Correspondence

A Cyber Disagreement

Jon R. Lindsay
Lucas Kello

To the Editors (Jon R. Lindsay writes):

Policymakers and pundits have been sounding alarms about internet insecurity for years, so the first appearance of anything in *International Security* (*IS*) on this topic is a welcomed development. In the fall 2013 issue, Lucas Kello takes the security studies community to task for ignoring cyber perils, while Erik Gartzke argues that cyberwar is of limited political utility.[1] Kello writes that "[t]he Clausewitzian philosophical framework misses the essence of the cyber danger and conceals its true significance: the virtual weapon is expanding the range of possible harms between the concepts of war and peace, with important consequences for national and international security" (p. 22). Gartzke counters, "War is fundamentally a political process, as Carl von Clausewitz famously explained. . . . The internet is generally an inferior substitute for terrestrial force in performing the functions of coercion or conquest" (p. 42). If Kello is right, then the long silence in *IS* on cybersecurity suggests that scholars have neglected a major transformation in security affairs. If Gartzke is right, then scholars can be forgiven their bemusement with inflated cyber rhetoric.

In my investigations of American and Chinese activities, I have found cyber interventions to be more complicated and less effective than generally believed.[2] Arguments from technology are common in cybersecurity discourse and have excited policymakers, so they should be taken seriously. Yet Kello's characterization of the skeptical viewpoint as "more visceral than analytical" (p. 9) misrepresents the analytical literature that does exist. Kello insists that "scholarly inattention toward the cyber issue . . . must change" (ibid.), but he disparages the field while ignoring relevant scholarship. My commentary addresses the technological determinism of Kello's argument and his

Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California San Diego School of International Relations and Pacific Studies.

Lucas Kello is Senior Lecturer in International Relations at Oxford University.

[1] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 7–40; and Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 41–73. Further references to Kello's article appear parenthetically in the text.

[2] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (July 2013), pp. 365–404; and Jon R. Lindsay and Tai Ming Cheung "From Exploitation to Innovation: Acquisition, Absorption, and Application," in Lindsay, Cheung, and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press, forthcoming).

International Security, Vol. 39, No. 2 (Fall 2014), pp. 181–192, doi:10.1162/ISEC_c_00162

misrepresentation of the state of the field. I do not comment on Gartzke's article because I read earlier drafts of it, and we are collaborators on a related project.

DOES TECHNOLOGY DRIVE POLITICS?

Kello's article asks, "Does the new technology require a revolution in how scholars and policymakers think about force and conflict?" (p. 7). In an important book published in 1977, Langdon Winner assesses a number of myths about technology: that it leads to domination by the state that possesses it or to revolutionary subversion, that its essential nature requires particular policies, that complex infrastructure leads to societal paralysis, and various other imperatives.[3] Winner's critique is as relevant to the internet age as it was to Marxist expectations of the factory age. Military history, in particular, is littered with arguments from technology that failed in experience: the stirrup will transform the feudal order; the tank will sweep away infantry; the bomber will zip through defenses to cripple the enemy; and sensor-to-shooter networks will make war quick and decisive. Almost every study of technology and war finds that doctrine, organization, and the circumstances of employment matter as much as, or more than, the characteristics of weapons for military performance.[4]

Kello instead argues that poor performance results from misunderstanding the true nature of new technology: "Historically, bad theories of new technology have been behind many a strategic blunder. In 1914, British commanders failed to grasp that the torpedo boat had rendered their magnificent surface fleet obsolescent. In 1940, French strategic doctrine misinterpreted the lessons of mechanized warfare and prescribed no response to the Nazi tank assault" (p. 14). These examples are unfortunate choices. It was not the battleship but the torpedo boat that became obsolete, despite the revolutionary expectations of the French Jeune École. The British adopted searchlights, close-range small-caliber guns, and thicker armor to defend their ships, and the Royal Navy successfully kept the High Seas Fleet bottled up after Jutland.[5] Blitzkrieg played out

[3] Langdon Winner, *Autonomous Technology: Technics-Out-of-Control as a Theme in Political Thought* (Cambridge, Mass.: MIT Press, 1977).

[4] See, inter alia, Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Ithaca, N.Y.: Cornell University Press, 1984); Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, N.Y.: Cornell University Press, 1991); Williamson Murray and Allan Reed Millett, *Military Innovation in the Interwar Period* (New York: Cambridge University Press, 1996); Stephen Biddle, "The Past as Prologue: Assessing Theories of Future Warfare," *Security Studies*, Vol. 8, No. 1 (Autumn 1998), pp. 1–74; MacGregor Knox and Williamson Murray, *The Dynamics of Military Revolution, 1300–2050* (New York: Cambridge University Press, 2001); and Keir A. Lieber, *War and the Engineers: The Primacy of Politics over Technology* (Ithaca, N.Y.: Cornell University Press, 2005).

[5] Edward N. Luttwak discusses the torpedo boat as an example of how specialized weapons fall prey to specialized countermeasures. See Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, Mass.: Belknap, 2001), pp. 34–35. The torpedo boat was hardly the only technological development in the decades leading up to World War I; the Fisher dreadnought revolution was far more significant, although here, too, the technological advantages offered were both temporary and contextual. See Holger H. Helwig, "The Battlefleet Revolution, 1885–1914," in Knox and Murray, *The Dynamics of Military Revolution*, pp. 114–131. On the rise and fall of the Jeune École and reactions to Jutland, see Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present* (Cambridge: Cambridge University Press, 2010), pp. 234–254.

quite differently against the French in 1940 and the Russians in 1941, and even the disaster of 1940 had as much to do with intelligence failures and bad luck on the battlefield as bad doctrine. By late 1944, moreover, the Nazi masters of blitzkrieg had resorted to static defenses along the very same Maginot Line to counter the Allied advance.[6] In a violent political contest between determined adversaries, there are no technological silver bullets or vouchsafed doctrines for their use. The dialectical logic of strategy has a way of undermining simple extrapolations of any one factor. Why should the internet be any different?

Kello reviews many of the supposedly revolutionary properties of cyberspace, such as the potency of virtual weapons to cause physical or economic harm, their unpredictability and undetectability, their wide affordability, and the high costs of cyber defense. Each of these claims can be disputed. If, for example, cyberspace is so offense dominant, then where are all the major cyberattacks? Indeed, there is only one known historical case of cyberattack that has damaged physical infrastructure: the Stuxnet attack on Iranian enrichment infrastructure discovered in late 2010. Kello describes this as "a case cherished by skeptics who challenge the common wisdom of offense dominance [in cyberspace]" (p. 30), even as he elsewhere cites Stuxnet as evidence for the cyber revolution (pp. 14, 19–20, 27–28). As one of said skeptics, I point out that "the [George W.] Bush administration reportedly authorized $300 million for 'joint covert projects' aimed at Iran's nuclear program . . . [yet] this pricetag . . . does not include the substantial infrastructure, expertise, and experience already paid for and embodied in agencies like the NSA, CIA, and Mossad."[7] There is little to suggest that the Iranians paid anything like, as Kello writes, the "enormous costs of defense against a cyberattack" (p. 27), and they seemed to have neglected numerous cheap and easy prophylactic measures, instead relying on default passwords and failing to patch publicly known vulnerabilities exploited by Stuxnet (in addition to its "zero days"). Once Stuxnet was discovered, moreover, Iran paid nothing for all of the free expertise and patches it received from the global open-source cybersecurity community. Far more importantly, the years of planning and reconnaissance that preceded the attack on Natanz, and the restraint shown in the design of the attack payload (which merely degraded enrichment efficiency rather than caused a catastrophic breakdown), suggests that American and Israeli planners were quite concerned about getting caught by Iranian defenses, such as they were. Kello writes, "Stealth was a genial feature of this multistage operation" (p. 28), but stealth also bounded the ambitions of the attack, which relied on secrecy to accomplish anything at all. Sensitivity to compromise is a common limitation of any covert action, cyber or otherwise. There is nothing categorically offense dominant about cyberspace.

Even if one grants all of Kello's determinist claims about cyber capabilities, there is no reason that they would necessarily be useful for politics. There are myriad ways to cause harm in the world with everyday objects, such as box cutters, yet most of them

[6] Ernest R. May, *Strange Victory: Hitler's Conquest of France* (New York: Hill and Wang, 2000); Williamson Murray, "May 1940: Contingency and Fragility of the German RMA," in Knox and Murray, *The Dynamics of Military Revolution*, pp. 154–174; and Rick Atkinson, *The Guns at Last Light: The War in Western Europe, 1944–1945* (New York: Henry Holt, 2013).

[7] Lindsay, "Stuxnet and the Limits of Cyber Warfare," p. 388.

never come to pass because perpetrators do not benefit from inflicting harm. Box cutters became lethal in the hands of al-Qaida because the terrorists were motivated to cause violence, but we do not need a theory of box cutter warfare to explain why. Terrorists use bombs to terrify, but there is little frightening about internet outages or even temporary drops in the stock market caused by computer glitches, which we have experienced aplenty. More dramatic cyber harm is possible, to be sure, such as the disruption of air traffic control or the release of dangerous chemicals via computer malfunction; most imagined cyber weapons are useless, however, for communicating threats because they depend on secrecy to be effective (and advertised computer vulnerabilities can be readily patched). Surprise attack can be useful for conquest, rather than coercion, but only as long as the attacker is able to exploit the temporary advantages that surprise creates by following through with kinetic attack. Otherwise the cyber sucker punch does not change the balance of power and may even invite retribution. Those who worry about a digital Pearl Harbor would do well to remember Japan's experience after the real Pearl Harbor.

Kello counters that "the cyber revolution is influencing the tendencies of anarchical politics, rather than merely altering the strategic dealings of states; that is, the cyber domain exhibits both fundamental and instrumental forms of instability" (p. 39). Thus skeptics ignore "threats that appear to lack an overtly physical character or that do not rise to the level of interstate violence [and thus] are intellectually uninteresting" (p. 11). So what are these perils short of war? Naval blockades and economic sanctions were used to harass countries long before Estonia suffered distributed denial of service attacks on its web servers; yet while these economic harms produce civilian suffering, their political influence has proved more limited. There is no doubt that cyberspace enhances intelligence collection, but espionage is only one of many other inputs into a policy decision or industrial result, not a decisive advantage. Crowds, public firebrands, and media outlets have been able to agitate noisily for ages, but their ability to influence elites through symbolic demonstration alone is questionable. Terrorism, insurgency, and population targeting have blurred the line between military and civilian affairs ever since Julius Caesar campaigned in Gaul. Kello never clearly spells out just what phenomena between peace and war he is most worried about and why cyberspace somehow makes them more worrisome. Escalation to kinetic warfare via cyberspace simply takes us back to the political question of *cui bono*.

Kello's claim about the dangerous expansion of harms short of war can, in fact, be turned around. Precisely because cybersecurity is not very useful by itself for coercion or conquest, it is more useful for activities that fall well short of war, such as espionage, blockade, piracy, and protest. Cyberspace—or any technological means of influence—does not escape Clausewitzian logic; it is ruthlessly constrained by it. There are many interesting questions about how cyber operations short of war or in time of war might actually be employed, or about the strategic logic that constrains their combination with other forms of power, or the institutional arrangements best suited for their domestic and international management. These outstanding questions do not necessitate a departure from a realist paradigm, however, and they do not compel us to adopt Kello's rhetorical tactics, to which I now turn.

a dereliction of duty?

Kello accuses security scholars of "theoretical stagnation" (p. 12) and an "unwillingness to break free from their preconceptions as to what constitutes a serious threat" (p. 22). As evidence for the seriousness of the threat, Kello approvingly quotes a number of statesmen, soldiers, and spies. Remarkably, he never takes seriously the possibility that such sources are exaggerating or simply wrong. There are good reasons to expect bureaucratically or industrially motivated threat inflation to increase, even as actual security risks decrease.

Far more troublingly, Kello fails to mention literature by scholars who have undertaken serious evaluations of the cyber threat. An empirical study of cyberattacks between rivals from 2001 to 2011 found activity to be regionalized and restrained rather than global and disruptive.[8] My study of Stuxnet finds that the facts of this important case actually undermine several key tenets of the cyber revolution thesis.[9] Assessment of public response to historical disasters and bombings undermines expectations of panic and instability in the wake of cyberattack.[10] Government agencies and the cybersecurity industry are found to have strong incentives to exaggerate cyber threats, using the language of national security rather than, say, public health and safety, industrial policy, or law enforcement.[11] Other scholars question the strategic utility of cyber weapons even while envisioning some utility for support to battlefield operations.[12] Kello's article even omits scholarship that is sympathetic to his viewpoint yet was published a decade ago,[13] to say nothing of more recent academic offerings.[14] It is true that "[t]he

[8] Brandon Valeriano and Ryan Maness, "The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype," *Foreign Affairs*, November 21, 2012, http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar; and Brandon Valeriano and Ryan Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011," *Journal of Peace Research*, Vol. 51, No. 3 (May 2014), pp. 347–360. Although the latter article had not yet appeared when Kello's article was published, Valeriano and Maness's core findings were published in "The Fog of Cyberwar" in 2012.

[9] Lindsay, "Stuxnet and the Limits of Cyber Warfare."

[10] Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics*, Vol. 10, No. 1 (February 2013), pp. 86–103.

[11] Myriam Dunn Cavelty, "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology & Politics*, Vol. 4, No. 1 (October 2008), pp. 19–36; Paul Ohm, "The Myth of the Superuser: Fear, Risk, and Harm Online," *University of California Davis Law Review*, Vol. 41, No. 4 (April 2008), pp. 1327–1402; and Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy" (Arlington, Va.: Mercatus Center, George Mason University, 2011).

[12] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, Calif.: RAND Corporation, 2009); David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed," *Journal of Strategic Studies*, Vol. 35, No. 5 (October 2012), pp. 689–711; and Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013). Kello briefly cites one minor point by Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012), pp. 401–428. He does not, however, mention Liff's overall skepticism about the scope and significance of the threat that cyberweapons pose.

[13] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, Mass.: MIT Press, 2001).

[14] Derek S. Reveron, ed., *Cyberspace and National Security: Threats, Opportunities, and Power in a*

number of articles in academic international relations journals that focus on security aspects of the cyber revolution is small" (p. 8 n. 5), so it should not have been hard for Kello to adequately review the literature. He argues that scholars must "accept the existence of the cyber peril" or else "articulate theoretical and empirical challenges to the conventional policy wisdom" (p. 9). Yet skeptics have, in fact, done as Kello asks. Florid warnings from self-interested politicians make for poor counterargument. Indeed, Kello's rhetoric has something to offend everyone. He complains that "technologists are unequipped to address" international security because "technical virtuosity is not identical to strategic insight" (p. 16). However, leading computer security experts such as Ross Anderson and Bruce Schneier emphatically stress that security is a matter of political and economic incentives more than engineering design.[15] Elsewhere Kello objects to "the overly technical tone" (p. 16 n. 27) of Martin Libicki's work, but in fact Libicki uses strategic and political considerations to debunk technological fears and to advocate for an alternative focus on international standards policy.[16] Kello never engages the substance of Libicki's arguments or cites the rest of his substantial and cogent output on the topic.[17]

Furthermore, Kello makes dubious technical claims throughout his article, all the while excoriating scholars for not understanding computers. Why is it that "not all threats propagated through the web can transmit via the internet" (p. 17), when anything that can propagate through the HTTP protocol, which defines the world wide web, can certainly transmit through the internet in principle? Whether a particular web server is connected to the global internet or stranded in Kello's "cyber archipelago" (p. 17) is quite another question. Kello insists that "the interesting segmentation of cyberattack effects lies at the logical, not the physical, boundary of cyberspace" (p. 20), but the distinction of programming semantics from engineering implementation in computer science, or the common vocabulary in a major National Research Council study of cyberattack,[18] or the pragmatic value of rules of engagement that distinguish reversible damage to code versus irreversible damage to equipment, all imply that the physical boundary is very important to strategic and pragmatic analysis. Kello discusses Stuxnet's "intrusion into the Natanz PLC" and "six vulnerabilities in the PLC" (p. 27), but the programmable logic controller (PLC) was just one piece of equipment in

Virtual World (Washington, D.C.: Georgetown University Press, 2012); and Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens: University of Georgia Press, 2011).

[15] Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. (Indianapolis: Wiley, 2008); and Bruce Schneier, *Liars and Outliers: Enabling the Trust That Society Needs to Thrive* (Indianapolis: Wiley, 2012).

[16] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007)

[17] Especially surprising is the omission of Libicki, *Cyberdeterrence and Cyberwar*, and Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, Calif.: RAND Corporation, 2012).

[18] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academies Press, 2009).

the larger industrial control system at Natanz, which also included firewalls, Windows servers, operator stations, Siemens software, ersatz Iranian software, and peripherals besides PLCs. The vulnerabilities that facilitated Stuxnet's propagation were emphatically not in the PLCs, but in Windows and Siemens software. Kello's very definition of cyberspace as "all computer systems and networks in existence" (p. 17) omits all the technicians, network operators, vendors, regulators, and institutions that the internet studies field recognizes as essential to the "sociotechnical" fabric of cyberspace.[19] So much for "common technical concepts" (p. 17). Even if one accepts the dubious claim that technology determines strategy, Kello's misrepresentation of "the features of the technology and its related phenomena that are most relevant to the field" does little to improve understanding (ibid.).

STILL AWAITING THE REVOLUTION

The flaws in Kello's article make it hard to recommend even as representative of the cyber revolution side of the debate.[20] Kello's conflation of technological possibility and political consequence hinders rather than helps inquiry into the complex issues that are sure to occupy scholars and practitioners well into the future. Many cybersecurity issues, moreover, will be better addressed in the domain of political economy rather than traditional security (i.e., the governance of internet protocols and international trade policy). Scholars in security studies are not compelled to retool themselves in order to examine various and sundry topics throughout the rest of political science if their main interests lie in the causes and consequences of serious political violence. At the same time, information technologies have long been useful in war and will continue to be indispensible for all types of belligerents. It is possible and desirable to clear away the hype and misconceptions about cybersecurity without dismissing new and interesting problems altogether. Neither Gartzke nor anyone else has yet had the final word on cybersecurity, so there remains much for future articles in *IS* to explore. Information technology provides new ways and means for actors in anarchy to pursue their interests, and networks may yet catalyze an increase in complexity of their interactions. Nevertheless, technology does not free actors from the political logic of strategy.

—*Jon R. Lindsay*
La Jolla, California

[19] Greg Downey, "Virtual Webs, Physical Technologies, and Hidden Workers: The Spaces of Labor in Information Internetworks," *Technology and Culture*, Vol. 42, No. 2 (April 2001), pp. 209–235; David D. Clark et al., "Tussle in Cyberspace: Defining Tomorrow's Internet," *IEEE/ACM Transactions on Networking*, Vol. 13, No. 3 (June 2005), pp. 462–475; and Laura DeNardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge, Mass.: MIT Press, 2009).

[20] Perhaps more useful for this purpose is William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, September 1, 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

Lucas Kello Replies:

The cyber revolution will not cease at the frontiers of the international system because theorists want it to. Some aspects of the cyber issue fit the frame of traditional notions of security. Others challenge the conventional models: the expansion of nonphysical threats to national security, the ability of nonstate players to instigate a diplomatic crisis, the erosion of the distinction between local and distant conflict, the deep penetration of the most basic infrastructures by unknown adversaries, and so on.

Skeptics dismiss these peculiar features of security in our times. Their main interest is to bring the virtual weapon to the rule of conventional statecraft, a task for which they invoke that unfailing servant of intellectual reactionism in the field of international security studies: Carl von Clausewitz. A finer dean of the school of skepticism does not exist: Clausewitz routinely neglected the important role of technology in his own age.[1] It is mistaken to suppose that his concepts can decipher the meaning of this new technology in ours.

Jon Lindsay is an adherent of this school. His skepticism has in relation to my article a dual method.[2] First, is a substantive challenge: he denies my claim that a revolution in security affairs is taking place. To support this view he invokes an arsenal of familiar concepts, principally, the Clausewitzian philosophical framework of interstate war—conceived for an age in which Thomas de Colmar's Arithmometer symbolized the quintessence of computing ability. Such disagreement is always welcome, for it reflects the heat of controversy that appropriately attaches to the strategic and moral conundrums arising from rapid technological change. Scholarly publications such as *International Security* will find in these contentions fertile soil for enriching debate.

One of Lindsay's substantive criticisms concerns the question of technological determinism: new technology, he argues, does not singly determine strategy; instead, strategy is at least as much a product of "doctrine, organization, and the circumstances of employment." As a proposition about states' responses to technological change, the point is unassailable, but as a criticism it falls flat. Mine is not a deterministic view. Recall a central statement of the article: "[M]ore important than the nature of a new weapon are the nature of its possessor and the purposes that instigate its use" (p. 32). In other words, the formation of strategy is an endogenous process shaped and constrained by the political and organizational milieus in which players adopt a new weapon into their arsenals. Take, for example, the advent of mechanized warfare in the early twentieth century. Not the emergence of the tank per se but the strategic ends ascribed to it by Nazi Germany, and, crucially, the inability of French and British military planners to decipher the role of mechanized units in Germany's plan of conquest, produced the fiasco of 1940 (p. 14). So, too, with cyberweapons. The new capability shapes not strategy, but strategic realities. This nuance is simple; its consequences for the de-

[1] See Michael Howard, *Clausewitz: A Very Short Introduction* (Oxford: Oxford University Press, 2002), p. 22.

[2] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 7–40. Subsequent references to this article appear parenthetically in the text.

bate far-reaching: strategic blunders in the cyber domain can occur not because they are predestined, as Lindsay construes my argument, but because "threats and opportunities arising from a new class of weapon produce pressures to act before the laborious process of strategic adaptation is concluded" (ibid.).

Technological revolution, in short, enables but does not foreordain strategic reversals. The contemporary cyber peril derives at least as much from the abiding lag in doctrinal adjustment to new realities as from the virtual weapon's intrinsic character. Readers may note the various references in my study to the multifactorial relationship among new technology, theory, and action, as well as the general caution that conclusions about this relationship are necessarily limited and provisional.

Elsewhere, Lindsay continues the Clausewitzian technique that has become commonplace among cyber skeptics: he emphasizes that the new technology is not very useful for interstate coercion and does not alter the means of conquest; consequently, new concepts to analyze it are unnecessary. He makes a bizarre analogy to box-cutters in supporting his point. "Box-cutters became lethal in the hands of al-Qaida [on September 11] because the terrorists were motivated to cause violence," he writes, "but we do not need a theory of box-cutter warfare to explain why." The analogy is specious. Enormous civilian aircraft, not utility knives, inflicted mass casualties on September 11. Moreover, the social, economic, and physical consequences of cyberattack are plainly more potent than what is achievable with a blade. These include convulsion of a small nation's financial and government activities (Estonia cyberattack); paralysis of a country's central bank and communications infrastructure (Georgia attack); destruction of hundreds of nuclear centrifuges (Olympic Games operation); and incapacitation of tens of thousands of machines at the world's largest oil firm (Shamoon virus). These cases display an almost sequential accretion of harm that exposes the tenuity of skeptical thinking. Moreover, however alarming, they do not convey the limits of possibility of cyber conflict; scientists widely recognize the potential for graver consequences. The absence of more severe cyberattacks, therefore, does not prove the impotence of the new weapons. It may instead indicate their severity if fear of retaliation and blowback are restraining factors. To the question: Where are all the catastrophic cyberattacks? The easy and obvious response is: Where are all the nuclear attacks?

The trajectory of proven potency, in brief, has few clear limits; one should not seek to impose them on so novel and volatile a capability. We must not be complacent about the cyber phenomenon: it may yet produce devastating surprises. At any rate, physical catastrophe does not exhaust the spectrum of conceivable cyber conflict; although the gravest concern, it may be the least probable danger.

Let us grant that—so far—the new capability has produced no fatalities or physical destruction equivalent to war. Concede, further, that weaponized code is an ineffective tool of coercion. There is still the problem of inadvertent cyber conflict. Accidental crises can occur even among rational state adversaries that seek to avert them; even in situations of non-offensive behavior, for example, if one player misinterprets cyber-exploitation as a prelude to attack. But that is not all. There are also the twin dangers of power diffusion and conflict escalation: nonstate actors can inflict alarming harm; they may do so in ways that propel a crisis beyond the ability of governments to control. All future cyber conflict will face this risk that civilian culprits will disturb the fragile political framework of interstate dealings. On this core concern of the article, Lindsay can answer only by conjuring Clausewitz's dictum that events will be "ruthlessly constrained" by state interests. This view ignores salient facts. In Estonia in 2007, the world witnessed the potential for nontraditional players to precipitate a major diplomatic showdown, one involving Russia and NATO's collective defense clause, which Estonian officials considered setting in motion as their essential infrastructures crashed.

The cyber revolution's greatest dislocations, in the end, may be felt not in the balance of power but in the balance of players. The diffusion of cyber technology elevates to a higher order of significance what some traditionalists in security studies wish to expel from theoretical existence: the nonstate actor. By conscribing the problem of conflict escalation to state purposes—Clausewitz's holy notion—skeptics omit a central and peculiar feature of the new phenomenon. The cyber arena is an interlocking jigsaw of relations among diverse actors—states, corporations, militant groups, "hacktivists," lone agents, and so on—in which the disturbance of a single piece can disrupt all others.

A second set of challenges in Lindsay's letter is graver: he directs fire at the article's portrayal of existing scholarship and technical correctness. About every critic, a key question is: What drives the objection? Lindsay is more translucent in his methods than his motives; thus I can offer only a conjectural account of his more serious censure: it is a tactic to dispel the cyber danger by discrediting those who would call it real. It incites people to ask: Who else but a misconstruer of the new technology could affirm its transforming potential? The more searching question, however, is: Are we entering an epoch of change in security affairs? It is impossible here to provide a complete response to such criticism. What follows is a basic reply.

Lindsay correctly notes that the article does not reference important works about cyber conflict; he denies there is a scholarship gap. For the avoidance of injury: each of the writings he cites makes an important contribution to the political, strategic, or tactical understanding of cyber issues. Yet these works barely (or not at all) integrate the virtual weapon into the theoretical matter of international relations. Therein lies the gap: very little of the prevailing scholarship systematically addresses how cyber activity affects foundational notions such as "anarchy," "system," "regimes," "identity," and "the balance of power," which are the prime units of intellectual currency in international relations. Students in other disciplines hopefully will derive insights from my article. Its designated readership, however, is the international relations community, in which the impression exists that to discuss cyber questions is to risk confusion or—worse—boredom.

Lindsay questions the observation that technologists are unfit to evaluate core aspects of international security. True, computer specialists have recognized that cybersecurity is not primarily a technical problem, but a challenge to political—even philosophical—understandings. But they frame this problem differently than do political scientists, to whom a technical criterion may not always seem appropriate. Well that such disciplinary divisions exist. So many professions—computer science, engineering, law, economics, political science, and so forth—gather at the congress of cyber studies that a distribution of competencies among them is vital. Interdisciplinarity is not the same as unidisciplinarity: it teaches by synthesis, not assimilation. Each delegation, therefore, must identify its strengths (and limits) and conserve its own conception;

other forms are neither superior nor worse, merely different, to be judged according to the standards of their parent disciplines. For international relations scholars, this common form will be our theory—the body of concepts and orderly propositions that select and organize the complex phenomena we study. In this regard, our discipline has yet to fill its presence in the chamber. Evasion of the cyber issue by theorists and analysts only defers difficult questions and produces larger puzzles; hence the need to test our models against it. This crucial assignment belongs to us. We cannot relinquish it to other professions.

Finally, Lindsay raises three technical objections. First, he asks: Why is it that not all threats propagating through the web can transmit via the internet? The web is a subset of the internet. Web-based cyberattacks cannot reach computer systems that do not run web servers—even if these systems are joined to the internet via other protocols (e.g., a virtual private network). To hit such targets, an attacker would have to employ an alternative attack mode, which may require a special development effort. In sum, the web is one of only many access vectors for cyberattack, but it is perhaps the most open form of internet connectivity and thus raises important security concerns.[3]

Lindsay's second technical objection concerns the Olympic Games operation against Iran's Natanz nuclear facility. The vulnerabilities exploited by the Stuxnet worm "were emphatically not in the [plant's] PLCs [programmable logic controllers]," Lindsay observes. On pure definitional terms, he is correct, the vulnerabilities resided in the engineering station (i.e., the machines ordinarily used to access and configure PLCs). But that was hardly the point. More important, the engineering station (and its vulnerabilities) represented a weakness in the very design and operation of the PLCs—the manipulation of which was the attackers' ultimate goal. The industrial controllers relied on it for their proper functioning and proved incapable of detecting or neutralizing threats in it.[4] Lindsay's focus on the fine technical argot obscures this important point; it gives the impression the PLCs existed in isolation.

Third, Lindsay challenges my study's treatment of cyberspace as all computer systems and networks in existence. He can be excused the desire to contest this definition: the meaning of cyberspace is disputed, as the article notes. It is not axiomatic, therefore, that the notion includes "technicians, network operators, vendors, regulators, and institutions." If anything, the common working concept leaves out social agents.[5] At any rate, there are strong reasons to reject Lindsay's definition. We already possess a suitable term for his expansive notion: "cyber domain," which encompasses the bevy of human and institutional actors that operate and regulate cyberspace itself. The two notions, it is important to realize, are distinct. Cyberspace is a technical plane

[3] The author thanks Scott O. Bradner for these insights.

[4] According to Ralph Langner, who uncovered Stuxnet's operational aims, the defenders could have remedied this problem in the security of industrial control systems, for example, "by using a PLC (ladder logic) version control that is independent of the engineering station." Author interview, June 16, 2014.

[5] See Nazli Choucri and David Clark, "Cyberspace and International Relations: Towards an Integrated System," paper presented at Massachusetts Institute of Technology, Cambridge, Massachusetts, August 2011, p. 8.

comprising machines and networks whose uniform feature is manipulability by code; in contrast, the cyber domain is primarily a political and social plane subject to wholly different interventions and behavioral rules. We require separate concepts to capture their separate essences.

Cyber conflict has ceased to be tomorrow and has become today. This makes new demands on security studies scholars: the forces shaping the cyber peril can be reduced only if they are grasped. "The Meaning of the Cyber Revolution" represents an initial attempt to lay out conceptual guideposts for future analysis of the new phenomenon and for a post-Clausewitzian paradigm of security commensurate with it. Few thinkers in our field warn about this danger. Fewer still merge it into theory. The fewest who do both are a battered party; skeptics hurl old concepts at them. Ours is an arguing profession. For an author, instigating such debate in a rising area of study is always welcome. But if disbelievers are to dispose of the cyber revolution, they will have to focus on matters of real substance. Technical and definitional contrivances will not go far.

—Lucas Kello
Oxford, England