspace. This qualitative approach sets the stage for their subsequent tests, but also concisely frames much of the existing literature on cyber coercion. By examining disruption, intimidation, swaggering, espionage, deception, blackmail, denial, attrition, cost imposition, decapitation, punishment, risk, and control as means of cyber coercion, their exhaustive list of coercive methods is independently examined and critiqued.[56]

The deliberative approach by which Valeriano et al., establish the strengths, and perhaps more importantly the weaknesses, of cyber operations to achieve coercive power builds a place for cyber conflict within security studies more broadly. While unfairly criticized by some as

pessimists or for not fully grasping the "value" of cyber brings to modern state interactions, their middle-of-the-road, measured approach detracts nothing from cyber's future value and importance. Valeriano et al.'s analysis, both in *Cyber Strategy and Cyber War vs. Cyber Realities*, provides a solid foundation for the field. Cyberspace is important, but not clearly any more or less so than other forms of conflict. Their approach to collecting and analyzing data is valuable, but limited. Their data help elucidate the concepts they examine, but they do not rely solely on data without substantial case comparison and analysis within the broader context of security studies. Their work serves as a bridge between the largely qualitative works to date and a potential quantitative future open to cyber conflict scholars.

They conclude by highlighting the need for norms, information sharing, and public private frameworks, not because these matrices would mitigate challenges of cyberspace, but rather, because they would reemphasize and ensure global connectivity, education, communications, and economic markets rather than conflict. The work of Valeriano et al., serves as an azimuth test for the development of cybersecurity as a subdiscipline within IR and security studies. The data they collect, while in its early stages in comparison to long-established conflict datasets such as the Correlates of War Project or The Peace Research Institute Oslo Conflict, is a major step forward and allows for testing of auxiliary hypotheses against core theories within IR. Their work initiates a process of pulling together disparate pieces of a puzzle for testing.

BEYOND HYPERBOLE

Cyber conflict studies are advancing rapidly. As with any new and evolving field of inquiry, there are multiple approaches for a scholar. This article explains why the philosophy of science literature and concepts proposed by Imre Lakatos, predicated on building outward from a core by adding and testing auxiliary hypotheses, help generate new understanding without as yet unsupported and hence thus far, excessive claims.[57] The works considered in this essay follow three distinct tracks. The first follows the trajectory continued by Lucas Kello, and likely includes Alex Andrew Futter's *Hacking the Bomb*[58] and Clarke and Knake's, *Cyber War: The Next Threat to National Security and What to Do About It,*[59] among others. These works rightly raise alarm over a field many consider as receiving too little attention within the wider IR community. Their works are contentious, aggressive, and scoff at the constraints of conventional theoretical paradigms. Yet, they elevate the conversation with some hyperbole mixed in, plus a great deal of thought as to how cyberspace might influence security and conflict more broadly. These works are rigorous and well informed but are not beholden to the existing canon. In short, they cause scholars to rethink what the core of the research paradigm should be and whether maintaining a hold on conventional theories helps or hurts the study of a newly expanding domain of inquiry. They often do this by ignoring the existing core research programs of IR or security studies more specifically. The second track is populated by what is best referred to as informed commentators. These works span a wide spectrum of individuals and their audience is not academic. These works are filled with insider accounts, historical analyses, and case studies.

Works by journalists such as David Sanger,[60] Kim Zetter,[61] Ted Koppel,[62] Shane Harris,[3] and others are immensely valuable. They provide access and insights not otherwise available to many in the IR community. This track also includes individuals who have formally left the national security community, such as Richard Clarke,[65] John Carlin,[60] and Michael Hayden.[66] These works help scholars from both the first and third tracks understand the ontological nature of cyberspace and interactions within it. These works do not challenge the theoretical core of the research program but rather provide fodder for those seeking either to discard the core or to build auxiliary hypotheses to buttress it.

The third track of works includes those by Peter Shane and Jeffrey Hunker,[67] Nazli Choucri,[68] Tim Stevens,[69] Tim Maurer,[70] Herb Lin and Amy Zegart,[71] Alexander Klimburg,[72] and Adam Segal,[73] and more than a dozen others. Collectively, these works form a cohort of scholars best referred to as theoretical expansionists. Each attempt to take up conventional theories and build on them in unique ways, some more successfully than others. Yet, all have an eye toward expanding the reach of theories within IR and security studies more specifically to encompass topics relating to cyber security and conflict. The four works reviewed after Kello's book fit nicely within this third track. Each build upon the more conventional works within the IR canon while seeking to address both mundane and novel phenomena in a rigorous and informed manner within existing paradigms. They buttress the core and expand knowledge with auxiliary hypotheses to further existing research programs. In so doing, they generally avoid hyperbole due to the nature of the existing research programs they seek to build upon.

The subfield of cyber security and conflict studies will grow even more important as the penetration of cyberspace extends to more of the global population and the role and number of Internet-connected devices dominating economic, social, environmental, and political domains increase. Many of the most valuable contributions to date come in the form of edited volumes that span issue areas, including works by Van Puyvelde and Brantly;[74] Reveron;[5] Lindsay, Cheung, and Reveron;[76] Schaub;[77] and Jarmon and Yannakogeorgos;[78] plus journal articles that engage specific concepts or challenges associated with cyber conflict including Garzke and Lindsay,[79] Smeets,[80] Brantly,[81] Schneider, McDonald, and Krepps[82] and even policy pieces on websites such as War on the Rocks, Foreign Policy, or others. Multiple journals have published increasingly on cyber security and conflict, to include *International Security, Security Studies, Journal of Conflict Resolution, Survival, Journal of Cyber Policy, Journal of Cybersecurity, Intelligence and National Security, International Studies Review*, and others. The underlying tenets of security and conflict among states will rightly remain primary topics of study. However, the means by which to influence or prevent conflict, or potential avenues by which to escalate or deescalate, are likely finding increasing sources within cyberspace.

Cyber conflict is developing novel effects and is increasing in importance relative to the number and types of systems interconnected with a tendency to substitute complexity or hyperbole at the expense of sound social science. Works by scholars such as Valeriano et al. and Eric Jardine highlight how various attributes of cyberspace lead to bias, and, by extension, hyperbole.[83]

Those five works demonstrate is an increasing ability to engage the broader discipline of security studies while simultaneously surveyed here build understanding of cyber security and conflict within an expanding scope. Testable hypotheses developed to explain new forms of conflict offers fertile ground for future inquiry. Conventional theory remains important, if only as a sounding board (Kello) or a foundation (Buchannan, Mandel, Perkovich & Levite, Valeriano, Jensen, and Maness) for analysis. Each of the three tracks above has a place within the subdiscipline, and each has a role in informing the other tracks, scholarship, and policy.

BIBLIOGRAPHY

Arquilla, John. "From Pearl Harbor to the "Harbor Lights"." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

———. "An Ounce of (Virtual) Prevention?". Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Blank, Stephen. "Cyber War and Information War a La Russe." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Blum, Andrew. Tubes : A Journey to the Center of the Internet. Ecco. Ecco, 2013.

Borghard, Erica D., and Shawn W. Lonergan. "The Logic of Coercion in Cyberspace." [In English]. Security Studies 26, no. 3 (2017): 452 81. https://doi.org/10.1080/09636412.2017.1306396.

Brantly, Aaron F. "Aesop's Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace." Intelligence and National Security 31, no. 5 (2015): 674-85. https://doi.org/10.1080/02684527.2015.1077620.

———. "The Cyber Deterrence Problem." (2018): 31-54. https://doi.org/10.23919/cycon.2018.8405009.

———. The Decision to Attack: Military and Intelligence Cyber Decision-Making. University of Georgia Press, 2016.

Buchanan, Ben. "Cyber Deterrence Isn't Mad; It's Mosaic." Georgetown Journal of International Affairs, no. 4 (2014): 130-40.

———. The Cybersecurity Dilemma Hacking, Trust and Fear between Nations. Oxford University Press, 2017.

Carlin, John P., and Garrett M. Graff. The Dawn of the Code War : America's Battle against Russia, China, and the Rising Global Cyber Threat. New York: NY: PublicAffairs, 2019.

Cavelty, Myriam Dunn. Cyber-Security and Threat Politics : Us Efforts to Secure the Information Age. 2009.

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

Clarke, Richard A. "The Risk of Cyber War and Cyber Terrorism." Journal of International Affairs 70, no. 1 (October 24, 2018 2018): 179-81.

Clarke, Richard A., and Robert Knake. Cyber War: The Next Threat to National Security and What to Do About It. Harper-Collins Publishers, 2010.

Demchak, Chris. "Rise of a Cybered Westphalian Age." 10.1126/science.aar6404. Science (New York, N.Y.) 362, no. 6419 (2018): 1140-44. https://doi.org/papers3://publication/doi/10.1126/science.aar6404. http://www.sciencemag.org/lookup/doi/10.1126/science.aar6404.

Denning, Dorothy E., and Bradley J. Strawser. "Active Cyber Defense: Applying Air Defense to the Cyber Domain." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Elman, Colin, and Miriam Fendius Elman. Progress in International Relations Theory: Appraising the Field. Cambridge, MA: MIT Press, 2003.

Feaver, Peter, and Kenneth Geers. ""When the Urgency of Time and Circumstances Clearly Does Not Permit...": Pre-Delegation in Nuclear and Cyber Scenarios." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Futter, Andrew. Hacking the Bomb: Cyber Threats and Nuclear Weapons. Washington, D.C.: Georgetown University Press, 2018.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." 10.1162/ISEC_a_00136. International Security 38, no. 2 (2013): 41-73. https://doi.org/papers3://publication/doi/10.1162/ISEC_a_00136. http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00136.

Gartzke, Erik, and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." Security Studies 24, no. 2 (2015/04/03 2015): 316-48. https://doi.org/10.1080/09636412.2015.1038188. https://doi.org/10.1080/09636412.2015.1038188.

Gavin, Francis J. "Crisis Instability and Preemption." In Understanding Cyber Conflict: 14 Analogies. Understanding Cyber Conflict: 14 Analogies. Washington, D.C.: Georgetown University Press, 2017.

George, Alexander L., and Richard Smoke. Deterrence in American Foreign Policy: Theory and Practice. New York: Columbia University Press, 1974.

Glaser, Charles. Deterrence of Cyber Attacks and U.S. National Security. Cyber Security Policy and Research Institute (Washington, D.C.: 2011).

BIBLIOGRAPHY

Goldman, Emily O., and Michael Warner. "Why a Digital Pearl Harbor Makes Sense...And Is Possible." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Harris, Shane. @War: The Rise of the Military-Internet Complex. Boston, MA: Houghton Mifflin Harcourt, 2014.

Hayden, Michael V. Playing to the Edge : American Intelligence in the Age of Terror. New York, New York: Penguin Audio,, 2016. spoken word, 13 sound discs (17 hr.) : digital, CD audio ; 4 3/4 in., PRHA 5499 Penguin Audio.

Healey, Jason. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association, January 1, 2013, 2013.

Hunker, Jeffrey. "U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away." Journal of National Security Law & Policy 4, no. 2008 (January 1, 2010 2010): 197-216.

Huth, Paul K. "Deterrence and International Conflict: Emprical Findings and Theoretical Debates." Annual Review of Political Science (January 1, 1999 1999): 25-48.

In Athena's Camp. Edited by Arquilla John. Santa Monica, CA: The Rand Corporation, 1998.

Jardine, Eric. "Global Cyberspace Is Safer Than You Think: Real Trends in Cybercrime." SSRN Electronic Journal (2015). https://doi.org/10.2139/ssrn.2634590.

Jarmon, Jack A., and Panayotis A. Yannakogeorgos. The Cyber Threat and Globalization : The Impact on U.S. National and International Security. Lanham, UK: Rowman and Littlefield, 2018.

Jasper, Scott. Strategic Cyber Deterrence the Active Cyber Defense Option. Rowman & Littlefield. Rowman & Littlefield, 2017.

Jervis, Robert. "Cooperation under the Security Dilemma." World Politics 30, no. 2 (1978): 167-214. https://doi.org/10.2307/2009958. www.jstor.org/stable/2009958.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." International Security 38, no. 2 (2013): 7-40. https://doi.org/10.1162/ISEC_a_00138. https://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00138 %X While decisionmakers warn about the cyber threat constantly, there is little systematic analysis of the issue from an international security studies perspective. Some scholars presume that the related technology's scientific complexity and methodological issues prohibit orderly investigation; only a minimum degree of technical acuity is needed, however, revealing the scope of maneuver in the cyber domain. Other skeptics argue that the cyber peril is overblown, contending that cyber weapons have no intrinsic capacity for violence and do not alter the nature or means of war. This view misses the essence of the danger and conceals its true significance: the new capability is expanding the range of possible harm and outcomes between the concepts of war and peace—with important implications for national and international security. The cyber domain, moreover, features enormous defense complications and dangers to strategic stability: offense dominance, attribution difficulties, technological volatility, poor strategic depth, escalatory ambiguity, and proliferation to nontraditional and subversive actors. But even if the cyber danger is overstated, the issue merits serious scholarly attention. Whatever the current cyber revolution signifies, it is detrimental to the intellectual progress and policy relevance of the field to continue to avoid its central questions.

———. The Virtual Weapon and International Order. Yale University Press. Yale University Press, 2017.

Klimburg, Alexander. The Darkening Web: The War for Cyberspace. Penguin Books. New York, NY: Penguin Books, 2017.

Koppel, Ted. Lights Out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath. New York, NY: Crown Publishers, 2015.

Kostyuk, Nadiya, and Yuri M. Zhukov. "Invisible Digital Front." [In English]. Journal of Conflict Resolution 9, no. 1 (2017). https://doi.org/10.1177/0022002717737138.

Kramer, Franklin D, Stuart H Starr, and Larry K Wentz. "Cyberpower and National Security." (January 1, 2009 2009).

Kreps, Sarah, and Jacquelyn Schneider. "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics." Journal of Cybersecurity 5, no. 1 (2019): 1-11.

Lambert, Nicholas A. "Brits-Krieg: The Strategy of Economic Warfare." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Libicki, Martin C. Cyberdeterrence and Cyberwar. RAND Corporation, 2009.

Libicki, Martin C., Rand Corporation, and issuing body. "Conquest in Cyberspace : National Security and Information Warfare." (2007).

BIBLIOGRAPHY

Lin, Herbert, and Amy B. Zegart. Bytes, Bombs, and Spies : The Strategic Dimensions of Offensive Cyber Operations. Washington, D.C.: Georgetown University Press, 2019.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron. China and Cybersecurity : Espionage, Strategy, and Politics in the Digital Domain. New York: Oxford University Press, 2015.

Macdonald, Julia, and Jacquelyn Schneider. "Presidential Risk Orientation and Force Employment Decisions." Journal of Conflict Resolution 61, no. 3 (2017): 511-36. https://doi.org/10.1177/0022002715590874.

Mandel, Robert. Optimizing Cyberdeterrence : A Comprehensive Strategy for Preventing Foreign Cyberattacks. Washington, DC: Georgetown University Press, 2017.

Maurer, Tim. Cyber Mercenaries : The State, Hackers, and Power. Cambridge, UK: Cambridge University Press, 2018.

Mazanec, Brian M., and Bradley A. Thayer. Deterring Cyber Warfare : Bolstering Strategic Stability in Cyberspace. 2015.

Nye Jr, Joseph S. "Deterrence and Dissuasion in Cyberspace." International Security 41, no. 3 (2017): 44-71. http://www.mitpressjournals.org/doi/10.1162/ISEC_a_00266.

Passeri, Paolo. "Hackmageddon: Information Security Timelines and Statistics." 2010. https://www.hackmageddon.com/.

Puyvelde, Damien Van, and Aaron F. Brantly. "Us National Cybersecurity." (2017). https://doi.org/10.4324/9781315225623.

Reveron, Derek S. Cyberspace and National Security : Threats, Opportunities, and Power in a Virtual World. Washington, DC: Georgetown University Press, 2012.

Rid, Thomas. "Cyber War Will Not Take Place." Journal of Strategic Studies 35, no. 1 (2012/02/01 2012): 5-32. https://doi.org/10.1080/01402390.2011.608939. https://doi.org/10.1080/01402390.2011.608939.

Sanger, David E. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. New York, NY: Broadway Books, 2018.

Schaub, Gary. Understanding Cybersecurity : Emerging Governance and Strategy. Rowman and Littlefield, 2018.

Schelling, Thomas. Arms and Influence. New Haven, Conn: Yale University Press, 1966.

Schmiddle Jr., Robert E. , Michael Sulmeyer, and Ben Buchanan. "Nonlethal Weapons and Cyber Capaiblities." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Schneider, Jacquelyn. "What War Games Tell Us About the Use of Cyber Weapons in a Crisis." Council on Foreign Relations (2018). cfr.org/blog/what-war-games-tell-us-about-use-cyber-weapons-crisis.

Segal, Adam. The Hacked World Order : How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. Second edition. ed. New York: PublicAffairs, 2017.

Smeets, Max. "A Matter of Time: On the Transitory Nature of Cyberweapons." [In English]. Journal of Strategic Studies 41, no. 1-2 (2018): 6-32. https://doi.org/10.1080/01402390.2017.1288107.

Snyder, Glenn H. "Deterrence and Power." 4, no. 2 (June 1, 1960 1960): 163-78.

Stevens, Tim. Cyber Security and the Politics of Time. Cambridge, UK: Cambridge University Press, 2015.

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

Valeriano, Brandon, and Ryan C. Maness. Cyber War Versus Cyber Realities: Cyber Conflict in the International System. Oxford University Press. Oxford University Press, 2015.

Warner, Michael. "Cybersecurity: A Pre-History." Intelligence and National Security 27, no. 5 (2012): 781-99.

———. "Intelligence in Cyber-and Cyber in Intelligence." Understanding Cyber Conflict: 14 Analogies: Georgetown University Press, 2017.

Wiener, Norbert. Cybernetics or Control and Communication in the Animal and the Machine. MIT Press, 1965.

Zetter, Kim. "Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon." (January 1, 2014).

NOTES

1. Andrew Blum, *Tubes: a journey to the center of the Internet*, Ecco, (Ecco, 2013).
2. *In Athena's Camp*, ed. Arquilla John (Santa Monica, CA: The Rand Corporation, 1998).
3. Michael Warner, "Cybersecurity: A Pre-history," *Intelligence and National Security* 27, no. 5 (2012).
4. Norbert Wiener, *Cybernetics Or Control and Communication in the Animal and the Machine* (MIT Press, 1965).
5. This is a term used by Chris Demchak to describe the role of cyberspace in society – i.e. forming a socio-technical-economic substrate.
6. Chris Demchak, "Rise of a Cybered Westphalian Age," 10.1126/science.aar6404, *Science (New York, N.Y.)* 362, no. 6419 (2018), https://doi.org/papers3://publication/doi/10.1126/science.aar6404, http://www.sciencemag.org/lookup/doi/10.1126/science.aar6404.
7. Martin C. Libicki, Rand Corporation, and issuing body, "Conquest in cyberspace : national security and information warfare," (2007).
8. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009).
9. Franklin D Kramer, Stuart H Starr, and Larry K Wentz, "Cyberpower and national security," (January 1, 2009 2009).
10. Myriam Dunn Cavelty, *Cyber-security and Threat Politics : us efforts to secure the information age* (2009).
11. Richard A Clarke, "The Risk of Cyber War and Cyber Terrorism," *Journal of International Affairs* 70, no. 1 (October 24, 2018 2018).
12. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012/02/01 2012), https://doi.org/10.1080/01402390.2011.608939, https://doi.org/10.1080/01402390.2011.608939.; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," 10.1162/ISEC_a_00136, *International Security* 38, no. 2 (2013), https://doi.org/papers3://publication/doi/10.1162/ISEC_a_00136, http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00136.
13. Brandon Valeriano and Ryan C. Maness, *Cyber war versus cyber realities: cyber conflict in the international system*, Oxford University Press, (Oxford University Press, 2015).
14. Aaron F. Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making* (University of Georgia Press, 2016).
15. Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association, January 1, 2013, 2013).
16. Lucas Kello, *The virtual weapon and international order*, Yale University Press, (Yale University Press, 2017); Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013), https://doi.org/10.1162/ISEC_a_00138, https://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00138 %X. While decisionmakers constantly warn about the cyber threat, there is little systematic analysis of the issue from an international security studies perspective. Some scholars presume that the related technology's scientific complexity and methodological issues prohibit orderly investigation; only a minimum degree of technical acuity is needed, however, revealing the scope of maneuver in the cyber domain. Other skeptics argue that the cyber peril is overblown, contending that cyber weapons have no intrinsic capacity for violence and do not alter the nature or means of war. This view misses the essence of the danger and conceals its real significance: the new capability is expanding the range of possible harm and outcomes between the concepts of war and peace—with important implications for national and international security. The cyber domain, moreover, features enormous defense complications and dangers to strategic stability: offense dominance, attribution difficulties, technological volatility, poor strategic depth, escalatory ambiguity, and proliferation to nontraditional and subversive actors. But even if the cyber danger is overstated, the issue merits serious scholarly attention. Whatever the current cyber revolution signifies, it is detrimental to the intellectual progress and policy relevance of the field to continue to avoid its central questions.
17. Kello, *The virtual weapon and international order.*
18. See Jacquelyn Schneider, "What War Games Tell Us About the Use of Cyber Weapons in a Crisis," *Council on Foreign Relations* (2018), cfr.org/blog/what-war-games-tell-us-about-use-cyber-weapons-crisis.
19. Kello, *The virtual weapon and international order.*
20. Kello, T*he virtual weapon and international order.*
21. Kello, T*he virtual weapon and international order.*
22. Rid, "Cyber War Will Not Take Place."
23. Ben Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations* (Oxford University Press, 2017).
24. 2018 *Cyber Strategy.*

NOTES

25. Robert Jervis, "Cooperation Under the Security Dilemma," World Politics 30, no. 2 (1978), https://doi.org/10.2307/2009958, www.jstor.org/stable/2009958.
26. Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations.*
27. Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017), https://doi.org/10.1080/09636412.2017.1306396.
28. Robert Mandel, *Optimizing cyberdeterrence : a comprehensive strategy for preventing foreign cyberattacks* (Washington, DC: Georgetown University Press, 2017).
29. Id.
30. Scott Jasper, *Strategic cyber deterrence the active cyber defense option,* Rowman & Littlefield, (Rowman & Littlefield, 2017).
31. Brian M. Mazanec and Bradley A. Thayer, *Deterring cyber warfare: bolstering strategic stability in cyberspace* (2015).
32. Joseph S. Nye Jr, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017), http://www.mitpressjournals.org/doi/10.1162/ISEC_a_00266.
33. Aaron F. Brantly, "The cyber deterrence problem," (2018), https://doi.org/10.23919/cycon.2018.8405009; Charles Glaser, *Deterrence of CYber Attacks and U.S. National Security,* Cyber Security Policy and Research Institute (Washington, D.C., 2011); Ben Buchanan, "Cyber Deterrence Isn't MAD; It's Mosaic," *Georgetown Journal of International Affairs,* no. 4 (2014).
34. Alexander L. George and Richard Smoke, *Deterrence in American foreign policy: theory and practice* (New York: Columbia University Press, 1974); Thomas Schelling, *Arms and Influence* (New Haven, Conn: Yale University Press, 1966); Glenn H Snyder, "Deterrence and Power," 4, no. 2 (June 1, 1960 1960); Paul K Huth, "Deterrence and International Conflict: Empirical Findings and Theoretical Debates," *Annual Review of Political Science* (January 1, 1999).
35. Mandel, Optimizing cyberdeterrence : a comprehensive strategy for preventing foreign cyberattacks.
36. Mandel, Optimizing cyberdeterrence : a comprehensive strategy for preventing foreign cyberattacks.
37. Michael Warner, "Intelligence in Cyber-and Cyber In Intelligence," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017).
38. Warner, "Intelligence in Cyber-and Cyber In Intelligence."
39. Robert E. Schmiddle Jr., Michael Sulmeyer, and Ben Buchanan, "Nonlethal Weapons and Cyber Capaiblities," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017).
40. Stephen Blank, "Cyber War and Information War a la Russe," *Understanding Cyber Conflict: 14 Analogies* (Georgetown University Press, 2017).
41. John Arquilla, "An Ounce of (Virtual) Prevention?," *Understanding Cyber Conflict: 14 Analogies* (Georgetown University Press, 2017).
42. Francis J. Gavin, "Crisis Instability and Preemption," in *Understanding Cyber Conflict: 14 Analogies*, Understanding Cyber Conflict: 14 Analogies (Washington, D.C.: Georgetown University Press, 2017).
43. Nicholas A. Lambert, "Brits-Krieg: The Strategy of Economic Warfare," U*nderstanding Cyber Conflict: 14 Analogies* (Georgetown University Press, 2017).
44. John Arquilla, "From Pearl Harbor to the "Harbor Lights"," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017); Emily O. Goldman and Michael Warner, "Why a Digital Pearl Harbor Makes Sense...and Is Possible," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017).
45. Dorothy E. Denning and Bradley J. Strawser, "Active Cyber Defense: Applying Air Defense to the Cyber Domain," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017).
46. Peter Feaver and Kenneth Geers, ""When the Urgency of Time and Circumstances Clearly Does not Permit...": Pre-Delegation in Nuclear and Cyber Scenarios," Understanding Cyber Conflict: 14 Analogies (Georgetown University Press, 2017).
47. Paolo Passeri, "Hackmageddon: Information Security Timelines and Statistics," (2010). https://www.hackmageddon.com/.
48. Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front," *Journal of Conflict Resolution* 9, no. 1 (2017), https://doi.org/10.1177/0022002717737138.
49. Valeriano and Maness, *Cyber war versus cyber realities: cyber conflict in the international system.*
50. Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber strategy: the evolving character of power and coercion,* Oxford University Press, (Oxford University Press, 2018).
51. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*

NOTES

52. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*
53. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*
54. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*
55. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*
56. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion.*
57. Colin Elman and Miriam Fendius Elman, *Progress in international relations theory: appraising the field* (Cambridge, MA: MIT Press, 2003).
58. Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Washington, D.C.: Georgetown University Press, 2018).
59. Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (HarperCollins Publishers, 2010).
60. David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York, NY: Broadway Books, 2018).
61. Kim Zetter, "Countdown to Zero Day : Stuxnet and the launch of the world's first digital weapon," (January 1, 2014 2014).
62. Ted Koppel, *Lights Out: a Cyberattack, a Nation Unprepared, Surviving the Aftermath* (New York, NY: Crown Publishers, 2015).
63. Shane Harris, *@War: the rise of the military-Internet complex* (Boston, MA: Houghton Mifflin Harcourt, 2014).
64. Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It.*
65. John P. Carlin and Garrett M. Graff, *The Dawn of the Code War : America's Battle Against Russia, China, and the Rising Global Cyber Threat* (New York: NY: PublicAffairs, 2019).
66. Michael V. Hayden, *Playing to the edge: American intelligence in the age of terror* (New York, New York: Penguin Audio,, 2016), spoken word, 13 sound discs (17 hr.): digital, CD audio ; 4 3/4 in., PRHA 5499 Penguin Audio.
67. Jeffrey Hunker, "U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away," *Journal of National Security Law & Policy* 4, no. 2008 (January 1, 2010).
68. Nazli Choucri, *Cyberpolitics in international relations* (Cambridge, MA: MIT Press, 2012).
69. Tim Stevens, *Cyber Security and the Politics of Time* (Cambridge, UK: Cambridge University Press, 2015).
70. Tim Maurer, *Cyber mercenaries : the state, hackers, and power* (Cambridge, UK: Cambridge University Press, 2018).
71. Herbert Lin and Amy B. Zegart, B*ytes, bombs, and spies : the strategic dimensions of offensive cyber operations* (Washington, D.C.: Georgetown University Press, 2019).
72. Alexander Klimburg, *The Darkening Web: the war for cyberspace*, Penguin Books, (New York, NY: Penguin Books, 2017).
73. Adam Segal, *The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age*, Second edition. ed. (New York: PublicAffairs, 2017).
74. Damien Van Puyvelde and Aaron F. Brantly, "US National Cybersecurity," (2017), https://doi.org/10.4324/9781315225623.
75. Derek S. Reveron, *Cyberspace and national security : threats, opportunities, and power in a virtual world* (Washington, DC: Georgetown University Press, 2012).
76. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, *China and cybersecurity : espionage, strategy, and politics in the digital domain* (New York: Oxford University Press, 2015).
77. Gary Schaub, *Understanding cybersecurity: emerging governance and strategy* (Rowman and Littlefield, 2018).
78. Jack A. Jarmon and Panayotis A. Yannakogeorgos, *The cyber threat and globalization: the impact on U.S. national and international security* (Lanham, UK: Rowman and Littlefield, 2018).
79. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015/04/03 2015), https://doi.org/10.1080/09636412.2015.1038188, https://doi.org/10.1080/09636412.2015.1038188.
80. Max Smeets, "A matter of time: On the transitory nature of cyberweapons," *Journal of Strategic Studies* 41, no. 1-2 (2018), https://doi.org/10.1080/01402390.2017.1288107.
81. Aaron F. Brantly, "Aesop's wolves: the deceptive appearance of espionage and attacks in cyberspace," *Intelligence and National Security* 31, no. 5 (2015), https://doi.org/10.1080/02684527.2015.1077620.

NOTES

82. Sarah Kreps and Jacquelyn Schneider, "Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics," *Journal of Cybersecurity* 5, no. 1 (2019); Julia Macdonald and Jacquelyn Schneider, "Presidential Risk Orientation and Force Employment Decisions," *Journal of Conflict Resolution* 61, no. 3 (2017), https://doi.org/10.1177/0022002715590874.
83. Valeriano, Jensen, and Maness, *Cyber strategy: the evolving character of power and coercion*; Eric Jardine, "Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime," *SSRN Electronic Journal* (2015), https://doi.org/10.2139/ssrn.2634590.