2015

H-Diplo

H-Diplo Article Reviews

No. 541
Published on 17 July 2015

H-Diplo Article Review Editors: Thomas Maddux and Diane Labrosse

Web and Production Editor: George Fujii

Commissioned for H-Diplo by Thomas Maddux

Jon R. Lindsay. "The Impact of China on Cybersecurity: Fiction and Friction." *International Security* 39:3 (2015): 7-47. DOI: 10.1162/ISEC_a_00189.
http://dx.doi.org/10.1162/ISEC_a_00189

URL: http://tiny.cc/AR541

Reviewed by **Xiaoyu Pu**, University of Nevada, Reno

As Geoffrey Blainey, the prominent Australian scholar, wrote long ago, "For every thousand pages published on the causes of wars, there is less than one page directly on the causes of peace."[1] The field of international security studies seems to have such an alarmist tendency, as most publications focus on conflict and war rather than stability and peace. Regarding cybersecurity, scholars and pundits have sounded alarms for years. In such a context, Jon R. Lindsay's article is refreshing and unusual. Challenging the conventional wisdom, Lindsay argues that the threat from China on cyberspace is overblown, and Chinese vulnerabilities and Western strengths are underappreciated. Furthermore, cyberspace is fundamentally more stable than we conventionally assume. While the proliferation of information technology might enable "numerous instances of friction below the threshold of violence," (9) cyberwar between United States and China is highly unlikely. Lindsay does not suggest that we should ignore the existence of cyber threats. What he proposes is an analytical framework that makes sense of these threats. Whether or not readers share his cautiously optimistic view, Lindsay's article will have an enduring relevance to the discussions of cybersecurity, U.S.-China relations, and international relations. My comments focus on the broad implications of his article for international relations and U.S.-China relations.

The relationship between technological innovation and international politics is a classical topic. The United States and the Soviet Union took decades to learn how to adapt and

[1] Geoffrey Blainey, *The Causes of War* (New York: The Free Press, 1973), 3.

respond to nuclear technology after 1945.[2] As a relatively new technological development, cyberspace has generated frustrations, uncertainties, and anxieties everywhere. To make sense of the cyber threats, Lindsay reminds us to see the entanglement between technological innovation and political environment as the core question. Lindsay constructs a "typology of cyber threat narratives" based on "different assumptions about what is possible and probable, technologically and politically" (11). The political factor is divided into "cooperative political environment" and "competitive political environment," while the technology factor is divided into "evolutionary technology" and "revolutionary technology" (12). There are four ideal types of cyber threat narratives, including "open internet, cybersecurity norms, contested cyberspace, and cyber warfare" (12). The analytical framework could help us understand some fundamental dilemmas posed by information technology and cyberspace. For instance, openness promotes Chinese economic growth, but Chinese leaders see openness as a threat to their regime's security. The political control of Chinese internet might strengthen the legitimacy of Chinese government temporally. However, the control measures could also undermine China's cybersecurity inadvertently because they could degrade China's economic efficiency and hinder China's technological innovation. In a more general sense, the choice between national security and global openness should resonate to policy makers of many countries, and the analytical framework provided by Lindsay has wide implications beyond China.

Lindsay's article has direct relevance for U.S.-China relations. In recent years, cybersecurity has become an extremely controversial topic in U.S.-China relations. We see an increasing number of tit-for-tat accusations, frustrations, and confusions. The bilateral discussions of the cyber issue are one-sided, and each side often accuses the other without acknowledging their mutual concerns and common interests. According to Lindsay, it is counterproductive to exaggerate the cyber threats from China and to ignore the common interests. While the 'friction' over cyberspace will continue to occur, the United States and China have rational incentives to moderate their cyber exploitation. Furthermore, Lindsay demystifies the 'fiction' of the China threat narrative. He 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" (9).

The United States and China have different priorities on cybersecurity: while the United States prioritizes the protection of intellectual property rights, China is highly sensitive about political information that might impact Chinese regime security. Based on Lindsay's analysis, a deep understanding of mutual concerns and common interests could help the United States and China to mitigate their mistrust and zero-sum thinking. Admittedly the United States and China have political differences, but the two countries also have an important common ground: both of them have benefited enormously from

[2] Joseph S. Nye, "*Nuclear Lessons for Cyber Security,*" *Strategic Studies Quarterly* (Winter, 2011), 19-38.

an open and globalized economy. Preserving an open and interconnected cyberspace serves the common interests of both countries. Furthermore, even on the issue of intellectual property rights, China should have increasingly common interests with the United States in the long term. As Lindsay points out, simply copy-catting American technology will not make China a powerhouse of advanced technology, and it might strengthen China's dependency on foreign technology. As China's economy moves up the value chain, the protection of intellectual property rights will serve China's interests. Only by overcoming its own institutional and legal barriers can China become a more innovative society.

While largely sharing Lindsay's cautiously optimistic view, I have two quibbles. First, Lindsay argues that "the bad news about cybersecurity is good news for global security" (47). There might be a reversed question: could bad news for global security be bad for cyber security? Even cyber security as an independent variable might not be that troublesome, cyber security as a dependent variable could still be worrisome. Although we should not exaggerate cyber instability, politically-motivated threat inflations might still cause serious troubles. For instance, if the United States and China cannot get their strategic relationship right, competitions in traditional security domains will surely inflate cyber challenges. Second, while the United States has its technological advantages over China, one factor that might contribute to instability is under explored in Lindsay's article. Given the power gap between the United States and China, it is not rational for China to play a catch-up game with the United States in the foreseeable future. However, China might take an asymmetrical strategy to pose challenges without catching up.[3] Although scholars have discussed this asymmetric interaction in conventional security domains, these dynamics might exist in cyberspace as well. That said, the incentives for restraint that are highlighted by Lindsay should serve as stabilizing factors even under an asymmetrical strategic relationship.

Overall, Lindsay's article is a welcome addition to the growing literature on cybersecurity and U.S.-China relations. His argument is refreshing and innovative, and his analysis is supported by original and rich resources. While focusing on cyberspace and China, the article has broad theoretical and policy implications. Such an article will have a long shelf life within the scholarly literature of international security studies.

Xiaoyu Pu is an assistant professor of political science at the University of Nevada, Reno. Previously he was a postdoctoral research fellow in the Princeton-Harvard China and the World Program. He received his Ph.D. from Ohio State University. His research interests include Chinese foreign policy, emerging powers (BRICS), and international relations

[3] Thomas J. Christensen, "Posing Problems Without Catching Up: China's Rise and Challenges for US Security Policy", *International Security* 25: 4 (2001): 5-40; Thomas J. Christensen, *The China Challenge: Shaping the Choices of a Rising Power* (New York: W.W. Norton & Company, 2015), 95-114.

theory. His research has appeared in *International Security, The China Quarterly, Chinese Journal of International Politics, Asian Affairs* as well as in the edited volume "Status in World Politics" (Cambridge, 2014). He serves on the international editorial boards of *Foreign Affairs Review* (Beijing) and *Global Studies Journal* (Hong Kong). He is working on a book tentatively entitled "Limited Rebranding: Status Signaling, Multiple Audiences, and China's Diplomatic Repositioning."