The Impact of China on Cybersecurity

Fiction and Friction

Jon R. Lindsay

The ubiquity and interconnectedness of computers in global commerce, civil society, and military affairs create crosscutting challenges for policy and conceptual confusion for theory. The challenges and confusion in cybersecurity are particularly acute in the case of China, which has one of the world's fastest growing internet economies and one of its most active cyber operations programs. In 2013 U.S. National Security Adviser Tom Donilon singled out Chinese cyber intrusions as "not solely a national security concern or a concern of the U.S. government," but also a major problem for firms suffering from "sophisticated, targeted theft of confidential business information and proprietary technologies . . . emanating from China on an unprecedented scale."[1] One U.S. congressman alleged that China has "established cyber war military units and laced the U.S. infrastructure with logic bombs." He suggested that "America is under attack by digital bombs."[2] The discourse on China and cybersecurity routinely conflates issues as different as political censorship, unfair competition, assaults on infrastructure, and internet governance, even as all loom large for practical cyber policy. Although they involve similar information technologies, there is little reason to expect different political economic problems to obey the same strategic logic, nor should one necessarily expect China to enjoy relative advantage in all spheres.

Indeed, the intelligence leaks from Edward Snowden in 2013 underscored the sophistication and extent of internet surveillance by the United States and its allies against targets worldwide, including in China.[3] The Snowden

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.

The author would like to thank Ben Bahney, Michael Beckley, Tai Ming Cheung, Paul Cornish, Erik Gartzke, Derek Reveron, Julian Snelder, Jack Jiakun Zhang, and the anonymous reviewers for their helpful comments on this project. This research was supported by the Department of Defense Minerva Initiative and Office of Naval Research Grant N00014-14-1-0071.

1. Tom Donilon, "The United States and the Asia-Pacific in 2013," Asia Society, New York, March 11, 2013 (Washington, D.C.: White House, March 2013), http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.
2. Charles Cooper, "House Hearing: U.S. Now Under Cyber Attack," CNET, April 24, 2012, http://news.cnet.com/8301-1009_3-57420229-83/house-hearing-u.s-now-under-cyber-attack/.
3. Jeffrey T. Richelson, ed., "The Snowden Affair: Web Resource Documents the Latest Firestorm

International Security, Vol. 39, No. 3 (Winter 2014/15), pp. 7–47, doi:10.1162/ISEC_a_00189

revelations not only invigorated debate about the balance between security and privacy in a democracy but also undercut the moral force of American complaints about Chinese penetration of commercial, government, and defense networks.[4] Chinese writers hasten to compare the United States to "a thief crying stop thief."[5] Meanwhile U.S. officials attempt to distinguish between acceptable data collection for national security and unacceptable criminal economic espionage.[6] Notably, a May 2014 grand jury indicted five alleged members of the Chinese People's Liberation Army (PLA) on several counts of industrial espionage, but omitted mentioning that the same PLA unit targets military interests as well.[7] Chinese critics reject the American distinction between legitimate and illegitimate internet surveillance and deny allegations of hacking. They also call for the restriction of American internet firms from the Chinese domestic market in order to protect Chinese infrastructure from subversion.[8] Cyber operations and the rhetorical reactions to them on both sides of the Pacific have undermined trust in the Sino-American relationship.[9]

Exaggerated fears about the paralysis of digital infrastructure and growing concerns over competitive advantage exacerbate the spiral of mistrust. Closer consideration of domestic factors within China and China's strategic interac-

---

over the National Security Agency," *National Security Archive Electronic Briefing Book* (Washington, D.C.: National Security Archive, George Washington University, September 4, 2013), http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/.

4. See, for example, Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009–2011* (Washington, D.C.: Office of the National Counterintelligence Executive, October 2011).

5. Zhong Sheng, "The United States Bears Primary Responsibility for Stopping Cyber War," *People's Daily Online*, February 7, 2013.

6. For example, the United States forbids "the collection of foreign private commercial information or trade secrets . . . to afford a competitive advantage to U.S. companies and U.S. business sectors commercially." See Office of the Press Secretary, White House, "Signals Intelligence Activities," Presidential Policy Directive/PPD-28 (Washington, D.C.: White House, January 17, 2014).

7. U.S. Department of Justice, Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," press release, May 19, 2014, http://www.justice.gov/opa/pr/2014/May/14-ag-528.html. For further details on the Second Bureau of the PLA General Staff Department Third Bureau (3/PLA), see Mandiant, "APT1: Exposing One of China's Cyber Espionage Units" (Alexandria, Va.: Mandiant, February 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

8. Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, September 20, 2013, http://carnegieendowment.org/2013/09/20/chinese-views-on-cybersecurity-in-foreign-relations.

9. Kenneth G. Lieberthal and Wang Jisi, "Addressing U.S.-China Strategic Distrust" (Washington, D.C.: Brookings Institution, March 2012).

tion with the United States reveals a more complicated yet less worrisome situation. This article argues that for every type of purported Chinese cyber threat, there are also serious Chinese vulnerabilities and Western strengths that reinforce the political status quo. Cyberwar between the United States and China, much like U.S.-China conventional war, is highly unlikely. Nevertheless, the economically driven proliferation of information technology enables numerous instances of friction to emerge below the threshold of violence. From a technical perspective, cyber operations are often thought to be inexpensive and effective, but there are underappreciated institutional costs involved in their employment. Moreover, even if actors can overcome the operational barriers associated with ambitious cyber penetrations, they still have incentives to moderate the intensity of their exploitation in order to preserve the benefits that make exploitation worthwhile in the first place. This logic culminates in a relentlessly irritating but indefinitely tolerable stability in the cyber domain. China and the United States can look forward to chronic and ambiguous intelligence-counterintelligence contests across their networks, even as the internet facilitates productive exchange between them.

This article proceeds in six sections. The first section marshals debates about cybersecurity and the rise of China to frame four prominent threat narratives. The next four sections analyze the empirical manifestations of, respectively, political, espionage, military, and institutional cyber threats in the case of China. The concluding section draws out generalizations about interactions across these categories and offers reasons to expect a measure of restraint in cyberspace.

Cybersecurity and International Relations

Claims about Chinese cyber threats fall at the intersection of two different debates, one about the impact of information technology on international security and the other about the political and economic future of a rising power. The technological debate centers on whether ubiquitous networks create revolutionary dangers or just marginal evolutions of computer crime, signals intelligence, and electronic warfare.[10] One side of this debate argues that inter-

10. For collections of perspectives on both sides of the debate, see Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: Potomac, 2009); and Derek S. Reveron, ed., *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, D.C.: Georgetown University Press, 2012). For balanced introductions to cybersecurity policy, see P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What*

connected infrastructure and easily accessible hacking tools make advanced industrial powers particularly vulnerable to serious disruption from weaker states or even nonstate actors.[11] The other side argues that the defense industry and national security establishment greatly exaggerate the cyber threat.[12] The political debate offers contrasting liberal and realist interpretations of China's meteoric growth.[13] One side argues that China is increasingly integrated into

Everyone Needs to Know (New York: Oxford University Press, 2014); and National Research Council, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (Washington, D.C.: National Academies Press, 2014).

11. See, inter alia, Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, Mass.: MIT Press, 2001); Scott Borg, "Economically Complex Cyberattacks," *IEEE Security and Privacy Magazine*, Vol. 3, No. 6 (November/December 2005), pp. 64–67; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Ecco, 2010); Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin, 2011); Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Vol. 5, No. 4 (Winter 2011), pp. 18–36; Timothy J. Junio, "How Probable Is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," *Journal of Strategic Studies*, Vol. 36, No. 1 (February 2013), pp. 125–133; Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies*, Vol. 36, No. 1 (February 2013), pp. 120–124; and Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 7–40.

12. On cyber threat inflation, see 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 (February 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; Evgeny Morozov, "Cyber-Scare: The Exaggerated Fears over Digital Warfare," *Boston Review*, Vol. 34, No. 4 (July/August 2009), http://www.bostonreview.net/us/cyber-scare-evgeny-morozov; 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); Bruce Schneier, *Liars and Outliers: Enabling the Trust That Society Needs to Thrive* (Indianapolis: Wiley, 2012); and 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. Many skeptics attempt to balance the debunking of exaggerated rhetoric with assessments of the potential of emerging substitutes for low-intensity aggression and complements for high-intensity warfare. See, for example, Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007); Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 5 (February 2012), pp. 5–32; David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed," *Journal of Strategic Studies*, Vol. 35, No. 5 (October 2012), pp. 689–711; 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; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (August 2013), pp. 365–404; 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.

13. Alastair Iain Johnston, "Is China a Status Quo Power?" *International Security*, Vol. 27, No. 4 (Spring 2003), pp. 5–56; Aaron L. Friedberg, "The Future of U.S.-China Relations: Is Conflict Inevitable?" *International Security*, Vol. 30, No. 2 (Fall 2005), pp. 7–45; Thomas J. Christensen, "Fostering Stability or Creating a Monster? The Rise of China and U.S. Policy toward East Asia," *International Security*, Vol. 31, No. 1 (Summer 2006), pp. 81–126; Avery Goldstein, "Power Transitions, Institutions, and China's Rise in East Asia: Theoretical Expectations and Evidence," *Journal of Strategic Studies*, Vol. 30, Nos. 4–5 (August 2007), pp. 639–682; Robert S. Ross and Zhu Feng, eds., *China's*

the global economy and international institutions and, furthermore, that the Communist government is committed to growth and stability to maintain its legitimacy.[14] The other side argues that Chinese military modernization and the relative decline of the United States heighten the potential for opportunistic aggression, miscalculation in a crisis, or preventive war.[15] The very existence and magnitude of a shift in relative power is also a matter of debate.[16]

Technological and political questions become entangled in cybersecurity discourse, because the internet facilitates the expansion of trade while providing new tools for subversion. The novelty of cyber operations and the ambiguity of China's developmental trajectory compound the uncertainty. It is possible, however, to turn this practical ambiguity to analytical advantage. By taking the extremes of the conceptual debates that frame cyber policy discussions and combining them orthogonally, one can describe four ideal-type threat narratives that clarify the capabilities and motivations shaping cyber behavior. Each category in the typology makes different assumptions about what is possible and probable, technologically and politically.

Figure 1 presents each threat, along with counterarguments that I develop below.[17] The "open internet" quadrant describes a more or less cooperative

Ascent: Power, Security, and the Future of International Politics (Ithaca, N.Y.: Cornell University Press, 2008); and M. Taylor Fravel, "International Relations Theory and China's Rise: Assessing China's Potential for Territorial Expansion," *International Studies Review*, Vol. 12, No. 4 (December 2010), pp. 505–532.

14. Barry Naughton, *The Chinese Economy: Transitions and Growth* (Cambridge, Mass.: MIT Press, 2007); Daniel W. Drezner, "Bad Debts: Assessing China's Financial Influence in Great Power Politics," *International Security*, Vol. 34, No. 2 (Fall 2009), pp. 7–45; G. John Ikenberry, "Liberal Internationalism 3.0: America and the Dilemmas of Liberal World Order," *Perspectives on Politics*, Vol. 7, No. 1 (March 2009), pp. 71–87; and Edward S. Steinfeld, *Playing Our Game: Why China's Economic Rise Doesn't Threaten the West* (Oxford: Oxford University Press, 2010).

15. John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton, 2001), pp. 360–402; Christopher Layne, "The Unipolar Illusion Revisited: The Coming End of the United States' Unipolar Moment," *International Security*, Vol. 31, No. 2 (Fall 2006), pp. 7–41; Edward N. Luttwak, *The Rise of China vs. the Logic of Strategy* (Cambridge, Mass.: Harvard University Press, 2012); James Dobbins, "War with China," *Survival*, Vol. 54, No. 4 (August/September 2012), pp. 7–24; and Jonathan Kirshner, "The Tragedy of Offensive Realism: Classical Realism and the Rise of China," *European Journal of International Relations*, Vol. 18, No. 1 (March 2012), pp. 53–75.

16. Christopher Layne, "The Waning of U.S. Hegemony—Myth or Reality? A Review Essay," *International Security*, Vol. 34, No. 1 (Summer 2009), pp. 147–172; Michael Beckley, "China's Century? Why America's Edge Will Endure," *International Security*, Vol. 36, No. 3 (Winter 2011/12), pp. 41–78; Sean Starrs, "American Economic Power Hasn't Declined—It Globalized! Summoning the Data and Taking Globalization Seriously," *International Studies Quarterly*, Vol. 57, No. 4 (December 2013), pp. 817–830; Randall L. Schweller and Xiaoyu Pu, "After Unipolarity: China's Visions of International Order in an Era of U.S. Decline," *International Security*, Vol. 36, No. 1 (Summer 2011), p. 41–72; and Alastair Iain Johnston, "How New and Assertive Is China's New Assertiveness?" *International Security*, Vol. 37, No. 4 (Spring 2013), pp. 7–48.

17. Because this article evaluates the Chinese cyber threat—primarily to the United States—this typology emphasizes interactions among nation-states. Nonstate actors loom large in cyber dis-

Figure 1. A Typology of Cyber Threat Narratives

	Evolutionary Technology	Revolutionary Technology
Cooperative Political Environment	Open Internet Assumption: The internet enhances the value of social and economic exchange. Threat: State censorship and surveillance violate human rights and reduce trust in the internet. Counterargument: Prioritization of information control over technical defense exposes China to foreign and domestic cyber attack.	Cybersecurity Norms Assumption: States must adopt common norms to protect the internet from catastrophe. Threat: Authoritarian "internet sovereignty" norms imperil the liberal "multistakeholder" system. Counterargument: The institutional status quo is durable, and China cannot credibly commit to its proposed norms.
Competitive Political Environment	Contested Cyberspace Assumption: Cyber technology improves intelligence collection methods and opportunities. Threat: Chinese cyber espionage is systematically eroding the competitiveness of Western firms. Counterargument: Absorption of stolen data is a nontrivial obstacle, and Western intelligence also exploits China.	Cyber Warfare Assumption: Cyberspace is a dangerous, asymmetric, offense dominant warfighting environment. Threat: China can paralyze U.S. military command and control and civilian infrastructure at low cost. Counterargument: China's cyber capabilities do not live up to Chinese rhetoric, and "informatization" exposes China to attack.

political environment of connected states willing to tolerate a variety of minor threats. The internet has the potential to enhance liberal trade and discourse, but computer fraud and authoritarian censorship undermine this promise. The "contested cyberspace" quadrant describes a situation where competitive states engage in intelligence collection and harassment using evolutionary adaptations of familiar security practices. Discourse in this quadrant focuses less

course, and indeed, criminal and "hacktivist" threats create headaches even in the cooperative "open internet" quadrant. The most worrisome cyber activity observed to date, however, has been driven by states (e.g., PLA espionage and U.S. covert action). For an argument about how the cyber revolution diffuses power beyond the state, see Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), pp. 113–152. For a discussion of why states retain important advantages over nonstate actors, see David C. Benson, "Why the Internet Is Not Increasing Terrorism," *Security Studies*, Vol. 23, No. 2 (April/June 2014), pp. 293–328.

on the risks of a "cyber Pearl Harbor" and more on a "death by a thousand cuts" through Chinese espionage. The "cyberwarfare" quadrant is the culmination of the most pessimistic interpretations of technology and politics, where conflict-prone actors wield revolutionary cyber capabilities. Because U.S. power projection, like the U.S. economy, depends heavily on computer networks for command and control, many analysts worry that Chinese cyberattacks could blunt or dissuade U.S. intervention in an East Asia crisis. The final "cybersecurity norms" quadrant describes a more indirect threat emerging through international overreaction to the direct threats described in the other categories. The reform of internet governance predicated on Chinese "internet sovereignty" might, as many Western observers fear, legitimize authoritarian control and undermine the cosmopolitan promise of the "multistakeholder" system.[18]

At best, each narrative highlights different political, espionage, military, and institutional threats. At worst, they are mutually inconsistent, in which case some of them should be discounted or reconciled. All are present to some degree in political debate about China and cybersecurity, and they are often conflated. By identifying different assumptions about threat characterizations, one can also pose counterarguments in each category that either question the magnitude of the Chinese threat or point out countervailing Western advantages.

Political Threats to the Open Internet

Almost from its inception, the internet fostered hopeful expectations that connectivity might deliver economic and political liberalization for user populations, if not the outright transformation of digital society into a cosmopolitan utopia.[19] Economic drag from criminal hacking and information control by governments, however, challenge the techno-libertarian ideal. In particular, state censorship and surveillance target domestic and expatriate dissidents and minority groups, thus posing a digital threat to human rights.[20] As China

18. The term "multistakeholder" system is widely used by practitioners to describe the mélange of academic, corporate, regulatory, and nongovernmental actors in contemporary internet governance.
19. Vincent Mosco, *The Digital Sublime: Myth, Power, and Cyberspace* (Cambridge, Mass.: MIT Press, 2005); and Janet Abbate, *Inventing the Internet* (Cambridge, Mass.: MIT Press, 1999).
20. Sarah McKune, "'Foreign Hostile Forces': The Human Rights Dimension of China's Cyber Campaigns," in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, eds., *China and*

uses the internet more intensively and as the internet becomes increasingly Chinese, the global internet provides a channel for China's illiberal domestic politics to challenge liberal interests abroad.[21] These are important concerns, but they are only part of the picture: state internet control efforts do generate limited threats to civil society, but they can also inadvertently undermine the state's defense against other types of threats.

UNBUNDLING OPENNESS

Economic openness promotes growth, but China sees political openness as a threat to its legitimacy. As President Xi Jinping states, development and security go together like "two wings of a bird and two wheels of an engine," and therefore "[c]yberspace should be made clean and chipper."[22] In advanced industrial countries, networked computers have enhanced profit and performance in every sector from manufacturing to transportation, service, entertainment, governance, and public safety.[23] Similarly for China, internet-enabled supply chains tie its production lines into the global economy while information technology facilitates the modernization of infrastructure and boosts export-led growth.[24] Chinese "netizens" (*wangmin*)—more than

Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (New York: Oxford University Press, forthcoming).

21. According to the World Bank's World Development Indicators, in 2012 China had nearly a quarter of the global internet population (23 percent), more than double that of the United States (10 percent) and more than that of the entire European Union (15 percent). See World Bank, "World Development Indicators" (Washington, D.C.: World Bank, July 2014), http://data.worldbank.org/data-catalog/world-development-indicators.

22. "Xi Jinping Leads Internet Security Group," Xinhua news agency, February 27, 2014, http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm.

23. James W. Cortada, *The Digital Hand*, 3 vols. (Oxford: Oxford University Press, 2008). The so-called productivity paradox of the 1990s has been resolved through improved measurement of the relationship between computation and growth. See Erik Brynjolfsson and Adam Saunders, *Wired for Innovation: How Information Technology Is Reshaping the Economy* (Cambridge, Mass.: MIT Press, 2010); and Dale W. Jorgenson and Kevin J. Stiroh, "Raising the Speed Limit: U.S. Economic Growth in the Information Age," Brookings Papers on Economic Activity 2000, No. 1 (Washington, D.C.: Brookings Institution, 2000).

24. By one estimate, the internet contributed on average 21 percent of gross domestic product (GDP) growth from 2004 to 2009 for early adopters such as Germany, Japan, Sweden, and the United States (up from 10 percent during the previous decade) and a more modest 3 percent for later adopters such as Brazil, China, and India. The latter percentage will likely increase in the future. See Matthieu Pelissie du Rausas et al., "Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity" (New York: McKinsey Global Institute, May 2011), pp. 15–16. For comparable measurements and a discussion of the likelihood that internet newcomers will show greater growth in their internet contribution to GDP, see David Dean and Paul Zwillenberg, "Turning Local: From Moscow to Madrid, the Internet Is Going Native" (Boston: Boston Consulting Group, September 2011). The Organization for Economic Cooperation and Development (OECD) argues that internet growth studies typically underestimate the true impact of the internet on growth, because they count only internet-related jobs, not the broader impact of the internet on

600 million users as of 2013—enjoy expanded access to entertainment, shopping, gossip, and news.[25] To the degree that civil society exists in China, it does so predominantly online. As a 2010 State Council white paper asserts, however, "China advocates the rational use of technology to curb dissemination of illegal information online."[26] The result is the most sophisticated internet censorship architecture in the world (i.e., "the Great Firewall of China"). The government requires internet service providers to block politically sensitive websites and searches and to employ human censors to remove offending social media posts or guide discussion in more politically acceptable directions. Domestic security services often single out dissidents, domestic and expatriate alike, for more aggressive online harassment and service denial attacks.[27] China is the foremost counterexample to the myth that the borderless internet undermines the power of the state.[28]

Whereas the Western notion of cybersecurity emphasizes technical threats, China places greater weight on ideological threats. The Chinese notion of information security (*xinxi anquan*), accordingly, includes control of information content as well as, if not more than, technical network security (*wangluo anquan*) against malware. In 2010 the director of the State Council Information Office and External Propaganda Department of the Chinese Communist Party (CCP) linked "hostile foreign forces" and subversive "universal values" to internet penetration: "As long as our country's internet is linked to the global internet, there will be channels and means for all sorts of harmful foreign information to appear on our domestic internet."[29] An authoritative 2013 CCP

other sections of the economy. OECD, "Measuring the Internet Economy: A Contribution to the Research Agenda," OECD Digital Economy Papers, No. 226 (Paris: OECD, 2013), p. 19. See also George R.G. Clarke and Scott J. Wallsten, "Has the Internet Increased Trade? Evidence from Industrial and Developing Countries" (Washington, D.C.: World Bank, February 2004). For a discussion of the impact of information technology on China, in particular, see Dan Schiller, "Poles of Market Growth? Open Questions about China, Information, and the World Economy," *Global Media and Communication*, April 1, 2005, pp. 79–103; and James W. Cortada, *The Digital Flood: Diffusion of Information Technology across the United States, Europe, and Asia* (Oxford: Oxford University Press, 2012), pp. 443–490.

25. China Internet Network Information Center, "Statistical Report on Internet Development in China" (Beijing: China Internet Network Information Center, July 2013), p. 3.

26. State Council Information Office, "The Internet in China" (Beijing: State Council Information Office, June 8, 2010).

27. Ronald Deibert et al., eds., *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambridge, Mass.: MIT Press, 2012).

28. Jack L. Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006); and Daniel W. Drezner, "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly*, Vol. 119, No. 3 (Fall 2004), pp. 477–498.

29. McKune, "Foreign Hostile Forces."

directive "on the current state of the ideological sphere" warns more pointedly of "accelerating infiltration of the internet" by "Western anti-China forces and internal 'dissidents.'"[30]

CCP internet control is not absolute, however. Netizens playfully exploit Mandarin homophones to evade or ridicule censors.[31] The phenomenon of the "human flesh search" (*renrou sousuo*) or crowd-sourced vigilantism targets disgraced citizens and corrupt officials for public humiliation. While unruly behavior encourages the state to crack down on individuals branded as "rumor mongers," CCP officials tolerate internet discussion to identify brewing unrest or lapses in party discipline.[32] Thus censors do not block all criticism of the state, but only that which the CCP fears might mobilize public demonstration and dissent.[33]

China's Fragmented Cyber Defenses

The CCP's obsession with political "information security" has so far not translated into effective technical "network security."[34] Cybercrime thrives amid a fragmented bureaucracy. Lax and uneven law enforcement emboldens Chinese cybercriminals to prey on domestic targets and creates a blatantly open online underground economy in China. Chinese cybercriminals target Chinese victims given the relatively low risk of domestic police action; by comparison, Eastern Europe cybercriminals tend to avoid hacking at home, instead focusing their predation abroad. Stolen usernames and passwords, financial data, video game accounts, and hacker tools can be bought and sold

30. The Central Committee of the CCP General Office's "Document 9" also describes "Western freedom, democracy, and human rights" as a "political tool" "adopted by Western anti-China forces" amounting to a "serious form of political opposition." The full title of the April 2013 document is "Communiqué on the Current State of the Ideological Sphere." See ibid.

31. One widespread internet meme features contests between the "grass mud horse" (*caonima*) and "river crabs" (*hexie*), which are tonal puns on a vulgar insult and the word for ideological "harmonization," respectively. See Nigel Inkster, "China in Cyberspace," *Survival*, Vol. 52, No. 4 (August/September 2010), pp. 55–66. This is an internet-era manifestation of the logic described by James C. Scott, *Weapons of the Weak: Everyday Forms of Peasant Resistance* (New Haven, Conn.: Yale University Press, 2008).

32. Guobin Yang, *The Power of the Internet in China: Citizen Activism Online* (New York: Columbia University Press, 2009); and Susan L. Shirk, ed., *Changing Media, Changing China* (Oxford: Oxford University Press, 2011).

33. Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review*, Vol. 107, No. 2 (May 2013), pp. 326–343.

34. For a contrasting argument that censorship architecture improves Chinese situational awareness and thus cyber defense for at least some types of technical threats at national gateways, see Robert Sheldon, "The Situation Is Under Control: Cyberspace Situational Awareness and the Implications of China's Internet Censorship," *Strategic Insights*, Vol. 10, No. 1 (Spring 2011), pp. 36–51.

openly on Chinese social media forums such as Baidu and Tencent QQ. By one estimate, cybercrime damage to the economy exceeded $830 million and affected more than 20 percent of users and websites in 2011 alone.[35] Rampant cybercrime is a result, in part, of China's below-average cyber defenses.[36] Importantly, networks exposed to criminal predation are also vulnerable to foreign exploitation, because state intelligence services use some of the same technology and methods.

Cyber policy coordination among defense, law enforcement, and regulatory agencies is a challenge in any state, but China's lack of governmental transparency makes a hard problem worse. Prior to 2014, primary responsibility for cybersecurity policy resided in a subcommittee of the CCP State Informatization Leading Group (SILG), formed in 2001 to guide national information technology development or "informatization" (*xinxihua*) and chaired by the CCP premier. SILG's early focus on cybersecurity was eclipsed by the Chinese elite's preoccupation with the 2008 Beijing Olympics and financial crisis, leaving regulatory agencies and newly funded companies to their own devices. SILG updated its guidance criteria in 2012 to reflect renewed concerns about critical infrastructure and privacy, but elite focus remained sporadic. In February 2014, amid tension stemming from the Snowden leaks, the CCP announced the creation of the Cybersecurity and Informatization Leading Group (CILG), chaired by Xi Jinping (with twenty-one other Politburo or ministerial-level officials on the roster).[37] The CILG aids Xi's efforts to tighten Party discipline and respond to foreign cyber threats.[38] Greater attention by China's elite

35. Zhuge Jianwe et al., "Investigating the Chinese Online Underground Economy," in Lindsay, Cheung, and Reveron, *China and Cybersecurity*.

36. For an evaluation of legal and regulatory frameworks, technical infrastructure, industrial applications, and the economic and social context of cyberspace usage for twenty countries, see Economist Intelligence Unit, "Cyber Power Index" (McLean, Va.: Booz Allen Hamilton, December 2011), http://www.boozallen.com/insights/2012/01/cyber-power-index. China scored 34.6 on a 100-point scale; this can be compared with the United States at 75.4, Germany at 68.2, Japan at 59.3, Brazil at 38.6, Russia at 31.7, and India at 28.3. A more recent study scored China at 58.4 out of 100 and the United States at 86.3. See Tobias Feakin, Jessica Woodall, and Klée Aiken, "Cyber Maturity in the Asia-Pacific Region 2014" (Barton: International Cyber Policy Centre, Australian Strategic Policy Institute, April 2014). Because the two studies' methodologies are different, it is hard to say whether China has improved very much.

37. Liang Fulong, ed., "Zhōngyāng wǎngluò ānquán hé xìnxī huà lǐngdǎo xiǎozǔ chéngyuán míngdān 12 zhèngfù guó jí jiānzhí shēn gǎizǔ" [The Central Cybersecurity and Information Leading Group member list: Twelve with national or deputy national rank and also members of the Deepening Reform Leadership Group], Guancha.cn, February 28, 2014.

38. Notably, whereas SILG offices were housed in the Ministry for Industry and Information Technology, CILG offices are now under the State Council Internet Information Office (also known as the Cyberspace Administration of China), which oversees internet censorship. This move underscores the ideological component of "information security."

via CILG may improve cyber policy coordination, but prior experience does not bode well. In China, as in other states, a large and diverse set of public and private entities has a stake in the making of cyber policy, yet the steady stream of cyber friction does not add up to sustained elite pressure for reform. Policy elites with more pressing priorities usually do not focus consistent pressure on a heterogeneous set of bureaucratic interests.[39]

Numerous agencies under the State Council are responsible for the implementation of policy and the regulation of information technology in China. The People's Liberation Army, subordinate to the CCP rather than the state, has considerable military and intelligence cyber capacity as well as civilian regulatory responsibility (e.g., in the transportation sector). Provincial governments, furthermore, enjoy substantial de facto autonomy and compete fiercely for patronage. In response to a glut of funding for SILG initiatives, expenditure in China's information security industry grew from $527 million in 2003 to $2.8 billion in 2011. In the assessment of one industry observer, however, this expansion was marred by a "lack of overall planning," "decentralization of decisionmaking power," and a "lack of adequate communication."[40] As in other areas of Chinese policy, the implementation of cybersecurity is disjointed functionally and regionally, rife with rent seeking by bureaucratic agencies and enterprises. Haphazard interagency cooperation and industrial regulation create a permissive environment for cybercrime, which saps the potential of e-commerce and user trust in online services.

The Vulnerability of Internet Control

China's prioritization of political control over technical defense also creates incentives for hacking by foreign activists. From a Chinese perspective, state-sponsored internet freedom activism undermines Chinese cybersecurity, even as the ideological concept of information security encourages foreign efforts to do so. In a January 2010 speech on internet freedom following a major penetration of Google China, U.S. Secretary of State Hillary Clinton called for the development of "new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship."[41] Between

39. I describe China's cybersecurity policy system in more detail in Jon R. Lindsay, "China and Cybersecurity: Controversy and Context," in Lindsay, Cheung, and Reveron, *China and Cybersecurity*.
40. Wang Chuang, "Xìnxī ānquán: Zhèngcè hùháng chǎnyé zhuàngdà" [Information security: Policy driving industrial growth], *China Electronics News*, October 9, 2012.
41. Hillary Rodham Clinton, "Remarks on Internet Freedom," Newseum, Washington, D.C., January 21, 2010 (Washington, D.C.: U.S. Department of State, 2010), http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

2008 and 2012, the State Department and the U.S. Agency for International Development provided approximately $100 million for internet freedom initiatives.[42] Subversion of the Great Firewall is a major ideological threat for the CCP as well as official U.S. policy.

China's considerable investment in internet control is a signal that the regime places great value on it. Therefore, during a crisis the architecture of control would become a tempting countervalue target for Western information operations planners. The disruption of censorship and internet propaganda might encourage CCP paranoia about civil unrest or uncontrollable nationalism. The prospect of the disintegration of the Great Firewall would present the CCP with a dilemma of either accepting reduced ideological control at home or reducing economic connectivity abroad (by unplugging international connections); both options are potentially more costly to the CCP's legitimacy than is backing down in a limited crisis. At the same time, however, ideological attack could feed CCP fears of "hostile foreign forces" and encourage a stiffening of Chinese resolve in even a minor crisis. These trade-offs deserve further analysis. I mention them here only to highlight how Chinese challenges to human rights online create challenges in cybersecurity for China as well.

Intelligence Threats in Contested Cyberspace

The open internet quadrant in figure 1 is populated by digital evolutions of crime and illiberal domestic control in an international environment of broadly shared interests. The contested cyberspace quadrant, in turn, contains a more competitive environment in which actors adapt information technology for intelligence purposes. Since the introduction of the telegraph in the mid-nineteenth century and with every innovation in telephony, radio, and computation since, the sophistication of techniques for electronic interception and deception has increased without, however, creating lasting decisive advantages.[43] An intelligence contest is never one-sided, because the target reacts with operational security and counterintelligence measures, which in turn raise the political and technical barriers for attackers reliant on covert advantage. The mere fear of counterintelligence compromise can be as inhibiting as

42. Fergus Hanson, "Baked In and Wired: eDiplomacy @ State" (Washington, D.C.: Brookings Institution, October 2012), p. 26.
43. Daniel R. Headrick, *The Invisible Weapon: Telecommunications and International Politics, 1851–1945* (New York: Oxford University Press, 1991).

actual defenses. The novelty of computer network exploitation (CNE) lies mainly in the scope and diffusion of classic intelligence-counterintelligence contests. By virtue of the internet's reach and ubiquity, private firms and other nongovernmental organizations are increasingly involved in the sort of intelligence activities—as both participants and targets—that were once mainly the purview of state security agencies.

The exposure of profitable Western firms to Chinese espionage online raises particular concerns about the future competitiveness of such companies. A U.S. National Intelligence Estimate in early 2013 reportedly described Chinese CNE as a serious and persistent economic threat to U.S. firms and government institutions.[44] The chairman of the U.S. House Intelligence Committee alleged that there "is a concerted effort by the government of China to get into the business of stealing economic secrets to put into use in China to compete against the U.S. economy."[45] Director of the National Security Agency Gen. Keith Alexander described the result of this effect as "the greatest transfer of wealth in history."[46] Chinese espionage activity alone, however, cannot produce this result. To realize competitive advantage, China needs to be able to absorb and apply the data it steals. Moreover, the United States is also a formidable intelligence actor, which can be expected to offset Chinese advantages to some degree. The category of contested cyberspace highlights the increasing intensity of intelligence competition, not a clear advantage for one side or the other.

ADVANCED PERSISTENT THREAT

The term "advanced persistent threat" (APT) emerged as early as 2006 as an unclassified euphemism for intrusions traced to China.[47] Attribution to China is usually based on a wide range of individually circumstantial but collectively

44. Ellen Nakashima, "U.S. Said to Be Target of Massive Cyber-Espionage Campaign," *Washington Post*, February 10, 2013. The U.S. intelligence community has also released unclassified official reports alleging high levels of economic espionage originating in China, as well as Russia and other countries. See Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*.

45. Jennifer Schlesinger, "Chinese Espionage on the Rise in US, Experts Warn," CNBC.com, July 9, 2012, http://www.cnbc.com/id/48099539.

46. Keith Alexander, "Cybersecurity and American Power: Addressing New Threats to America's Economy and Military," speech given at the American Enterprise Institute, Washington, D.C., July 9, 2012, http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/.

47. Richard Bejtlich, "Developments in China's Cyber and Nuclear Capabilities," testimony presented before the U.S.-China Economic and Security Review Commission, 112th Cong., 2nd sess., March 26, 2012, p. 16, http://www.uscc.gov/Hearings/hearing-developments-china%E2%80%99s-cyber-and-nuclear-capabilities. The term APT has since come to be used more generally for any

convincing bits of evidence, such as the use of Chinese-language malware and keyboard settings, internet addresses and domains registered in China, flagrant reuse of usernames and email accounts, idiosyncratic programming tics traceable to particular individuals, and patterns of activity peaking during Chinese work hours.[48] APT targets include Western government and military agencies, a wide range of firms in industries of particular relevance to China's growth strategy, expatriate Chinese minorities and religious dissidents, U.S. presidential candidates, Asian international institutions, and even the International Olympic Committee. Dozens of Chinese nationals prosecuted under the 1996 U.S. Economic Espionage Act have spied on similar targets, which suggests a continuity of collection priorities across human intelligence and CNE collection.[49]

Figure 2 lists thirty-seven cases of alleged Chinese CNE from 2005 through 2013, ordered by the date the intrusions were publicly reported in Western media and showing the estimated duration of each intrusion.[50] The first publicly reported major Chinese hacking, for example, was "Titan Rain," a U.S. government code word for intrusions into Department of Defense laboratories, NASA networks, and aerospace companies between September 2003 and August 2005.[51] These data track reporting on APTs rather than APT intrusions themselves, which are self-hiding by nature. One should thus be cautious when drawing inferences, because an increase in reporting may reflect an increase in the West's appetite for cyber reporting rather than an increase in Chinese

type of targeted intrusion, as distinguished from untargeted "bulk" cybercrime. Thus the NSA penetration of Huawei might reasonably be described as an APT.

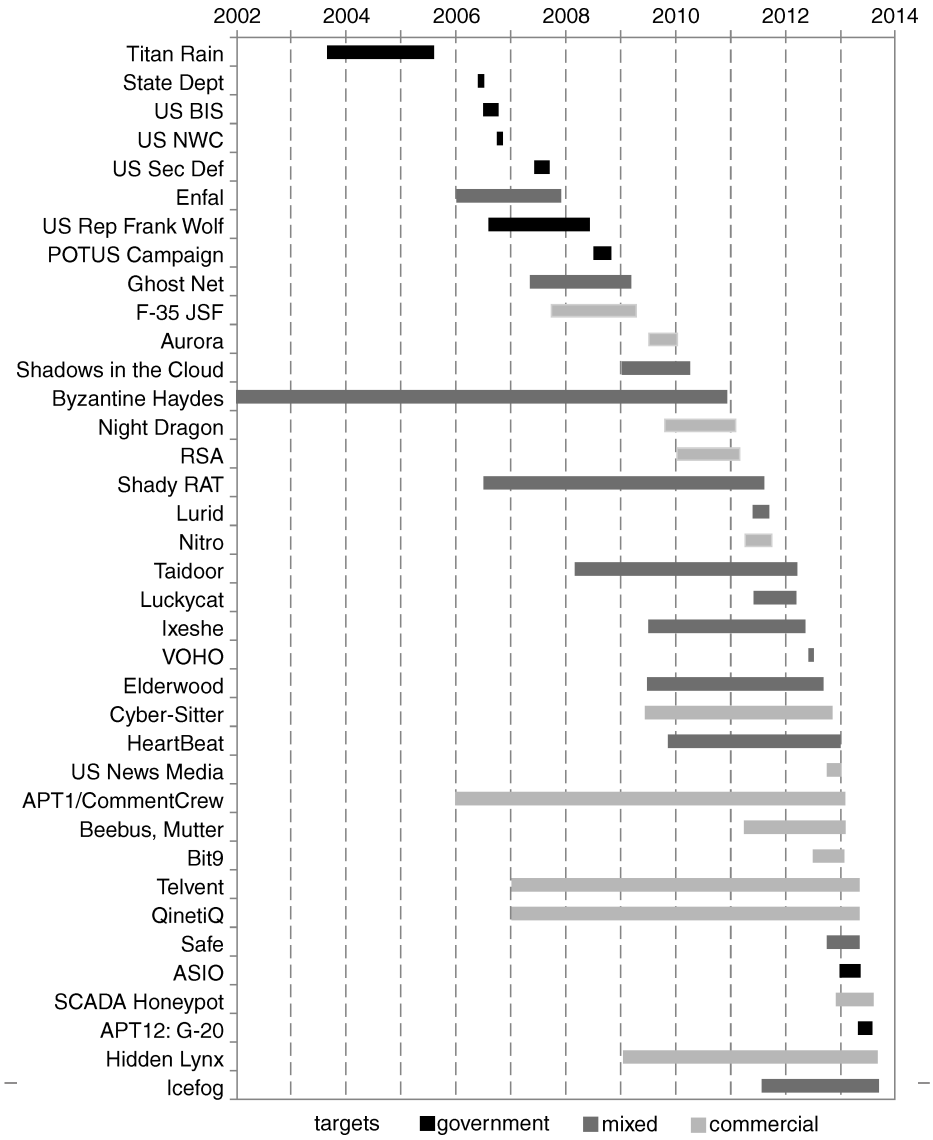
48. Chinese critics often reject Western allegations of Chinese CNE by pointing out that "[a]n IP address simply is not a valid proof for the source of a hacker." See Zhang Yixuan, "U.S. Finds an Excuse for Expanding Its 'Cyber Troop,'" *People's Daily Online* (overseas edition), February 4, 2013. Attribution to China rests on a much more comprehensive mass of evidence, however, with no reasonable alternative explanation for its totality.

49. Peter Toren, "A Report on Prosecutions under the Economic Espionage Act," paper presented at the American Intellectual Property Law Association annual meeting, Trade Secret Law Summit, Washington, D.C., October 23, 2012.

50. These data record reporting on Chinese APTs that have appeared in major English-language media outlets (using a search of Google news headlines) and that have been commonly cited in discussions of Chinese intrusions. This dataset is emphatically not the sum total of APT intrusions themselves, which is basically unknowable. Data point names refer to nicknames given to particular intrusion sets by Western cybersecurity firms, government agencies, or the targets of the intrusion. For further discussion and sourcing, see Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in Lindsay, Cheung, and Reveron, *China and Cybersecurity*.

51. Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them): An Exclusive Look at How the Hackers Called TITAN RAIN Are Stealing U.S. Secrets," *Time*, September 5, 2005, pp. 19–21.

Figure 2. Public Reporting on Chinese Intrusions, Ordered by Reporting Date and Displaying Estimated Duration



SOURCE: 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), table 3.1.

activity. Nonetheless, because Chinese intrusions drive the West's evolving awareness of Chinese APTs, it is possible to offer a few tentative interpretations of the data.

The earliest public reporting on APTs describes mostly government targets and defense contractors, but around 2010 there was a shift toward more emphasis on commercial targets. This shift is also reflected in the targeting patterns of PLA Unit 61398 (also known to Western security experts as "APT1" or "Comment Crew"), which increased the number and diversity of industrial targets in its CNE campaign.[52] The shift was roughly coincident with the implementation of China's "National Medium- and Long-Term Plan for the Development of Science and Technology (2006–2020)" or MLP. The MLP is the self-described "grand blueprint of science and technology development" for the "great renaissance of the Chinese nation." According to one business analyst, the MLP "is considered by many international technology companies to be a blueprint for technology theft on a scale the world has never seen before."[53] It is possible that the MLP's emphasis on foreign technology transfer encouraged heightened APT targeting of Western firms, especially those in the advanced technology categories highlighted in the MLP.

The frequency of overall reporting and the reporting on long-duration intrusions also increased after 2011.[54] In addition to more intensive commercial CNE spurred by the MLP, journalists' appetite for reporting on Chinese hacking almost certainly increased after the 2010 Google intrusion, and cybersecurity firms began to discover and report on much more widespread APT activity. Front-page news about the Chinese cyber threat and an expanding civilian cybersecurity industry have improved public and professional understanding of APTs. Prior to 2010, Western firms could be accused of complacency regarding cybersecurity. Since then, however, Western cybersecurity defenses, technical expertise, and government assistance to firms have improved. Also, the increased reporting on long-duration APTs (i.e., those that might be expected to be the most difficult to root out) may reflect a growing discovery rate of hard-to-find APTs by network defenders.

The potential improvement in Western cyber defense stands in stark con-

52. Mandiant, "APT1," p. 23.
53. James McGregor, "China's Drive for 'Indigenous Innovation': A Web of Industrial Policies" (Washington, D.C.: Global Intellectual Property Center, U.S. Chamber of Commerce, 2010).
54. The "Byzantine Haydes" intrusion set is an outlier, because it was tracked by U.S. intelligence from 2002 until the public compromise of its code name by Pfc. Bradley (now Chelsea) Manning and Wikileaks. The other APTs are reported mainly by civilian cybersecurity firms.

trast to the popular perception of helplessness in the face of growing Chinese intrusion threats. It is possible that one day Chinese cyber operators may look back on 2010–13 much the way German submariners looked back on the "happy time" of 1940–41—namely, as a brief period rich in easy targets before victims learned how to develop active tracking and countermeasures to protect themselves. This dynamic highlights a basic dilemma of covert action: the more aggressively one exploits stealth and anonymity to inflict harm, the more likely one will lose that very protection as the target realizes it must improve its counterintelligence posture. An actor that wants to keep cyber operations covert therefore needs to show restraint and eschew ambitious gambits.[55]

Obstacles to the Absorption of Stolen Data

Remote access to target networks is only the first step toward developing an intelligence advantage, much less downstream competitive advantage. Although Western cyber defenders can observe the exfiltration of petabytes of data to Chinese servers, they cannot so readily measure China's ability to use the data. It is possible, for example, that operators in the Third Department of the PLA General Staff are simply rewarded for the number of foreign targets penetrated and terabytes exfiltrated, with little attention to the satisfaction of the intelligence customer, thereby creating lots of measurable CNE with little improvement in national competitiveness. The acquisition, absorption, and application of foreign information from any source is a complicated process. Transaction costs at every step along the way caused by information overload, analytic misinterpretation, or bureaucratic silos can undermine the translation of stolen data into new production knowledge and successful competition in the marketplace.

Technology transfer by any means is both a priority and a challenge for China. The MLP promotes a policy of "indigenous innovation" (*zizhu chuangxin*), which involves "enhancing original innovation through co-innovation and re-innovation based on the assimilation of imported technologies."[56] This policy involves a four-part process for converting foreign

55. On deception as a strategy for defense, see Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies*, forthcoming. For a technical approach emphasizing counterintelligence surveillance, see Richard Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response* (San Francisco, Calif.: No Starch, 2013).

56. Government of the People's Republic of China, "National Medium- and Long-Term Plan for the Development of Science and Technology (2006–2020)," quoted in McGregor, "China's Drive for 'Indigenous Innovation,'" p. 4.

technology into remade domestic variants that Chinese sources describe as "introduce, digest, assimilate, and re-innovate" (IDAR). As of 2006, there were around 50,000 personnel in 400 foreign information analysis and diffusion centers (35 of them with the central government and the rest distributed provincially) charged with interpreting open-source science and technology data to support defense and civilian enterprises. Chinese expenditure on IDAR grew substantially, from $1.4 billion in 1991 to $7 billion in 2011. Strikingly, the ratio of expenditure on back-end assimilation relative to front-end acquisition increased from 5 percent to 45 percent during the same period.[57] Assimilation does not happen automatically, and it appears to be getting harder, as Chinese collection targets the higher end of the value chain.[58] Furthermore, espionage is just one of many channels for foreign technology transfer, which also includes joint ventures, Chinese nationals abroad, and open-source IDAR.[59] The incorporation of data stolen through CNE, which is necessarily bereft of social context, can only add additional coordination challenges and expense to the already complex IDAR process.

China faces major challenges in converting foreign inputs into innovative output given the notoriously compartmentalized and hierarchical nature of Chinese bureaucracy, underdeveloped high-end equipment manufacturing capacity, and chronic dependence on foreign technology and know-how. Reliance on Russia for fighter jet engines despite years of access to technical design information and assistance from Russian technicians is a particularly notable but hardly unique example in the Chinese defense industry. Foreign expertise is only one input in the overall innovation process, which also requires "hard" factors such as materials, universities, skilled labor, laboratories, and factories, as well as "soft" factors such as leadership, regulation, contract enforcement, standards and protocols, and an innovative culture. The utility of even the best CNE is sensitive to the performance of the rest of these factors working in synergy, and China still has far to go in integrating them.[60]

Similar considerations extend from economic to defense competitiveness.

57. Lindsay and Cheung, "From Exploitation to Innovation."
58. In private conversation with the author, the chief security officer of a major cybersecurity firm noted that APTs have recently begun to target business process and human relations data, not just intellectual property. This suggests that the problem of recovering the social context of valuable data has become apparent to Chinese collectors as well.
59. William C. Hannas, James C. Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (New York: Routledge, 2013).
60. Tai Ming Cheung, "The Chinese Defense Economy's Long March from Imitation to Innovation," *Journal of Strategic Studies*, Vol. 34, No. 3 (June 2011), pp. 325–354.

According to the U.S. Defense Science Board, China has obtained design information on more than two dozen major U.S. weapons systems, including theater ballistic missile defense components, the Joint Strike Fighter, and the Littoral Combat Ship.[61] These data could be used to develop countermeasures to these systems or to close the defense technology gap with the United States. Both are undesirable outcomes, and it is important to improve operational security and counterintelligence support for the U.S. defense industry. Worries about a wholesale erosion of U.S. defense competitiveness resulting from cyber espionage, however, are premature. The Soviet Union's reliance on systematic industrial espionage to catch up with the West provides a cautionary tale: the Soviet system became optimized for imitation rather than innovation and was thus locked into a form of second-place dependency, even as it shortened research and development timelines.[62] Chinese espionage can potentially narrow the gap with the West, but only at the price of creating dependency through investment in a large-scale absorption effort. Chinese CNE poses a genuine intelligence threat, to be sure, but it is neither singularly grave nor unprecedented.

Western exploitation of Chinese networks

Whatever advantages China gains through CNE, the intelligence contest with the West is hardly one-sided. In the wake of the Snowden leaks, U.S. officials made a categorical distinction between spying for profit and spying for security. Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey observed that all "nations on the face of the planet always conduct intelligence operations in all domains," but "China's particular niche in cyber has been theft and intellectual property."[63] A White House spokesperson insisted, "We do not give intelligence we collect to U.S. companies to enhance their international competitiveness or increase their bottom line."[64] In practice, however, this line can blur. The U.S. government might spy on a foreign trade delegation to improve its position in negotiating trade agreements, which would benefit U.S. firms indirectly. It might spy on foreign defense firms and pass on weapon designs

61. Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," *Washington Post*, May 27, 2013.
62. Central Intelligence Agency, "Soviet Acquisition of Militarily Significant Western Technology: An Update" (Langley, Va.: Central Intelligence Agency, September 1985), http://www.dtic.mil/dtic/tr/fulltext/u2/a160564.pdf.
63. David Alexander, "Top Officer Rejects Comparison of U.S., Chinese Cyber Snooping," Reuters, June 27, 2013.
64. David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *New York Times*, March 22, 2014.

to U.S. contractors to develop countermeasures or future requirements, which could improve their profitability. In the past, the U.S. government has provided cyber expertise to firms—for example, when the National Security Agency (NSA) aided Google in the wake of the 2010 intrusion by a Chinese APT. Exploitation of foreign firms—for example, the NSA penetration of Huawei—can also provide insight into foreign decisionmaking or support follow-on collection operations. Stansfield Turner, a director of central intelligence in Jimmy Carter's administration, has even suggested that the United States should provide economic intelligence to major U.S. firms to enhance their international competitiveness.[65]

China's uneven industrial development, fragmented cyber defenses, uneven cyber operator tradecraft, and the market dominance of Western information technology firms provide an environment conductive to Western CNE against China. Investigative journalists describe a secretive unit within the NSA focused on penetrating sensitive Chinese networks.[66] Documents leaked by Edward Snowden describe extensive NSA penetration of Chinese telecommunications giant Huawei.[67] Snowden also alleged in an interview with a Hong Kong newspaper that the NSA had tapped Chinese communications via a civilian university circuit. As a result, anti-American protests and support for Snowden spread throughout China, coinciding with the first summit between Presidents Barack Obama and Xi Jinping.[68] Some of the Snowden leaks suggest a combination of witting and unwitting assistance to the NSA from U.S. internet firms, ranging from the sharing of metadata and technical design information to exploitation of technical control points in cloud infrastructure located on U.S. soil.[69] Notably, it took an insider leak to compromise the NSA, but lax operator tradecraft has compromised Chinese CNE; this imbalance suggests a higher degree of competency and attention to detail in U.S. tradecraft.

Ironically, and contrary to the death-by-a-thousand-cuts narrative, it may be

65. Stansfield Turner, "Intelligence for a New World Order," Foreign Affairs, Vol. 70, No. 4 (Fall 1991), http://www.foreignaffairs.com/articles/47148/stansfield-turner/intelligence-for-a-new-world-order.
66. Matthew M. Aid, "Inside the NSA's Ultra-Secret China Hacking Group," *Foreign Policy*, June 10, 2013, http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group.
67. Sanger and Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat."
68. China, no friend of political dissidents, evinced both schadenfreude over U.S. hypocrisy and embarrassment over the publicity received by Snowden himself. See An Gang, "The Snowden Factor," *Beijing Review*, July 29, 2013, http://www.bjreview.com.cn/world/txt/2013-07/29/content_557717.htm.
69. Richelson, "The Snowden Affair."

American CNE against China, rather than Chinese CNE against the United States, that ends up adversely affecting the competitiveness of American firms. The Snowden trove has provided China with credible evidence of CNE via some major American internet firms. This, in turn, has prompted a wider backlash against the "eight King Kongs" (*bada jingang*)—Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle, and Qualcomm. Cisco reported an 18 percent drop in orders from China in the fall quarter of 2013, while Hewlett-Packard, IBM, and Microsoft also reported declining Chinese sales.[70] A Chinese "De-IOE" movement—short for IBM, Oracle, and EMC—emerged to advocate uninstalling Western technology in the Chinese banking and e-commerce industry and replacing it with products from Chinese rivals such as Huawei and Inspur.[71] Shortly after the U.S. indictment of five alleged PLA members for espionage in May 2014, the Chinese Central Government Procurement Center banned the Microsoft Windows 8 operating system from all government offices.[72] In addition to concerns prompted by the Snowden leaks, China points to actions taken by the United States and Australia to exclude Huawei from sensitive projects based on suspicions of Chinese espionage.[73] Both sides accuse the other of carrying out protectionist activities rather than implementing genuine security measures. Retaliatory Chinese technical barriers to trade compound the economic costs to the United States (in addition to whatever is lost to espionage), but there has been little cost-benefit analysis of these trade-offs in cyber policy.

Chinese espionage is impressive in its scope, but it does not translate easily into industrial absorption, which is a prerequisite for competitive advantage. Furthermore, U.S. intelligence appears to be more technically adept, even if its target set differs somewhat from China's. Both sides are engaged in commercial and intelligence contests using a range of political, economic, and technical tools. Charges of unfair competition and attempts to redress it will remain a

70. Spencer E. Ante, Paul Mozur, and Shira Ovide, "NSA Fallout: Tech Firms Feel a Chill inside China," *Wall Street Journal*, November 14, 2013.
71. Li Xiaoxiao et al., "China Pulling the Plug on Foreign Mainframes," *Caixin*, June 25, 2014, http://english.caixin.com/2014-06-25/100695344.html.
72. "China Excludes Windows 8 from Government Computers," Xinhua news agency, May 20, 2014, http://news.xinhuanet.com/english/china/2014-05/20/c_133347210.htm.
73. Mike Rogers and Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," paper prepared for the U.S. House of Representatives Permanent Select Committee on Intelligence, 112th Cong., 2nd sess., October 8, 2012, committee print; and Maggie Yueyang Lu, "Australia Bars Huawei from Broadband Project," *New York Times*, March 26, 2012.

chronic feature of U.S.-China relations. There is no reason to expect the side playing catch-up to realize an enduring advantage for technical reasons alone.

Military Threats of Cyberwarfare

Just as the social context of exploitation and adversary counteraction combine to blunt the potential of cyber espionage, similar challenges in operational weaponization and strategic interaction constrain the potency of more disruptive cyber threats. Yet conventional wisdom holds that a multitude of technical factors favor offense over defense in cyberspace and that the difficulty of attribution undermines the credibility of deterrence; therefore, weaker actors can attack the control systems of superior adversaries to achieve levels of physical disruption possible previously only through kinetic bombing. As President Obama writes in a *Wall Street Journal* opinion article, "Computer systems in critical sectors of our economy—including the nuclear and chemical industries—are being increasingly targeted. . . . In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we've seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill."[74] A number of former U.S. government officials have even likened the advent of cyberweapons to a new atomic age and have wondered why a catastrophic cyberattack has not yet occurred.[75] Chinese military doctrine similarly envisions cyberwarfare to be a low-cost, long-range, highly effective counter to a superior adversary.[76] There are reasons, however, to doubt the PLA's ability to implement these ideas or to defend itself against cyberattacks launched by a superior adversary.

74. Barack Obama, "Taking the Cyberattack Threat Seriously," *Wall Street Journal*, July 19, 2012.
75. Mike McConnell, "Cyberwar Is the New Atomic Age," *New Perspectives Quarterly*, Vol. 26, No. 3 (Summer 2009), pp. 72–77; Clarke and Knake, *Cyber War*; and Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012.
76. James C. Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Roy Kamphausen, David Lai, and Andrew Scobell, eds. *Beyond the Strait: PLA Missions Other Than Taiwan* (Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, 2009), 253–286; and Kevin Pollpeter, "Controlling the Information Domain: Space, Cyber, and Electronic Warfare," in Ashley J. Tellis and Travis Tanner, eds., *Strategic Asia 2012–13: China's Military Challenge* (Seattle, Wash.: National Bureau of Asian Research, 2012), pp. 163–196.

CHINESE CYBER DOCTRINE

The aggressive tenor of Chinese writings on cyberwarfare and the copious APT activity described above are the major sources of evidence that Western analysts usually offer to characterize the Chinese cyberwarfare threat. Official Chinese military doctrine and sources in Chinese military professional literature consistently describe cyberwarfare as a revolutionary development in military affairs. Senior Col. Ye Zheng, author of books published by the Chinese Academy of Military Science entitled *On Informationalized Warfare* and *Information Warfare Course*, writes, "Although the main melody of the times—peace and development—is still playing strongly, the dark spirit of network warfare is lurking in the sky above humanity." This rhetorical construction implies that the cyber revolution undermines Deng Xiaoping's diagnosis of the largely stable nature of the international environment. Ye singles out the United States for experimenting with cyberweapons such as Stuxnet (used in the attack on Iranian enrichment infrastructure) and hints at the prospect of more to come: "[J]ust as nuclear war was the strategic warfare of the industrial age, network warfare will be the strategic warfare of the information age. It has already become a 'top level' form of operation that is highly destructive and relates to national security and survival."[77] He further describes cyberwarfare as an integral force multiplier as well as an instrument for achieving more strategic effects such as paralyzing another state's economy or exerting psychological influence on entire populations. Similarly, an author in the PLA's *Science of Information Operations* writes that cyber strikes "can seek to achieve partial or large-scale paralysis of enemy systems. As soon as a virus enters the enemy's command and control system, it will have tremendous destructive impact. . . . Therefore computer network war is an important means for paralyzing the enemy in wars of the future."[78]

The PLA recognizes the existence of an "information domain" (*xinxi lingyu*), although as with "information security" it encompasses a wider range of subcategories to include computer network and electronic warfare as well as psychological and intelligence operations.[79] Information operations are con-

77. Ye Zheng and Zhao Baoxian, "Wǎngluò zhàn, zenme zhàn" [How do you fight a network war?], *China Youth Daily*, June 3, 2011.
78. Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," in Lindsay, Cheung, and Reveron, *China and Cybersecurity*.
79. Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias," in Lindsay, Cheung, and Reveron, *China and Cybersecurity*.

sidered so vital for the limited high-technology wars the PLA envisions fighting that information supremacy is thought to be a precondition for gaining military supremacy anywhere else. The PLA's general strategic principle of "active defense" stresses offensive operations to seize the initiative. The authoritative *Science of Campaigns* thus states that the beginning of a network war will determine its outcome: "Whoever strikes first prevails."[80] PLA strategists assert that the vital targets of an advanced technology adversary are its information systems, and by attacking them covertly from beyond the range of enemy weapon systems it is possible to cause paralysis of the enemy's organization, strategic decisionmaking, and national economy. As an important article by Gen. Dai Qingmin on the concept of "integrated network-electronic warfare" points out, "Information operations in high-tech warfare are, to a very great extent, a struggle which revolves around the destruction and the protection of C4ISR systems."[81] Chinese writers argue that a relatively weaker PLA can achieve information superiority against a stronger military only as long as it is able to launch paralyzing strikes at the beginning of a conflict.

The Chinese perspective on using information technology to improve awareness, synchronization, and precision is inspired by 1990s-era American writings about the "revolution in military affairs [RMA]."[82] RMA ideas were themselves inspired by Soviet strategists, and the common Marxist-Leninist belief that "technology determines tactics" surely influences PLA thought.[83] Yet the most recent and relevant inspiration comes from Chinese study of U.S. operations in Iraq and the Balkans and analysis of the U.S. military's heavy dependence on communication and logistics networks.[84] In particular, the

80. Quoted in Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," p. 142.
81. Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," *China Military Science*, February 1, 2002, pp. 112–117. C4ISR—command, control, communications, computers, intelligence, surveillance, and reconnaissance—is the computer-intensive nervous system of a military organization.
82. Andrew F. Krepinevich, ed., *The Military-Technical Revolution: A Preliminary Assessment* (Washington, D.C.: Center for Strategic and Budgetary Assessments, Office of Net Assessment, 2002); William A. Owens and Edward Offley, *Lifting the Fog of War* (New York: Farrar, Straus and Giroux, 2000); and Eliot A. Cohen, "Change and Transformation in Military Affairs," *Journal of Strategic Studies*, Vol. 27, No. 3 (September 2004), pp. 395–407.
83. Dima P. Adamsky, "Through the Looking Glass: The Soviet Military-Technical Revolution and the American Revolution in Military Affairs," *Journal of Strategic Studies*, Vol. 31, No. 2 (April 2008), pp. 257–294; and Dennis J. Blasko, "'Technology Determines Tactics': The Relationship between Technology and Doctrine in Chinese Military Thinking," *Journal of Strategic Studies*, Vol. 34, No. 3 (June 2011), pp. 355–381.
84. Jacqueline Newmyer, "The Revolution in Military Affairs with Chinese Characteristics," *Journal of Strategic Studies*, Vol. 33, No. 4 (August 2010), pp. 483–504.

accidental U.S. bombing of the Chinese embassy in Belgrade prompted President Jiang Zemin to direct the PLA to develop so-called assassin's mace (*shashoujian*) weapons to solve the problems of "seeing far, striking far, and striking accurately." Jiang reasoned that "what the enemy is most fearful of is what we should be developing."[85] As the consummately "network centric" U.S. military leverages data links to reduce its force size—substituting information for mass in the RMA formula for success—those links become vulnerabilities and thus tempting targets for the PLA. Insofar as the cyber revolution thesis is influential in U.S. strategic planning, moreover, the specter of PLA cyberwarfare may indeed have some success in creating fear and encouraging restraint in U.S. planning.

Remarkably, however, there appears to be little mention in Chinese writings of the considerable controversy over the RMA in Western strategic literature or considerations of the downsides of the RMA.[86] The United States has fought several regional wars in recent decades and in the process has experienced no small amount of confusion and the "fog of war" as computer systems break down unexpectedly, adversaries refuse to conform to the assumptions of network-centric doctrine, and service members resort to ad hoc improvisations to muddle through. The PLA, by contrast, has not had the opportunity to test its ideas of "integrated network electronic warfare" in combat, and realistic command and control training is notoriously hard to achieve absent interaction with a real enemy and complex environment. The following review of Chinese cyber capabilities suggests that similar skepticism is also warranted for Chinese cyberwarfare.

Chinese cyber capabilities

Although Chinese writers emphasize the revolutionary potential of cyberwarfare, episodes of Chinese aggression in cyberspace have been more mundane. China's "hacker wars" flare up during episodes of tension in Chinese

85. Kevin Pollpeter notes that the roots of this program are mentioned in a biography of a former vice chairman of the Central Military Commission. See Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," p. 149.

86. See, inter alia, Stephen Biddle, "The Past As Prologue: Assessing Theories of Future Warfare," *Security Studies*, Vol. 8, No. 1 (Autumn 1998), pp. 1–74; Richard J. Harknett and the JCISS (Joint Center for International Security Studies) Study Group, "The Risks of a Networked Military," *Orbis*, Vol. 44, No. 1 (Winter 2000), pp. 127–143; John Ferris, "Netcentric Warfare, C4ISR, and Information Operations: Towards a Revolution in Military Intelligence?" *Intelligence & National Security*, Vol. 19, No. 2 (Summer 2004), pp. 199–225; and Jon R. Lindsay, "Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations," *Journal of Strategic Studies*, Vol. 36, No. 3 (June 2013), pp. 422–453.

foreign relations, as between Taiwan and the mainland between 1996 and 2004 in the wake of Taiwanese elections, between the United States and China following the 1999 bombing of the Chinese embassy in Belgrade and the 2001 EP-3 spy plane collision, and between China and Japan throughout the past decade during controversies involving the Yasukuni Shrine and the Senkaku/Diaoyu Islands.[87] Nationalist hackers (as distinguished from PLA units) deface foreign websites and launch temporary distributed denial of service attacks. Nationalist online outbursts may take place with the tacit consent or encouragement of the Chinese government, yet patriotic "hacktivism" is essentially just another form of symbolic protest. There has been speculation that PLA "cyber militias" associated with Chinese universities maintain a more potent reserve capability, but one study of open sources suggests that they are oriented toward more mundane educational and network defense activities.[88]

The majority of known PLA cyber operations are CNE for intelligence rather than computer network attacks to cause disruption.[89] Nevertheless, many analysts worry that CNE is "only a keystroke away" from CNA, thereby generating dangerous ambiguity between intelligence gathering and offensive operations. Intrusion techniques developed for industrial espionage might be used to plant more dangerous payload code into sensitive controllers or constitute reconnaissance for future assaults. Chinese probing of critical infrastructure such as the U.S. power grid is aggressive, to be sure, so a latent potential for the PLA to convert CNE into CNA cannot be discounted.[90] The discovery of access vectors and exploitable vulnerabilities, however, is only the first step to achieving effective reconnaissance of a target, and effective reconnaissance is just one step toward planning and controlling a physically disruptive attack. The most significant historical case of kinetic CNA to date, the Stuxnet attack on Iran's enrichment infrastructure, suggests that painstaking planning, careful rehearsals, and sophisticated intelligence are required to control a co-

87. Desmond Ball, "China's Cyber Warfare Capabilities," *Security Affairs*, Vol. 17, No. 2 (Winter 2011), pp. 81–103; and Scott J. Henderson, *The Dark Visitor: Inside the World of Chinese Hackers* (Fort Leavenworth, Kans.: Foreign Military Studies Office, 2007).

88. Sheldon and McReynolds, "Civil-Military Integration and Cybersecurity."

89. For background on CNE and CAN, see 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).

90. The primary example cited as motivating this fear appears to be Chinese intrusion into a company that monitors North American oil and gas pipelines; technical characteristics of the intrusion suggested that it was just a case of economically motivated espionage. See Nicole Perlroth, David E. Sanger, and Michael S. Schmidt, "As Hacking against U.S. Rises, Experts Try to Pin Down Motive," *New York Times*, March 4, 2013.

vert disruption.[91] The U.S. military also considered using cyberattacks to take down Libya's air defense system in 2011, but reportedly it would have taken too long to develop the option.[92] The latency between CNE and CNA is more complicated than generally assumed.

The PLA does have access to considerable resources, human capital, and engineering skill, so it might in principle overcome operational barriers to weaponization, but its observed operational focus and experience are concentrated on intelligence operations. The PLA has considerable organizational infrastructure for cyber operations, most notably in the Third and Fourth Departments of the PLA General Staff. The Third Department is the Chinese equivalent of the U.S. National Security Agency, with responsibilities for both signals intelligence and network defense. The Fourth Department (formerly headed by Gen. Dai Qingmin) is primarily responsible for electronic warfare, but its cyber mission, if any, is less clear. Western analysts have begun to piece together the bureaucratic organization of the Third Department through open-source intelligence.[93] Meanwhile Western corporate and governmental cybersecurity experts have had ample opportunity to observe this organization in action given the routine neglect of operational security by Chinese cyber operators. Lax tradecraft in CNE does not inspire confidence for the sophistication and attention to detail required for serious CNA. If the U.S. cyber community with all its experience and technical savvy still struggles with the weaponization of cyberspace, as difficulties with known U.S. operations suggest, then the untried PLA should be expected to encounter still more operational challenges in the implementation and coordination of cyberwarfare. PLA competency in CNA cannot be simply inferred from high levels of CNE.

the downside of "informatization"

China's ambition to become a world-class military power will lead the PLA to become more like the U.S. military in its dependence on networks and space

91. Lindsay, "Stuxnet and the Limits of Cyber Warfare."
92. Ellen Nakashima, "U.S. Accelerating Cyberweapon Research," *Washington Post*, March 18, 2012.
93. Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure" (Arlington, Va.: Project 2049 Institute, November 11, 2011); Mark A. Stokes and L.C. Russell Hsiao, "Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests" (Arlington, Va.: Project 2049 Institute, October 29, 2012); and Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, report prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp. (Washington, D.C.: U.S.-China Economic and Security Review Commission, March 7, 2012).

assets. This modernization will undermine the asymmetry of vulnerability thought to make cyberweapons so dangerous to the United States and instead put some of the PLA's own most sophisticated systems at risk. PLA antiaccess capabilities against U.S. power projection also include antiship ballistic missiles, cruise missile boats, antisatellite weapons, and fifth-generation aircraft. The PLA requires traditional forces, moreover, for other missions that might require warfighting, military operations other than war, or coercive diplomacy (a role ill-suited for secret and intangible cyberweapons). China's goal of "winning local wars under the conditions of informatization" requires the PLA to "enhance [its] warfighting capabilities based on information systems."[94] This transformation into a modern "informatized" force, inspired in no small part by American RMA ideals and force structure, entails greater reliance on C4ISR systems and computer networks. Yet China's pursuit of the promise of the RMA will also reveal its liabilities.

In imagining and planning for a potential war with the United States, the PLA has to worry about the demonstrated ability and willingness of the U.S. military to conduct cyber operations on the battlefield (in Iraq and Afghanistan) and in covert action (e.g., the Stuxnet attack). If cyberwarfare is as effective as Chinese writers believe it is but they underestimate the costs of mastery, then the PLA is doubly disadvantaged. Chinese attacks can be expected to be less skillfully coordinated against more robust U.S. defenses, and vice versa. The United States already has, while China still struggles to develop, the institutional complements and experience required to plan and control cyber operations in synchrony with the larger battle. Meanwhile the fear of cyberwarfare has prompted considerable U.S. military investment in network protection, active cyber defense measures (e.g., counterintelligence deception and "hack back" counterattack), and exercises in cyber-degraded conditions. The vaunted asymmetry of cyberwarfare, usually posed as an advantage for the weaker power, in fact runs in the opposite direction, giving the stronger and more experienced force the advantage.[95] If the military utility of cyber-

94. State Council Information Office, "The Diversified Employment of China's Armed Forces" (Beijing: State Council Information Office, April 2013), http://news.xinhuanet.com/english/china/2013-04/16/c_132312681.htm.

95. Desmond Ball concludes that China "would be unable to systematically cripple selected command and control, air defence and intelligence networks and databases of advanced adversaries, or to conduct deception operations by secretly manipulating the data in these networks. The gap between the sophistication of the anti-virus and network security programs available to China's cyber-warriors as compared to those of their counterparts in the more open, advanced IT societies, is immense." See Ball, "China's Cyber Warfare Capabilities," p. 101.

warfare is actually more limited than Chinese doctrine writers seem to believe, then conventional considerations about military effectiveness (e.g., the balance of power as well as skill in combined arms warfare and joint operations) should be expected to dominate strategic calculation and operational interaction in any conflict.

Two considerations complicate this discounting of the potency of cyberwarfare. First is the problem of misperception. The assumption that cyberwarfare is a potent, low-cost means for achieving an advantage is widespread in Chinese military writing. Although the RMA debate over whether information technology is an evolutionary complement or a revolutionary disruption in warfare is prominent in Western cyber literature, it is virtually absent in Chinese writings. Given the complexity of the cyber operating environment (i.e., remote intrusions through layers of heterogeneous technical systems and imperfectly understood organizational practices), there is nontrivial potential for an attacker to become confused, deceived, or compromised, especially against more ambitious and sensitive targets. There is also little Chinese discussion of the unintended consequences and collateral damage risks of cyber operations—for example, that one's own malware might cause blowback or harm friendly civilian infrastructure.[96]

Second, and related, is the risk of inadvertent escalation. Chinese doctrine stresses that striking first and striking hard against the most important networked targets is essential, because victory at the beginning of a war will determine its end. These beliefs are false.[97] Yet they could lead the PLA to authorize preemptive cyber strikes on high-value targets such as U.S. satellites or the civilian power grid in the false hope that these would paralyze or intimidate an adversary. The contrast between offense-dominant cyber dogma and a more complicated reality recalls the mismatch between "the cult of the offensive" before World War I and the defensive advantages of machine guns and barbed wire.[98] Preemptive PLA cyberattacks that fizzle could be worse than nothing at all if they reveal hostile intent and thereby encourage U.S. "cross domain" retaliation with more kinetic weapons. Conversely, U.S. commanders who wrongly fear the existence of a PLA "assassin's mace" in cyberspace may be tempted to preemptively strike PLA assets by the same first-mover logic. This possibility is particularly troubling in light of the PLA Second Artillery's

96. Pollpeter, "Chinese Writings on Cyberwarfare and Coercion."
97. For the strategic argument on this point, see Gartzke, "The Myth of Cyberwar."
98. Jack L. Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca, N.Y.: Cornell University Press, 1984); and Stephen Van Evera, *Causes of War: Power and the Roots of Conflict* (Ithaca, N.Y.: Cornell University Press, 1999).

dual command of both conventional antiship ballistic missiles and nuclear forces. Misperception of cyber offense dominance, heightened by the secrecy of cyber capabilities on both sides, is a recipe for U.S.-China crisis instability.[99] At the same time, the PLA's cautious and probing behavior in recent years during tensions with China's neighbors is at odds with its doctrinal musing about rapid operations. The dynamics (and likelihood) of a crisis between cyber-enabled opponents, and this dyad in particular, is a problem for future research.

Normative Threats to Internet Governance

In contrast to the direct threats posed by cyber operations such as internet control, industrial espionage, and military disruption, the "cybersecurity norms" quadrant in figure 1 concerns an indirect threat to the institutional governance of the internet. Under the assumption that states have a mutual interest in preserving the benefits of online exchange while limiting damage to their critical infrastructure, some advocate the universal adoption of codes of conduct, arms control agreements, and even the redesign of management institutions.[100] Yet some policy reactions to major cyber threats could have the perverse effect of undermining the very properties of the internet that make it worth protecting: the cure might kill the patient. The previous sections raised questions, however, about the severity or even reality of threats that might justify such drastic measures. Furthermore, in the realm of internet governance there are additional Chinese constraints and Western strengths that make deleterious reorganization unlikely.

China's challenge to internet governance

China, together with Russia and other members of the Shanghai Cooperation Organization, has for a decade promoted reforms for internet governance. The organizing principle of "internet sovereignty" entails international agreement:

99. David C. Gompert and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability," *Survival*, Vol. 56, No. 4 (August/September 2014), pp. 7–22; and Avery Goldstein, "First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations," *International Security*, Vol. 37, No. 4 (Spring 2013), pp. 49–89.

100. See, for example, Rex Hughes, "A Treaty for Cyberspace," *International Affairs*, Vol. 86, No. 2 (March 2010), pp. 523–541; Duncan B. Hollis, "An E-SOS for Cyberspace" (Rochester, N.Y.: Social Science Research Network, September 1, 2010); and Paul Meyer, "Cyber-Security through Arms Control: An Approach to International Co-operation," *RUSI Journal*, Vol. 156, No. 2 (April/May 2011), pp. 22–27. On the applicability of international law to cybersecurity, see Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

first, to abstain from uninvited influence of any kind within any state's information space and, second, to regulate the internet through an international forum, such as the United Nations' International Telecommunication Union. The first element is at odds with liberal norms of open connection and freedom from censorship, and the second envisions primary responsibility for standards setting to reside with states rather than the constellation of multistakeholder institutions that has historically governed internet protocols and global network management. China and Russia proposed an "International Code of Conduct for Information Security" at the United Nations in September 2011 that reflects both of these points.[101] To promote "constructive and responsible behavior, and enhance their cooperation in addressing common threats and challenges," the Code asks countries to voluntarily cooperate with one another in combating "criminal and terrorist activities" to include "curbing dissemination of information which incites terrorism, secessionism, and extremism" (also known in CCP jargon as "the three evils"). This wording reflects the expansive Chinese (and Russian) definition of information security to encompass content control as well as defense against malware. The code also urges the "establishment of a multilateral, transparent, and democratic international management of the Internet" as an alternative to existing institutions. Its supporters expect the reforms to not only facilitate improved national information controls, but also to curb what they perceive to be excessive and unfair American influence.

The American roots of legacy governance institutions and some enduring links of those institutions to the U.S. government are points of growing contention internationally, even as China and other states generally benefit greatly from connection to the internet.[102] The open internet was designed to work and grow in a decentralized fashion, but this network of networks still re-

101. The proposal has not been formally debated or widely endorsed, but it has served as a lightning rod to focus awareness on the challenge to internet governance. As recently as the November 2014 "World Internet Conference" in Wuzhen, China, the Chinese government continued to champion themes articulated in the Code of Conduct. For the text, see Ministry of Foreign Affairs of the People's Republic of China, "China, Russia, and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations" (Beijing: Ministry of Foreign Affairs of the People's Republic of China, September 13, 2011), http://nz.chineseembassy.org/eng/zgyw/t858978.htm.

102. Laura DeNardis, *The Global War for Internet Governance* (New Haven, Conn.: Yale University Press, 2014); Andrew Whitmore, Namjoo Choi, and Anna Arzrumtsyan, "One Size Fits All? On the Feasibility of International Internet Governance," *Journal of Information Technology & Politics*, Vol. 6, No. 1 (February 2009), pp. 4–11; and Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, Mass.: MIT Press, 2010).

quires common protocols and technician collaboration to facilitate interconnection. In the early days of the internet, consensus on technical standards developed through circulation and discussion of "request for comment" memos. A slightly more formal process developed under the auspices of the Internet Engineering Task Force, created by the U.S. government, and later the Internet Society. These institutions have a heterogeneous membership of academics, commercial engineers, government representatives, nonprofit groups, and network users; infrastructure vendors such as Cisco and Huawei can voluntarily adopt proposals that emerge from their conversation. Furthermore, while internet traffic routing is decentralized, the internet does depend on some hierarchical components—in particular, the Domain Name System, which translates numerical addresses into human-friendly text addresses. The addressing system is managed by the Internet Corporation for Assigned Names and Numbers, headquartered in Los Angeles under contract to the U.S. Department of Commerce. These and other institutions (known as the "I-star" group) knit together a loose coalition of nonprofit, corporate, and state entities. Technoliberal norms of open connectivity, shared source code, and freedom from censorship developed with internet pioneers. Such norms now enjoy cosmopolitan support from multistakeholder advocates worldwide, particularly in Europe, North America, and Oceana.

The internet sovereignty versus multistakeholder debate involves not only technical standards and protocols, but also alternative visions of global political order, one based on authoritarian states and the other on liberal globalization. The Sino-Russian Code of Conduct was proposed just months after the Obama administration released its *International Strategy for Cyberspace*. The latter defends a normative vision of "an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation."[103] These ideals reflect the values of the open internet, the status quo throughout recent decades; the multistakeholder position is thus an ironically conservative vision for a technology often characterized in terms of constant change. The *International Strategy* links the ideology of the open internet to American values and interests; and indeed, the United States has an interest in maintaining the historical organization of the internet while also expanding its reach. Although China is not named explicitly, the chal-

103. White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, D.C.: White House, May 2011), p. 8.

lenges China poses to the open internet are mentioned throughout the document; for example, internet censorship is illegitimate, and the United States will work against it; intellectual property theft is unacceptable, and all countries must enforce laws protecting ideas; exporting domestic internet abuse abroad through internationally connected circuits should be opposed; and the United States will retain the right to retaliate against unacceptable attacks with either cyber operations or military force. China has taken exception to the portrayal of multistakeholder values as universal and seeks to redefine them.

Nevertheless, major reform to the current regime of internet governance is unlikely for two reasons. First, China cannot credibly commit to abide by its own norm of internet sovereignty. And second, China benefits from the current system.

China's credibility problem

Assuming that the clash of values matters for internet governance, China cannot credibly commit to adhere to its preferred norm of internet sovereignty. The CCP regime has political incentives to use CNE against dissident groups, ethnic minorities, and Western media abroad. China's indigenous innovation policy provides economic incentives for state agencies to use CNE to steal intellectual property and sensitive data from foreign firms. The PLA has military incentives to use CNE for reconnaissance to identify enemy vulnerabilities and understand the threats it faces. All of this activity relies on deception and is not officially acknowledged. Exploitation of the open internet is too tempting and too hard to detect for China to voluntarily abstain from indulging in it. A reform to an international institution has little chance of being implemented if its leading champion cannot credibly commit to supporting it.

If parties to an agreement believe that the weapons they are being asked to abandon are useful for achieving their security objectives, then they will be unlikely to agree in the first place. There is universal agreement that nuclear weapons are terribly destructive and technically amenable to monitoring and control, but it can still be exceedingly difficult to agree about how to control them.[104] Successful agreements are more often the product rather than the source of prior incentives for cooperation, just as arms racing reflects rather than creates a security dilemma, although these points are debated.[105]

104. Marc Trachtenberg, "The Past and Future of Arms Control," *Daedalus*, Vol. 120, No. 1 (Winter 1991), pp. 203–216; and Joseph S. Nye Jr., "Arms Control and International Politics," *Daedalus*, Vol. 120, No. 1 (Winter 1991), pp. 145–165.
105. Albert Wohlstetter, "Is There a Strategic Arms Race?" *Foreign Policy*, Summer 1974, pp. 3–20;

The technical monitoring and enforcement challenges associated with cyber capabilities support this logic. For most weapons of mass destruction, it is technically possible in principle, though often politically difficult in practice, to use inspections or remote surveillance to track progress toward the acquisition, modernization, or deployment of weapons and thus to monitor and verify compliance with ratified agreements. Compared to the obvious destructiveness of nuclear weapons, for instance, there remains immense uncertainty about both the potency and applications of cyberweapons. Moreover, the dual-use aspect of cyberspace is fundamental to its weaponization: both military cyberweapons and civilian information technology run software on commercial computing infrastructure, the former relying on deception to exploit the latter. Directly regulating the proliferation of cyberattack methodologies is not feasible.

An alternative might be to agree to limit malicious actions in cyberspace (e.g., through universal operationalization of internet sovereignty norms). Yet, whereas the identity of the state responsible for a nuclear attack would be obvious, the dual-use ambiguity of cyberspace and the wider availability of malware complicate attribution, which in turn renders enforcement of an agreement challenging.[106] It is difficult to determine who should be punished in the event of a serious cyberattack, let alone agree on what constitutes seriousness given the ambiguous nature of some cyberattacks. Institutional solutions to address these challenges could include (1) requiring official state agencies to refrain from proscribed activity in order to reduce the pool of potential miscreants; (2) penalizing states for any bad activity emanating from their borders in order to encourage them to police their infrastructure; (3) creating information-sharing regimes to better identify bad actors who cross borders and to monitor overall cybersecurity; (4) harmonizing domestic legal definitions and enforcement practices; and (5) providing collective assistance to states injured by a cyberattack. The Council of Europe's Convention on Cybercrime, opened for signature in Budapest in 2001 and ratified by forty countries (including the United States but not China), is one such attempt to

Trachtenberg, "The Past and Future of Arms Control"; and Andrew Kydd, "Arms Races and Arms Control: Modeling the Hawk Perspective," *American Journal of Political Science*, Vol. 44, No. 2 (April 2000), pp. 228–244.

106. Nuclear terrorism is thought to present similar attribution challenges, but the political context of proliferation greatly mitigates this concern. See Keir A. Lieber and Daryl G. Press, "Why States Won't Give Nuclear Weapons to Terrorists," *International Security*, Vol. 38, No. 1 (Summer 2013), pp. 80–104. On cyber attribution, see David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), pp. 25–40.

achieve these goals. Given widespread agreement that computer theft and fraud are major nuisances, establishing an effective regime to limit it should have been politically feasible. The Convention has proved largely ineffective, however, in curbing even these threats given its vague definitions, voluntary compliance, cumbersome policing coordination, and lack of enforcement mechanisms.[107]

As discussed in the previous sections, China and the United States currently perceive there to be some positive utility from engaging in aggressive CNE against each other and developing a military cyberwarfare capacity. Cyber arms control would require both states to agree to forgo these real benefits while being unable to convince one another that they have done so. The absence of evidence of cyber operations is not evidence of their absence, especially if the adversary has strong tradecraft. Covert collection could, in principle, continue undetected by the target despite whatever norms or agreements were endorsed publicly. The CCP will continue to have ample motivation to pursue CNE against political, economic, and military targets.

the internet as a liberal institution

Chinese complaints of American "internet hegemony" are not without some merit: the internet does indeed reinforce American dominance, but it does so through a light regulatory touch that relies on the self-interest of internet stakeholders. Although a technological artifact, the internet acts like an international institution in this respect.[108] Actors voluntarily connect to the internet because they believe there is more to gain than lose by adopting common networking protocols. The internet grows in a self-organized fashion, not through any technological imperative, but because actors have incentives to pursue increasing returns to interconnection. States may disagree on the margins about particular types of transactions even while agreeing about the desirability of transacting reliably and repeatedly across borders. Moreover, the profit-driven expansion of networks and markets through more reliable and voluminous transactions and more innovative products (cloud services, mobile computing,

107. Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View" (Stanford, Calif.: Hoover Institution, 2011).

108. Douglass C. North describes institutions as human-devised constraints on human behavior. See North, *Institutions, Institutional Change, and Economic Performance* (Cambridge: Cambridge University Press, 1990). This definition might be extended to encompass the material constraints of human-built technology as well as the normative and power-based constraints typically associated with institutions. To extend North's famous analogy, the "rules of the game" also require a "playing field" and "game equipment" to constrain the behavior of the players.

embedded computing, etc.) tends to reinforce the economic competitiveness of the United States. Like other major international institutions, the open internet facilitates American hegemony even if its daily operation is not directly under U.S. government control.[109]

The loose guidance of I-star institutions and the financial motives of leading U.S. internet firms (i.e., the "eight King Kongs") work indirectly to realize an American vision of an integrated, liberal, globalized world. Path dependence and increasing returns then reinforce the multistakeholder system. Tussles around internet governance are thus more likely to result in minor change at the margins of the system, not a major reorganization that shifts the definition of standards and internet regulation to the United Nations. One reason, therefore, that the ideological threat of internet sovereignty is overstated is that technoliberal values have played only a secondary role compared to institutional economics in the growth of the internet. The spread of cosmopolitan values associated with the open internet may marginally reinforce democratic values and institutions abroad, yet as discussed above, Beijing can resist by unbundling political and economic openness through the innovation of the Great Firewall. The number of states invested in the current global architecture has grown, ironically enough, because the internet is sufficiently flexible to handle "applications" such as censorship and surveillance. The flexibility of the legacy internet enables China to buy into and benefit from the very system it complains about.

Large shocks are usually needed to overcome high levels of institutional inertia, especially when reinforced by a durable and profitable technological infrastructure. The danger associated with the cybersecurity norms quadrant in figure 1 is predicated on an international overreaction to the systemic risk of cyber catastrophe or erosion of competitiveness. The previous sections on the cyberwarfare and contested cyberspace quadrants, however, call both of these threat narratives into question. Internet governance may become more complex as more actors come online, but the problem of internet governance is as old as the internet itself. The world's richest states—especially the U.S. hegemon—benefit greatly from the institutional status quo, even if it is operationally managed by nonstate actors such as commercial service providers and

109. On the general logic of liberal institutions, see, inter alia, Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton, N.J.: Princeton University Press, 1984); and G. John Ikenberry, *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars* (Princeton, N.J.: Princeton University Press, 2001).

other I-star stakeholders.[110] Major networked powers have no incentives to substantially overhaul internet governance, especially trading states such as China that are highly invested in the system.

Conclusion

Overlap across political, intelligence, military, and institutional threat narratives makes cybersecurity a challenging policy problem, which can lead to theoretical confusion. For each category, I have argued that the threat from China is exaggerated whereas the threat to China is underappreciated. By prioritizing political information control over technical cyber defense, China has inadvertently degraded the economic efficiency of its networks and exposed them to foreign infiltration. Although China also actively infiltrates Western networks, its ability to absorb stolen data is questionable, especially at the most competitive end of the value chain, where the United States dominates. Similarly, China's military cyber capacity cannot live up to its aggressive doctrinal aspirations, even as "informatization" creates vulnerabilities that more experienced foreign cyber operators can attack. Outmatched by the West, China has resorted to a strategy of institutional reform, but it benefits too much from multistakeholder governance to pose a credible alternative. The secrecy of cyber capabilities and operations on all sides makes it difficult to estimate with confidence the magnitude of the gap between China and the United States in the balance of cyber power, but it is potentially growing, not shrinking.

My examination of the case of China provides further support for critics of the cyber revolution thesis. The social context of exploitation matters tremendously for cyber performance. The more ambitious the infiltration, the greater the reliance on technical expertise, reliable intelligence, and organizational capacity to contend with mounting complexity and risk of compromise. This stands in contrast to the popular and erroneous belief that hacking is cheap and easy. It is a mistake to infer conclusions about high-impact cyber operations from more prosaic and plentiful cybercrime. Cyberspace enables numerous variations on familiar themes in political demonstration, crime, propaganda, signals intelligence, and electronic warfare, and it diffuses these activities widely. But cyber capabilities work as complements to power, not substitutes for it, and they are certainly not revolutionary game changers. This finding effectively shrinks two of the four quadrants in my typology, leaving

110. Drezner, "The Global Governance of the Internet."

only the evolutionary end of the technological threat spectrum. The normative politics of internet governance return to the open internet quadrant (where they have always been), and cyberwarfare collapses largely into contested cyberspace. Military cyber operations will emphasize exploitation for intelligence over disruption, even as the latter plays an adjunct role in combined arms warfare and covert action. The main problem of cybersecurity thus reduces to the evolving pursuit of marginal and deceptive advantage amid the benefits of open interconnection. Hallmarks of this development include 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.

On the political dimension, cybersecurity reflects the thoroughly ambiguous relationship between China and the United States, distinguished by deep economic interdependence as well as rivalry and mistrust in the security arena. Harassment in cyberspace, which relies on cooperative deception, both exploits and amplifies the ambiguity in the political relationship. Vibrant online exchange invites covert exploitation; but to preserve an internet worth exploiting, attackers must avoid crossing lines that might trigger costly counteraction. Broad agreement persists among major powers on the desirability of interconnection across borders, and lucrative new opportunities continue to open up with every innovation in computing, from virtualized services ("the cloud") to mobile and embedded devices ("the internet of things"). Indeed, the main reason actors worry about cybersecurity at all is because the internet is so useful most of the time. Most competition depends on some cooperation, and contested cyberspace is likewise predicated on the open internet. Internet openness enables contestation in cyberspace while competitors calibrate their exploitation to avoid closure. States and firms may throw up barriers to connection to deal with security externalities, even adopting national networking protocols with reduced interoperability.[111] Yet thorough internet fragmentation is unlikely to occur, because the economic benefits of interconnection are too great and cyber threats are too ambiguous. The internet has made China and the West richer than they would otherwise be, and ambiguous friction in cyberspace is just the price of doing business.

111. At the extreme, the "Balkanization of the internet" would erode the innovative potential and commercial efficiency of technology because of numerous public goods problems. See Roger Hurwitz, "Depleted Trust in the Cyber Commons," *Strategic Studies Quarterly*, Vol. 6, No. 3 (Fall 2012), pp. 20–45.

There is one remote but serious danger, however. Although limited war between the United States and China is extremely unlikely given the high costs of naval warfare and the disruption of trade, it is possible to imagine some paths to war through miscalculation in a crisis involving Japan or Taiwan. Misperceptions about the coercive potency of cyberwarfare or mistakes in the integration of cyber with other warfighting domains would inject additional uncertainty into such a crisis and make it more unstable. Chinese ability to manage the complex intelligence and command integration necessary to create predictable (and thus usefully weaponized) effects through cyberspace is questionable, even as Chinese doctrine calls for the early and paralyzing use of cyberattacks. Cyberweapons are highly classified, even as their effectiveness is poorly understood and often exaggerated. These properties are as likely to confuse friendly commanders as they are to muddy signals to an adversary, with ambiguous implications for escalation.[112] Importantly, this particular risk emerges via misperception rather than through the actual potency of an "assassin's mace" weapon.

Barring gross misperception, however, one can expect the risk of unwanted escalation from cyber to other military domains to deter both sides from resorting to more destructive forms of computer network attack in most situations.[113] Yet although nuclear or conventional deterrence might be able to check catastrophic cyberattack, it cannot credibly discourage minor cyber aggression such as nationalist hacktivism, industrial espionage, or harassment of dissident expatriates. Indeed, 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. In the original formulation of the paradox, mutual vulnerability to nuclear retaliation inhibits nuclear war but encourages conventional war in peripheral theaters where nuclear threats are not credible.[114] Today, the intensity of cyber aggression is bounded

112. Problems associated with cross-domain operations and strategy are still poorly understood. See Erik Gartzke and Jon R. Lindsay, "Cross-Domain Deterrence: Strategy in an Era of Complexity," paper presented at the International Studies Association annual meeting, Toronto, March 25–29, 2014.

113. U.S. officials increasingly stress the feasibility of deterrence against large-scale cyberattack. During his Senate confirmation hearing as director of the NSA and commander of U.S. Cyber Command, Adm. Michael Rogers observed, "Deterrence in cyberspace is achieved through the totality of U.S. actions, including the United States' overall defense posture and the resilience of our networks and systems." See Rogers, testimony before the Senate Armed Services Committee, 113th Cong., 2nd sess., March 11, 2014 (Washington, D.C.: Congressional Record, 2014).

114. Glenn H. Snyder, "The Balance of Power and the Balance of Terror," in Paul Seabury, ed., *The Balance of Power* (San Francisco, Calif.: Chandler, 1965), pp. 184–201 ; and Jeffrey Arthur Larsen and Kerry M. Kartchner, eds., *On Limited Nuclear War in the 21st Century* (Redwood City, Calif.: Stanford University Press, 2014).

by the risk of any form of military retaliation as well as the need to preserve interconnection and protect sources and methods that rely on deception. Cyberattackers intentionally keep the costs they inflict below the assessed threshold of even limited military retaliation by opponents, occupying a region where military threats of punishment would be utterly noncredible. The aggressor's freedom of action is further constrained by the need to maintain stealth and plausible deniability for ongoing operations. Actors that are deterred by threats of military punishment, on the one hand, and threats of counterintelligence detection or loss of connection, on the other, are encouraged to find more limited ways to inflict costs. The complexity of modern computer network infrastructure, in particular, offers many inexpensive ways to inflict minor costs. One implication is that cyberspace creates more scope for nontraditional security concerns (e.g., harassment of human rights organizations and vulnerable user communities) that powerful actors usually ignore in their focus on protecting high-value economic and military assets.[115]

As long as dense interconnection and economic interdependence remain mutually beneficial for powers such as the United States and China, they will be able to tolerate the irritants that they will inevitably inflict on one another. The modern intelligence-counterintelligence contest plays out in a complicated sociotechnical space where states take advantage of economic cooperation and hedge against security competition. If their broader mutual interest frays, however, then cyberwarfare becomes just one facet of a more serious strategic problem involving more dangerous means. Exaggeration of the cyber threat feeds spirals of mistrust, which make this undesirable outcome slightly more likely.

The United States and China should discuss the interaction of cybersecurity and traditional military force in depth and take steps to limit misunderstandings about the other's intentions. They might even learn to interpret chronic cyber friction as a sign that more truly dangerous threats have been constrained. Contrary to conventional wisdom, the emergence of complex cyber threats may be a positive development in the tragic history of international politics: the bad news about cybersecurity is good news for global security.

115. The same APT organizations target both Fortune 500 and government interests as well as human rights organizations and other nongovernmental organizations. See Ronald Deibert et al., *Communities @ Risk: Targeted Digital Threats against Civil Society* (Toronto: Munk School of Global Affairs Citizen Lab, University of Toronto, November 2014), https://targetedthreats.net/.