H-Net Reviews
in the Humanities & Social Sciences

Brandon Valeriano, Benjamin M. Jensen, Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion.* New York: Oxford University Press, 2018. 320 pp. $34.95, cloth, ISBN 978-0-19-061809-4.

Reviewed by Richard Harknett

Published on H-Diplo (October, 2018)

Commissioned by Seth Offenbach (Bronx Community College, The City University of New York)

"Analyzing the efficacy of cyber strategies is an empirical question that requires theory and evidence to support policy" (p. 20). Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness have offered a contribution that seeks to provide a research design that tests a core theory of security studies, grounds that test in a quantitative data set, and translates those findings into prescriptive guidance. This is no small task in any social science context, but one that faces particular challenges in the still emerging field of cyber security studies.

The first challenge is methodological—specifically, how best to access and organize one's empirical data. To date, much of the development within the field of cyber security studies has been deductively driven either leveraging heuristic cases or small-set qualitative case studies. In large measure, this approach is the result of the fact that most cyber activities are either considered state secrets or, in the corporate context, shielded because of intellectual proprietary rights and concerns over public disclosures. Many cyber security companies now produce quality forensic reports concerning unauthorized computer intrusions and the development of malware, but such reports have an inherent selection bias problem potential as well as financial incentive bias (much of this work is actually quite good and useful, but from a social science perspective the limitations of working with such third party business-generated data needs to be acknowledged). Valeriano, Jensen, and Maness take on this challenge directly and offer their own data set of 192 "publicly attributed cyber incidents between rival states" drawn from their "Dyadic Cyber Incident and Dispute Dataset (DCID) Version 1.1" (p. 55). They cross-reference leading forensic releases with government reports and journalist investigations and provide the reader with a useful appendix to guide people through their coding methods. For this effort, the three authors will likely be cited often, because it is an important start to a quantitative methodological approach to cyber security studies (they tend to use "quantitative" and "empirical" interchangeably in the book, but of course strong qualitative methods do support empirical theory-testing and development as well).

The authors acknowledge that creating this data set for quantitative methods use in the study of cyber operations will remain somewhat constrained. Unlike traditional conflict, the opaqueness of cyber activity is distinctly problematic for academic research. While a certain percentage of incidents are reported publicly, we still remain in an environment where even active rivals might be unaware of the fact that an intrusion is underway. So public reports of incidents give us a picture of intrusions that occurred previously, were typically discovered later, and then either reported or leaked. What we do not have access to in great abundance as academic researchers is objective witnessing of the dynamics of cyber operations while they are occurring (we do not have battlefield reporting) or detailed access to those operations in an historical accounting. This raises again some distinctive challenges that we are going to have to work through as a community of scholars. The three authors' main methodological contribution is to engage the field with a first-generation model that will be leveraged and improved upon as this field of inquiry grows, and they will receive due credit for that effort.

The main challenge, however, that the authors take on is to test an important core theory—coercion—and related concepts such as escalation. Their tests lead to their headline finding that cyber operations are fairly limited coercive tools, which rarely produce concessions among rivals. An attendant finding is that these same cyber operations tend ***not*** to be escalatory.

Why are these important conclusions? The authors put it quite bluntly and harshly, for some: "The greatest risk ... may lie not in the inherent capabilities of cyber operations but in the corresponding threat inflation wrought by an academic and policy community eager to capture headlines and imagine future wars. Pundits and cyber security analysts who profit from overstating the cyber threat to the United States risk producing crises where none need exist" (pp. 200-01). Two aspects of this quote need to be separated out, because their core finding need not impugn the intent or nature of analysts, who to date may offer different assessments than the one offered in this book. There is no doubt that the first wave of literature in the 1990s that focused on cyber conflict jumped to the term "cyber war" early to describe the dynamics that might be associated with cyber aggression. The focus on war and large-scale attacks in academic work continued, in part, because the literature of security studies that was built up over the past fifty years rested on such a focus. Journalistic reporting has amplified this war terminology. Additionally, policy in the United States also drove this threat focus in that the strategy of deterrence was seen as a central anchor for organizing security in cyberspace and such a strategy tended to overemphasize concern about potential large-scale attacks on critical infrastructure. So, one need not attribute ill intent (publicity or profit-seeking motives) to those who may have gotten the analysis wrong. There has been plenty of inertia behind this problem-framing and resultant analysis.

Of course, the more important issue here is whether the three authors have gotten the threat assessment right. The answer is yes and no. ***Cyber Strategy*** provides a strong case that those concerned about cyber campaigns as coercive, compellent, and potentially war escalatory means can rest a little easier. The threat of cyber coercion may be manageable. This is an important finding. It rests on the testing of three sets of related but distinct hypotheses concerning coercion, signaling, and campaigns (essentially defined as cyber means combined with other state power tools). The authors specify and operationalize three forms of cyber strategies—disruption, espionage, and degradation—and test each in relation to coercion, signaling, and campaigns. The research design rests on a solid treatment of established literature on coercion, bargaining (from which the signaling focus is derived), and coercive diplomacy. ***Cyber Strategy*** is in many ways a very traditional security studies book, drawing from very traditional authors to examine this emerging means of conflict. It is focused on theory-testing, rather than theory development in that sense. This turns out to be a very important choice the authors have made. From that choice perspective the book is a success, but to be frank, a maddening one at that, because it could propel the field so much further than it does. Hopefully, those that build on this book, including the three authors, will take up this most critical next step, for essentially the book tells us in a convincing manner what cyber strategies are not, but does not offer an equally compelling explanation as to exactly what they actually are.

This follows from the core choices made in establishing the research design. The authors ask, "Do cyberattacks really achieve the goals of the attacker? Do they compel the adversary to change their behavior through either demonstrated attacks or the fear of future attacks (p. 20)? These are two very distinct questions, but throughout the design they are combined. For their design, the authors assume coercion is the goal and do not test other possible overarching goals directly. What the book essentially studies is whether cyber means lead to coercion, in the form of direct compellence or indirectly through influence, across the incidents in their database, including related variables such as signaling and shaping. The evidence supports their conclusion that, for the most part, cyber coercion is not happening.

What the book does not examine is whether coercion is actually the primary "goal of the attacker." It provides enough evidence to suggest it is not. Chapters 5, 6, and 7 are case studies of the three leading cyber states (Russia, China, and the United States). In each of the cases, the authors provide evidence that cyber coercion is not significant, nor are cyber incidents creating escalatory dynamics. As a pivot in the literature away from focusing on cyber incidents as war, again, this is an important finding, but it begs the question: is what the authors are discovering due to the nature of cyber means or is it due to the goals of the attackers? What if the goal is not coercion (that is, direct concession, crisis management, or shaping influence), but straightforward power competition? What if the objective of states is to use cyber means to undercut their rivals' national sources of power over time and, when possible, increase their own sources of power? The book, in places, walks up to this tantalizing theory-development water's edge, but never jumps in. For example, the authors conclude that "Russia had no direct coercive success in cyberspace" (p. 118), but on the next page note that "Russia uses intrusions ... to launch information operations in Western rival states to distort public opinion and undermine confidence in the target government's institutions" (p. 119). So, perhaps the Russians have no direct coercive success because they are not attempting to coerce directly in their use of cyber means. If this is the case, then what we need to be testing to get at cyber strategies is whether Russia is successful in distorting opinion and undermining confidence, since as an attacker that might be Russia's primary goal. This theory-testing opportunity over alternative goals applies equally to China and the United States based on the evidence presented in both of those chapters.

Early in the book, the authors tell us correctly that "we must broaden our gaze beyond coercion" (p. 11) and yet offer us a book designed to study coercion. In fact, they know where that broader gaze must go when they write, "rival states use indirect cyber instruments to shape long-term competition more than they seek immediate concessions" (p. 11). Although it is not the focus of the book, the evidence leads to the argument that coercion is not the only option to pursue strategic competition and may not be the primary one being pursued by any of the three major cyber states studied. When the authors conclude that "unpacking the strategic logic of cyber conflict as a new means of coercing political opponents demands that we understand the realities and limits of this innovation" (p. 202), they have only unpacked, by their own good evidence, a small box inside a much larger one. They are absolutely correct that "we need to move the discourse toward the reality of what cyber tools are good for, how they work, and how they achieve effects" (p. 209). That requires scholars to move not only beyond war constructs, as they argue, but also the coercion variables (signaling, escalation, and shaping) locked in the small box studied in this book. The authors are on to something bigger that they recognize. The quantitative and qualitative empirical data suggests states leveraging cyber means are doing so for strategic ends tied to power competition. They are not signaling resolve nor managing crisis dynamics, but rather competing with each other's core sources of national power short of war. Such a hypothesis can certainly be substantiated from all three chapters looking at the behavior of Russia, China, and the United States and it would be fascinating for the data set to be used to test some alternative theories of state strategic behavior. Again, much of the data presented to show that cyber means are limited as coercive tools, points to how potentially effective they are as competition tools.

This book will play an interesting role within the literature. It is most convincing in telling scholars that we have been looking at the wrong thing—war and fear of war—when studying state cyber behavior. But it remains too tightly tied to the literature it leveraged for that conclusion to tell us convincingly what states are actually up to in cyberspace. Yes, they may signal, and shape, but there seems enough evidence to suggest that more is going on than those limited actions. There may be more cyber strategies than coercion. If more who read this book have that take-away and are thus better positioned to analytically unpack strategic competition in cyberspace, then Valeriano, Jensen, and Maness have done the field of cyber security studies a service. Two observations might live side by side: cyber means are not revolutionary as coercive tools, but may have strategic potential if states see them as fundamental to competition short of war. While the authors might prove correct that there has been threat inflation in the construct of cyber war, it might be equally true that a threat worthy of deep continued study and policy concern actually exists.

If there is additional discussion of this review, you may access it through the network, at https://networks.h-net.org/h-diplo

Citation: Richard Harknett. Review of Valeriano, Brandon; Jensen, Benjamin M.; Maness, Ryan C. *Cyber Strategy: The Evolving Character of Power and Coercion.* H-Diplo, H-Net Reviews. October, 2018.

URL: https://www.h-net.org/reviews/showrev.php?id=52426