This response will appear in slightly modified form in the forthcoming issue of *International Security*, and is published here with their permission.

Response to Jon Lindsay

Joel Brenner[1]

Jon R. Lindsay ("The Impact of China on Cybersecurity: Fact and Friction," International Security, Vol. 39, no. 3 [Winter 2014/15], pp. 7-47) asserts that the threat of Chinese cyber operations, while "relentlessly irritating," is greatly exaggerated; that China has more to fear from U.S. cyber operations than the other way round; and that U.S.-China relations are reasonably stable. He worries that "[o]verlap across political, intelligence, military, and institutional threat narratives … can lead to theoretical confusion." By focusing almost exclusively on military-to-military operations, however, where he persuasively argues that the U.S. retains a significant qualitative advantage, Lindsay mischaracterizes the state of affairs in civilian networks and draws broad conclusions that have doubtful application in circumstances short of a full-out armed conflict with China. At the same time he pays no attention to sub-threshold conflicts that characterize, and are likely to continue to characterize, this symbiotic but strife-ridden relationship.

The proposition that American infrastructure is safe from nation-state attack would astonish any group of corporate security officers. To support it, Lindsay cites a similar conclusion by Desmond Ball, who relies on 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 attacks is nonsense. Anti-virus programs are flimsy filters designed to catch only some of what their designers know about. They miss a great deal. New malware enters

---

[1] Joel Brenner is a Robert Wilhelm Fellow at MIT's Center for International Studies 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.

[2] Lindsay, "Impact of China," p. 35, n. 94, quoting Desmond Ball, "China's Cyber Warfare Capabilities," *Security Affairs*, Vol. 17, No. 2 (Winter 2011), p. 101.

the market at the rate of about 160,000 per day.[3] Filters, whether employed by the military or not, cannot 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 upon in a crisis. On this subject Lindsay says only that Chinese ability to attack our grid "cannot be discounted." In contrast, Admiral Mike Rodgers, director of the National Security Agency and commander, U.S. Cyber Command, recently testified that China and "one or two" other countries *could* shut down the power grid and other critical systems in the United States.[4]

The joint operations, military-on-military perspective from which Lindsay writes is important. But it is too narrow a perspective from which to draw broad conclusions about "The Impact of China on Cybersecurity." It also fails to address the relationship between non-military vulnerabilities and the exercise of national power. For example, when Russian intruders penetrated Chase Bank last year during tensions over Ukraine, no one could tell President Obama whether Putin was sending him a an implied threat.[5] Taking down a major bank would have enormous economic repercussions, and the bank'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 intention of the intrusion in that case, the incident demonstrated the way in which a critical vulnerability in the civilian economy could constrain the exercise of national power, including military power, in a crisis.

---

[3] Luis Corrons, "Malware still generated at a rate of 160,000 new samples a day in Q2 2014," *Panda News*, August 29, 2014, at http://www.pandasecurity.com/mediacenter/press-releases/malware-still-generated-rate-160000-new-samples-day-q2-2014/.

[4] Ken Dilanian, "NSA Director: Yes, China Can Shut Down Our Power Grids," AP, November 20, 2014, at http://www.businessinsider.com/nsa-director-yes-china-can-shut-down-our-power-grids-2014-11.

[5] See Joel Brenner, "Nations Everywhere," supra, note 1.

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] Rather than being over-reported, as he suggests, and in spite of SEC guidance, 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 (IP) are complicated; 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. But these are not contested propositions. Insurance carriers certainly understand them – which is largely why IP cannot be insured against theft. It is a *non sequitur*, however, to conclude from this, as Lindsay implies, 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. Chinese intruders have also stolen negotiation strategies to good effect, as more than a few companies could testify (but won't). And in the case of solar-power technology, Chinese IP thieves had no trouble absorbing stolen secrets and

---

[6] U.S. Securities and Exchange Commission, Corporate Finance Division, "CF Disclosure Guidance: Topic No. 2: Cybersecurity," October 13, 2011, at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

penetrating western markets.[7] Some descriptions of the economic losses have been hyperbolic, no doubt; and the losses have eluded persuasive quantification. But the problem is real and substantial.

The overall state of our networks and of private-sector capabilities simply looks drastically different from the picture Lindsay paints of our military. Take attribution. Public reports that NSA can often – 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 NSA can't 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." In fact, very few companies receive government help with intrusions. If he means that private sector defenses have gotten better when measured against themselves, that's right but irrelevant. Attacks have also increased in sophistication, and when measured against the offense, defenses have not improved. All our defenses are version of Whac-a-Mole, and there are too many moles to whack them all.[8]

All this leaves us with a lumpy landscape, not subject to cheerful generalizations about China's impact on U.S. cybersecurity, or vice versa. In this landscape, Lindsay and I agree that the current and foreseeable state of technology "enables numerous instances of friction to emerge below the threshold of violence." This is what I have called "the gray space between war

---

[7] See *United States v. Dong*, Crim. No. 14-118 (W.D. Pa., filed May 1, 2014), at 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 Cyber Security," *Politico*, January 21, 2015, at http://www.politico.com/magazine/story/2015/01/state-of-the-union-cybersecurity-obama-114411.html?ml=m_u1_1#.VPi6C0LKy9d.

and peace." If this environment is showing signs of strategic stability, it is partly, as he argues, because mutual vulnerability is creating mutual restraint. 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.