International Studies, lists cooperation with the United States to safeguard cyberspace from cyber crime as one of four countermeasures against U.S. preemptive cyber strikes. [8]

The third theme is the importance of developing a global framework or international information security code of conduct, but one that preserves the sovereignty of governments to control content and information flow. This position has been noted by U.S. defense analysts as well.[9]

## Legal Frameworks and U.S. Hegemony

Chinese analysts also call attention to the views held by scholars who study legal issues involving cyber attacks and warfare, which can be summarized in three schools of thought. The first considers current laws to be largely adequate to address all scenarios involving military actions—cyber and kinetic. The second school argues for complete abandonment of existing cyber regulations. This group believes that the Internet can be free of hostilities as a self-governing system. The third school holds that existing laws governing warfare are helpful but not completely adequate for addressing cyber-specific dynamics, leading this group to call for a special class of laws specifically addressing cyber scenarios.[10]

It appears that ideologically Chinese scholars largely fall into the third school of thought. Even though they vary regarding the best approach to develop new international legal regimes, a consistent theme in the literature is that the current legal regulations are inadequate to address the unique features of cyber warfare, which is partly due to the perceived power imbalance in cyberspace. The Chinese literature is consistent in presenting the PRC as an underdog in every respect in cyberspace, particularly vis-à-vis the United States:

> American hegemony exists throughout cyberspace in every area, in every corner of the Internet the U.S. has hegemony—hegemony in technology, hegemony in resources, hegemony in information and hegemony in the legal context—the U.S. has absolute advantage in at least these four areas.[11]

Chinese cyber security experts Zheng Zhilong and Yu Li, from Zhengzhou University in central China, are funded by the Chinese National Social Science Fund to conduct research exploring the diplomatic and strategic implications of cyber power under a grant titled, "The Internet and Our Country's Countermeasures through Our Role in International Politics." While the authors bemoan U.S. hegemony, they also predict a future shift in power from the United States to more populous and rapidly modernizing countries such as India and the PRC. Yu and Zheng conclude that the cyber realm is not a neutral space for state actors. The power of cyberspace is such that hegemonic states can advance a global political agenda and its comprehensive national strength by maintaining a lead in information technology. At the same time, the authors view cyberspace as a domain holding promise for a progressive transfer of power from hegemons to emerging nations that invest in information technology and technical education.[12]

To understand the way the PRC intends to achieve dominance in cyberspace it is necessary to look deeper than the cyber infrastructure, programs, and official pronouncements—areas easier to quantify—and peer into Chinese cultural and philosophical underpinnings. Some of the literature surveyed provides such a glimpse, but a deeper historical study would be necessary to capture sufficiently these factors. In particular, writings, which debate not only strategic issues but also ethical ones, from legal publications such as *The Journal of Xian Politics Institute* are exceptionally insightful. This segment of the literature provides an invaluable glimpse into the internal philosophical debates among Chinese academics and influential decision makers. It is research into this layer of the Chinese cyber community that is most needed, especially as the United States seeks new ways of understanding Chinese decision makers and steering them toward peaceful and mutually beneficial resolutions in the early stages of conflict.

For the moment, the United States maintains a healthy advantage in the crucial and increasingly pivotal domain of cyberspace. Continued prioritization of cyber research and development funding, a sustained effort on safeguarding sensitive cyber technologies, and a fresh grasp of Chinese views on cyberspace are critical to maintaining this advantage in an uncertain future.

1. 王孔祥 [Wang Kong Xiang], 计算机网络攻击的法律规制 ["Legal Regulation of Cyber Attacks"], 西安政治学院学报 [*Journal of Xian Politics Institute*], vol. 26, no. 3, (2013): 104–10.
2. Reuven Cohen, "The White House and Pentagon Deem Cyber-Attacks 'An Act of War,'" *Forbes.com*, 5 June 2012, www.forbes.com/sites/reuvencohen/2012/06/05/the-white-house-and-pentagon-deem-cyber-attacks-an-act-of-war.
3.胡晓峰 [Hu Xiao Feng], 许相莉 [Xu Xiang Li], and 杨镜宇 [Yang Jing Yu], 基于体系视角的赛博空间作战效能评估 ["Cyberspace Operational Effectiveness Evaluation Based on System of Systems View"], 军事运筹与系统工程 [*Military Operations Research and Systems Engineering*], vol. 27, no. 1, (March 2013), 5–9.
4. 刘金星 [Liu Jin Xing], 陈哨东 [Chen Shao Dong], and 王芳 [Wang Fang], 赛博空间的战术机动 ["The Tactical Maneuver in Cyberspace"], 电光与控制 [*Electronics Optics & Control*], vol. 21, no. 9, (September 2014), 1–6.
5. 王孔祥 [Wang Kong Xiang], 计算机网络攻击的法律规制 [Legal Regulation of Cyber Attacks]," 104–10.
6. Ibid.
7. 杨晋 [Yang Jin], 斯诺登的"多棱镜 ["Snowden's Prism"], 国际政治 [International Politics], vol. 9, (2013), 13–15.
8. 徐龙第 [Xu Long Di], 美国"先发制人"网络打击政策:背景、条件与挑战 ["U.S. 'Pre-emptive' Cyber Strike Policy: Background, Conditions, and Challenges"], 国际政治 [International Politics], vol. 9 (2013), 51–54.
9. U.S. Department of Defense, *Annual Report to Congress on Military Strength and Developments Involving the People's Republic of China*, Washington, DC: U.S. Department of Defense, 2013.
10. 郑志龙 [Zheng Zhi Long] and 余丽 [Yu Li], 互联网在国际政治中的"非中性作用 ["Non-Neutral Effects of the Internet in International Politics"], 国际政治 [International Politics], vol. 3, (2013), 36–43.
11. Ibid.
12. Ibid.

**Mr. Knight is a Naval Sea Systems Command computer scientist currently detailed to the Science & Technology Office at U.S. Pacific Command. He previously served as a China policy analyst at the U.S.-China Economic and Security Review Commission. He is the author of several articles on Chinese open-source science and technology literature.**