HARVARD Kennedy School
BELFER CENTER for Science and International Affairs
Policy Brief • May 2015

QUARTERLY JOURNAL: *INTERNATIONAL SECURITY*

Exaggerating the Chinese Cyber Threat

BOTTOM LINES

- **Inflated Threats and Growing Mistrust.** The United States and China have more to gain than lose through their intensive use of the internet, even as friction in cyberspace remains both frustrating and inevitable. Threat misperception heightens the risks of miscalculation in a crisis and of Chinese backlash against competitive U.S. firms.
- **The U.S. Advantage.** For every type of Chinese cyber threat—political, espionage, and military—there are also serious Chinese vulnerabilities and countervailing U.S. strengths.
- **Protection of Internet Governance.** To ensure the continued high performance of information technology firms and the mutual benefits of globalization, the United States should preserve liberal norms of open interconnection and the multistakeholder system—the loose network of academic, corporate, and governmental actors managing global technical protocols.

By Jon R. Lindsay

This policy brief is based on "The Impact of China on Cybersecurity: Fiction and Friction," which appears in the Winter 2014/15 issue of International Security.

INFLATED THREATS AND GROWING MISTRUST

Policymakers in the United States often portray China as posing a serious cybersecurity threat. In 2013 U.S. National Security Adviser Tom Donilon stated that Chinese cyber intrusions not only endanger national security but also threaten U.S. firms with the loss of competitive advantage. One U.S. member of Congress has asserted that China has "laced the U.S. infrastructure with logic bombs." Chinese critics, meanwhile, denounce Western allegations of Chinese espionage and decry National Security Agency (NSA) activities revealed by Edward Snowden. The *People's Daily* newspaper has described the United States as "a thief crying 'stop thief.'" Chinese commentators increasingly call for the exclusion of U.S. internet firms from the Chinese market, citing concerns about collusion with the NSA, and argue that the institutions of internet governance give the United States an unfair advantage.

The rhetorical spiral of mistrust in the Sino-American relationship threatens to undermine the mutual benefits of the information revolution. Fears about the paralysis of the United States' digital infrastructure or the hemorrhage of its competitive advantage are exaggerated. Chinese cyber operators face underappreciated organizational challenges, including information overload and bureaucratic compartmentalization, which hinder the weaponization of cyberspace or absorption of stolen intellectual property. More important, both the United States and China have strong incentives to moderate the intensity of their cyber exploitation to preserve profitable interconnections and avoid costly punishment. The policy backlash against U.S. firms and liberal internet governance by China and others is ultimately more worrisome for U.S. competitiveness than espionage; ironically, it is also counterproductive for Chinese growth.

The United States is unlikely to experience either a so-called digital Pearl Harbor through cyber warfare or

death by a thousand cuts through industrial espionage. There is, however, some danger of crisis miscalculation when states field cyberweapons. The secrecy of cyberweapons' capabilities and the uncertainties about their effects and collateral damage are as likely to confuse friendly militaries as they are to muddy signals to an adversary. Unsuccessful preemptive cyberattacks could reveal hostile intent and thereby encourage retaliation with more traditional (and reliable) weapons. Conversely, preemptive escalation spurred by fears of cyberattack could encourage the target to use its cyberweapons before it loses the opportunity to do so. Bilateral dialogue is essential for reducing the risks of misperception between the United States and China in the event of a crisis.

THE U.S. ADVANTAGE

The secrecy regarding the cyber capabilities and activities of the United States and China creates difficulty in estimating the relative balance of cyber power across the Pacific. Nevertheless, the United States appears to be gaining an increasing advantage. For every type of purported Chinese cyber threat, there are also serious Chinese vulnerabilities and growing Western strengths.

Much of the international cyber insecurity that China generates reflects internal security concerns. China exploits foreign media and digital infrastructure to target political dissidents and minority populations. The use of national censorship architecture (the Great Firewall of China) to redirect inbound internet traffic to attack sites such as GreatFire.org and GitHub in March 2015 is just the latest example of this worrisome trend. Yet prioritizing political information control over technical cyber defense also damages China's own cybersecurity. Lax law enforcement and poor cyber defenses leave the country vulnerable to both cybercriminals and foreign spies. The fragmented and notoriously competitive nature of the Communist Party state further complicates coordination across military, police, and regulatory entities.

There is strong evidence that China continues to engage in aggressive cyber espionage campaigns against Western interests. Yet it struggles to convert even legitimately obtained foreign data into competitive advantage, let alone make sense of petabytes of stolen data. Absorption is especially challenging at the most sophisticated end of the value chain (e.g., advanced fighter aircraft), which is dominated by the United States. At the same time, the United States conducts its own cyber espionage against China , as the Edward Snowden leaks dramatized, which can indirectly aid U.S. firms (e.g., in government trade negotiations). China's uneven industrial development, fragmented cyber defenses, erratic cyber tradecraft, and the market dominance of U.S. technology firms provide considerable advantages to the United States.

Despite high levels of Chinese political harassment and espionage, there is little evidence of skill or subtlety in China's military cyber operations. Although Chinese strategists describe cyberspace as a highly asymmetric and decisive domain of warfare, China's military cyber capacity does not live up to its doctrinal aspirations. A disruptive attack on physical infrastructure requires careful testing, painstaking planning, and sophisticated intelligence. Even experienced U.S. cyber operators struggle with these challenges. By contrast, the Chinese military is rigidly hierarchical and has no wartime experience with complex information systems. Further, China's pursuit of military "informatization" (i.e., emulation of the U.S. network-centric style of operations) increases its dependence on vulnerable networks and exposure to foreign cyberattack.

To be sure, China engages in aggressive cyber campaigns, especially against nongovernmental organizations and firms less equipped to defend themselves than government entities. These activities, however, do not constitute major military threats against the United States, and they do nothing to defend China from the considerable intelligence and military advantages of the United States.

PROTECTION OF INTERNET GOVERNANCE

Outmatched by the West in direct cyber confrontation yet eager to maintain the global connectivity supporting economic growth, China (together with Russia and

other members of the Shanghai Cooperation Organization) advocates for internet governance reform. These changes, predicated on so-called internet sovereignty, would replace the current multistakeholder system and its liberal norms of internet openness with a formal international regulator, such as the United Nations' International Telecommunication Union, and strong norms of noninterference with sovereign networks.

Chinese complaints of U.S. internet hegemony are not completely unfounded: the internet reinforces U.S. dominance, but it does so through a light regulatory touch that relies on the self-interest of stakeholders—academic scientists, commercial engineers, government representatives, and civil society organizations. The internet expands in a self-organized fashion because adopters have incentives to pursue increasing returns to interconnection. The profit-driven expansion of networks and markets through more reliable and voluminous transactions and more innovative products (e.g., cloud services, mobile computing, and embedded computing) tends to reinforce the economic competitiveness of the United States and its leading information technology firms.

Many Western observers fear that cyber reform based on the principle of internet sovereignty might legitimize authoritarian control and undermine the cosmopolitan promise of the multistakeholder system. China, however, benefits too much from the current system to pose a credible alternative. Tussles around internet governance are more likely to result in minor change at the margins of the existing system, not a major reorganization that shifts technical protocols and operational regulation to the United Nations. Yet this is not a foregone conclusion, as China moves to exclude U.S. firms such as IBM, Oracle, EMC, and Microsoft from its domestic markets and attempts to persuade other states to support governance reforms at odds with U.S. values and interests.

CONCLUSION

Information technology has generated tremendous wealth and innovation for millions, underwriting the United States' preponderance as well as China's meteoric rise. The costs of cyber espionage and harassment pale beside the mutual benefits of an interdependent, globalized economy. The inevitable frictions of cyberspace are not a harbinger of catastrophe to come, but rather a sign that the states inflicting them lack incentives to cause any real harm. Exaggerated fears of cyberwarfare or an erosion of the United States' competitive advantage must not be allowed to undermine the institutions and architectures that make the digital commons so productive.

• • •

Statements and views expressed in this policy brief are solely those of the author and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

RELATED RESOURCES

Krekel, Bryan, Patton Adams, and George Bakos. "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corporation (Washington, D.C.: U.S.-China Economic and Security Review Commission, March 7, 2012), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press, 2015).

Swaine, Michael D. "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, October 7, 2013, http://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf.

ABOUT THE BELFER CENTER

The Belfer Center is the hub of the Harvard Kennedy School's research, teaching, and training in international security affairs, environmental and resource issues, and science and technology policy.

The Center has a dual mission: (1) to provide leadership in advancing policy-relevant knowledge about the most important challenges of international security and other critical issues where science, technology, environmental policy, and international affairs intersect; and (2) to prepare future generations of leaders for these arenas. Center researchers not only conduct scholarly research, but also develop prescriptions for policy reform. Faculty and fellows analyze global challenges from nuclear proliferation and terrorism to climate change and energy policy.

ABOUT *INTERNATIONAL SECURITY*

International Security is America's leading peer-reviewed journal of security affairs. It provides sophisticated analyses of contemporary, theoretical, and historical security issues. International Security is edited at Harvard Kennedy School's Belfer Center for Science and International Affairs and is published by The MIT Press.

For more information about this publication, please contact the *International Security* editorial assistant at 617-495-1914.

ABOUT THE AUTHOR

Jon R. Lindsay is an assistant research scientist at the University of California, San Diego. In the summer of 2015, he will become Assistant Professor of Digital Media and Global Affairs at the University of Toronto Munk School of Global Affairs.

FOR ACADEMIC CITATION:

Lindsay, Jon R. "Exaggerating the Chinese Cyber Threat." Policy Brief, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2015.

Belfer Center for Science and International Affairs

Harvard Kennedy School
79 JFK St.
Cambridge, MA 02138

TEL: 617-495-1400
FAX: 617-495-8963
http://www.belfercenter.org