Chinese Views on Cybersecurity in Foreign Relations

Michael D. Swaine*

In recent months, the issue of cybersecurity has become a major source of both tension and potential cooperation for the U.S.-China relationship. However, little progress has occurred in reducing suspicion, and both countries are presumably strengthening their capacity to engage in both defensive and offensive cyber actions against each other. The apparent unanimity of support within China for the official position suggests it is unlikely that internal debates exist over this issue that could possibly provide an opening for a change in the Chinese position. In at least the near to medium term, obstacles remain on developing a common international approach to cybersecurity, and Beijing will likely continue to develop and utilize cybercapabilities against other states, for both national security and economic purposes.

During the past few years, cybersecurity has become a major concern among many countries, as a result of the continued rapid expansion and deepening technological sophistication of the Internet, alongside the growing reliance of governments and societies on cyberbased systems for everything from communications and information storage to military operations and commercial activities.[i]

In recent months, this issue has become a major source of both tension and potential cooperation for the U.S.-China relationship in particular. Stemming from a Western (and especially U.S.) assessment that a growing number of destructive cyberattacks on commercial enterprises and government institutions originate not only from Chinese individuals, but also most likely from Chinese government (and especially military) sources, Washington has greatly intensified its expression of concern to Beijing.[ii]

Beijing has repeatedly denied carrying out cyberattacks against any other country, while calling for both bilateral and multilateral cooperation, free from accusations, to formulate agreed-upon norms for the operation of the global Internet as well as place its oversight in the hands of a broadly representative international structure. The United States has resisted the latter proposal.

These developments have elevated the issue of cybersecurity to a top priority within the overall bilateral relationship. In response to the importance and urgency of the issue, Washington and Beijing recently agreed to form a Cyber Working Group (CWG) as part of the bilateral Strategic and Economic Dialogue (S&ED),[iii] with the first Bilateral Cybersecurity Working Group Dialogue held in Washington D.C. on 8 July.[iv]

---

* I am greatly indebted to Audrye Wong for her invaluable assistance in the preparation of this article.

Thus far, however, little progress has occurred in reducing suspicion and developing cooperation in this area. To the contrary, the United States and presumably China are strengthening their capacity to engage in both defensive and offensive cyber actions against each other, presenting the prospect of a cyber arms race while potentially intensifying the already high level of distrust between the two countries.[v]

To understand the challenges and opportunities presented to the Sino-U.S. relationship by the cybersecurity issue, it is important to examine in some detail the views, beliefs, and apparent assumptions of Chinese observers toward the subject. This article addresses Chinese thinking on four basic aspects of the issue:

The Definition of Cybersecurity and the Challenge It Presents

The Cybersecurity Threat Posed by the United States and Other Countries

The Origins and Motives Behind Foreign Cybersecurity Threats

Chinese Preferences for Mitigating Cybersecurity Threats

As they have in several previous editions of *CLM*, our examination of Chinese views on these topics will distinguish between three basic types of Chinese sources: authoritative; quasi-authoritative; and non-authoritative.[vi]

For each area, particular attention is given to: a) the authoritative PRC government viewpoint (if publicly available); b) views toward the United States in particular; and c) any variations that might exist among Chinese commentators, in both substance and tone. The article addresses several specific questions: to what extent and in what manner do Chinese definitions of cybersecurity and Chinese views on the cybersecurity threat differ from those of the United States and other countries? How do Chinese sources respond to U.S. and Western accusations against China? In all these areas, can one discern any significant differences: among authoritative Chinese sources, between military and civilian sources (of all types), and among authoritative, quasi-authoritative, and non-authoritative sources in general?

The article concludes with a summary and some implications for the future.

The Chinese Definition of Cybersecurity and the Challenge It Presents

Authoritative Chinese sources do not provide a detailed definition of cybersecurity and the challenge it poses. PRC government statements largely refer in general terms to the growth of the Internet, the increasing dependence of many nations on cyberbased activities, the potential dangers posed by cyberbased attacks or incursions, and the need for governments to provide more supervision over the Internet.[vii]

Nonetheless, such general statements, combined with the more detailed discussion of such issues appearing in non-authoritative sources, suggest that most Chinese conceive of cybersecurity in a similar manner to observers in other countries. That is, it involves the protection of the Internet against harmful activities directed against or having the effect of undermining national security or commercial, social, and individual interests. Such interests include the capacity of the state to defend itself and society, the ability to compete fairly and productively in the national and global economic order, the preservation of social norms, and the privacy and security of the individual citizen.

Most Chinese have the same concerns as much of the rest of the world about harmful cyberactivities, including: efforts to crash, slow, or paralyze vital cyberbased infrastructure; the promulgation of information or images harmful to the polity, society, or the economy (such as pornography, false or misleading commercial information, and the advocacy of violent political revolution); espionage; the theft of proprietary commercial data or information; and specific actions designed to weaken the capacity of the state to defend itself through military and other means.[viii] Thus, both authoritative and other Chinese observers believe that "cyber security is an international . . . issue and hacker attack is a common challenge facing the whole world."[ix]

The Chinese also seem to agree with observers in other countries that cybersecurity is a particularly challenging issue because of the technical characteristics of the Internet and the growing presence of cybercrimes and other forms of dangerous behavior. As Zhong Sheng states: "[the Internet is] transnational and anonymous; it involves multiple fields and multiple agencies; there is a coexistence of hardware and software; there is an overlap of the virtual world and reality."[x]

Both Ministry of Foreign Affairs and Ministry of Defense officials repeatedly state that "China is a major victim of hacker attacks."[xi] Various Chinese sources provide data on the scope of the cyber problem confronting China, but the Chinese military in particular has cited statistics on the number of cyberattacks on its systems, in large part to rebut foreign (and especially U.S.) accusations that the PLA is conducting huge numbers of attacks on others (see below).[xii]

In response to such threats, and the overall security challenge presented by cyberactivities, authoritative Chinese sources repeatedly declare:

> The Chinese Government always opposes and strictly prohibits any illegal criminal activity by hackers. The Chinese law stipulates unequivocally that those who commit cyber crimes should undertake criminal liability in accordance with the Criminal Law of the People's Republic of China.[xiii]

Beyond such general concerns, the PRC regime, and many interested Chinese observers, place a particularly strong emphasis on the challenges posed by cyberactivities that threaten existing domestic social and political norms or values (such as the dissemination of false rumors) as well as the sovereignty of the nation-state. In particular, many non-authoritative sources, both civilian and especially military, introduce the concept of

sovereign, "virtual territory" on the Internet (termed "cyber sovereignty" by some Chinese sources),[xiv] and advocate the need for a government to identify the boundaries of such territory and protect it against cyberbased threats.[xv]

To support their contention that the Internet poses a major threat to the sovereign authority of nation-states, non-authoritative Chinese sources frequently cite the disruptive impact on Middle Eastern governments of social networking websites such as Twitter, as well as various blogging websites. The supposedly negative impact of such activities in the aftermath of the Iranian presidential elections is often offered as a specific example.[xvi]

Such a viewpoint leads to a more state-centric orientation toward cybersecurity than is the case in Western democratic nations. As an article in *People's Daily* states: "It is a crucial test for countries around the world to bring the use of internet into line with state administration, timely and effectively collect and analyze online diplomatic data as well as make diplomatic decisions with consideration to cyber opinions."[xvii] Another observer asserts that "[i]t has become a consensus worldwide that government should play the role of the Internet "administrator" and set examples in Internet governance because it possesses the most management resources and management tools."[xviii]

This viewpoint reflects to a great extent the long-standing and strong Chinese concern with social disorder, along with the related need for a strong, supervisory state to uphold societal norms and preserve social harmony.[xix] It also undoubtedly reflects the acute sensitivity of the PRC regime to the potential threats posed by any "unregulated" activity.

Both authoritative and non-authoritative Chinese sources (and military sources in particular) thus identify cyberspace as a non-traditional yet critical national security interest. For example, one Academy of Military Science (AMS) researcher states: "The strategic significance of the Internet lies in the fact that it has become an effective tool that breaks national boundaries, communicates information worldwide, and influences international and domestic affairs."[xx]

While stating opposition to cyberattacks and highlighting the defense of sovereign "virtual territory," many non-authoritative civilian and military Chinese sources acknowledge that China's cyberinfrastructure and internet laws are vulnerable and weak compared to those of other countries, and that it is difficult to identify the boundaries that require protection.[xxi] Moreover, non-authoritative sources repeatedly assert that China is highly vulnerable to cyberattacks because it relies primarily on developed countries—and especially the United States—for core network technologies.[xxii]

In response to largely Western criticisms that a state-centric approach to Internet administration will lead to efforts to curtail freedom of speech and other individual liberties, a non-authoritative Chinese observer argues that:

> The government management of the Internet mainly aims to monitor harmful information, crack down on cyber crimes, maintain order in the

> cyber world as well as fill the network gap, lift information use efficiency and bring more people the convenience of the Internet.[xxiii]

At the same time, the same source, along with many other Chinese sources, authoritative and otherwise, also asserts that "freedom on the internet is . . . subject to laws and morality."[xxiv] Although largely unobjectionable as a general standard for Internet behavior, for many Chinese, and especially for authoritative and quasi-authoritative observers, such a notion involves a more direct, activist, and ideological role for government than most Western observers would countenance. As one observer in the *Liberation Army Daily* (LAD) opined, "raising the ideological and moral standard of the citizens [is] a basic standard for achieving the unification of cyber freedom and cyber self-discipline."[xxv]

For these Chinese observers, the "ideological" dimension of cybersecurity usually refers to the defense and expansion of "socialist ideology and culture." Both civilian and military officials and observers assert that to protect China's sovereignty and the authority of the PRC government, the Internet in China must reflect socialist "cyber culture" and resist "ideological infiltration and political instigation."[xxvi]

Authoritative Chinese sources do not present such a clear and detailed description of the ideological and regime-oriented dimensions of Internet supervision. For example, while declaring that China supports freedom of speech and the free exchange of information on the Internet, former Foreign Minister Yang Jiechi points out that "there are different social systems in the world," and that Beijing needs to "do regulatory work according to law and according to what is in the best interest of China."[xxvii] Although Yang did not give specifics, it is highly likely that such "regulatory work" includes the type of ideological defense and advocacy as presented in the non-authoritative sources above.

Finally, in addressing the general issue of cybersecurity, many quasi- and non-authoritative Chinese sources assert that U.S. dominance and de facto control over Internet technologies and the cyberinfrastructure is unfair, presenting a source of instability and potential danger for the global cybersystem. One non-authoritative Chinese observer asserts that the U.S. "enjoys global monopoly status in research and development in both software and hardware."[xxviii]

As evidence in support of such a viewpoint, many Chinese sources declare that 10 (or according to some Chinese observers, all) of the 13 so-called root servers essential to the function of the Internet are located in the United States.[xxix] One source also claims that "eighty percent of the worldwide Internet data transmission and processing occurs in the United States."[xxx]

A quasi-authoritative source states that "all root servers are under the unified control of ICANN (Internet Corporation for Assigned Names and Numbers), which has the mandate of the U.S. government. It is responsible for the management of Internet root name servers, domain name systems and IP addresses worldwide." According to this source, such supposed U.S. control "implies the right to control other countries' Internet presence and access."[xxxi] Similarly, Hu Yanping, the founder and president of the China Internet

Data Center and past editor of *China Internet Weekly*, asserts that, as a result of U.S. dominance over the Internet, "the Chinese Internet industry is running in the hands of the U.S."[xxxii]

More ominously, according to some non-authoritative sources, such as Major General Wu Jianguo, the United States allegedly uses such technological advantages to "display its fist of hegemony everywhere," depriving others of sharing information on the Internet, creating backdoors in its software to facilitate hacking, and exporting inferior microchips.[xxxiii]

The Cybersecurity Threat to China Posed by the United States and Other Countries

In general, authoritative Chinese sources do not publicly identify the United States government, much less Western governments in general, as the verifiable source of the major types of cybersecurity threats outlined above. While Foreign Ministry officials point out, "as far as we know, cyber attacks against China mainly originate from the U.S."[xxxiv] (as indicated by the apparent location of the attacker's IP address), they also state, "we are keenly aware of the complexity of the Internet environment so we do not come to the conclusion that it is the U.S. institutions or individuals that have carried out the attacks."[xxxv] Authoritative military sources have echoed this view, asserting that, because cyberattacks are "transnational, anonymous, and deceptive," often percolating IP addresses, "we do not point fingers at the United States."[xxxvi]

Similarly, quasi-authoritative sources such as Zhong Sheng state: "Even though these data show, from the technical angle, the situation of cyber attacks on China from the United States, relevant quarters in China have never made any simplistic assumptions and accusations regarding the source of attack, which is worlds apart from the U.S. side's attitude. The reason why China acts this way is that the openness of the Internet has determined that hacking attacks know no national boundaries and we cannot hold that U.S. hackers have launched an attack just because we see the IP address of the source of attack is in the United States; otherwise, the argument obviously would be less than professional."[xxxvii]

That said, in describing the supposedly many cyberattacks undertaken against Chinese military websites, Defense Ministry officials have on occasion explicitly stated that many such attacks "originated from the U.S.," thus contradicting the Chinese claim that it is impossible to determine with certainty the origin of attacks.[xxxviii]

In fact, many authoritative, quasi-authoritative, and non-authoritative Chinese sources assert that the United States is the source of a large number (indeed, a majority, according to some sources) of cyberattacks on China, based on the IP address of the attacker. For example, a Foreign Ministry spokesperson, in listing the numbers of cyberattacks China suffered in 2012, stated: "Attacks originating from the United States rank the first among these hackings."[xxxix] Perhaps this apparent contradiction reflects a Chinese distinction between cyberattacks originating in the U.S. and attacks made by the U.S. government.

Yet the supposed unreliability of IP addresses should presumably apply equally in both cases.

Many Chinese sources regard Western and U.S. accusations that China engages in numerous cyberactivities against other countries as a sort of threat to China. They consistently and vehemently deny such accusations as groundless, fraudulent, unsubstantiated, and hence unprofessional (usually by asserting the above-outlined problems involved in identifying the source of attacks), while repeating the claim that China is opposed to all hacking and other forms of cyberattacks.[xl]

At the same time, authoritative, quasi-authoritative, and non-authoritative Chinese sources also charge the United States with pursuing a double standard by accusing others of cyberattacks while conducting cyberespionage itself (as confirmed by the Snowden leaks of the U.S. Prism program, termed "Prism gate" by many Chinese). In addition, some sources claim that Western accusations blacken China's image and obstruct efforts to develop a common approach against cyberattacks.

Foreign Ministry officials are generally less direct and critical in presenting this viewpoint than their Defense Ministry counterparts. Statements by the former – almost always in response to press questions – are essentially similar to the following reply by Foreign Ministry spokesperson Hua Chunying at a press conference, that "taking a double standard on cyber security does not help solve the issue" while expressing the hope that "both sides could take an even-tempered, level-headed and objective approach to the issue, build up understanding and trust and enhance cooperation through dialogue and communication so as to jointly build a peaceful, secure, open and cooperative cyberspace."[xli]

In partial contrast, Defense Ministry officials state that "Prism gate" "reflects the real face and hypocritical deeds of a certain country [read the United States] . . . This kind of double standard of taking advantage of advanced information technology to seek selfish gains on the one hand while making unfounded allegations against other countries is not conducive to peace and stability in cyberspace."[xlii]

Quasi-authoritative sources are more direct in their criticism of the United States. Though avoiding outright accusations that the U.S. government engages in large-scale cyberattacks against China, such sources claim that American support for "internet freedom" is used to facilitate intervention in the politics of other countries while also serving to consolidate "the cyberhegemony of the United States."[xliii]

The "double standard" charge against the United States is echoed, with even greater stridency, in many non-authoritative Chinese sources, especially those appearing in military media such as the *Liberation Army Daily* or those penned by military scholars and analysts.[xliv]

Some non-authoritative military sources describe the U.S. approach as a "so-called dual strategy": "On the one hand, it uses so-called 'cyber freedom' as an important

supplemental means for U.S. global diplomacy, and on the other, it uses 'cyber security' to suppress competitors and maintain U.S. security. However, such a strategy means that other nations must 'open wide the gate' to their Internets, while the United States can wear the tall hat of 'protecting national security' and use means such as strangling 'WikiLeaks' to close the 'gate' to their own Internet."[xlv]

Finally, in response to Washington's explanation that its cybersurveillance activities only apply to foreigners, one AMS scholar further highlights how it indicates that while "the privacy right of the American people is treated with due respect . . . that of the people of other countries is not as important."[xlvi]

In addition to the above perceived cyberthreats posed to China by the United States (and other Western countries), a wide array of primarily quasi- and non-authoritative Chinese sources also allege that, by developing the means to conduct offensive cyberwarfare, the U.S. is militarizing cyberspace and prompting an international cyber arms race, thereby undermining efforts to increase cybersecurity and aggravating Sino-U.S. relations.

Among authoritative sources, the few discussions of the threat posed by U.S. cyberwarfare are primarily found among military sources. For example, a Defense Ministry spokesperson reportedly stated that U.S. plans to enlarge the size of its cyberwarfare force, make cyberwarfare rules, and "adopt a preemptive cyber attack policy" are "not conducive to the joint efforts of the international community to enhance network security."[xlvii]

Quasi- and non-authoritative Chinese military and civilian sources (but especially the former) are far more numerous, and go further, in accusing "certain countries" or in some instances explicitly the West—not least the United States—of developing the notion of cyberwarfare as a new means of threatening other nations. Such sources view the United States as having first militarized the Internet through the introduction of the concept of cyberwarfare, as well as the development of a cyberwarfare strategy and specific cyberweapons.[xlviii]

Zhong Sheng provides a typical example of this argument in a February 2013 article. The author(s) state(s):

> certain countries are now speeding up the development of cyber war forces, seeking military superiority in cyberspace, giving impetus to applying armed conflict methods in cyberspace, and drawing up cyber warfare rules in disguised fashion, with the result that the risk of military conflict in cyberspace is continuing to grow, posing an increasingly obvious threat to national security and international peace.[xlix]

The author(s) take aim specifically at the United States elsewhere in the article, stating:

> The United States ought to clearly understand that taking the lead in developing cyber warfare capability and pursuing absolute military superiority will trigger a

> cyberspace arms race and military conflict, and this could cause unforeseeable disastrous consequences for human society.

The author(s) add that, given the United States' own high reliance on computer-based information systems, "engaging in cyber war is not in America's own interests."[l] An article appearing in *People's Daily* makes the same point, somewhat ominously asserting that U.S. dependence on cybersystems could "leave the country more vulnerable and turn out to be the lower-hanging fruit in the face of cyber attacks."[li]

In criticizing the United States, some non-authoritative Chinese sources raise questions regarding the feasibility and reliability of any cyberwarfare doctrine or set of weapons. For example, one military analyst asks several basic questions: how does one define and identify a cyberattack? At what point does it constitute something equivalent to a conventional military attack, requiring a military response of some sort? How can one identify with certainty the source of the attack? And what rules or procedures would prevent unwanted collateral damage to innocents?[lii]

Despite such complications, the supposedly dire threats presented by Washington's alleged militarization of cyberspace prompt many Chinese observers (and in particular military analysts) to assert that China and other countries have no choice but to respond, in order to protect themselves, by acquiring cyberwarfare capabilities of their own. As one observer states: "Now that a rising number of militaries are setting up cyber warfare commands to protect their national interests, it is natural for the People's Liberation Army to catch up and launch a similar command responsible for defending China's cyber security."[liii]

One very authoritative military source, the most recent PRC Ministry of Defense "Defense White Paper 2012," clearly states an intention to defend China's cyberspace, stating that the goal of China's national defense efforts is (among other things) to:

> protect national maritime rights and interests and national security interests in outer space and cyber space. "We will not attack unless we are attacked; but we will surely counterattack if attacked." Following this principle, China will resolutely take all necessary measures to safeguard its national sovereignty and territorial integrity.[liv]

Several non-authoritative military sources explore in considerable detail the various dimensions and requirements of cyberwarfare.[lv] However, most Chinese sources characterize such responses as purely "defensive" efforts designed to counter or deter cyberwarfare attacks. The term "cyberdefense" is usually employed to describe the function of China's military-oriented cybercapabilities.[lvi]

To reinforce this notion, one authoritative military spokesperson has declared that "China does not have any soldiers engaging in cyber warfare." He adds, in response to the announcement in May 2011 that the PLA had formed a "Cyber Blue Team" within the Guangzhou military region: "The inclusion of "blue teams" in Chinese military drills is

done to enhance the country's ability to safeguard cyber security and is not related to conducting cyber attacks."[lvii] Other analysts similarly assert, in response to criticism that the PLA's cybersystems include offensive capabilities, that China's blue teams "are not hackers."[lviii]

The Origins and Motives Behind Foreign Cybersecurity Threats

As suggested above, the vast majority of Chinese commentary on the origins and motives of the cybersecurity threats confronting China focuses on the actions of the United States. In the realm of military and national security, these sources contain a multitude of different variations on a single general theme: Washington is using cybertechnology and developing cyberwarfare capabilities to undermine or overthrow nations it opposes, justify cyberattacks in the name of national security, and thereby support its efforts to maintain global hegemony.

An explicit emphasis on sustaining U.S. hegemony as a motive for Washington's actions, common to Chinese analysis of many aspects of U.S. foreign and defense policy, is in this instance found only in quasi- and non-authoritative sources, as far as we can discern. Authoritative sources are more circumspect and vague. In one instance, responding to a press query on the Snowden leaks detailing U.S. intrusion into Chinese cybernetworks, a Foreign Ministry spokesperson states: "We believe that what we need in cyber space are rules and cooperation rather than war or hegemony."[lix] In other instances, both Foreign and Defense Ministry spokespersons state, in response to press queries, that U.S. or U.S. government–related allegations of Chinese cyberattacks are "driven by ulterior motives," and constitute interference in China's internal affairs, as a result of a "Cold War mentality."[lx]

Probably the most explicit authoritative reference to U.S. motives occurs in the economic realm. For example, when asked to comment on U.S. congressional legislation requiring government agencies to make a formal assessment of "cyber-espionage or sabotage" risk when considering purchase of information technology systems from China, a Foreign Ministry spokesperson states that the legislation uses cybersecurity as "an excuse to take discriminatory steps against Chinese companies."[lxi]

Quasi-authoritative sources are far more direct and critical. Most focus on U.S. motives behind the development of cyberwarfare capabilities. There have been several accusations of Chinese hacking attacks on the United States in recent Pentagon reports on the Chinese military,[lxii] as well as a February 2013 report by Mandiant,a U.S.-based information security company, describing the massive and widespread cyberattacks on the U.S. and other powers and on commercial entities, allegedly conducted by a Chinese organization termed PLA Unit 61398 based near Shanghai.[lxiii] In response, Zhong Sheng argues that "the intention is to have justification for the U.S. launch of cyberattacks," "put a cloak of legality on its 'preemptive strike' strategy in cyber warfare," and "gain spending support and international law grounds, and [reverse] its negative international image of sabotaging cyberspace peace." All such actions are purportedly done to maintain U.S. hegemony.[lxiv]

Similar but more detailed and disparaging arguments are most commonly found in non-authoritative sources. A typical refrain, in this case contained in a *Liberation Army Daily* article, asserts that "the United States is trying to solely seize the hegemonic status in global cyberspace and also dominate the formulation of the rules of the game for cyber warfare through a series of strategic measures, thus capturing the commanding height of future cyber warfare."[lxv]

Non-authoritative sources make a clear connection between the above argument of U.S. hegemony and the U.S. accusation that China engages in cyberattacks, asserting that the latter is part of the overall "China threat theory" espoused by Washington and others to justify their containment strategy against China and sustain large defense budgets, and hence U.S superiority.[lxvi]

Unsurprisingly, this argument is also linked to the economic domain. In responding to accusations that the PRC government and others in China engage in large-scale attacks on commercial entities, non-authoritative sources assert that the United States and U.S.-backed companies are motivated by efforts to weaken China as an economic competitor, facilitate trade protectionism, levy more technology restrictions on China, protect commercial software interests, compensate for U.S. economic losses, and generate business for U.S. corporations.[lxvii]

Chinese Preferences for Mitigating Cybersecurity Threats

In addition to portraying China as a victim of cyberattacks and making blanket denials of any Chinese involvement in cyberattacks on others, authoritative sources most often address the issue of how best to deal with the growing cybersecurity problem. In this regard, Foreign Ministry sources repeatedly offer variations of the following two related statements:

> China stands ready to work with the international community including the U.S. to carry out constructive dialogues and cooperation in the principles of mutual respect and trust so as to jointly safeguard "peace, security, openness and cooperation" of the cyberspace.[lxviii]

and

> The United Nations, we believe, is the most appropriate forum for deliberation and formulation of . . . international norms and rules on information and cyber-space security.[lxix]

According to authoritative sources, such a broad, UN-structured international effort to formulate norms and rules should begin with the development of "a code of conduct of responsible countries for cybersecurity."[lxx] To this end, in 2011, China, along with Russia, Tajikistan, and Uzbekistan, submitted to the United Nations a draft International Code of Conduct for Information Security, which Zhong Sheng claims is "the first

relatively comprehensive, systematic document of rules in the field."[lxxi] Such a code would in turn presumably lay the foundation for the "establishment of a fair, democratic and transparent internet management mechanism," according to former Foreign Minister Yang Jiechi.[lxxii] In support of this effort, the Chinese Foreign Ministry recently set up a "cyber affairs office" to coordinate diplomatic activities regarding cyberaffairs.[lxxiii]

As a major part of this undertaking, authoritative Chinese sources also stress the need to work bilaterally with key actors such as the United States. Through such mechanisms as the annual China-U.S. Forum on the Internet Industry and the recently created Cyber Working Group under the framework of the S&ED, Beijing and Washington should "respect and accommodate the other side's concerns and jointly pursue cooperation through frank exchanges and dialogue." Specifically, according to one authoritative source, the two countries should "make use of the existing cooperative mechanism to provide each other with judicial assistance as they crack down on hacking, phishing, and other Internet crime, and regularly exchange views on the maintenance of cyber security…and step up consultations on such important issues as the equitable utilization of global Internet resources, the formulation of rules for the governance of cyberspace, and the control of a cyber arms race."[lxxiv]

Quasi- and non-authoritative sources generally echo the above statements, emphasizing the need to cooperate under the auspices of the UN to develop a common set of norms and regulations governing the Internet.[lxxv] However, many sources go beyond such general statements in support of official PRC policy, arguing that: a) the notion of "cyber sovereignty" should constitute a key principle guiding the establishment of common norms; and b) such an international effort should oppose the militarization of cyberspace and ultimately end the allegedly unjust and threatening pattern of U.S. dominance over the Internet.[lxxvi] Several non-authoritative sources criticize the United States, either directly or indirectly, for taking advantage of the absence of international norms and regulations to, in the words of one observer, "run amuck, to seek…political, economic, and military superiority over other countries, and to pursue…absolute security."[lxxvii]

Not all non-authoritative Chinese sources, however, take such a critical and in some cases hostile stance toward the United States. One source states that: "Instead of pointing fingers at each other, China and the U.S. need to get down to real business and find effective ways to crack down on cyber crimes, manage cyber conflicts, and consult each other on ways to construct the global norms of cyberspace."[lxxviii] Another source suggests that "As long as joint efforts are made, it is completely possible that cyberspace will become a converging point of interests between China and the United States for expanding consensus and improving bilateral relations."[lxxix] Such statements usually appear during a period of Sino-U.S. comity, when, for example, Xi Jinping is visiting the United States. Finally, several non-authoritative sources call for stronger PRC laws to govern the Internet, as part of the overall effort to develop a common approach in this area.[lxxx]

Conclusions and Observations

Several overall conclusions can be drawn from the above examination of Chinese views on cybersecurity. First, there is remarkable consistency across different types of sources (authoritative or otherwise, civilian and military) regarding the definition of cybersecurity, and the challenge that it presents. Authoritative sources, such as Foreign Ministry spokespersons and senior officials, offer only very general statements on these topics, while other sources provide much greater detail.

But all types of sources seem to agree that cyberspace is an increasingly critical realm relevant to the activities of the nation-state, various types of (especially governmental and commercial) organizations, and individual citizens around the world. Moreover, all interested Chinese seem to conclude that cybersecurity is thus a global problem encompassing threats to national security, economic development, and individual social, political, and moral rights. In addition, most Chinese, but especially military observers, seem to place a relatively high stress on the threat that cyberactivities pose to state sovereignty as well as the ability of the government to maintain order, ensure social stability, and keep the nation (and by implication the PRC regime) free from attacks, both domestic and foreign.[lxxxi]

In this regard, many Chinese view it as the duty of the government to take a highly activist role in supervising and controlling the Internet, and in defending China's "cyber sovereignty" against all threats. At the same time, many Chinese, and authoritative sources in particular, also stress the need for the international community as a whole to devise rules, norms, and structures that reinforce each nation's individual supervisory and enforcement mechanisms and processes. While many Chinese apparently think that such an undertaking should occur as a logical consequence of the dangers presented by the common threats to cybersecurity faced by all nations and societies, in fact China's approach (along with that of other authoritarian states) is more statist and interventionist than in the case of most if not all Western nations. And it is certainly more overtly oriented toward political and ideological objectives, such as the upholding of "socialist morality and culture."

This difference in approach toward the role of the state in cybersecurity arguably constitutes the most significant obstacle to efforts to develop a common international cyberregime or a set of rules and mechanisms to ensure cybersecurity. Western nations, including the United States, believe that governments should take a relatively low profile in supervising and ordering the Internet, preferring instead a "multi-stakeholder approach," as reflected in the existing ICANN process. This approach emphasizes the role of the private sector, civil society, academia, and other stakeholders, in contrast to a top-down model driven by intergovernmental decisions, whether via the UN or other entities.[lxxxii]

According to U.S. officials, international agreements on cyberbehavior should largely focus on maintaining as much freedom as possible, and avoid a "traditional top-down regulatory model" characterized by "rigid procedures, bureaucracy, and stalemate,"[lxxxiii]

while presumably remaining compliant with existing international and national criminal laws, including prohibitions against child pornography, theft, slander, and other types of images and speech that are usually deemed illegal by societies around the world.

Thus, the United States and other Western governments do not support apparent Chinese intentions to enshrine the concept of "cyber sovereignty" in international agreements, and to establish the UN as the supreme rule-making and supervisory entity over the global Internet. Washington and others fear that such a development would result in a highly statist and rigid international cyberregime that limits many activities deemed unacceptable by authoritarian but not democratic states (such as freedom of political speech), while additionally stifling commercial innovation. It is notable, but perhaps not surprising, that no nongovernmental (i.e., non-authoritative) Chinese sources that we can identify raise the danger to individual (and corporate) freedoms that might result from the mainstream Chinese approach to this complex problem.

Another area of consistency within the Chinese viewpoint concerns the nature of the threat posed to China by the United States and, to a much lesser degree, by other foreign states. While authoritative sources avoid naming those governments they believe pose cyberthreats to China, seeking to focus instead on the need to work together on a common problem, other types of sources almost invariably depict the United States as the major culprit in cyberbased efforts to keep China (and the rest of the world) subordinate, as Washington allegedly strives to maintain its global hegemony. As discussed in many previous editions of *CLM*, charges of hegemonic behavior by the United States are commonplace among Chinese analyses of foreign policy issues. The cyberrealm offers a particularly robust and multidimensional example of how such hegemonic behavior, supposedly the most typical of all American traits, is identified as motivating all sorts of actions, from using cyberspace to promote trade protectionism to providing a justification for preemptive conventional military attacks on China and other countries.

As indicated above, non-authoritative Chinese sources are particularly voluble and energetic in their criticism of the United States for four alleged sins related to its never-ending search for hegemony: 1) the militarization of cyberspace; 2) the pursuit of a double standard in claiming cyberfreedom for itself while attacking or limiting such freedom for others; 3) engaging in completely groundless, destructive, and self-serving accusations against China; and 4) unfairly dominating the current global cybersystem.

In many of these areas, it is remarkable to note the degree to which many Chinese observers seem to deliver these criticisms without much, if any, real knowledge of how states behave and how the Internet operates—and in some cases in the face of evidence to the contrary. For example, Chinese sources seem to believe that if the United States had not chosen to embark on the development of a cyberwarfare capability, no other states would have done so. As indicated above, they assert that Beijing has been "forced" by U.S. actions to develop such a capability, although they stress that it is purely "defensive" and thus presumably lacks the capacity to attack other systems. 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.

Consistent with the stress on the possession of purely "defensive" systems, all Chinese sources insist, often vehemently, that American accusations of Chinese government (and in particular military) intrusions and attacks against both government and private (largely commercial) computer systems lack any credible evidence, and probably harbor "ulterior motives." The categorical and absolute nature of these denials, across all types of sources, is particularly noteworthy, especially since it flies in the face of what cyberspecialists regard as solid evidence to the contrary. Chinese sources almost uniformly cite the ability to percolate IP addresses as their primary reason for insisting that cyberintrusions and attacks are "anonymous" and hence that U.S. accusations are "groundless." Yet, even if this assertion is true, other highly reliable methods do exist, and have been presented both publicly (such as in the Mandiant report) and privately to the PRC government.[lxxxiv]

For Chinese leaders and elites to claim that China possesses no offensive cybercapabilities and has never engaged in cyberactions against foreign states lacks credibility. Moreover, it also strongly suggests that if the United States engages in a double standard, China also does so, perhaps to an even greater degree. Washington at least does not deny that it engages in some forms of cybersurveillance and intrusions and the development of the capability to conduct cyberwarfare. One possible explanation for the Chinese position is that, for non-authoritative sources at least, the cyberrealm, as with other intelligence and surveillance matters, is too sensitive an issue to permit any divergence from the PRC government's official position. It is also an area with which few nongovernmental observers are familiar. For official, authoritative sources, however, China's unreasonable position perhaps reflects the need to sustain a public image of China as a peace-loving, harmony-seeking nation that remains outside the realm of power-seeking governments like the United States.

Finally, the Chinese criticism that the United States exercises an unfair and potentially threatening level of influence over the global cybersystem through its "control" over ICANN alongside its technological dominance constitutes a gross distortion of the actual situation. While it is true that the ICANN governance system originated within the U.S. Department of Commerce, it is not under the control of Washington, does not control Internet content, and cannot provide access connections to the Internet as an ISP (Internet Service Provider) does. It coordinates the Internet's naming system, and regulates the expansion and evolution of the Internet, with input from several representatives of both nongovernmental and governmental entities.[lxxxv] Moreover, although most root servers are operated by U.S. entities, according to knowledgeable specialists, they have no "physical" location per se, being comprised of a network of several identical copies distributed around the world, with no main server. Perhaps more important, root servers in themselves do not ensure control over the Internet, and China now possesses a root server network.

All together, Chinese views on cybersecurity and the threats presented to China contain many incredible elements. And the apparent unanimity of support within China for the official position suggests it is unlikely that internal debates exist over this issue that could possibly provide an opening for a change in the Chinese position. As a result, it is very likely that little significant progress will occur in at least the near to medium term in developing a common international approach to cybersecurity, and that Beijing will continue to develop and utilize cybercapabilities against other states, for both national security and economic purposes. That said, it is possible that sufficient pressure or incentives could be brought to bear to induce Beijing to reduce its cyberbased commercial espionage against the U.S. and other nations, especially when China faces stronger incentives to protect its own proprietary commercial assets.

Notes

[i] Jonathan Masters, "Backgrounder: Confronting the Cyber Threat," Council on Foreign Relations, May 23, 2011, http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577. See also "Cyberwar: The threat from the internet," *Economist*, July 1, 2010; and "War in the fifth domain: Cyberwar," *Economist*, July 1 2010. For a discussion of economic and commercial threats posed by cyberespionage, see "Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011," Office of the National Counterintelligence Executive, Washington DC, October 2011.

[ii] The DoD report explicitly accuses China's military of launching cyberattacks on U.S. government computers and defense contractors. Thomas Donilon, the president's former national security adviser, has mentioned "cyberintrusions emanating from China on an unprecedented scale." See David Sanger, "U.S. Blames China's Military Directly for Cyberattacks," *New York Times*, May 6, 2013; and "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013," Office of the Secretary of Defense, Washington DC, 2013, http://www.defense.gov/pubs/2013_china_report_final.pdf. Also see "Remarks By Tom Donilon, National Security Advisor to the President: 'The United States and the Asia-Pacific in 2013'," Asia Society, New York, March 11, 2013, http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

[iii] David Sanger and Mark Landler, "U.S. and China Agree to Hold Regular Talks on Hacking," *New York Times*, June 1, 2013.

[iv] "US-China S&ED, CWG and SSD Key Outcomes," United States Information Technology Office, undated, http://www.usito.org/news/us-china-sed-cwg-and-ssd-key-outcomes. See also the U.S. State Department media note: "U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track," Office of the Spokesperson, U.S. Department of State, Washington DC, July 12, 2013, http://www.state.gov/r/pa/prs/ps/2013/07/211861.htm

[v] Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and U.S.-China Relations," Brookings Institution, Washington DC, February 2012. For a discussion on how the new cyberspace domain complicates the Sino-U.S. relationship and potential competition, see Bill French, "China and the Cyber Great Game," *National Interest*, March 20, 2013, http://nationalinterest.org/commentary/china-the-cyber-great-game-8241; and Wilson VornDick, "The Real U.S.-Chinese Cyber Problem," *National Interest*, July 30, 2013, http://nationalinterest.org/commentary/the-real-us-chinese-cyber-problem-8796. See also James A. Lewis, "Cyber War and Competition in the China-U.S. Relationship," China Institutes of Contemporary International Relations, Beijing, May 13, 2010, http://csis.org/files/publication/100510_CICIR%20Speech.pdf. The U.S. government has produced a slew of cyberstrategy reports in recent years. See, for example, "Department of Defense Strategy for Operating in Cyberspace," Department of Defense, Washington DC, July 2011; and "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," Defense Science Board, Department of Defense, Washington DC, January 2013.

[vi] Several types of PRC sources are considered authoritative in the sense of explicitly "speaking for the regime." They generally include Ministry of Foreign Affairs and Ministry of Defense (MFA and MND) statements and briefings and remarks by senior civilian and military officials appearing in the leading Chinese Communist Party Central Committee (or CCP CC) and military (People's Liberation Army or PLA) newspapers: *People's Daily* (人民日报) and *Liberation Army Daily* (解放军报). Authoritative statements include, in descending order of authority, PRC government and CCP statements, MFA statements, MFA spokesperson statements, and MFA daily press briefings. Authoritative commentaries in *People's Daily* and *Liberation Army Daily* include, in descending order, "editorial department articles," editorials, and commentator articles.

Several types of usually homophonously bylined articles appearing in the *People's Daily* are considered quasi-authoritative in the sense that, although indirect and implicit, they are intended to convey the view of an important PRC organization. A major example of this is articles using the byline Zhong Sheng (钟声), which is an apparent homophone for "the voice of the Central," and appears to be written by the editorial staff of the *People's Daily* International Department. Other quasi-authoritative homophonous bylines include "Ren Zhongping" (任仲平, homophonous with "important *People's Daily* commentary"), "Zhong Zuwen" (仲组文, homophonous with "CC Organization Department article"), and "Zhong Xuanli" (钟轩理, homophonous with "CC Propaganda Department commentary").

Many types of low-level commentary and signed articles appearing in a wide variety of PRC and Hong Kong media convey notable yet decidedly non-authoritative views. Such articles appear in the PRC government news service (Xinhua), CCP and PLA newspapers, the Hong Kong–based (and *People's Daily*–owned) Global Times (环球时报), and many minor PRC and Hong Kong newspapers and academic publications. Despite the view expressed by some pundits, nothing published in the *Global Times* is "authoritative" in any meaningful sense, "because the newspaper is a commercial vehicle and doesn't stand for the *People's Daily*, even though it is subordinate to that organ." Alice Miller, personal correspondence, June 27, 2012.

[vii] For example, "Cyber security involves government and commercial secrets and personal privacy." "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on May 7, 2013," Ministry of Foreign Affairs of the People's Republic of China, May 8, 2013.

[viii] The quasi-authoritative source Zhong Sheng states that threats to cybersecurity involve activities: "[f]rom stealing private information to conducting cyber fraud, from international hacker attacks to paralyzing infrastructure operation," Zhong Sheng, "Joint efforts needed to improve cyber space rule," *People's Daily*, July 12, 2013, http://english.peopledaily.com.cn/202936/8323784.html. For the original Chinese version, see "填补网络空间 '规则空白'," 人民日报, July 9, 2013, http://www.people.com.cn/24hour/n/2013/0709/c25408-22123842.html. See also Zhong Sheng, "Fill in 'Regulation Blank' in Cyberspace," *People's Daily*, July 9, 2013, translated by Open Source Center (hereafter OSC), CHO2013070906405359. A specialist from the Chinese Academy of Engineering provides greater details:

> Information security refers to the prevention of any leakage of information when it is generated, transmitted, used, and stored so that its usefulness, secrecy, integrity, and authenticity can be preserved; and so that the reliability and controllability of the information system can be ensured. This is a very a complex systems engineering project. The most outstanding issue now is how to ensure the security of the cyber-information system. Its main threats include its being tempered with (sic), altered, stolen, or sabotaged by virus, or by hackers who take advantage of the Internet to intrude into the system to collect and transmit sensitive information, using computers' CPUs, or through pre-installing an information collecting and sabotaging program in the computer's operating system, data managing system, and application system; or to monitor and intercept information, using the computer's electromagnetic leaks and its peripheral equipment.—Shen Changxiang, "Information Security—an Important Contemporary Issue," *Liberation Army Daily*, April 4, 2001, translated by OSC, CPP20010404000084.

See also Tang Chaojing, "Information Security Plays a Decisive Role in Military Struggles," *Liberation Army Daily*, July 17, 2002, translated by OSC, CPP20020718000089.

[ix] "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on May 28, 2013," Ministry of Foreign Affairs of the People's Republic of China, May 29, 2013. The quasi-authoritative Zhong Sheng echoes this view, stating that "[c]yber security is a comprehensive issue confronting all countries in the world today." Zhong Sheng, "Joint efforts needed to improve cyber space rule," *People's Daily*, July 12

2013. (For the original Chinese version, see http://www.people.com.cn/24hour/n/2013/0709/c25408-22123842.html). A non-authoritative source states: "With the accelerated process of global informatization, the influence and impact of hacking activities have risen dramatically. The attacks and gains of hackers have already been upgraded from the "industrial chain" of Internet crimes to become a significant force that affects international affairs and stability as well as undermines the interests and security of a state." See Chen Yiming, "Much Arguments over Hackers' War," *People's Daily*, August 5, 2011, translated by OSC, CPP20110805787008.

[x] Zhong Sheng, "Joint efforts needed to improve cyber space rule." This quasi-authoritative view is echoed by authoritative sources. For example, the MFA spokesperson has stated that: "cyber crimes are transnational and anonymous." "Foreign Ministry Spokesperson Jiang Yu's Regular Press Conference on October 26, 2011," Ministry of Foreign Affairs of the People's Republic of China, October 27, 2011, http://www.fmprc.gov.cn/eng/xwfw/s2510/t872091.shtml. In Feb 2012, another MFA spokesperson reiterated the same view: "Foreign Ministry Spokesperson Liu Weimin's Regular Press Conference on February 6, 2012," Ministry of Foreign Affairs of the People's Republic of China, February 7, 2012.

[xi] For example, see "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 13, 2013," Ministry of Foreign Affairs of the People's Republic of China, June 14, 2013; and "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 28, 2013," Ministry of Foreign Affairs of the People's Republic of China, June 29, 2013.

[xii] For example, a PLA spokesperson has stated that the MND website and the China Military Online site were attacked by overseas hackers on an average of 144,000-odd times per month in 2012. "MND website and China Military Online attacked by overseas hackers 144,000-odd times per month," Ministry of National Defense of the People's Republic of China, March 1, 2013. See also: "Defense Ministry spokesman Geng Yansheng's press conference on February 28, 2013," Ministry of National Defense of the People's Republic of China, March 5, 2013. "Defense Ministry spokesperson Yang Yujun's regular press conference on March 29, 2012," Ministry of National Defense of the People's Republic of China, April 1, 2012; and "China is victim of cyber attacks: spokesman," Xinhua, March 30, 2012.

[xiii] "Foreign Ministry Spokesperson Liu Weimin's Regular Press Conference on December 12, 2011," Ministry of Foreign Affairs of the People's Republic of China, December 13, 2011. This statement is echoed almost identically by both quasi- and non-authoritative Chinese sources. For example, Qian Xiaoqian, deputy director of the China State Internet Information Office, states that "China is opposed to any form of cyber attack, any form of network warfare and cyberspace arms races." Wang Tian, Wen Xian, and Zhang Yang, "Chinese Representatives to China-US Internet Forum See Internet as Positive Factor in Development of China-US Relations," *People's Daily*, December 10, 2011, translated by OSC, CPP20111210708002. Also see Zhong Sheng, "Groundless Accusation Harmful to Cyber Security Cooperation," *People's Daily*, November 16, 2012, translated by OSC, CPP20121116787001.

[xiv] For example, see Zhong Sheng, "Fill in 'Regulation Blank' in Cyberspace," *People's Daily*, July 9, 2013, translated by OSC, CHO2013070906405359.

[xv] For example, one PLA strategist (Major General Wu Jianguo) states: "In a cyber century, the economic, political, and cultural sovereignty as well as the military security of a country depend more and more on its effective jurisdiction over the "virtual territory" . . . the information flowing there is more important than the petroleum resources in the Earth and is as strategically important as the efforts to defend the sovereign right over territorial sky, waters, and land. Nowadays, a country's sovereignty can be regarded integrated only when it has fully tapped the potentials of its "virtual territory" and effectively controlled this territory." See Wu Jianguo, "Defending the Cyber Territory," *Liberation Army Daily*, March 1, 2000, translated by OSC, CPP20000302000067.

Yu Xiaoqiu, a senior adviser to the China Information Technology Security Evaluation Center who frequently writes on cyberissues, states: "Since people have realized that there is a "border" for the Internet, the safeguarding of national information sovereignty will naturally become the new content and topic of state interests and sovereignty in the information and cyber era, along with the Internet playing an increasingly important role in the economic, social, cultural, and other fields of all countries." Yu Xiaoqiu, "An Attempt to Increase Internet Independence," *People's Daily*, July 21, 2011, translated by OSC, CPP20110722702012. Another non-authoritative source appearing in *People's Daily* similarly states: "Information about a country's domestic and foreign affairs can be spread all over the world via the Internet. Sovereignty can be infiltrated under such circumstances. . . . It will be an important theme to dominate sovereign information rights and maintain leading discourse rights in the future." "Information

age changes world diplomacy," *People's Daily Online*, July 13, 2009, http://english.people.com.cn/90001/90780/91343/6699007.html. Also see Katie Chan (Chen Fusheng), "Spreading Gunpowder Smoke of Cyber Warfare and How We Can Counter It (Watchtower)," *People's Daily* (Overseas Edition), June 7, 2012, translated by OSC, CPP20120607787001.

[xvi] For example, an article appearing in *People's Daily* states: "The role of the Internet once again caused controversy during the recent Iranian presidential election turmoil. Social networking and blogging websites such as Twitter passed a large amount of information to Iranian voters. In particular, the websites transmitted criticism of the Iranian government by foreign media to opposition parties, and especially young Iranians, who are energetic and easily excited. This is tantamount to adding fuel to the fire, and endangers Iranian sovereignty and social stability." "Cyber Warfare—An Emerging Non-Traditional Security Topic," *People's Daily Online*, July 13, 2009, http://english.people.com.cn/90001/90780/91343/6699026.html. For similar discussions of the Iranian case, see the following sources: Li Hongmei, "How Far Twitter Pushes Forward E-age?," *People's Daily Online*, July 3, 2009, http://english.people.com.cn/90002/96417/6692821.html; Chen Yiming, "US Covertly Building 'Shadow Internet'," *People's Daily*, June 15, 2011, translated by OSC, CPP20110615787005; Yang Ziyan, "'Cut Off the Internet' to Challenge Internet Control Power," *People's Daily* (Overseas Edition), August 9, 2012, translated by OSC, CPP20120809702002; Shen Yi, "US Cyber Diplomacy Is to Hold the Old Wine With a New Bottle," *Liberation Army Daily*, May 2, 2012, translated by OSC, CPP20120502787009; and He Zhenhua, "'Internet Freedom' and 'Smart Power' Diplomacy," *People's Daily Online*, January 25, 2010, http://english.people.com.cn/90001/90780/91343/6878072.html.

[xvii] "Cyber diplomacy brings changes to traditional diplomatic mode," *People's Daily Online*, July 13, 2009, http://english.people.com.cn/90001/90780/91343/6699012.html.

[xviii] "Internet Management Does Not Equal Thought Control," *People's Daily Online*, May 10, 2011, translated by OSC, CPP20110510702007.

[xix] One non-authoritative source explicitly contrasted China's state-oriented approach to Internet governance with the market-oriented approach of the United States: "An important point to consider is that the China-U.S. conflict over Internet governance can be traced back to the first World Summit on Information Society (WSIS) in Geneva, 2003. China insisted on the role of state leadership in Internet governance, while the U.S. proposed market leadership. Both countries had their own reasons. For China, the state plays an important role in development and market issues. State authorities also manage the media to maintain social stability. The U.S. will not loosen its grip over core Internet resources because it is a gathering place for a myriad of commercial interests." Xu Peixi, "Interpreting the second wave of cyber security threats to China," CCTV.com, March 4, 2013.

[xx] "Experts Discuss Prospects of 'Cyber Defense' and National Defense," *Liberation Army Daily*, January 4, 2011, translated by OSC, CPP20110106702001. Non-authoritative sources also characterize "network warfare" as "an important topic in the field of *non-traditional* security." "Cyber Warfare—An Emerging Non-Traditional Security Topic," *People's Daily Online*, July 13, 2009, http://english.people.com.cn/90001/90780/91343/6699026.html; italics by author

[xxi] Major General Wu writes: "in the current cyber world, new technologies are emerging in an endless stream and the cyber space and 'boundaries' are even more complex and changeable." Wu Jianguo, "Defending the Cyber Territory."

Ye Zheng, a researcher at the Academy of Military Sciences (AMS), writes: "our Internet defense ability is weak. . . . we are subject to the manipulation of our core network technology by other countries." Cited in "Experts Discuss Prospects of 'Cyber Defense' and National Defense."

Su Hao, an expert on international security at the China Foreign Affairs University, states: "Our current protection input is not enough, and the scale and size is far less intensive compared to that of Europe and the United States." Ai Yang, "Nation needs 'more Internet security'," *China Daily*, December 29, 2010, http://www.chinadaily.com.cn/cndy/2010-12/29/content_11768563.htm.

[xxii] Katie Chan (Chen Fusheng), "Spreading Gunpowder Smoke of Cyber Warfare and How We Can Counter It (Watchtower)."

[xxiii] "Internet Management Does Not Equal Thought Control," *People's Daily Online*.

[xxiv] "Internet Management Does Not Equal Thought Control," *People's Daily Online.* See also the response by Zhang Difei, from the Supervision Bureau of Beijing Discipline Inspection Committee, as quoted in "Highlights: *People's Daily*'s 'New Media' Page," *People's Daily Online*, November 22, 2011, translated by OSC, CPP20111125715049.

[xxv] Jing Nanxiang, "Cyber Freedom and Cyber Self-Discipline," *Liberation Army Daily*, December 20, 2011, from "Summary: JFJB on Cyber Freedom and Cyber Self-Discipline for PRC Netizens," translated by OSC, CPP20111221088010.

[xxvi] "Opinion on Strengthening Online Ideological and Political Education in the Military Forces," *Liberation Army Daily*, June 29, 2012, translated by OSC, CPP20120629702005. From the civilian side, Wang Chen, director of the Information Office of the State Council, has asserted that "Cyber culture is an important component of socialist culture with Chinese characteristics and is the culture responding to the development requirements of advanced productivity and serving the masses. We must…promote the theme of cyber ideology and culture." He adds: "We should…firmly seize the correct guidance of public opinion, work hard to organize the on-line publication of advanced deeds, promote mainstream public opinions, arouse the enthusiasm of the entire society, and offer strong support of public opinions for promoting scientific development and social harmony." "Looking Forward to Great Development, Great Prosperity of Culture—Leaders of Related Departments Interpreting Decision of Sixth Plenary Session," *People's Daily* (Overseas Edition), November 4, 2011, translated by OSC, CPP20111104702004. Hou Shelin, secretary general of the General Office of the Beijing Military Region Political Department, discusses how it is critical to "seize the information heights in the 'virtual reality' and control opinion dominance on the 'digital platform' so as to create a good cyber ideological and cultural environment" and achieve "national defense education for the people" against the "social ideological trends outside our country." Hou Shelin, "Actively Occupy the Cyber Ideological and Cultural Position," *Zhanyou Bao* (战友报), May 2, 2013, translated by OSC, CHO2013071804079301. *Zhanyou Bao* is the official newspaper of the Communist Party committee of the Beijing Military Region. Another observer highlights how China is "designing the architecture of an online social democracy" as opposed to "foreign cyber-ideologues," while criticizing the "deep decline" of U.S. constitutional democracy and "disintegration of US civic culture"; see Yoichi Shimatsu, "US Cyberspying An Affront To Tsinghua University's Open Culture," *South China Morning Post*, June 25, 2013, http://www.scmp.com/comment/insight-opinion/article/1267982/us-cyberspying-affront-tsinghua-universitys-open-culture; and Clifford Kiracofe, "Disintegration of Democratic Values Threatens Future of US," *Global Times Online*, June 21, 2013, http://www.globaltimes.cn/content/790543.shtml. For further discussion on the government role in "guiding Internet culture" and supervising online public opinion, see Zhou Zhixin, Liao Baoqi, and Chen Yaoqiang, "Dynamic Monitoring of Cyber Network Public Opinion Conditions is Included as Part of Operation Shift Duty—Sanya Garrison Devotes Great Efforts to Improving the Cyber Network Public Opinion Supervision Mechanism," *Zhanshi Bao* (战士报), June 22, 2012, translated by OSC, CPP20121109680011. *Zhanshi Bao* is the official newspaper of the Communist Party committee of the Guangzhou Military Region; and Qin An, "Create a National Cyberspace Administration System," *Global Times Online*, July 11, 2013, translated by OSC, CHR2013071658204375.

[xxvii] Yang Jiechi, "Question and Answer Session With Foreign Minister Yang Jiechi At Munich Security Conference," February 5, 2010, http://www.fmprc.gov.cn/eng/zxxx/t656702.shtml.

[xxviii] Yu Xiaoqiu, "Sincerity Is Needed for International Cooperation in Cybersecurity," *People's Daily*, March 1, 2010, translated by OSC, CPP20100301702003. An article in the *Global Times* states that "the global network is under the management and regulation of the U.S. . . . The U.S. has publicly harmed other countries' interests through the Internet because it is the one that makes the rules." "Hacker claims reflect US intention of cyber hegemony," *Global Times*, February 21, 2013, http://www.globaltimes.cn/content/763429.shtml.

[xxix] See Katie Chan (Chen Fusheng), "Spreading Gunpowder Smoke of Cyber Warfare and How We Can Counter It (Watchtower)"; Chen Yiming, "US Covertly Building 'Shadow Internet'," *People's Daily*, June 15, 2011, translated by OSC, CPP20110615787005; Yang Ziyan, "'Cut Off the Internet' to Challenge Internet Control Power," *People's Daily* (Overseas Edition), August 9, 2012, translated by OSC, CPP20120809702002.

[xxx] Katie Chan (Chen Fusheng), "Spreading Gunpowder Smoke of Cyber Warfare and How We Can Counter It (Watchtower)."

[xxxi] Zhong Sheng, "To Defend 'Freedom', or to Defend Hegemony?" *People's Daily*, January 26, 2010, http://english.peopledaily.com.cn/90001/90780/91343/6879251.html.

[xxxii] "Crossover: Chinese citizens on hacking allegation," CCTV.com, February 21, 2013, http://english.cntv.cn/program/china24/20130221/106873.shtml

[xxxiii] Wu Jianguo, "Defending the Cyber Territory," *Liberation Army Daily*, March 1, 2000, translated by OSC, CPP20000302000067.
[xxxiv] "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on February 20, 2013," Ministry of Foreign Affairs of the People's Republic of China, February 21, 2013.
[xxxv] "Foreign Ministry Spokesperson Liu Weimin's Regular Press Conference on February 6, 2012," Ministry of Foreign Affairs of the People's Republic of China, February 7, 2012.
[xxxvi] "China defense ministry refutes cyber attack allegations," Xinhua, February 20, 2013, http://news.xinhuanet.com/english/china/2013-02/20/c_132180777.htm.
[xxxvii] Zhong Sheng, "Groundless Accusation Harmful to Cyber Security Cooperation," *People's Daily*, November 16, 2012, translated by OSC, CPP20121116787001.
[xxxviii] For example, a Defense Ministry spokesperson stated:

> China like other countries is also facing severe threat in cyber attack. China is one of the worst stricken countries in the world in terms of cyber attack. Since the Chinese Defense Ministry website and the Chinamil.com.cn went online, they have been threatened by numerous cyber attacks, especially in recent years, [and] the number of cyber attacks has been increasing…Among these attacks, 62.9% of them were originated from the U.S. —"Defense Ministry spokesman Geng Yansheng's press conference on February 28, 2013," Ministry of National Defense of the People's Republic of China, March 5, 2013.

Also, the Defense Ministry spokesperson has stated that "almost two thirds" of the abovementioned 144,000 cyberattacks per month on two PLA websites originated in the U.S. See "China accuses U.S. hackers of targeting its websites," Associated Press, February 28, 2013, http://www.cbc.ca/news/world/story/2013/02/28/china-hackers.html; and also "US main source of cyberattacks against China," CCTV.com, March 11, 2013, http://english.cntv.cn/20130311/102049.shtml.
[xxxix] "Attacks originating from U.S. rank first among overseas hackings in China: FM," Xinhua, February 20, 2013, http://english.cntv.cn/20130220/105966.shtml. In addition, Zhong Sheng writes: "It needs to be pointed out that quite a few data showed that among the attacks on China's networks from outside its territory, those from malicious IP addresses in countries such as the United States precisely were the ones that most seriously threatened the country. An investigation by the National Computer Network Emergency Response Technical Team and Coordination Center found that in 2011, 9,528 IP addresses from the United States were controlling nearly 8.85 million host computers within our territory and 3,328 US IP addresses were controlling 3,437 websites here. In addition, 72.1 percent of the IP addresses faking as bank websites within the territory of our country were from the United States. See Zhong Sheng, "Groundless Accusation Harmful to Cyber Security Cooperation," *People's Daily*, November 16, 2012, translated by OSC, CPP20121116787001.

Non-authoritative sources include a CCTV report in March 2013 entitled "US main source of cyberattacks against China," which cited IP addresses, among other supposed evidence, to support its contention. See http://english.cntv.cn/20130311/102049.shtml. Another source states: "facts have proved that the government of the United States, the birthplace of Internet technology, and other Western countries have been conducting cross-border network monitoring and information theft, which has made the already serious network security situation even worse." Si Zhuang, "'Double Standard' Not Accepted in Cyber Security," *People's Daily*, June 21, 2013, translated by OSC, CPP20130621787006.
[xl] For authoritative denials see "Defense Ministry spokesperson Yang Yujun's regular press conference on March 29, 2012," Ministry of National Defense of the People's Republic of China, April 1, 2012; "Foreign Ministry Spokesperson Jiang Yu's Regular Press Conference on October 26, 2011," Ministry of Foreign Affairs of the People's Republic of China, October 27, 2011, http://www.fmprc.gov.cn/eng/xwfw/s2510/t872091.shtml; "Foreign Ministry Spokesperson Liu Weimin's Regular Press Conference on February 6, 2012," Ministry of Foreign Affairs of the People's Republic of China, February 7, 2012; "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on October 31, 2012," Ministry of Foreign Affairs of the People's Republic of China, November 1, 2012; "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on Nov 14, 2012," Ministry of Foreign Affairs of the People's Republic of China, November 15, 2012; "China Focus: Chinese media lambaste U.S. hacking allegations," Xinhua, February 22, 2013, http://english.cntv.cn/20130222/107560.shtml; David Barboza, "In Wake of Cyberattacks, China Seeks

New Rules," *New York Times*, March 10, 2013; "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on May 2, 2013," Ministry of Foreign Affairs of the People's Republic of China, May 3, 2013; "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on May 7, 2013," Ministry of Foreign Affairs of the People's Republic of China, May 8, 2013; "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on May 28, 2013," Ministry of Foreign Affairs of the People's Republic of China, May 29, 2013; "Linking hackers' cyber attacks with Chinese government, military groundless: Defense spokesman," Xinhua, February 25, 2010, http://news.xinhuanet.com/english2010/china/2010-02/25/c_13187564.htm; "China is victim of cyber attacks: spokesman," Xinhua, March 30, 2012; "Defense Ministry spokesman Geng Yansheng's press conference on February 28, 2013," Ministry of National Defense of the People's Republic of China, March 5, 2013.

For quasi- and non-authoritative denials, see Meng Yan and Zhou Yong, "Annoying and Yet Ludicrous 'Hackers," *People's Daily* (Overseas Edition), February 22, 2013, translated by OSC, CPP20130222787001; Wang Tian, "United States Exaggerates China is Starting 'Internet Cold War," *People's Daily*, December 16, 2011, translated by OSC, CPP20111216702004; "Commentary: Pentagon's annual China military report exposes U.S. Cold War mentality," Xinhua, May 18, 2012; Lu Desheng, "False assessment of China's military power will only damage Sino-U.S. relations," *Liberation Army Daily*, May 21, 2012; and "US main source of cyberattacks against China," CCTV.com, 2013, http://english.cntv.cn/special/cyber_attack/homepage/index.shtml.

[xli] For example, see "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 13, 2013," Ministry of Foreign Affairs of the People's Republic of China, June 14, 2013. Also see Zhong Sheng, "Do Not Treat Cyberspace as a War Theater; Avoid Harming Others and Damaging Oneself," *People's Daily*, February 27, 2013, translated by OSC, CPP20130227702002: "Since last year [2012] there has been a nonstop din from American research institutions, media, and enterprises hyping up the "theory of the Chinese cyber threat," and US intentions in erecting investment and trade barriers, blackening China's image, and sabotaging China's development environment have been laid bare."

[xlii] "Defense Ministry spokesman Yang Yujun's regular press conference on June 27, 2013," Ministry of National Defense of the People's Republic of China, July 2, 2013.

[xliii] Zhong Sheng, "To Defend 'Freedom', or to Defend Hegemony?" *People's Daily*, January 26, 2010, http://english.peopledaily.com.cn/90001/90780/91343/6879251.html. Zhong Sheng also emphasizes, in the aftermath of the Snowden leaks, that Washington "is obligated to give the necessary explanation, in the manner of seeking truth from facts, of cyber attacks and so on carried out by the US Government agencies concerned." It additionally states that "[a]ll countries . . . should not say one thing and do another, and still less can they adopt fraudulent methods of a thief crying stop thief." Zhong Sheng, "HK Handles Snowden Case in Accordance with Law," *People's Daily*, June 24, 2013, translated by OSC, CPP20130624787001.

[xliv] As a particularly nasty example of the alleged U.S. double standard, one AMS researcher asserts that "the United States has on the one hand carried out large-scale hacking against China and stolen political, economic, technological, and military intelligence, while on the other it has frequently made a fuss in international circles about 'Chinese hackers'." The same source states that "under the premise of lacking evidence, it has fabricated rumors to smear the Chinese government and armed forces, and blacken China's image . . . In a certain sense, the United States has degenerated from an 'example of human rights' into an 'eavesdropper,' a centralized 'manipulator' of the international Internet, and a mad 'invader' of other countries' Internet." Wang Xinjun, "The 'Prism' Program: Who Should Be More Expressing Dissatisfaction?" *People's Daily* (Overseas Edition), June 25, 2013, translated by OSC, CPP2013062578700.

[xlv] Lu Desheng, "US Military Looking for New Excuse To Use Force Abroad—Pentagon To Announce First Cyber Strategy," *Liberation Army Daily*, June 8, 2011, translated by OSC, CPP20110608787015. See also Shen Yi, "US Cyber Diplomacy Is to Hold the Old Wine With a New Bottle," *Liberation Army Daily*, May 2, 2012, translated by OSC, CPP20120502787009. Also see Si Zhuang, "'Double Standard' Not Accepted in Cyber Security." The author states: "In our opinion, the kind of practice—which, on the one hand, loudly calls for abolishing control of the Internet and advocates 'free flow of information' and, on the other, secretly monitors and watches citizens in private; and which, on the one hand, poses as a victim in denouncing other countries for launching cyberspace war and, on the other, organizes cross-border cyber-attack—is not only very hypocritical but also has a ulterior motive."

[xlvi] Lu Jinghua, "U.S. should not hold multiple standards in cyber world," *Liberation Army Daily*, June 18, 2013. For similar arguments in civilian sources, see He Zhenhua, "'Internet Freedom' and 'Smart Power' Diplomacy," *People's Daily Online*, January 25, 2010, translated by OSC, CPP20100127702001; and Si Zhuang, "'Double Standard' Not Accepted in Cyber Security."

[xlvii] "Defense Ministry spokesman Geng Yansheng's press conference on February 28, 2013," Ministry of National Defense of the People's Republic of China, March 5, 2013. Another MND spokesperson also said, "We notice that the U.S. side, on one hand, irresponsibly accused other countries of engaging in cyber attacks, while on the other hand, leave no stone unturned to develop offensive cyber troops"; see "Defense Ministry spokesman Yang Yujun's regular press conference on March 28, 2013," Ministry of National Defense of the People's Republic of China, April 7, 2013." Most recently, General Chang Wanquan, China's minister of national defense, stated at a Pentagon press briefing with U.S. Secretary of Defense Chuck Hagel, "We oppose of having any kind of arms race in the cyber domain, and we oppose of taking use of information and technology to conduct any kind of operation and hostility towards another party in the cyber domain." "Department of Defense Press Briefing with Secretary Hagel and Gen. Chang from the Pentagon," U.S. Department of Defense, Washington DC, August 19, 2013, http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5289.

[xlviii] As one *People's Daily* article asserts: "The United States was the first country to openly introduce the war machine onto the Internet." Yu Xiaoqiu, "Sincerity Is Needed for International Cooperation in Cybersecurity," *People's Daily*, March 1, 2010, translated by OSC, CPP20100301702003.

[xlix] Zhong Sheng, "The United States Bears Primary Responsibility for Stopping Cyber War," *People's Daily*, February 7, 2013, translated by OSC, CPP20130207787011.

[l] Zhong Sheng, "The United States Bears Primary Responsibility for Stopping Cyber War."

[li] "Double-edged sword: US simulated cyber-attack," *People's Daily Online*, March 18, 2008, http://english.peopledaily.com.cn/90001/90780/91343/6375863.html. For similar statements on U.S. cyberwarfare by quasi- and non-authoritative sources, see Su Enze, "A Personal Look at the Innovations in China's Military Theory," *Liberation Army Daily*, December 15, 1998, translated by OSC, FTS19990120001559; Zhong Sheng, "The United States Bears Primary Responsibility for Stopping Cyber War"; Chen Yiming, "Much Arguments over Hackers' War," *People's Daily*, August 5, 2011, translated by OSC, CPP20110805787008; "Military experts share views on 'cyber defense' and national defense," *Liberation Army Daily*, January 6, 2011, translated by OSC, CPP20110107702003; "94 pct of Netizens Support China's Establishment of Cyber Command," *People's Daily Online*, June 29, 2009, http://english.people.com.cn/90001/90776/90786/6688673.html; Wen Xian, "United States Expanding Its Cyber Space Hegemony," *People's Daily*, July 9, 2009, translated by OSC, CPP20090709710009; Meng Xiangqing, "Cyberspace Contention for Supremacy Becomes More Intense," *People's Daily*, July 14, 2009, translated by OSC, CPP20090715710011; Chen Yiming, "US Covertly Building 'Shadow Internet'," *People's Daily*, June 15, 2011, translated by OSC, CPP20110615787005; Yu Xiaoqiu, "US playing dangerous game with 'cyber deterrence'," *People's Daily*, July 26, 2011, http://english.people.com.cn/90001/90780/91343/7452284.html; Lu Desheng, "US Military Looking for New Excuse To Use Force Abroad -- —Pentagon To Announce First Cyber Strategy," *Liberation Army Daily*, June 8, 2011, translated by OSC, CPP2011060878701; Xu Qinghong, Li Daguang, "Cutting Down the Overall Defense Budget in the Next 10 Years and Substantially Increasing Input to New Elite Combat Forces, Why Did the Change by 'Reducing One Thing and Increasing the Other Thing' in the US Military's New Defense Report Show? (sic)" *Liberation Army Daily*, June 28, 2012, translated by OSC, CPP2012062870202; Luo Chaowen, "United States' Intention Is To Seek Absolute Information Superiority—US Military's Cyber Command To Increase From Present 900 People to 4,900 People and To See Its Position Adjusted," *Liberation Army Daily*, in "Summary: JFJB: PRC Professors on Expansion of United States Cyber Command," February 3, 2013, translated by OSC, CPP20130313088002; Zhong Sheng, "Groundless Accusation Harmful to Cyber Security Cooperation," *People's Daily*, November 16, 2012, translated by OSC, CPP20121116787001.

[lii] Lu Desheng, "US Military Looking for New Excuse To Use Force Abroad—Pentagon To Announce First Cyber Strategy," *Liberation Army Daily*, June 8, 2011, translated by OSC, CPP20110608787015.

[liii] Li Hong, "China's Cyber Squad Is for Defense," *People's Daily Online*, May 31, 2011, translated by OSC, CPP20110531702017; also see "Military experts share views on 'cyber defense' and national defense"; "Experts Discuss Prospects of 'Cyber Defense' and National Defense," *Liberation Army Daily*, January 4, 2011, translated by OSC, CPP20110106702001.

[liv] "China's National Defense in 2010," PRC Information Office of the State Council, March 2011, http://www.fmprc.gov.cn/eng/wjb/zzjg/jks/kjfywj/t812036.shtml.
[lv] For example, one AMS analyst asserts that "'cyber defense' should be considered as an important component of the national defense and included in the national defense development." China should "construct the cyberspace strategies which will form a complete system with China's national security strategies and military strategies to provide a top-level guidance for the national development of "cyber defense." It should also "establish military-civilian mechanisms for cyberspace security threat information sharing and early-warning, security management cooperation and attack-and-defense action coordination as soon as possible to form a complete and reasonable cyberspace security mechanism." "Military experts share views on 'cyber defense' and national defense." Another source states that China must "regard building our information security as important a matter as developing the 'atom and hydrogen bombs and one man-made satellite'"; Shen Changxiang, "Information Security—an Important Contemporary Issue," *Liberation Army Daily*, April 4, 2001, translated by OSC, CPP20010404000084. For similar statements on the need for China to develop a cyber military strategy and capability, see "Experts Discuss Prospects of 'Cyber Defense' and National Defense," *Liberation Army Daily*, January 4, 2011, translated by OSC, CPP20110106702001.
[lvi] For example, see "Military experts share views on 'cyber defense' and national defense"; Jing Nanxiang, "Cyber Freedom and Cyber Self-Discipline," *Liberation Army Daily*, December 20, 2011, from "Summary: JFJB on Cyber Freedom and Cyber Self-Discipline for PRC Netizens," translated by OSC, CPP20111221088010; Qin An, "China Should Guard Against Craze for Enlarging Cyber Armies," *Liberation Army Daily*, April 8, 2013, OSC CPP20130409702002.
[lvii] Ministry of National Defense of the People's Republic of China, "China has no cyber warfare troops: spokesman," Xinhua, March 1, 2013, http://news.xinhuanet.com/english/china/2013-02/28/c_132199193.htm.
[lviii] Guo Lei, Gu Caiyu, and Wu Nan, "Why Has China Established Cyber Blue Army," *People's Daily Online* (Overseas Edition), June 27, 2011, translated by OSC, CPP20110627702005.
[lix] "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 14, 2013," Ministry of Foreign Affairs of the People's Republic of China, June 15, 2013.
[lx] See "Foreign Ministry Spokesperson Liu Weimin's Regular Press Conference on February 6, 2012," Ministry of Foreign Affairs of the People's Republic of China, February 7, 2012; "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on Nov 14, 2012," Ministry of Foreign Affairs of the People's Republic of China, November 15, 2012; "Linking hackers' cyber attacks with Chinese government, military groundless: Defense spokesman," Xinhua, February 25, 2010, http://news.xinhuanet.com/english2010/china/2010-02/25/c_13187564.htm; and Yu Xiaoqiu, "Sincerity Is Needed for International Cooperation in Cybersecurity," *People's Daily*, March 1, 2010, OSC CPP20100301702003. It is sometimes not clear if the authoritative Chinese source is referring to the U.S. government or a government-related entity such as the U.S.-China Economic and Security Review Commission when it attributes such motives.
[lxi] "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on March 28, 2013," Ministry of Foreign Affairs of the People's Republic of China, March 29, 2013.
[lxii] See "Annual Report to Congress: Military and Security Developments involving the People's Republic of China 2012," Office of the Secretary of Defense, Washington DC, May 2012, section entitled "Cyber Espionage and Cyberwarfare Capabilities"; and "Annual Report to Congress: Military and Security Developments involving the People's Republic of China 2013," Office of the Secretary of Defense, Washington DC, 2013, section entitled "Cyber Activities Directed Against the Department of Defense."
[lxiii] For the full report, see "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
[lxiv] Zhong Sheng, "Blackening China Can Hardly Conceal the Evil Behavior of the 'Hackers' Empire'," *People's Daily*, May 8, 2013, OSC CPP20130508787003. Zhong Sheng, "The United States Bears Primary Responsibility for Stopping Cyber War," *People's Daily*, February 7, 2013, OSC CPP20130207787011; Zhong Sheng, "Do Not Treat Cyberspace as a War Theater; Avoid Harming Others and Damaging Oneself," *People's Daily*, February 27, 2013, OSC CPP20130227702002.
[lxv] Xu Qinghong, Li Daguang, "Cutting Down the Overall Defense Budget in the Next 10 Years and Substantially Increasing Input to New Elite Combat Forces, Why Did the Change by "Reducing One Thing and Increasing the Other Thing" in the US Military's New Defense Report Show?" *Liberation Army Daily*,

June 28, 2012, translated by OSC, CPP20120628702021. An AMS military researcher similarly argues that the U.S. is attempting "to apply the superiority of U.S. information technology to topple the political power of the hostile nations and maintain U.S. hegemony." Chen Yiming, "US Covertly Building 'Shadow Internet'," *People's Daily*, June 15, 2011, translated by OSC, CPP20110615787005. Also see PD Wang Tian, Wen Xian, and Zhang Yang, "Chinese Representatives to China-US Internet Forum See Internet as Positive Factor in Development of China-US Relations," *People's Daily*, December 10, 2011, translated by OSC, CPP20111210708002; "Summary: RMRB Cites PRC Expert on Expansion of US Cyber Security Force," *People's Daily*, January 30, 2013, translated by OSC, CPP20130130695015. Another observer curiously speculates that, in addition to being part of the effort to strengthen U.S. "supremacy in cyberspace," the U.S. establishment of a Cyber Command "might even be driven by a long-term consideration of setting up a [undefined] 'strategic trap' for potential adversaries." Meng Xiangqing: "Cyberspace Contention for Supremacy Becomes More Intense," *People's Daily*, July 14, 2009, translated by OSC, CPP20090715710011.

A PD source adds a wrinkle to this argument by maintaining that the U.S. is transferring the strategic focus from the traditional military realm to the cyberrealm, where the U.S enjoys clearly superior capabilities, because U.S. strength in the former area is declining in the aftermath of the "anti-terrorist wars." See "Don't Become a Tool of Hegemony, Google!" *People's Daily Online*, January 27, 2010, translated by OSC, CPP20100127702006. The argument that the U.S. emphasis on cyber issues reflects an attempt to compensate for declining capacities in other areas is made by several non-authoritative sources. For example, see "China defense ministry refutes cyber attack allegations," Xinhua, February 20, 2013. The article cites an American studies expert: "As the United States is losing its traditional superiority, the cards it can play are getting fewer and fewer, but accusing China of cyber attacks becomes a new one."

[lxvi] Zhang Yixuan, "US Finds an Excuse for Expanding Its 'Cyber Troop'," *People's Daily* (Overseas Edition), February 4, 2013, translated by OSC, CPP20130204787004; "Chinese experts slam U.S. hacking accusations," Xinhua, February 5, 2013; "China defense ministry refutes cyber attack allegations," Xinhua, February 20, 2013; "China Focus: Chinese media lambaste U.S. hacking allegations," Xinhua, February 22, 2013, http://english.cntv.cn/20130222/107560.shtml.

[lxvii] Most of these criticisms occurred as parts of Chinese responses to the Mandiant report. For a summary of over 20 different alleged U.S. motives for that document, according to Chinese sources, see Timothy Thomas, "China's Cyber Incursions: A Theoretical Look at What They See and Why They Do It based on a Different Strategic Method of Thought," U.S. Army Foreign Military Studies Office, March 2013. Also see "U.S. Main Source of Cyberattacks against China," CCTV.com, http://english.cntv.cn/special/cyber_attack/homepage/index.shtml; "Crossover: Chinese citizens on hacking allegation," CCTV.com, February 21, 2013, http://english.cntv.cn/program/china24/20130221/106873.shtml; Zhang Jingya, "U.S. hacking accusations carry political motive: cybersecurity expert," CCTV.com, April 12, 2013, http://english.cntv.cn/20130412/104309.shtml; Xu Peixi, "The wolf and the lamb," *People's Daily Online*, July 29, 2013, http://english.people.com.cn/90777/8344375.html.

[lxviii] Ministry of Foreign Affairs of the People's Republic of China, "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on March 12, 2013," March 13, 2013.

[lxix] Ministry of Foreign Affairs of the People's Republic of China, "Statement by h. E. Mr. Wang qun, ambassador for disarmament affair of china , at the general debate of the first committee of the 66th session of unga, Oct 7 2011" October 8, 2011, http://www.fmprc.gov.cn/eng/wjb/zzjg/jks/jkxw/t865572.shtml. Also see "Yang Jiechi's Remarks on the Results of the Presidential Meeting between Xi Jinping and Obama at the Annenberg Estate," Ministry of Foreign Affairs of the People's Republic of China, June 9, 2013; "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 14, 2013," Ministry of Foreign Affairs of the People's Republic of China, June 15, 2013.

[lxx] "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on February 20, 2013," Ministry of Foreign Affairs of the People's Republic of China, February 21, 2013. "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 14, 2013," Ministry of Foreign Affairs of the People's Republic of China, June 15, 2013. "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on July 1, 2013," Ministry of Foreign Affairs of the People's Republic of China, July 2, 2013.

[lxxi] Zhong Sheng, "Groundless Accusation Harmful to Cyber Security Cooperation," *People's Daily*, November 16, 2012, translated by OSC, CPP20121116787001.

[lxxii] "Yang Jiechi's Remarks on the Results of the Presidential Meeting between Xi Jinping and Obama at the Annenberg Estate," Ministry of Foreign Affairs of the People's Republic of China, June 9, 2013.
[lxxiii] "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 14, 2013," Ministry of Foreign Affairs of the People's Republic of China, June 15, 2013.
[lxxiv] Deputy Director Qian Xiaoqian of the China State Internet Information Office, quoted in Wang Tian, Wen Xian, and Zhang Yang, "Chinese Representatives to China-US Internet Forum See Internet as Positive Factor in Development of China-US Relations," *People's Daily*, December 10, 2011, translated by OSC, CPP20111210708002. For similar authoritative statements, see "Wang Yi Points out that China and U.S. Should Work Together to Maintain a Peaceful, Safe, Open and Cooperative Cyber Network Environment," Ministry of Foreign Affairs of the People's Republic of China, April 13, 2013; "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on June 3, 2013," Ministry of Foreign Affairs of the People's Republic of China, June 4, 2013; and "Xi Jinping and US President Obama Hold Joint Press Conference," Ministry of Foreign Affairs of the People's Republic of China, June 8, 2013.
[lxxv] For example, Zhong Sheng states that: "Information security has become a global issue and the countering of hackers can hardly do without international cooperation . . . Dialogue and cooperation alone is the only correct way to respond to various global challenges including cyber security." Zhong Sheng, "Groundless Accusation Harmful to Cyber Security Cooperation," *People's Daily*, November 16, 2012, translated by OSC, CPP20121116787001. Also see Zhong Sheng, "Joint efforts needed to improve cyber space rule," *People's Daily*, July 12, 2013. A typical PD article states: "The drafting of the international policy on the Internet should be a matter for the whole world and should strictly follow the "UN Charter" and other internationally acknowledged basic norms." Also see Wang Tian, Wen Xian, and Zhang Yang, "Chinese Representatives to China-US Internet Forum See Internet as Positive Factor in Development of China-US Relations," *People's Daily*, December 10, 2011, translated by OSC, CPP20111210708002; Ding Gang, "China and the United States Should Do Less on Subtraction and More on Addition," *People's Daily* (Overseas Edition), July 13, 2013, translated by OSC, CHO2013071303816688; "Summary: RROE Views Importance of Cyber Security in 'Post Prism Gate Era'," *People's Daily* (Overseas Edition), July 22, 2013, translated by OSC, CHO2013072223516117; and Lu Jinghua, "Cyber Cooperation: The New Converging Point of Interests Between China and the United States," *Liberation Army Daily*, June 15, 2013, translated by OSC, CPP20130617716001.
[lxxvi] Zhong Sheng praised the work of the "UN Information Security Government Experts Group" in June 2013 for "affirming the principle of 'cyber sovereignty' and laying down an important foundation for and pointing out the direction of formulating regulations in the cyber field." Zhong Sheng, "Fill in 'Regulation Blank' in Cyberspace," *People's Daily*, July 9, 2013, translated by OSC, CHO2013070906405359. A PD article cites a military researcher of the National Defense University stating that China proposes "the establishment of a fair and rational cyber international governance organ with the extensive participation of various nations under the UN framework, which opposes all forms of cyber warfare and online arms race as well as hegemony and power politics in the cyber space." "Summary: RROE Views Importance of Cyber Security in 'Post Prism Gate Era'," *People's Daily* (Overseas Edition), July 22, 2013, translated by OSC, CHO2013072223516117; An article in LAD asserts that China should "launch multilateral dialogues and discuss handing over the right of the Internet management under the absolute control of the U.S. to the United Nations (UN). Qin An, "China Should Guard Against Craze for Enlarging Cyber Armies," *Liberation Army Daily*, April 8, 2013, translated by OSC, CPP20130409702002. Also see Zhong Sheng, "Joint efforts needed to improve cyber space rule," *People's Daily*, July 12, 2013.
[lxxvii] Zhong Sheng, "Fill in 'Regulation Blank' in Cyberspace."
[lxxviii] "Commentary: Unprecedented Xi-Obama summit highlights unparalleled task of redefining inter-power ties," Xinhua, June 7, 2013.
[lxxix] Ding Gang, "China and the United States Should Do Less on Subtraction and More on Addition," *People's Daily* (Overseas Edition), July 13, 2013, translated by OSC, CHO2013071303816688. Also see Yang Qingchuan, "Commentary: Don't let cyber security overshadow key China-U.S. dialogue," Xinhua, July 9, 2013.
[lxxx] See "Summary: RMRB Interviews PRC Academic on Stepping Up Cyber Legislation," *People's Daily*, December 24, 2012, translated by OSC, CPP20121224702011; "Summary: Renmin Ribao Interviews PRC Academic on Protecting Information Security," *People's Daily Online*, December 28, 2012, translated by OSC, CPP20121228704008; and "Summary: *People's Daily* Column Calls For 'Legal Boundaries' for Online Platform," *People's Daily*, December 28, 2012, translated by OSC, CPP20121228704009.

[lxxxi] As indicated above, while some Chinese observers address the potential positive aspects of cyberspace, as a new realm for promoting cooperation among nations, economic enterprises, and individuals, the vast majority of Chinese commentary address the threats that cyberactivities present.

[lxxxii] The Obama administration's "International Strategy for Cyberspace" report of May 2011 declared its intention to "promote and enhance multi-stakeholder venues for the discussion of Internet governance issues" in order to preserve the freedom of innovation, expression, and association on the Internet. It also indicated support for venues such as the Internet Governance Forum, "which embodies the open and inclusive nature of the Internet by allowing nongovernment stakeholders to contribute to the discussion on equal footing with governments." See "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," White House, Washington DC, May 2011. Also see "Testimony of Fiona M. Alexander, Associate Administrator, NTIA, before the House Committee on Energy and Commerce, Subcommittee on Communications and Technology," December 14, 2011, http://www.ntia.doc.gov/speechtestimony/2011/testimony-associate-administrator-alexander-icann-s-top-level-domain-name-progr.

[lxxxiii] "Remarks by Lawrence Strickling, Assistant Secretary of Commerce for Communications and Information, National Telecommunications and Information Administration, Department of Commerce, before the PLI/FCBA Telecommunications Policy & Regulation Institute," Washington, DC, December 8, 2011, http://www.ntia.doc.gov/speechtestimony/2011/remarks-assistant-secretary-strickling-practising-law-institutes-29thannual-te. Also see "Defending an Open, Secure, Global, and Resilient Internet: Independent Task Force Report no. 70," Council on Foreign Relations, June 2013; and Lennard G. Kruger, "Internet Governance and the Domain Name System: Issues for Congress," Congressional Research Service, Washington DC, April 23, 2013.

[lxxxiv] In the words of one knowledgeable specialist: "The U.S. government has presented [to Beijing] highly detailed technical evidence of the Chinese origins of the intrusions . . . [including] very precise attribution of a number of high-profile intrusions." Moreover, according to the same individual, the Mandiant report "provides dozens of pieces of non-IP address evidence of [Chinese intrusions]." Private correspondence, James Mulvenon, Vice President of Defense Group, Inc.'s Intelligence Division, August 14, 2013.

[lxxxv] For a brief discussion of this issue, see Hal Stevens, "Does the U.S. Indirectly Control the Internet?" Networkequipment.net Blog, February 21, 2011, http://networkequipment.net/2011/02/21/does-the-us-indirectly-control-the-internet/. Also see Lennard G. Kruger, "Internet Governance and the Domain Name System: Issues for Congress," Congressional Research Service, Washington DC, April 23, 2013.