U.S.-China Economic and Security Review Commission
Staff Report

May 6, 2014

China and International Law in Cyberspace

Kimberly Hsu
Policy Analyst, Security and Foreign Affairs

with

Craig Murray
Senior Policy Analyst, Security and Foreign Affairs

The authors thank Gary Brown, James Lewis, and Joe McReynolds for their very helpful review of early drafts. Reviewers may or may not agree with this staff research report, and any errors should be attributed to the authors.

The Chinese government states it intends to work with the "international community to promote the building of a peaceful, secure, open, and cooperative cyberspace." Similarly, U.S. government policy is to "work internationally to promote an open, interoperable, secure, and reliable" cyberspace. [1] While this semantic overlap in officially stated goals suggests strong similarities between China and the United States in their viewpoints on international law and norms in cyberspace, they are more different than similar. China's participation in a 2013 UN report affirming the applicability of international law to cyberspace is a promising development. The same UN group will gather in 2014 to address some of the more challenging and divisive concepts regarding state responsibility and use of force in cyberspace. Any fractures in the debate at this meeting will likely reflect some of the major differences between the United States and China on cyberspace policy. These differences will likely endure as Beijing is presently unwilling to compromise on issues such as Internet sovereignty and information control, which it judges as critical to the maintenance in power of the Chinese Communist Party (CCP) regime.

Central Themes in Chinese Views on Cyberspace

Official Chinese statements, Chinese press, and People's Liberation Army (PLA) strategists and academics emphasize the following themes regarding cyberspace:

China expresses concern about a "digital divide" between developed countries and developing countries, placing itself in the latter category.[2] Beijing has long viewed the United States as using its position as a leader in global information technology and Internet governance to establish international norms for cyberspace favorable to the United States.

- In 2012, then PLA Deputy Chief of General Staff General Ma Xiaotian conveyed these sentiments in an influential party newspaper: "A small number of countries rely on their obvious superiority in information networking technology to control and manage global information network development, and they are trying to hold the authority to set network rules. The networks of developing countries are under their control. . . ."[3]

- Having voiced concern about U.S. stewardship of the Internet Corporation for Assigned Names and Numbers (ICANN) since its inception in the late 1990s, China appears to view the U.S. Department of Commerce's recent announcement of its intention to transition key ICANN functions to the "global multistakeholder community" as a positive development. The quasi-authoritative *People's Daily* editorial voice Zhong Sheng considered the move a "positive signal for global Internet governance," but regarded U.S. intentions warily in a separate editorial: "People generally think that whether ICANN can be smoothly transitioned is primarily a function of the extent to which the United States can restrain its impulse to force its methods of governance on the world." [4]

China publicly portrays its cyber-related military capabilities as a defensive response to what it views as "hegemonic" efforts by the United States to militarize cyberspace with offensive capabilities. In their writings, PLA academics consider a multidimensional information warfare environment more complex than a binary offense-defense scenario in cyberspace. However, China publicly portrays U.S. cyber policies as indicative of offensive U.S. intentions in cyberspace requiring China's defensive response. [5,*]

[*] Michael Swaine challenges this point of view in a recent essay: "As any military analyst can attest, it is extremely difficult to distinguish between offensive and defensive systems; in most cases, 'offensive' capabilities are developed as an effective and necessary means of defense and deterrence. To imply that no government (and China in particular) would have done this, absent U.S. efforts, is highly problematic. . . .For Chinese leaders and elites to claim that China possesses no offensive cyber capabilities and has never engaged in cyber actions against foreign

For example, Chinese press and state-affiliated academics portrayed the U.S. government's "International Strategy for Cyberspace," particularly the declaration that "the United States will respond to hostile acts in cyberspace as we would to any threat to our country," as an unwarranted militarization of cyberspace.[6]

- Both the 2010 and 2012 editions of China's biannual Defense White Paper refer to the development of advanced military technologies by "major powers" to maintain an advantage in cyberspace.[7] Chinese military press – particularly quasi-authoritative and non-authoritative military commentators – tend to be more explicit about naming the United States among these "major powers," according to Michael Swaine, a China security scholar at the Carnegie Endowment for International Peace. One opinion piece published in the PLA's leading newspaper, for example, states "the United States is officially attempting to monopolize the status . . . of cyberspace and single-handedly write the rules of the game for cyber warfare to occupy the high ground in future cyber wars."[8]

- Chinese commentators tend to attribute a cyber deterrence strategy to the United States even though the United States has not publicly espoused such a concept in official policy documents.[9] In 2013, Zhong Sheng wrote: "The United States has vigorously pushed the building of its cyber warfare capability, expanded its cyber military alliance, advocated cyber deterrence, and attempted to spur the international community into drawing up rules for cyber warfare, in order to put a cloak of legality on its 'preemptive strike' strategy in cyber warfare."[10, †]

China supports the extension of state sovereignty and non-interference to cyberspace. China prefers sovereign states be the principal governing entity in cyberspace, just as in the physical world.[11] Beijing generally emphasizes two corollaries of this principle.

- First, states should be able to assert sovereignty in cyberspace over both their own and foreign citizens and organizations within their borders. On this aspect, China diverges from the United States, which is highly protective of individual freedom of speech and other individual liberties, and views state efforts to control online content as "inappropriate."[12]

- Second, states should not interfere with the sovereignty of other states in cyberspace. States should refrain from "using their resources, critical infrastructures, core technologies and other advantages to undermine the right of other countries" to exert sovereignty within their own borders.[13]

China's Approach to Cyberspace in International Bodies

These themes suggest China likely will reject any measures it judges would constrain its ability to reform what is currently a U.S.-dominated Internet infrastructure.[14] China also probably will seek to promote its interest in "democratizing" Internet governance under the auspices of the United Nations. As stated in Beijing's 2010 white paper, "The Internet in China": "China supports the establishment of an authoritative and just international Internet administration organization under the UN system through democratic procedures on a worldwide scale."[15]

---

states lacks credibility." Michael Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, no. 42 (Fall 2013): p. 14-15.

† Several days prior to this editorial, a Chinese foreign ministry spokesperson used nearly the same language in a press conference. The spokesperson did not make reference to the United States but instead referred to "some countries [treating] the Internet as a battlefield." Ministry of Foreign Affairs (PRC), Transcript of regular news conference, February 25, 2013. Open Source Center transcription. ID: CPP20130225364001.

- China's most significant multilateral effort to introduce cyberspace norms is the International Code of Conduct for Information Security, circulated to the UN General Assembly in 2011. China, Russia, Tajikistan, Uzbekistan, Kazakhstan, and Kyrgyzstan co-sponsored the code, which the United States, the European Union, and other Western nations have been reluctant to accept due to their differing priorities in cyberspace.[16] While the Code of Conduct remains part of China's official position on international cyber security, its failure to gain widespread acceptance suggests it is no longer viable as a negotiating instrument. The document incorporates 11 principles echoing central themes in China's cyber policy priorities, including "respect for the sovereignty, territorial integrity, and political independence of all States," "respect [for] rights and freedom in information space . . . on the premise of complying with relevant national laws and regulations," and the "[promotion of] the important role of the United Nations in formulating international norms . . . in the field of information security."[17]

- At the December 2012 World Conference on International Telecommunications (WCIT-12), held under the auspices of the UN International Telecommunications Union, China's position was generally aligned with those countries advocating a state-based model for Internet governance, as opposed to those mostly Western countries favoring bottom-up Internet oversight incorporating nongovernment stakeholders. Largely due to this divide, the conference was unable to come to a consensus on revisions to a 1988 global telecommunications treaty.[18] To some Chinese commentators, the inability of the WCIT-12 to come to an agreement demonstrates the limited sustainability of a Western-dominated Internet agenda.[19]

- China's refusal to accede to the Budapest Convention on Cyber Crime also reflects its developing state-centric approach to international agreements on cyberspace. The Convention is a multilateral agreement that serves as a framework for international cooperation on cyber crime and a guide for the development of national cyber crime legislation. The United States ratified the Convention in 2006 and continues to express strong support for its principles.[20] In Track II discussions in 2012 between the U.S. think tank Center for Strategic and International Studies (CSIS) and the Chinese state-affiliated think tank China Institutes of Contemporary International Relations (CICIR), CICIR opined a UN treaty would better address the needs of developing countries in fighting cyber crime than does the Council of Europe-developed Convention. CICIR was also concerned that Convention provisions on transnational evidence collection for prosecutions of cyber crimes could violate state sovereignty.[21]

Applicability of International Law to Cyberspace

Despite major differences on cyberspace policy between the United States and China, a recent development at the United Nations illustrates basic areas of agreement. China is one of 15 countries, including the United States, comprising the UN Group of Government Experts (GGE), a group of national experts from UN member states selected by the Secretary General to review "the existing and potential threats from the cyber-sphere and possible cooperative measures to address them."[22] In June 2013, the GGE achieved consensus on a report on "Developments in the Fields of Information and Telecommunications in the context of International Security," affirming the application of international law to cyberspace. The report's "Recommendations on norms, rules and principles of responsible behavior of States" suggest China agrees in principle not only to the general application of international law to cyberspace, but also the application of specific aspects of international law, including the law of state responsibility, concepts in the UN Convention relating to the use of military force, and the law of armed conflict.

Law of State Responsibility. The GGE report condemns the use of non-state proxies for the "unlawful use of ICT [information and communication technologies]," stating, "States must meet their international obligations regarding internationally wrongful acts attributable to them."[23] The report echoes language in the UN's "Draft Articles on the Responsibility of States for Internationally Wrongful Acts," which is regarded as an authoritative understanding of the international law of state responsibility.[24]

- Compelling evidences indicates the Chinese government, the PLA, and Chinese state-owned enterprises utilize cyber techniques to conduct espionage.[25] China's committed, long-term investment in developing a professional corps of cyber operators and engineers suggests China's tacit agreement to the law of state responsibility may not lead to a reduction in the scope and scale of cyber espionage by these non-state proxies acting on behalf of the Chinese government.

- James Lewis, senior fellow and director of the Strategic Technologies Program at CSIS, was cautiously optimistic about the influence of the GGE on China's cyber behavior in 2013 testimony to the House Foreign Affairs Committee: "a Chinese official said in reference to the GGE that 'China's position was evolving in the light of international experience.' . . . As this effort progresses and there is international consensus on responsible behavior in cyberspace, China's cyber espionage will be difficult to sustain."[26]

UN Charter and Law Relating to Use of Military Force. By stating in clear terms the applicability of the UN Charter to cyberspace, the GGE report represents progress toward international understanding on the use of force in the cyber domain. The UN Charter prohibits "the threat or use of force against the territorial integrity or political independence of any state," as well as the use of force unless in "individual or collective self-defense if an armed attack occurs."[27] As reflected in the GGE report, there is an implicit, general consensus on the definitions of key terms such as "use of force" and "armed attack" in cyberspace, but states are hesitant to formalize these understandings because they fear inadvertently conceding an advantage to potential adversaries. As a result, in practice, rules intended to constrain behavior among states in cyberspace will remain unclear.[28]

- Doctrinal writings on the PLA's legal warfare concept indicate China would seek to publicly justify a use of military force by invoking domestic and international law.[29] Beijing supports the general prohibition against the use of force and the peaceful settlement of international disputes under the UN Charter, but appears to advocate for the flexibility of each sovereign state to determine "a way of the rule of law suitable for its own national conditions."[30]

- For the United States and China, which by their own accounts experience a high volume of malicious cyber activities directed against them, achieving consensus on the acceptable use of force in cyberspace could clarify appropriate responses to cyber activities that fall below the threshold of what could be considered a "use of force" or "armed attack." When the GGE meets in July 2014 to consider this threshold among other topics,[31] any consensus reached on this matter would strengthen stability in the cyber domain between the United States and China.

Law of Armed Conflict. China's participation in the GGE 2013 report could indicate a turn toward acceptance of the applicability of law of armed conflict (LOAC)[§] norms in cyberspace.[32] The PLA recognizes an information warfare domain and trains its soldiers to apply LOAC on the physical battlefield. However, the specific applicability of LOAC to cyberspace remains under debate in

[§] The law of armed conflict, also known as international humanitarian law, includes principles such as distinction between military and civilian targets, proportionality, military necessity, and limitation during warfare. International Committee of the Red Cross, "The Law of Armed Conflict: Basic Knowledge," June 2002, pp. 12-14. *http://www.icrc.org/eng/assets/files/other/law1_final.pdf.*

policymaking circles in China and in other countries.[33] In contrast, the United States position is that existing international norms and treaties governing LOAC "should regulate the use of cyber tools in hostilities, just as it does other tools."[34]

- China supports the protection of civilians and the limitation of suffering during war – a key basis for LOAC – but appears to prefer the development of a separate cyber-specific regime to limit suffering and protect civilians during hostilities. CICIR's proposal for sanctuaries to shelter civilian targets and a prohibition of cyber attacks against purely civilian targets – offered at the 2012 CSIS-CICIR Track II dialogue – are illustrative of such an approach.[35]

- The 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare* represents the perspectives of an international panel of legal and technical experts on widely-held international norms relevant to cyber warfare. A quasi-authoritative opinion piece published in Chinese press expressed suspicion about its contents, stating "its viewpoint is precisely the same as the U.S. State Department view, and obviously wants to put a cloak of legality on U.S. cyber warfare."[36]

Beijing is unlikely to depart from its strongly-held position regarding the centrality of state sovereignty in cyberspace, particularly as most nations generally accept this concept. The 2013 GGE report incorporated language reflecting this position: "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory." Furthermore, coming to a consensus as part of the 2013 GGE has not precluded Beijing from continuing to socialize its proposed Code of Conduct as its vision for cyberspace.[37]

Domestic Cyber Policy in China and Implications for Development of International Norms

China has until recently developed and executed cyber policies without a coordinated approach to cyberspace. Since the early 2010s, however, China has begun to increase interagency coordination on cyber policy. This may be a response to the increasing number and sophistication of Internet users in China, the perceived role of the Internet in fueling social and political movements in China and in the "color revolutions" of the late 2000s, and the growing need to align foreign and domestic policy priorities in cyberspace.

In late February 2014, China announced a new Central Internet Security and Informatization Leading Group. President Xi Jinping chairs the leading group, reflecting the importance Beijing ascribes to the issue. Leading groups are deliberative committees at the top levels of the CCP that influence policy through their coordinating function and recommendations to the Politburo Standing Committee, the top-level decision-making body in China. The new cyber leading group is tasked with drafting a national cybersecurity strategy and the coordination of cybersecurity across multiple government entities, including the Ministry of Public Security, State Encryption Bureau, Ministry of State Security, Ministry of Industry and Information Technology, and the PLA.[38] The establishment of this body indicates China likely is developing a national-level cyber policy, and by extension an authoritative viewpoint on the applicability of legal principles to cyberspace.

As China and other countries have not yet crystallized their positions on various aspects of international law in cyberspace, the 2014 GGE meeting is an opportunity for the United States to continue to socialize cyberspace norms internationally. According to Christopher Painter, Coordinator for Cyber Issues at the U.S. Department of State, the upcoming meeting will "look more closely at how international law applies to state-on-state conduct in cyberspace." In addition, the GGE will discuss "additional norms of responsible state behavior, grounded in existing international law, that apply to the spectrum of cyber activity that falls below the use-of-force threshold."[39] In the intervening year since the last meeting,

revelations about the United States' cyber espionage activities, particularly those against China, have further fraught the cyberspace policy discussion between the United States and China with tension.[40] The United States distinguishes between China's "cyber-enabled economic espionage" against U.S. companies and government-to-government espionage for state purposes, whereas China does not recognize this distinction.[41] Having laid significant groundwork in 2013, the GGE now faces the challenge of consensus on the more divisive and difficult policy issues in cyberspace.

[1] Ministry of Foreign Affairs (PRC). Transcript of regular news conference, March 31, 2014. OSC ID: CHR2013033141468008.; Shen Jian, "An International Code of Conduct for Information Security – China's perspective on building a peaceful, secure, open, and cooperative cyberspace," (Geneva, February 10, 2014), p. 3. *http://www.unidir.ch/files/conferences/pdfs/a-cyber-code-of-conduct-the-best-vehicle-for-progress-en-1-963.pdf*; Government of the United States, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. (Washington, DC: May 2011), p. 8; Christopher Painter, "Remarks at Georgetown University Institute for Law Science and Global Security's 2014 International Engagement on Cyber Conference," (Washington, DC, March 4, 2014). *http://www.state.gov/s/cyberissues/releasesandremarks/223075.htm*.

[2] Joe Mc Reynolds, "Chinese Thinking of Deterrence and Compellence in the Network Domain," forthcoming; Lu Wei, "Liberty and Order in Cyberspace," (Keynote speech at the Fifth China-UK Internet Roundtable, September 9, 2013), *http://news.xinhuanet.com/english/china/2013-09/09/c_132705681.htm*.

[3] Ma Xiaotian, "Pay Attention to Cyberspace Security, Construct a Harmonious Online World," *Study Times*, August 20, 2012. OSC ID: CPP20120820786001.

[4] Milton L. Mueller, "China and Global Internet Governance: A Tiger by the Tail," in Ronald Deibert, et al, eds. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. (Cambridge, MA: MIT Press, 2011), p. 182-185; U.S. National Telecommunications and Information Administration, "NTIA Announces Intent to Transition Key Internet Domain Name Functions," March 14, 2014. *http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions*; Zhong Sheng, "Norms and Standards Are Key in Internet Governance," *People's Daily*, April 28, 2014. OSC ID: CHN2014042808720692; Zhong Sheng, "Internet Administration Should Be Done In Line With Trends," *People's Daily*, March 31, 2014. OSC ID: CHR2014033128503554.

[5] Michael Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, no. 42 (Fall 2013), p. 6-9. He Weibao, "Comprehensive Report on Symposium on 'Cyber Security Issue in Sino-US Relations,'" *Meiguo Yanjiu* (American Studies) (Beijing), September 5, 2013. OSC ID: CHL2014011468577056.; Joe McReynolds, "Chinese Thinking on Deterrence and Compellence in the Network Domain," forthcoming.

[6] Li Zhang, "A Chinese perspective on cyber war," *International Review of the Red Cross* 94:886 (Summer 2012): 801-802; Lu Desheng, "US Military Look for New Excuse to use Force Abroad – Pentagon to Announce First Cyber Strategy," *PLA Daily*, June 8, 2011. OSC ID: CPP20110608787015; Zhou Biao, "International Law Dilemma of U.S. Military's New Cyberspace Strategy, 'Sovereign Boundary' Hard To Be Defined for Cyber Attacks," June 6, 2011. OSC ID: CPP20110612163006.

[7] Information Office of the State Council (PRC), *The Diversified Employment of China's Armed Forces* (Beijing, China: April 16, 2013); Information Office of the State Council (PRC), *China's National Defense in 2010* (Beijing, China: March 31, 2011).

[8] Lu Desheng, "US Military Look for New Excuse to use Force Abroad – Pentagon to Announce First Cyber Strategy," *PLA Daily*, June 8, 2011. OSC ID: CPP20110608787015; Michael Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, no. 42 (Fall 2013), p. 7-8. *http://carnegieendowment.org/files/CLM42MS_092013Carnegie.pdf*.

[9] Yu Xiaoqiu, "Cyber Deterrence is a Dangerous Game," *Renmin Ribao* (People's Daily) (Beijing), July 25, 2011. OSC ID: CPP20110725787008; Luo Chaowen, "US 'Strategy for Operating in Cyberspace' Can Hardly Cover Its Offensive Character," July 16, 2011. OSC ID: CPP20110718716001; Tang Lan and Zhang Xin, "Can Cyber Deterrence Work?" in East West Institute, *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway*. (New York: April 2010), p. 1.

[10] Zhong Sheng,"Do Not Treat Cyberspace as a War Theater; Avoid Harming Others and Damaging Oneself," *Renmin Ribao* (People's Daily) (Beijing), February 27, 2013. OSC ID: CPP20130227702002.

[11] Delegation to UN General Assembly (PRC). "Statement by the Chinese Delegation on Information and Cyber Security at the Thematic Debate at the First Committee of the 68th Session UNGA" (New York, October 2013). *http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_30-Oct_ODMIS_China.pdf*; Lu Wei, "Liberty and Order in Cyberspace," (Keynote speech at the Fifth China-UK Internet Roundtable, September 9, 2013), *http://news.xinhuanet.com/english/china/2013-09/09/c_132705681.htm*; Wang Zhonglun, "Online Sovereignty Is of Prime Importance," *Guangming Daily* (Beijing), April 28, 2012. OSC ID: CPP20120430787010; Milton L. Mueller, "China and Global Internet Governance: A Tiger by the Tail," in Ronald Deibert, et al, eds. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. (Cambridge, MA: MIT Press, 2011), p. 178-182; Tobias Feakin, "ARF, and how to change the tune of the cyber debate," *The Strategist: The Australian*

Strategic Policy Institute Blog. October 14, 2013. *http://www.aspistrategist.org.au/arf-and-how-to-change-the-tune-of-the-cyber-debate/*.

[12] Christopher Painter, "Remarks at Georgetown University Institute for Law Science and Global Security's 2014 International Engagement on Cyber Conference," (Washington, DC, March 4, 2014). *http://www.state.gov/s/cyberissues/releasesandremarks/223075.htm*.

[13] Shen Jian, "An International Code of Conduct for Information Security – China's perspective on building a peaceful, secure, open, and cooperative cyberspace," (UN Institute for Disarmament Research Cyber Stability Seminar 2014: Preventing Cyber Conflict, Geneva, February 10, 2014), p. 3. *http://www.unidir.ch/files/conferences/pdfs/a-cyber-code-of-conduct-the-best-vehicle-for-progress-en-1-963.pdf*.

[14] Joe McReynolds, "Chinese Thinking on Deterrence and Compellence in the Network Domain," forthcoming; Leshuo Dong, "From 'Chinanet' to 'Internet Sovereignty': Historical Development of China's Internet Policy," *Center for Global Communication Studies Media Wire*, March 10, 2014. *http://cgcsblog.asc.upenn.edu/2014/03/10/from-chinanet-to-internet-sovereignty-historical-development-of-chinas-internet-policy/*

[15] Delegation to UN General Assembly (PRC). "Statement by the Chinese Delegation on Information and Cyber Security at the Thematic Debate at the First Committee of the 68th Session UNGA" (New York, October 2013). *http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_30-Oct_ODMIS_China.pdf*; State Council Information Office (PRC), "Active International Exchanges and Cooperation," *The Internet In China* (Beijing, China: June 8, 2010).

[16] Tobias Feakin, "ARF, and how to change the tune of the cyber debate," *The Strategist: The Australian Strategic Policy Institute Blog*. October 14, 2013. *http://www.aspistrategist.org.au/arf-and-how-to-change-the-tune-of-the-cyber-debate/*.

[17] Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, *https://disarmament-library.un.org/UNODA/Library.nsf/f446fe4c20839e50852578790055e729/329f71777f4b4e4e85257a7f005db45a?OpenDocument*.

[18] Eric Pfanner, "U.S. Rejects Telecommunications Treaty," *New York Times*, December 13, 2012. *http://www.nytimes.com/2012/12/14/technology/14iht-treaty14.html?pagewanted=1&_r=2*; Larry Downes, "Requiem for Failed UN Telecom Treaty: No One Mourns the WCIT," *Forbes*, December 17, 2012. *http://www.forbes.com/sites/larrydownes/2012/12/17/no-one-mourns-the-wcit/*.

[19] He Weibao, "Comprehensive Report on Symposium on 'Cyber Security Issue in Sino-US Relations,'" *Meiguo Yanjiu* (American Studies) (Beijing), September 5, 2013. OSC ID: CHL2014011468577056.

[20] Christopher Painter, "As Prepared Remarks," (Georgetown University Institute for Law, Science and Global Security's 2014 International Engagement on Cyber Conference, March 4, 2014). *http://www.state.gov/s/cyberissues/releasesandremarks/223075.htm*; Council of Europe, Convention on Cybercrime Status as of April 15, 2014. *http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG*.

[21] China Institute of Contemporary International Relations and Center for Strategic International Studies, *Joint Statement* (Track 2 Sino-U.S. Cybersecurity Dialogue: June 2012). *http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf*.

[22] UN Office for Disarmament, "Development in the Field of Information and Telecommunications in the Context of International Security," *http://www.un.org/disarmament/topics/informationsecurity/*.

[23]UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Paragraph 23, *Developments in the Field of Information and Telecommunications in the Context of International Security* (June 7, 2013). *http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98*.

[24] UN International Law Commission, "Chapter 1: General Principles," *Draft Articles on the Responsibility of States for Internationally Wrongful Acts* (2001). *http://legal.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf*; U.S.-China Economic and Security Review Commission, *Annual Report to Congress* (Washington, DC: November 2013), p. 249.

[25] Mandiant, *APT 1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: February 2013). *http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf*; Adam Segal, "The Rise of Asia's Cyber Militas," *Atlantic*, February 23, 2012. *http://www.theatlantic.com/international/archive/2012/02/the-rise-of-asias-cyber-militias/253487/* .

[26] U.S. House Foreign Affairs Committee, Subcommittee on Oversight and Investigations, *Hearing on Asia: The Cyber Security Battleground*, testimony of James Lewis. July 23, 2013; U.S. House Energy and Commerce

Committee, *Hearing on Cyber Espionage and the Theft of U.S. Intellectual Property and Technology*, testimony of James Lewis. July 9, 2013.
[27] Article 2(4), Chapter I: Purposes and Principles, Charter of the United Nations. Article 51, Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Charter of the United Nations.
[28] Catherine Lotrionte, "A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence," *Georgetown Journal of International Affairs*, 2013, p. 83.
[29] *Science of Military Strategy*, cited in Larry Wortzel, *The Chinese People's Liberation Army and Information Warfare* (Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2014), p. 37-38.
[30] Xinhua, "No Model Rule of Law For All Countries: Chinese Envoy," February 20, 2014. OSC ID: CHR2014022015460016; Xinhua, "Settlement of Int'l Disputes Should Abide by Principle of Sovereign Equality," October 10, 2013. OSC ID: CHR2013101086154911.
[31] Christopher Painter, "As Prepared Remarks," (Georgetown University Institute for Law, Science and Global Security's 2014 International Engagement on Cyber Conference, March 4, 2014). *http://www.state.gov/s/cyberissues/releasesandremarks/223075.htm*
[32] Information Office of the State Council (PRC), *The Diversified Employment of China's Armed Forces* (Beijing, China: April 16, 2013); Information Office of the State Council (PRC), *China's National Defense in 2010* (Beijing, China: March 31, 2011).
[33] International Committee of the Red Cross, "China's military: marching in step with the law of armed conflict," October 31, 2003. *http://www.icrc.org/eng/resources/documents/misc/5suefq.htm*; Tian Yiwei and Gao Jiquan, "International Symposium of 'International Society for Military Law and Law of War' Held," *PLA Daily*, November 11, 2011. OSC ID: CPP20111114702006; Guo Jingshan and Wang Yafu, "PLA Academy Attends 10th International Competition on LAC for Military Academies," *PLA Daily*, May 25, 2011. OSC ID: CPP20110526708005; Adam Segal, "China, International Law, and Cyberspace," *Asia Unbound*, October 2, 2012. *http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace/*; He Weibao, "Comprehensive Report on Symposium on 'Cyber Security Issue in Sino-US Relations,'" *Meiguo Yanjiu* (American Studies) (Beijing), September 5, 2013. OSC ID: CHL2014011468577056; Sydney J. Freedberg, "Cyber Command Lawyer Praises Stuxnet, Disses Chinese Cyber Stance," *Breaking Defense*, March 12, 2012. *http://breakingdefense.com/2012/03/cyber-command-lawyer-praises-stuxnet-disses-chinese-cyber-stanc/*; China Institute of Contemporary International Relations and Center for Strategic International Studies, *Joint Statement* (Track 2 Sino-U.S. Cybersecurity Dialogue: June 2012). *http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf*.
[34] Harold Hongju Koh, "International Law in Cyberspace," (Fort Meade, MD: September 18, 2012).
[35] China Institute of Contemporary International Relations and Center for Strategic International Studies, *Joint Statement* (Track 2 Sino-U.S. Cybersecurity Dialogue: June 2012). *http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf*; Li Zhang, "A Chinese perspective on cyber war," *International Review of the Red Cross* 94:886 (Summer 2012): 804.
[36] Zhong Sheng, "Blackening China Can Hardly Conceal the Evil Behavior of the 'Hackers' Empire," *Renmin Ribao* (People's Daily) (Beijing), May 8, 2013. OSC ID: CPP20130508787003.
[37] Shen Jian, "An International Code of Conduct for Information Security: China's perspective on building a peaceful, secure, open, and cooperative cyberspace." (Cyber Stability Seminar 2014: Preventing Cyber Conflict, Geneva, February 10, 2014). *http://www.unidir.ch/files/conferences/pdfs/a-cyber-code-of-conduct-the-best-vehicle-for-progress-en-1-963.pdf* .
[38] William Wan, "Chinese president Xi Jinping takes charge of new cybersecurity group," *Washington Post*, February 27, 2014. *http://www.washingtonpost.com/world/chinese-president-takes-charge-of-new-cyber-effort/2014/02/27/a4bffaac-9fc9-11e3-b8d8-94577ff66b28_story.html*; Adam Segal, "China's New Small Leading Group on Cybersecurity and Internet Management," *Forbes*, February 27, 2014. *http://www.forbes.com/sites/adamsegal/2014/02/27/chinas-new-small-leading-group-on-cybersecurity-and-internet-management/*; Shannon Tiezzi, "Xi Jinping Leads China's New Internet Security Group," *Diplomat*, February 28, 2014. *http://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/*.
[39] Christopher Painter, "As Prepared Remarks," (Georgetown University Institute for Law, Science and Global Security's 2014 International Engagement on Cyber Conference, March 4, 2014). *http://www.state.gov/s/cyberissues/releasesandremarks/223075.htm*
[40] Spiegel Online International, "Targeting Huawei: NSA Spied on Chinese Government and Networking Firm," March 22, 2014. *http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html*.

[41] U.S.-China Economic and Security Review Commission, *Annual Report to Congress 2013* (Washington, DC: November 2013), p. 250. *http://origin.www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%3B%20Section%202%20China%27s%20Cyber%20Activities.pdf*.