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

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

http://www.h-net.org/~diplo/ISSF
http://www.issforum.org

H-Diplo/ISSF Editors: **James McAllister and Diane Labrosse**
H-Diplo/ISSF Web and Production Editor: **George Fujii**
Commissioned for H-Diplo/ISSF by **James McAllister**

H-**Diplo** | **ISSF Review Essay** (No. 17)

Thomas Rid. ***Cyber War Will Not Take Place.*** London: Hurst & Company, 2013. ISBN: 9781849042802 (paperback, £14.99).

Published by H-Diplo/ISSF on **10 October 2013**

http://www.h-net.org/~diplo/ISSF/PDF/RE17.pdf

Reviewed by **Brandon Valeriano**, University of Glasgow

With *Cyber War Will Not Take Place*, Thomas Rid has written an important volume at a critical juncture of the cyber-conflict debate. In a rush to articulate a new threat after the end of the Cold War, the demise of regional powers in the Middle East and North Africa (such as Syria, Iraq, and Libya, making Israel more secure), and the near total rejection of the Global War on Terror, the next threat to materialize appears to be cyber war. This is the impression one might get if engaging the current security discourse. Both the United Nations and United States have argued that the threat of cyber warfare is greater than the danger of terrorism, a striking reversal barely ten years after 9/11. Yet, as Rid notes (along with others in this developing literature), the threat of cyber warfare often is overstated and near nonexistent.[1] Building on an article in *Journal of Strategic Studies (2012)*, Rid argues, very forcibly, that cyber war will not take place.[2]

[1] Others working from the skeptical or logical standpoint include: Erik Gartzke, "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth," forthcoming, *International Security,* 2013; Clement, Guitton, "Cyber insecurity as a national threat: overreaction from Germany, France, and the UK?" *European Security*, 2013, 22 (1): 21-35; Brandon Valeriano and Ryan C. Maness, "The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype." *Foreign Affairs,* November 2012.

His argument is based on logic and a careful engagement of what the term 'war' really means. Defining terms is important in this exercise. He defines war in the manner of Carl von Clausewitz and posits that it is an act of force and violence used in order to obtain a political objective. Since cyber war does not include violence or force in its conduct, it is tough to argue that cyber war will take place because the tactic rarely can breach the gap between violations of information and data, on one hand, and physical harm, on the other. Of course, one can make the argument that this breach can happen. The influential *Tallinn Manual* that evaluates customary international legal standards as they apply to cyber technologies points out that a pacemaker can be a target of hackers and even suggests this could be a legal step taken by a state.[3] At the recent Black Hat 2013 conference, it was demonstrated that smart cars can be taken over remotely, the same fear was put forth for the 787 Dreamliner plane when software flaws were pointed out.[4] Yet, these dangers are hypothetical; to make the leap from the hypothetical to the actual is perhaps disingenuous or, as some might argue, dangerous.

Overall, Rid's argument is nuanced. When Rid asserts that cyber war will not take place, he is speaking of something very specific - warfare in conventional terms. "Most cyber attacks are not violent and cannot sensibly be understood as a form of violent action" (12). Of course there will be cyber battles, but it is not at all clear that cyber security will dominate the international affairs landscape in the future. Rid notes that the cyber attacks that have happened in the past (specifically in Estonia and Georgia) have been very minor in terms of their impact. The rush to push the threat to the top of the security agenda in some ways makes the issue a self-fulfilling prophecy in that if the threat is overstated, then states will overreact to the fear and build their own cyber armies. This would then provoke the security dilemma and push the other side to react. Because of this process, a careful evaluation of the cyber threat is critical at this juncture.

Another important aspect of the book is its coverage of cyber weapons. By defining cyber weapons on a spectrum, Rid is able to carefully classify each tactic according to its actual usage and practices. A potential limitation of this discussion is that it is not detailed enough. There is room here, and a need, to educate non-cyber practitioners about the details of cyber actions.

http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar?page=show#.

[2] Thomas Rid, "Cyber War Will Not Take Place" *Journal of Strategic Studies* 2012, 35(1): 5-32.

[3] Michael Schmitt, "The Tallinn Manual on the International Law Applicable to Cyber Warfare." *NATO Cooperative Cyber Defence Center for Excellence.* New York and London: Cambridge University Press, 2013.

[4] Black Hat 2013, http://securitywatch.pcmag.com/security/314164-black-hat-2013-hacking-home-security-systems-cars-nsa .

The rest of the book covers many important issues in the cyber debate. Rid notes that the oft-stated attribution problem is a political, not a technical, problem. This is an important insight that many in the cyber community seem to miss. He also discusses the actual content of cyber attacks which are generally espionage or sabotage activities. Understanding the tactic in this manner pushes us away from frames of warfare and towards applications of defense and internal resiliency. Since governments have dealt with espionage and sabotage as long as humans have organized as collective enemies, why should cyber tactics be treated as something new when they are the continuation of age-old practices?

The main flaw of the book is simply that Rid does not take his argument beyond the context of war to examine the nature of cyber conflict in general. In the preface to the book he sets this question up by suggesting that cyber attacks are making conflicts less violent. This is an interesting and important hypothesis that needs more engagement. To be fair, this request does not reflect Rid's goal and perhaps goes beyond the bounds of this book. He has also addressed this question in other places - see his recent article in *Foreign Policy* entitled *Cyber Sabotage is Easy* where he engages the issue of a lack of sabotage operations.[5] In this volume he could have gone further, but here he sticks to a cohesive argument, develops it, and executes in a well written and easy to grasp style. In this context, *Cyber War Will Not Happen* is a foundational text in the cyber security field.

Rid's volume is an important piece of evidence in the cyber-conflict debate. Any responsible scholar should use this volume to counter the divergent perspective contained in the Clarke and Knake volume *Cyber War*, perhaps the most widely read tome in the field.[6] We are witnessing the development of a new strain of security research. This developing area differs different from past tactics that have been engaged in the security discourse such as nuclear warfare, terrorism, and counterinsurgency in that skepticism seems early on to have developed from the academic perspective. Rid's volume advances this perspective through a careful engagement of the term and the limitations of the practice of cyber war. Perhaps this is a positive development. Possibly we have learned our lessons from past failures to fully explore the implications and contexts of the security discourse before rushing to action in the policy sphere. There are many threats to society, and to meet them effectively we must fully dissect and engage those that would seek to articulate emerging threats on the landscape without challenge. In a rush to push the cyber threat, we might be missing more critical issues such as the consolidation of Arab Spring democracies (Egypt), mass-migration in the context of ongoing conflicts (Syria), and energy security (the post-Soviet States). It is likely that the cyber threat is overstated; Rid's volume is the first shot fired against those would seek to make cyberspace the realm of conflict.

[5] Thomas Rid, (2013) "Cyber-Sabotage is Easy." *Foreign Policy*, http://www.foreignpolicy.com/articles/2013/07/23/cyber_sabotage_is_easy_i_know_i_did_it

[6] Richard A. Clarke and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Harper Collins, 2010.

Brandon Valeriano (Ph.D. Vanderbilt University, 2003) is a Senior Lecturer at the University of Glasgow in the Department of Politics and Global Security. Dr. Valeriano's main research interests include investigations of the causes of conflict and peace as well as the study race/ethnicity from the international perspective. Ongoing research explores interstate rivalry, classification systems of war, arms buildups, cyber conflict, popular culture and foreign policy, and Latino foreign policy issues. Dr. Valeriano has published over two dozen articles and book chapters in such outlets as the *Journal of Politics*, *International Studies Quarterly, International Interactions, Third World Quarterly, and Policy Studies Journal*. He recently published a book on the origins of rivalry (*Becoming Rivals*, Routledge 2012) and a book on China, Tibet, and Hollywood (Palgrave, 2012). He is currently wrapping up production on two more books (one that empirically examines cyber conflict) and preparing a book length exploration of Latino International Politics.