Correspondence

Debating the Chinese Cyber Threat

Joel Brenner
Jon R. Lindsay

To the Editors (Joel Brenner writes):

In "The Impact of China on Cybersecurity: Fiction and Friction," Jon Lindsay asserts that the threat of Chinese cyber operations, though "relentlessly irritating," is greatly exaggerated; that China has more to fear from U.S. cyber operations than the United States does from China; and that U.S.-China relations are reasonably stable.[1] He claims that "[o]verlap across political, intelligence, military, and institutional threat narratives . . . can lead to theoretical confusion" (p. 44). In focusing almost exclusively on military-to-military operations, however, where he persuasively argues that the United States retains a significant qualitative advantage, Lindsay underemphasizes the significance of vulnerabilities in U.S. civilian networks to the exercise of national power, and he draws broad conclusions that have doubtful application in circumstances short of a full-out armed conflict with China. In addition, he does not discuss subthreshold conflicts that characterize, and are likely to continue to characterize, this symbiotic but strife-ridden relationship.

To begin, Lindsay argues that American infrastructure is safe from nation-state cyberattack. For support, he cites a similar conclusion by Desmond Ball, who touts the supposed "sophistication of the anti-virus and network security programs available" in advanced Western countries.[2] The notion that Western-made anti-virus and network security programs are effective against sophisticated cyberattacks would astonish any group of corporate security officers. Anti-virus programs are flimsy filters designed to catch only some of the malware that their designers know about. They miss a great deal. New malware enters the market at the rate of about 160,000 per day.[3] Filters, whether employed by the military or not, are unable to keep up. "Network security programs" vary in quality, are insufficiently staffed, and are often not implemented at all across the economy. The Pentagon is expending huge sums to build its own power grids, even as its budget shrinks, precisely because the civilian grid cannot be relied

Joel Brenner is a Robert Wilhelm Fellow at the Center for International Studies at the Massachusetts Institute of Technology and a lawyer and consultant specializing in information security. He is a former inspector general and senior counsel of the National Security Agency and a former National Counterintelligence Executive in the Office of the Director of National Intelligence.

Jon R. Lindsay is Assistant Professor of Digital Media and Global Affairs at the University of Toronto Munk School of Global Affairs.

1. Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, Vol. 39, No. 3 (Winter 2014/15), pp. 7–47. Further references to Lindsay's article appear parenthetically in the text.
2. Ibid., p. 35 n. 94, quoting Desmond Ball, "China's Cyber Warfare Capabilities," *Security Affairs*, Vol. 17, No. 2 (Winter 2011), p. 101.
3. Luis Corrons, "Malware Still Generated at a Rate of 160,000 New Samples a Day in Q2 2014," *Panda News*, August 29, 2014, http://www.pandasecurity.com/mediacenter/press-releases/malware-still-generated-rate-160000-new-samples-day-q2-2014/.

International Security, Vol. 40, No. 1 (Summer 2015), pp. 191–195, doi:10.1162/ISEC_c_00208

upon in a crisis. On this subject, Lindsay says only that China's ability to attack the U.S. grid "cannot be discounted." In contrast, Adm. Michael Rogers, director of the National Security Agency (NSA) and commander of U.S. Cyber Command, testified in 2014 that China and "one or two" other countries could shut down the power grid and other critical systems in the United States.[4]

Lindsay's article also fails to address the relationship between nonmilitary vulnerabilities and the exercise of national power. For example, when Russian intruders penetrated JPMorgan Chase Bank's computer system in 2014 during tensions over Ukraine, no one could tell President Barack Obama whether Russian President Vladimir Putin was sending him an implied threat.[5] Taking down a major bank would have enormous economic repercussions, and Chase's vulnerability was there for all to see. When evaluating his options, could the president ignore the possibility that exercising one of them carried the palpable risk that a major U.S. bank could be taken down? Whatever the source and objective of the intrusion in the Chase case, the incident demonstrates the way in which a critical vulnerability in the civilian economy could constrain the exercise of national power, including military power, in a crisis.

Lindsay speculates skeptically about the increase in the reporting of commercial network exploitation since 2010 and wonders whether it may be spurred by self-interested disclosures by network defense firms seeking to scare up demand for their services. He does not mention that the Securities and Exchange Commission issued guidance in 2011 stating that public companies "should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents."[6] And despite Lindsay's claim that commercial network exploitation is overreported, virtually every private-sector lawyer and consultant I know in this field believes that publicly disclosed information understates the severity and frequency of attacks on corporate networks. The reasons are well known: companies resist disclosure for fear of harm to their brands and stock prices and to avoid shareholder derivative class-action lawsuits and regulatory action by the Federal Trade Commission.

Lindsay is on better footing when he denies that a network penetration, even when it results in the theft of intellectual property (IP), necessarily results in lost profit or market share. The absorption and application of stolen intellectual property are complicated processes; they require know-how as well as a recipe. This is one reason why IP theft and reverse engineering do not necessarily produce market share for the thief and the copy-cat. Thus China still cannot produce a jet engine, even though it has plenty of American and Russian engines to study, because it cannot master the fabrication process. These are not contested propositions, however. Insurance carriers certainly understand them, which is largely why IP cannot be insured against theft. It is incorrect, however, to imply from this, as Lindsay does, that IP theft is not a significant issue for many of its victims. China has no difficulty using stolen IP about, say, oil and gas exploration data and materials testing research. Both are prime targets.

4. Ken Dilanian, "NSA Director: Yes, China Can Shut Down Our Power Grids," Associated Press, November 20, 2014, http://www.businessinsider.com/nsa-director-yes-china-can-shut-down-our-power-grids-2014-11.
5. See Joel Brenner, "Nations Everywhere Are Exploiting the Lack of Cybersecurity," *Washington Post*, October 24, 2014.
6. U.S. Securities and Exchange Commission, Corporate Finance Division, "CF Disclosure Guidance: Topic No. 2: Cybersecurity" (Washington, D.C.: U.S. Securities and Exchange Commission, October 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2 .htm.

Chinese intruders have also stolen negotiation strategies to good effect, as more than a few companies could testify (but will not). And in the case of solar-power technology, Chinese IP thieves had no trouble absorbing stolen secrets and penetrating Western markets.[7] Some descriptions of the economic losses have been hyperbolic, no doubt; and the losses have eluded persuasive quantification. Nevertheless, the problem is real and substantial.

The overall state of American networks and of private-sector capabilities simply is drastically different from the picture Lindsay paints. Take attribution. Public reports that the NSA can often—though not always—do very good attribution does not mean that private companies can do it. Attribution has three levels: (1) identifying the device from which an intrusion was both launched and commanded; (2) identifying the actor at the keyboard; and (3) identifying the actor's affiliation. Even the NSA cannot always get to the second and third levels, as the Chase Bank incident demonstrated.

The most basic difference between the military-to-military situation and the corporate reality, however, is that militaries and intelligence agencies fight back. In contrast, companies are exposed to attack without the legal right to retaliate (for mostly good reasons) even when they have, or could buy, the ability to do so. In this environment, offense is unquestionably dominant. According to Lindsay, since 2010 "Western cybersecurity defenses, technical expertise, and government assistance to firms have improved" (p. 23). In fact, very few companies receive government help with intrusions. If he means that private-sector defenses have improved when measured against themselves, then that is true but irrelevant. Attacks have also increased in sophistication, and when measured against the offense, defenses have not improved. All defenses are versions of Whac-A-Mole, and there are too many moles to whack them all.[8]

In sum, Lindsay and I agree that the current and foreseeable state of cyber technology "enables numerous instances of friction to emerge below the threshold of violence" (p. 9). This is what I have called "the gray space between war and peace." If this environment is showing signs of strategic stability, it is partly, as Lindsay argues, because mutual vulnerability is creating mutual restraint among nation-states. But the vulnerabilities remain, and they could be exploited by China or Russia in a crisis and by a growing number of second-tier cyber players that are not so constrained.

—Joel Brenner
Washington, D.C.

Jon R. Lindsay Replies:

I am grateful for the opportunity to respond to Joel Brenner's commentary on my recent article.[1] Having held senior positions in the National Security Agency and the

7. See Indictment, *United States v. Dong*, Crim. No. 14-118 (W.D. Pa., filed May 1, 2014), http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.
8. For a brief statement of the defense conundrum, see Joel Brenner, "How Obama Fell Short on Cybersecurity," *Politico*, January 21, 2015, http://www.politico.com/magazine/story/2015/01/state-of-the-union-cybersecurity-obama-114411.html?ml=m_u1_1#.VPi6C0LKy9d.

1. Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, Vol. 39, No. 3 (Winter 2014/15), pp. 7–47. Further references to Lindsay's article appear parenthetically in the text.

Office of the Director of National Intelligence, Brenner has a deep appreciation for the cybersecurity challenges facing the U.S. government and the private sector, so there are few people more qualified to comment on this issue. I am thus glad to learn that we agree about the broad contours of the cyber threat. Indeed, my article addresses most of the points he criticizes me for ignoring.

Brenner writes that my article focuses "almost exclusively on military-to-military operations," where he agrees with me that "the United States retains a significant qualitative advantage." Yet the section on cyberwarfare takes up less than a quarter of its page count. The rest of the piece discusses Chinese public policy, espionage of all kinds, and internet governance, and I distinguish these from the military realm as ultimately more important for international cybersecurity. Brenner asserts, "Lindsay speculates skeptically about the increase in the reporting of commercial network exploitation since 2010," but he takes my reservations about data quality out of context. Far from disputing "the severity and frequency of attacks on corporate networks," I suggest that China's "indigenous innovation" policy contributes to the intensifying commercial focus in its cyber campaigns.

Brenner suggests that I downplay "the significance of vulnerabilities in U.S. civilian networks." Yet I state that, both as participants and targets, "private firms and other nongovernmental organizations are increasingly involved in the sort of intelligence activities that were once mainly the purview of state security agencies" (p. 20). Brenner faults me for failing to "discuss subthreshold conflicts that characterize, and are likely to continue to characterize, this symbiotic but strife-ridden relationship" between China and the United States. In my conclusion, however, I write that we should expect to see "continuous and sophisticated intelligence contests, the involvement and targeting of civilian entities, enduring great power advantage relative to weaker states and nonstate actors, noisy symbolic protest, and complicated politics of institutional design" (p. 45).

Our disagreement is thus not on whether cyber threats exist but rather what kinds of threats exist and what they imply for the economic and military power of the United States. I argue that incentives for restraint in cyberspace make it better suited for intelligence operations than for coercive diplomacy or strategic attack. When options for inflicting real harm are limited by operational barriers and strategic deterrence, then espionage and harassment become attractive, if less effective, alternatives. The recent breach of the U.S. Office of Personnel Management, for example, is a potentially major intelligence coup for Chinese collectors, but collection is only the first step. Even the best intelligence does not automatically translate into a competitive advantage if policymakers ignore it or institutions fail to absorb it. We should in fact expect the leaders in peaceful economic competition to attract more intelligence attention from abroad, so the increase in Chinese exploitation could be interpreted as a signal of American strength.

Brenner, by contrast, points to the discovery of major breaches and sophisticated intruders, despite lavish spending on corporate defenses, to describe a situation of heightened peril. I see the same as evidence that firms are both willing to invest in defenses and accept a degree of risk to realize the increasingly lucrative returns to business in the global networked economy. Counterintelligence and network security professionals confront huge challenges in addressing increasingly complex vulnerabilities and intelligence exploitation in part because they are getting better at preventing and mitigating many attacks. The cybersecurity industry grew by more than an order

of magnitude from 2002 to 2014, and venture capitalists are making large investments in whole new categories of protection.[2] Brenner highlights the so-called attribution problem—the difficulty of determining the identity of a cyber attacker—as an example of private-sector weakness; other experts point out, however, that "the market for attribution has grown significantly" and "attribution is getting easier" because of "[b]etter intrusion detection systems. . . . More adaptive networks . . . [and] improved law-enforcement cooperation."[3] In these circumstances, intrusions have to become more sophisticated to pose any kind of threat. Ironically, sophistication tends to limit the pool of suspects to actors with sufficient expertise and capacity, and these actors also happen to have more to lose. Without a doubt, as Brenner writes, "there are too many moles to whack them all," but defense and deterrence are steadily improving to counter the most worrisome threats. Meanwhile business in the networked economy grows more profitable than ever.

Cyberspace empowers stronger actors to exploit weaker ones, so the United States has advantages over China, and China has advantages over Western firms. The ambiguous willingness of the U.S. government to defend private firms (for good reasons such as avoiding moral hazard and market favoritism) is a permissive condition for the rampant threat Brenner observes. Nevertheless, the U.S. government is willing to respond to attacks that cross a threshold, as in the North Korean hack of Sony,[4] and U.S. cyber policy increasingly includes threats of consequences for serious attacks on firms.[5] Brenner notes that the JPMorgan Chase hacking incident shows that private vulnerability can become a national security issue because "no one could tell President Barack Obama whether Russian President Vladimir Putin was sending him an implied threat." Yet that same ambiguity also signals a lack of resolve from the sender, if it signals anything, so it is unsurprising if policymakers discount it.

Brenner and I ultimately agree about the growing salience of what he calls "the gray space between war and peace." I explain this trend by noting that "the observable pattern of Chinese (and American) cyber activity conforms to the logic of the Cold War stability-instability paradox, but in slightly revised form" (p. 46)—deterrence and the benefits of interconnection work together to constrain the severity of attacks, yet simultaneously increase the complexity of those that occur. Brenner chides me for giving short shrift to instability at the lower end of the paradox as I point out the reasons for stability at the higher end. Yet both fundamentally go together. Given the restrained nature of cyber threats, predicated on cyber profits, I see their proliferation as cause for cautious optimism about U.S.-China relations. Mutual reliance on cyberspace, exploitation and all, reflects a deepening of the institutional interdependence between the two great powers.

—Jon R. Lindsay
Toronto, Canada

---

2. Rick Gordon, "The Cyber Security Market Is Hot! Here's Why," *Information Week*, May 8, 2014, http://www.darkreading.com/risk/the-cyber-security-market-is-hot!-heres-why/a/d-id/1251128.
3. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, Vol. 38, Nos. 1–2 (2015), pp. 28, 32.
4. Stephan Haggard and Jon R. Lindsay, "North Korea and the Sony Hack: Exporting Instability through Cyberspace," AsiaPacific Issues No. 117 (Honolulu: East-West Center, May 2015).
5. Ash Carter, "Remarks by Secretary Carter at the Drell Lecture Cemex Auditorium, Stanford Graduate School of Business, Stanford, California" (Washington, D.C.: U.S. Department of Defense, April 23, 2015), http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5621.