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

Article Review 83
issforum.org

H-Diplo/ISSF Editors: **Seth Offenbach** and **Diane Labrosse**
H-Diplo/ISSF Web and Production Editor: **George Fujii**

Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* (2017): 72-109, and **Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace,"** *International Security* 41.3 (2017): 44-71.

Review by **Brandon Valeriano**, Marine Corps University

Published by ISSF on 26 July 2017

tiny.cc/ISSF-AR83
https://issforum.org/articlereviews/83-cyber
https://issforum.org/ISSF/PDF/ISSF-AR83.pdf

Offending and Defending in Cyberspace

Perhaps the most important question in modern cyber security revolves around the issue of the efficacy of cyber operations. We know very little about how states achieve their goals in cyberspace, whether in deterring action, which is maintaining the status quo and preventing attacks, or in compellence, which is changing behavior by going on the offensive.

Many statements in the field eschew the issue of efficacy in exchange for a focus on what might be called cyber hype. The assumption that cyber conflict 'works' as a strategic or tactical concept has taken precedent for the more basic question of how it might work and when. The more interesting recent wave of cyber security scholarship[1] counters the cyber hype- and cyber revolution-based motifs of early scholarship and public statements.[2] The turn towards more careful empirical and theoretical scholarship establishes a more rigorous approach that carefully calls into question recent pronouncements that we have seen a rise of a new

[1] Erik Gartzke, "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth," *International Security* 38:2 (2013):41-73; Gartzke, and Jon R. Lindsay. "Weaving tangled webs: offense, defense, and deception in cyberspace," *Security Studies*24:2 (2015): 316-348.

[2] Lucas Kello, "The meaning of the cyber revolution: Perils to theory and statecraft," *International Security* 38.2 (2013): 7-40; Richard A. Clarke, and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Ecco, 2010).

wave of warfare. The challenge is clear, as policy-makers struggle with integrating the evident normality and stability of cyber security practices with the grand sweeping changes suggested by the public discourse that is often focused on the motif of approaching "Cyber Pearl Harbors."[3]

Two new important articles which are part of this turn in critically questioning the utility of deterrence and assumptions of offensive dominance in cyberspace. The work of Joseph Nye, on cyber deterrence, and Rebecca Slayton, on the offensive-defensive balance, will surely provoke more scholarship and reactions because their approaches challenge the revolutionary assumptions of the cyber domain.

Both pieces offer much to the current generation of scholars who are diving into the topic of cyber security, suggesting critical starting points. Slayton's article, "What is the Cyber Offense-Defense Balance" perhaps focuses too much on the platform of the offensive-defense balance. In short, the theory holds that actions proliferate when offense is said to be cheaper than defense.[4] Adherents of the theory suggest that this process of offensive dominance can unlock the key cause of war[5], while others question the empirical basis of the perspective, suggesting that other theories give us more leverage in understanding the process of war and peace.[6]

What is important about Slayton's contribution is that it challenges the assumption that defense is more costly and difficult in cyberspace, pointing out that serious offensive operations in cyberspace are difficult and costly. As she notes, "sweeping claims about offensive advantage in cyberspace are deeply misguided" (74). Forthcoming research demonstrates that serious degrade operations meant to compel are rare and the utility of these operations falls well short when compared to other coercive methods.[7] Lindsay also calls into question the utility of the offense in relation to the Stuxnet case.[8]

Slayton makes the point that that second key frame from the offense-defense balance, the issue of "efficacy, explicitly includes the payoff of successful offense" (82). This is perhaps the more important thread to pull, rather than focusing on the costs of the offense in the enormous Stuxnet operation and the rather cheap security measures imposed by a hardened, unnetworked, isolated target such as Iran's Natanz plant.

[3] Sean Lawson and Michael Middleton, "Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991-2016" Paper presented at the "Legal and Policy Dimensions of Cybersecurity" Conference, George Washington University, Washington D.C., 27-29 September 2016.

[4] George H. Quester, *Offence and Defence in the International System*. (New York: John Wiley and Sons, 1977).

[5] Stephen Van Evera, "Offense, Defense, and the Causes of War." *International Security* 22:4 (1998):5-43.

[6] Y. Gortzak, Y. Haftel, Y. and K. Sweeney, "Offense-Defense Theory: An Empirical Assessment," *The Journal of Conflict Resolution* 49:1 (2005): 67-89.

[7] Brandon Valeriano, Benjamin Jensen, and Ryan Maness. *Cyber Coercion: Cyber Compellence in the Digital Age.* Unpublished Book Manuscript (2017).

[8] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22.3 (2013): 365-404.

Other scholars would do well to follow the lead of Slayton and empirically analyze the costs of both the defense and offense in cyber action, perhaps puncturing the myth that the offense is easy in cyberspace. For me, the issue is not so much about the difficulty of offensive action, but rather the difficulties of coercion and how this reflects the general restraint dynamics in cyberspace in that we rarely seek serious cyber actions that involve massive amounts of resources utilized and digital violence.[9]

The key takeaway from the Slayton piece is not the discussion of how the offense-defense balance works in cyberspace, a project hindered by the selection of the Stuxnet example, a case that is likely an outlier and not supported by any social science justification. The empirical rejection of the framework[10], plus the more complicated question of just how to measure what an offensive weapon is versus a defensive weapon, and the unexamined question of how to measure perceptions of these weapons, makes this framework problematic as a foundation for the article.

The key point to be taken from the article is that the talent and skill of cyber security professionals in the field is the variable that requires more study (82). While Slayton does not really follow up on this trend relating to skill and talent, this should be a key factor of research in the future. The issue begs for more careful case study explorations and quantitative analysis. Just how important are latent cyber capabilities and computer science capacity in achieving offensive and defenses goals in cyberspace? In short, talent matters in cyber interactions, often more than the current abilities of each state.

In terms of the defense side of the coin, Nye makes a valiant effort to evaluate the nature of deterrence in cyberspace and propose a way forward. Surveying works by such scholars as Libicki,[11] Nye notes the many of the problems with the conception of deterrence in cyberspace, including the challenges of punishment and denial strategies. I would add the more critical issue of credibility to the debate, which to date is a problematic frame since we have seen so few serious cyber incidents overall.[12]

Denial as a strategy is problematic because of the ubiquity of general intrusions. It is tough to deny an attacker access when there are so many points of entry where vulnerabilities can be exploited. As Nye notes, almost every single instance of intrusion in U.S. networks comes from human error (50). It should also be noted that many of these entry points come from third-party vendors, not direct attacks. There is a huge hole in deterrence theory if we are going to depend on denial to save us. While hardened military networks seem safe, there are points of entry across the system because of the proliferation of third-party contractors and simple human error.

[9] Valeriano, and Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. (Oxford University Press, 2015).

[10] Gortzak *et al.*, 2005.

[11] Martin C. Libicki, *Cyberdeterrence and cyberwar*. (Rand Corporation, 2009).

[12] Valeriano and Maness, "The dynamics of cyber conflict between rival antagonists, 2001–11," *Journal of Peace Research* 51:3 (2014): 347-360.

The more important part of the piece is the subtle progressive turn towards dissuasion and away from deterrence. The two terms are the not the same and are instead linked through the likeminded goal of preventing future attacks. The foundation of future dissuasion could be normative limitations or entanglement. Entanglement is connected to the issue of self-restraint, an issue we explore more fully in *Cyber War versus Cyber Realities.*[13]

The discussion of the normative underpinnings of dissuasion is the critical contribution of this article. If the United States and China can agree on limitations in targeting, then there is hope for a stable cyber future. Taboos are clearly developing (61) and institutionalizing taboos against aggressive action that would harm civilians seems to be the first step towards preventing future critical attacks. Citing examples such as the Budapest Convention on Cybercrime in 2001 (67) lends empirical support to a possible normative framework and expanding on the success, coverage, and structures of international agreements on cyberspace should be the first step for future researchers seeking to establish a normative system of dissuasion.

I disagree with Slayton's statement that "there is reason to doubt the precise probabilistic data will be produced" in cyber security (81). While all conflict data projects are fraught with problems of comprehensiveness, selection of cases, and secrecy, there is no reason to expect that cyber security scholarship is prone to these challenges more than other fields. In many ways, the evident public nature of cyber breaches, even espionage breaches, makes them ripe for systematic analysis. This is the challenge for others to take as we move forward in the future. One-case empirical evaluations are useful for some purposes, but this is mostly regulated to the perspective of explanatory support for theories and theory development. It is possible to construct cyber security databases that comprehensively account for these issues in the field; time will only lend credibility to this perspective as more efforts are funded.

Slayton also argues that it is difficult to analyze the probability of success in cyber operations, but this ignores the proliferation of wargames and cyber ranges at the classified and unclassified level (90). The main question, though, is why states would focus on the offense or defense in cyber operations, and this process can also be teased out through gaming scenario development, a key point of research in the future.

The final point is to consider just what issues drive international cyber conflicts. As Slayton notes, leaders were "unlikely to focus on costs" (75) of operations. This begs the question as to what, if not on costs, are they focused on. The questions of resolve, interest, and capability are left unexamined, and this is critical if we move to dissuasion instead of deterrence. States might escalate conflicts with cyber operations because the stakes are so high and the interests are so salient, not because the offense is dominant or deterrence does not work. As with the problem of nuclear scholarship, we leave out the issue of what drives states to fight in cyber security.

[13] Valeriano and Maness, *Cyber War versus Cyber Realities* (2015).

Moving beyond handed-down questions about deterrence and offense-defense will serve the field well and we should be forging a progressive path forward.[14] These pieces sow the seeds of this future and it is the responsibility of the rest of the cyber security field to mine the garden of fertile research questions that remain.

Brandon Valeriano is the Donald Bren Chair of Armed Politics at the Marine Corps University. He also serves as an adjunct fellow in cyber security for the Niskanen Center. Dr. Valeriano has published dozens of articles in such outlets as the *Journal of Politics*, *International Studies Quarterly, and Journal of Peace Research*. His two most recent coauthored books are *Cyber War versus Cyber Reality* at Oxford University Press (2015) and *Russian Coercive Diplomacy* at Palgrave (2015) with *Cyber Coercion* forthcoming.

[14] Sean Lawson, "Beyond Cyber-doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-threats." *Journal of Information Technology & Politics* 10:1 (2013): 86-103.