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**

The Skeptics Misconstrue the Cyber Revolution: A Response to Commentators on ISSF/H-Diplo and elsewhere[1]

by **Lucas Kello**, Harvard University

(Referencing H-Diplo/ISSF Review Essay No. 17 by **Brandon Valeriano** on **Thomas Rid. *Cyber War Will Not Take Place*.** London: Hurst & Company, 2013. Published by H-Diplo/ISSF on 10 October 2013 at **http://www.h-net.org/~diplo/ISSF/PDF/RE17.pdf**)

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

Let it be stated at the outset: the virtual weapon has not fundamentally changed the nature of war. Further, insofar as the consequences of its use do not rise to the level of traditional interstate violence, there will be no such thing as cyber 'war.' In these respects, those who claim that the contemporary cyber peril is overblown are correct. Yet the Clausewitzian philosophical framework—a cherished device of the cyber skeptics[2]—misses the essence of the cyber revolution: 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 disanalogy of war conveys only

[1] This statement draws from the author's forthcoming article titled, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," in the Fall 2013 issue of *International Security*: http://www.mitpressjournals.org/loi/isec . See http://www.h-net.org/~diplo/ISSF/PDF/RE17.pdf for a recent H-Diplo/ISSF review of Thomas Rid's *Cyber War Will Not Take Place* and the ensuing discussion in the October H-Diplo discussion logs, http://h-net.msu.edu/cgi-bin/logbrowse.pl?trx=lx&list=H-Diplo&user=&pw=&month=1310 .

[2] See for instance Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).

what the cyber issue is not; it does not reveal the true significance of the danger, and may even conceal it.

What, then, is the shape of the cyber danger? One can think of three main aspects. First is the potency of cyberweapons. True, the new capability has produced no fatalities or physical destruction comparable to a traditional war. Let us concede, further, that 'war by malware' is very costly to mount (on which more below). Two problems nevertheless persist for the skeptics. First, the upper threshold of proven harm has steadily been rising. Until recently, the use of code as a weapon to damage physical infrastructures was conceivable only in the abstract; the dazzling spectacle of the Stuxnet worm, which impaired hundreds of enrichment centrifuges at the Natanz nuclear facility in Iran, changed that. Moreover, the weapons' potential to cause loss of life is widely recognized—even if, so far, it has been unrealized. Second, nondestructive cyberattacks can inflict considerable harm on the political, economic, and social world. Take, for example, the attacks against computer systems in Estonia in 2007. Because there was no physical wreckage, the label of 'cyberwar' does not apply here; nevertheless, the attacks caused a national disruption of government and financial activities. (This, too, had once been deemed by many an implausible outcome of the cyber phenomenon.)[3]

The trajectory of proven harm, in short, has few clear limits. We should not seek to impose them on so novel and volatile a technology; negative claims about the future always suffer the possibility that the forecast will be spoiled by events. At any rate, destructive action may not pose the most pressing concern, as any Estonian official will attest.

A second manifestation of the cyber danger concerns the complications of defense. Practitioners in this domain have repeatedly warned that the cyber offense holds the advantage. Disbelievers challenge this view by emphasizing the very high costs of staging a sophisticated cyberattack. They cite the complex 'Olympic Games' operation against Iran to make their point. For this reason, some skeptics claim that the defense—not the offense—is superior. This conclusion, however, is only half complete; it does not account for the other side of the strategic picture: the enormous costs of defense. At least five factors weigh on the defender: (1) the difficulty of predicting—or even detecting—the precise method of attack impedes the design of measures to repulse it; (2) the possibility that attack code will reside undiscovered in an adversary's computer system affords the invader means to deprive the defense of the ability to manage its own protection; (3) the growing intricacy of computer systems at all levels of design and use tilts the work-load imbalance between the offense and defense in favor of the former (whereas the attacker need understand only the procedures of entry and attack it decides to employ, the defender must continuously protect the entire network surface against the vast universe of conceivable attacks); (4) the fragmentation of defense responsibilities within government and across the public and private sectors is a limiting factor when formulating a coherent response to a cyber

[3] Before the 2007 attacks, NATO repeatedly rebuffed calls by Estonia (officials in the country saw the peril) to establish a center of excellence in cyber defense. Alliance opinion turned after this event; presently eleven member states partake in the initiative, established in 2008.

emergency; and (5) the increasing reliance on off-shore manufacturers to stock hardware and software components introduces unknown vulnerabilities in the supply chain, which an opponent could manipulate in a future military or diplomatic crisis.

In sum, the thesis of defense dominance misses a crucial truth: the offense-defense equation is relative; thus the absolute measurement of offensive costs has meaning only in reference to the defender's expenses, which are far greater. At most, the high price of mounting a high-impact cyberattack limits the ability of traditionally weak players to harness cyberspace for asymmetrical gain. It does not eliminate the significant tactical advantages of a possessor of advanced code.

A third factor involves disturbances to strategic stability. This can occur in two general ways. One problem is instrumental instability, a condition in which poor 'if-then' knowledge of a new genus of conflict produces misinterpretation and accidents even among rational state adversaries. Six peculiar features of the cyber phenomenon contribute to this problem: (1) offense superiority instigates a race to arms, elevating not only the perceived advantages but also the opportunities of offensive cyber use; (2) attribution difficulties in the aftermath of a cyberattack weaken deterrence logics by reducing the assailant's expectation of unacceptable penalties; (3) the new capability's technological volatility impedes interpretation of the probable effects of its use, producing unknown dangers of collateral effect and blowback; (4) poor strategic depth—the very short time between the detection and impact of a cyberattack—strains traditional crisis management and response procedures; (5) the rising number of cyber-capable players within and beyond government can hinder the ability of states to act as coherent units in a crisis; last, (6) the inordinate degree of escalatory ambiguity in the new domain of conflict elevates the risks of an accidental or accelerating crisis. Consider the Equivalence Principle that underpins U.S. cyber defense policy. As a variation of the doctrine of 'calculated ambiguity,' the principle leaves open the possibility of a forcible response to a cyberattack without, however, specifying thresholds for such a response.[4] Here, then, is a danger that the skeptics overlook or downplay: what begins as a low-intensity cyber exchange could intensify into a major showdown, possibly of conventional proportions. A major crisis, moreover, could be set in motion by cyber exploitation if the defender misconstrues it as a step preparatory to attack and instigates a preemptive blow.

Another source of instability in the cyber domain is more fundamental: the dispersion of power away from governments. While states remain the most capable cyber players, they are not alone. The cyber revolution is empowering a variety of nonstate actors such as extremist militant groups, political activists, and criminal syndicates.[5] Although states have shown reserve in the use of cyber artifacts, nontraditional players may not be so inhibited.

[4] As one U.S. soldier put it rather cavalierly, "If you shut down our power grid, maybe we will put a missile down one of your smokestacks." Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, May 30, 2011.

[5] See Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), chapter 5.

They may use the new technology in ways that disrupt interstate dealings, perhaps initiating a 'catalytic' cyber event that instigates a diplomatic or military showdown. Thus, a dangerous separation of power and diplomacy is occurring: even if problems of instrumental instability in the cyber domain were soluble through intergovernmental agreement—a Sisyphean task thus far—private culprits could still unsettle the interstate equilibrium by defying the consensus. It must be emphasized: the cyberattacks that were conducted by nonstate actors to freeze financial activity in Estonia prompted officials in that country to contemplate invoking NATO's collective defense clause, a move that would have embroiled the Alliance in a major crisis with Moscow. In short, the diversity of relevant actors and the possibility of cooperation among them are likely to disturb established patterns of security competition.

The cyber revolution is still incipient: we are only at the initial stages of the great technological current. Whether security scholars grasp its implications for international security will depend on their ability to break free from their own preconceptions as to what constitutes a serious threat.

Lucas Kello is a Postdoctoral Research Fellow in the International Security Program and the Project on Technology, Security, and Conflict in the Cyber Age at the Harvard Kennedy School's Belfer Center for Science and International Affairs. He is also affiliated with the MIT-Harvard Project on Explorations in Cyber International Relations.