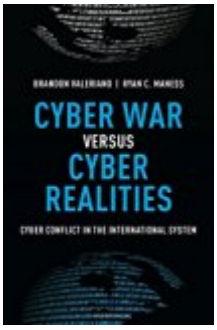
H-Net Reviews
in the Humanities & Social Sciences

Brandon Valeriano, **Ryan C. Maness**. *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* Oxford: Oxford University Press, 2015. 288 pp. $29.95 (cloth), ISBN 978-0-19-020479-2.



Reviewed by Joe Burton (Victoria University of Wellington)
Published on H-Diplo (April, 2016)
Commissioned by Seth Offenbach

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

In this respect, the book adds to a body of scholarship that questions the actual impact of contemporary security threats, including John Mueller's *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats and Why We Believe Them*, which analyzes the exaggeration of the terrorism threat in the post-9/11 era; the article by Thomas Rid, "Cyber War Will Not Take Place," and the book by Rid with the same title, which argue that cyber war will not take place because cyber attacks are never in-and-of-themselves acts of violence; and Mary O'Connell's article "Cyber Security without Cyber War," where she warns of the militarization of cyber security discourse and the negative impact that might have in developing effective responses to cyber security issues.[1] *Cyber War versus Cyber Realities* comes at an important historiographical juncture too, with considerable academic backlash against claims that social media was instrumental in the events of the Arab Spring, and in the aftermath of the Edward Snowden affair, which has revealed a massive accumulation of power over the Internet by national security agencies because of, arguably, overwrought fears about terrorism. Indeed, this book is part of a growing group of academics who are cyber skeptics and who question the role of information and communication technologies in international relations. This skepticism is welcome when considering the impact of new technologies on long-established patterns of international behavior.

This book takes a meticulous, quantitative approach to puncture some of the hype, using an extensive data set to analyze cyber incidents involving rival "dyads" (pairs of states) over a ten-year period between 2001 and 2011. One of the central claims of the book is that the use of malicious cyber attacks by rival states does not normally alter the propensity for those states to cooperate with each other. In other words, cyber attacks do not often fundamentally harm relations between states and rarely lead to serious repercussions. States will continue to cooperate even as they are targeted by the other state by cyber attacks. This finding appears to be borne out by recent events. Despite massive Chinese cyber espionage against the United States, for example, the two countries continue to cooperate in many areas in which they have core and shared interests. The September 2015 meeting between Presidents Barack Obama and Xi Jinping in Washington DC led to an agreement to reign in criminal organizations using the Internet for cyber crime, even while both countries continue to subvert and survey each other's digital networks for political and military gain.

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

Why do states appear to exercise restraint in cyber interactions? First, the authors claim a degree of cyber interdependence, particularly as the ability of states to attribute cyber attacks to specific actors has improved. Some degree of malicious cyber actions are also expected to occur by states and will be tolerated as part of the regular business of international relations, especially if they do not cross certain thresholds (at the most extreme end involving a loss of life). What the authors call "total cyber operations" remain off the table, as they are likely to lead to more serious consequences, including the destruction of infrastructure, significant collateral damage, significant economic losses, and even war. Cyber weapons can also be reverse engineered in a way that conventional weapons cannot, and this contributes to restraint around their deployment. Possible harm to civilians through collateral damage tilts the balance toward restraint dynamics in cyber conflicts and emerging norms of behavior in cyberspace also add to restraint between rival states in the cyber security sphere. Implicit in the argument of the authors is that cyber norms have already emerged, and can be seen in US reluctance to use cyber attacks in Iraq in 2003 and in Libya in 2011. A further restraint dynamic relates to how cyber attacks might have the unintended consequence of dragging third parties into a conflict, a type of cyber "entrapment," a concept first established by realist alliance scholars, and now applied to the cyber sphere. Finally, the fear that cyber attacks could lead to a conventional response by states also creates a degree of restraint. Again, this seems to be a highly relevant observation. The US government has explicitly acknowledged that all options are on the table in response to cyber attacks, including the use of conventional military force. NATO's cyber doctrine for the defense of its members takes the same position.[2]

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

Are the authors right? Is cyber war being overhyped and, if this is the case, why? If it is, moreover, what impact is this having on the development of cyber security policy? Certainly there appears to be a massive industry built up around cyber security, which is looking to profit from people's fears about cyber intrusions. President Dwight Eisenhower's prophetic warning of the emergence of a military industrial complex does not seem fantastical in the context of the billions of dollars being awarded by the US government for the safeguarding of digital infrastructure and the intrusive role that agencies like the National Security Agency have taken in cyberspace. Just as with the threat from terrorism in the

post-9/11 environment, an excessively military response to cyber attacks, combined with a failure to develop a wide range of civil and criminal mechanisms, may lead to less effective policy. It may even, as the authors contend, endanger the stability of the international system, deny society the positive effects of the Internet, and corrupt the way the Internet itself operates. One hopes that these claims also turn out to be an exaggeration of what's possible if the Internet continues to be exploited by states for narrow self-interest.

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

Notes

[1]. John Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats and Why We Believe Them* (New York: Free Press, 2006); Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5-32; Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013); and Mary O'Connell, "Cyber Security without Cyber War," *Journal of Conflict & Security Law* 17, no. 2 (2012): 187-209.

[2]. For a detailed discussion see Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," *Defence Studies* 15, no. 4 (2015): 297-319.