Managing Asymmetries in Chinese and American Cyber Power
Author(s): Greg Austin
Source: *Georgetown Journal of International Affairs*, International Engagement on Cyber IV (2014), pp. 141-151
Published by: Georgetown University Press
Stable URL: https://www.jstor.org/stable/43773657
Accessed: 06-05-2020 02:58 UTC

Managing Asymmetries in Chinese and American Cyber Power

Greg Austin

The need for cyber détente between the United States and China in cyber space is spelled out in a 2012 policy paper by the EastWest Institute (EWI).[1] It argued that both countries want some reduction in tension over military and political activities in cyberspace, and called out the asymmetry of power between the two countries in cyberspace as an important aggravating factor in the relationship. The paper advocated clarification of military strategic concepts of information dominance and preemption. At the Munich Security Conference in February 2013, an EWI briefing went further. It identified an urgent need at the global level to shape new understandings of strategic stability in cyber space by arguing that powerful states were driving for the technological frontier in military cyber capabilities, but paying little attention to the impact of such a push on the insecurities of their potential enemies or rivals. The briefing argued for "an explicit commitment by states to strategic stability in cyberspace within the framework of a fully articulated foreign policy and national security doctrine." In light of the sustained attention to China's recent cyber espionage inside the U.S. government and in the public domain, this short article expands on one question central

Greg Austin is a Professorial Fellow at the EastWest Institute, focusing on cyberspace and defense policy. He previously served as Vice President for the Worldwide Security Initiative, and is an author and editor of five books on China, including his most recent work, *Cyber Policy in China*.

to the problem: How does China view the United States' drive for dominance in cyber military power? This article argues that China views this as a threat to its security in a fundamental and game-changing way that undermines the possibility of a shared vision of stability in broader geopolitical relations. Many in the United States feel much the same way about China's emerging cyber power, though with less justification, given China's backwardness relative to the United States.

This article draws a sharp picture of China's "cyber" security dilemma. While there are useful analyses of where cyber military capability sits in China's strategic vision, most only briefly touch on China's sense of insecurity in the military cyber domain and how the fear of United States' cyber superiority could be driving China's plans.[2] This article takes the view that even as China may have closed the gap in some conventional military armaments between it and the United States, the gap in cyber warfare capability has probably widened. While we need much more information to reach a confident assessment, on the basis of available evidence, this author is inclined to agree with Desmond Ball's assessment that China's military leaders must be in a state of "despair at the breadth and depth of modern digital information and communications systems and technical expertise available to their adversaries."[3] Ball, who has worked for more than two decades researching the signals and intelligence capabilities of both the United States and China, has assessed that "China is condemned to inferiority in IW [information warfare] capabilities for probably several decades."

The United States and its allies exchange sensitive cyber technologies with each other in ways that not only exclude others, but in ways that are intended to maintain cyber superiority in as many domains as possible...

U.S. Cyber Dominance. China is now the biggest manufacturer of desktop computers, and recently claimed the position of building the fastest supercomputers in the world. There are other indicators of China's increasing capability in cyberspace, not least its espionage and its domestic surveillance. But Americans' invention and U.S. corporations' global commercialization of the internet, coupled with U.S. economic power and unchallenged pre-eminent position in advanced science, information and communications technology guaranteed its position as the single most powerful country in terms of wealth and power generated from the cyber domain. Beyond its pre-eminence in the civilian sector, the United States has a military strategy premised on "information dominance." It has been leading the world in developing information dominance as a military strategy, with associated weaponry, dedicated units, and dedicated planning elements in the Pentagon: the uniformed services and the intelligence agencies.

The United States sees itself as "pre-eminent in the fields of Intelligence, Cyber Warfare, Command and Control, Electronic Warfare and Battle & Knowledge Management," in the words of the Deputy Chief of Naval Operations for Information Dominance.[4] This military cyber power has combined with the country's pre-eminent conventional and nuclear forces, its superior economic power (twice the annual GDP of the nearest competitor), its global supremacy in the ICT industry, and its unequalled scientific capability to entrench in global affairs the "unipolar moment," a term coined in 1990.[5] This meant then, as now, that the United States is the lone superpower in world affairs.

This position is reinforced by the alliance relationships that the United States has established. In his very first observation about this unipolarity, the concentration of geopolitical gravity in the United States, Krauthammer included the Western alliances as a primary foundation of that power.[6] At that time, these included NATO members, Japan and Australia. Since then NATO has expanded, at the same time as countries like South Korea and Saudi Arabia, both members of the G20, have become solid allies of the United States on global issues beyond their own regional concerns. NATO is now actively cooperating on cyber defense with around ten countries outside its 28-member state alliance. This expansion of the American alliance base is central to understanding the political economy of the cyber world in the second decade of the 21st century and how China sees it. The largest flows of finance, investment, trade, and technology are still amongst the United States and its allies. This historically unprecedented suite of alliances entrenches the strategic power of the United States in the cyber realm relative to all countries outside that alliance. The United States and its allies exchange sensitive cyber technologies with each other in ways that not only exclude others, but in ways that are intended to maintain cyber superiority in as many domains as possible, whether it be military, technological, or commercial.

Countries outside the alliance include China, Russia, Brazil and India. The degree of exclusion from the alliance system varies for each of these. India has recognized the power of this alliance and is campaigning to be seen as a "like-minded country." It has secured the support of key Americans to be brought into the fold as an ally in cyber policy. For China, the picture is very different. From the point of view of many in the United States, China (like Russia) is definitely a "cyber adversary." This case is made in a number of places. One of the most prominent has been the 2011 report of the National Counter-Intelligence Executive.[7] The report observed that China and Russia see themselves as "strategic competitors with the United States," and "are the most aggressive collectors of U.S. economic information and technology," relying heavily on "open source information, human intelligence (HUMINT), signals intelligence

(SIGINT), and cyber operations—to include computer network intrusions and exploitation of insider access to corporate and proprietary networks." Their purpose, the report suggests, is to advance their own "national security and economic prosperity" by gaining a "competitive edge over the United States and other rivals."[8] In his 2013 State of the Union address on February 12, President Obama used the term "our enemies" without naming China only two days after leaked reports of a new National Intelligence Estimate singled out China as the most serious threat to the United States in cyber space.

In the cyber world, China—weak in cyber military power—has no cyber capable allies, except maybe Russia.[9] The United States—stronger in cyber military power than any other country—has at least twenty.[10]

China is concerned not just that the United States may have better cyber warfighting capabilities than China does, but that it can be used creatively as part of the total force package for strategic effects in other areas of war-fighting, the economy, and politics.

How Good is China's Military Cyber Capability relative to the United States?

Strategic stability as a public good may be an illusion in situations where the most powerful states can be divided into groups which contest fundamental political doctrines and values, and where development and deployment of advanced military technology and powerful armed forces to weaken or deter other states remains a primary goal. Yet for five centuries, the idea of strategic stability has proven to be a useful illusion. It sustained the idea that states can craft a sense of mutual satisfaction with geopolitical realities and contain the urge to further militarize and heighten military confrontations. The concept was always more political, and comparisons of military capabilities between rival countries was only ever one part. In fact, the idea of stability was not so much intended to contain improvement of capabilities as it was to shape military competition to make it more predictable, transparent, and to link it to political goals. The most serious manifestation of strategic instability in 2014 between the United States and China is the absence of mutual satisfaction with geopolitical realities in cyberspace and the concern that new cyber military capabilities may have undermined previous tendencies toward tension reduction by altering pre-existing assumptions of military power.

In this regard, it is important to understand that China (like the United States) does not see cyber military power as a question of computer versus computer, network versus network, or hacker versus hacker. China sees cyber military power as the leveraged relationship between military cyber assets and other forms of military power. This approach is described well in the following definition of 'cyber conflict': "broader than cyber warfare, including all conflicts and coercion between nations and groups for strategic purposes utilizing cyberspace where software, computers, and networks are both the means and the targets."[11]

Yet even if one limits the assessment of relative cyber military power just to China and the United States, it is plain not just that the United States is well ahead, as discussed below, but that it has used this to change the leveraged relationship between military cyber assets and other forms of military (and political) power.

In understanding this, we should not be distracted or overly preoccupied by China's cyber espionage. According to U.S. public and private sources, China appears to have scored some big successes in cyber espionage. By comparison, it is unknown how good the Americans have been. The Chinese successes suggest that the United States' defenses against some espionage are quite weak. Yet espionage is only a small fraction of the total picture of cyber military power.

How do we understand Chinese and American relative capabilities and the sense of insecurity created by the leveraged application of cyber military assets for strategic stability? There is not a detailed, public domain assessment of U.S. cyber military power, let alone a net assessment relative to China, leaving aside the impact of cyber assets on U.S. strategic planning in areas like nuclear strikes. In discussing the question with former U.S. senior military officers, the following determinants of United States military cyber power were judged to be essential reference points for understanding, and also to be seriously lacking in China's case:

- A strong tradition of joint operations refined in combat operations around the globe, almost non-stop since the Goldwater Nichols Act of 1986, but taking hold in the second half of the 1990's.
- Long experience of direct application of cyber operations in combat, beginning most notably in 1999 against Yugoslavia.
- An advanced private sector, with appropriate incentive mechanisms, to provide contractor services in military applications of IT.
- Access for unilateral purposes to a large talent pool of government technical staff, intelligence and university-based researchers from across its global alliances.
- The human and technical intelligence collection capabilities needed for effective cyber offensive operations against military targets.[12]

China's 2010 National Defense White Paper demonstrates how good China thinks its information warfare capability is. Addressing only the first point above, it notes that China has obtained only a "preliminary level" of interoperability between different elements of its armed forces within this sphere.[13] If China is weaker in joint operations, then it is weaker in cyber war capability. The corollary of that statement is that China sees itself as weak in joint operations, and so it sees its failure in military cyber power relative the United States. Some of the best informed American sources with knowledge of China's capabilities have concurred with this broad-brush assessment in discussions with me. China's armed forces are well short of their military cyber goals relative to the United States.[14]

China also sees itself as weaker and more dependent on the United States for development of the civilian cyber sector, which underpins the country's military cyber power. China definitely sees itself as lagging well behind in civil technology and protection of civil assets from U.S. cyber attacks. It knows how difficult it is for a country to achieve a level of technological preparedness in its armed forces that is significantly different from the technological foundations of the society as a whole (talent base, R&D climate, investment levels). A number of Chinese and international studies have consistently ranked China fairly low in terms of advanced cyber information technology.[15]

One element that needs to be factored into an assessment of Chinese perceptions of its relative capability in cyberspace is its sense of vulnerability to cyber-enhanced attacks. China is concerned not just that the United States may have better cyber warfighting capabilities than China does, but that it can be used creatively as part of the total force package for strategic effects in other areas of war-fighting, the economy, and politics. As much as the United States has been concerned about Chinese cyber intrusions into U.S. critical infrastructure, China shares similar concerns. Its government and its researchers have moved much more slowly that the United States in addressing cyber threats to its critical infrastructure.

As with the issue of cyber espionage being something of a distraction from the core issue of relative cyber military power in Chinese eyes, the prominence accorded by Western observers to Chinese attacks on civil infrastructure is also not the core issue. Such attacks are a threat and would affect military capability, but China (like the United States) does not see civil infrastructure as the main game in cyber warfare or in assessments of relative cyber military power. For China, the main focus is capability in all aspects of the military domain, referred to by Americans as C4ISTAR (command, control, communications, computers, intelligence, surveillance, target acquisition, reconnaissance). China focuses on assessing and defending against U.S. capabilities to degrade China's C4ISTAR in three fields: strategic nuclear operations, theatre missile operations against Taiwan or Japan, and conventional operations.

China is seriously planning for cyber warfare operations against the United States, and possibly more so than it is preparing for naval or air combat operations. China's cyber warfare capability is probably far more powerful but less lethal than its conventional military capabilities. That suits China enormously in both respects. China's military strategy is highly defensive, but to defend against possible U.S. operations against it over Taiwan, China has to rely mainly on unconventional operations, and these include cyber operations as well as psy-ops of the classic kind. In November 2012, China announced it would speed up the informatization of its armed forces, a term that includes both military operational cyber dimensions as well as more basic computerization of the military. In February 2014, China announced it would do everything necessary to become a cyber power. In June 2014, China officially established a Cyberspace Strategic Intelligence Research Center in its General Armaments Department.[16]

What to Do? "Strategic Cyber Stability" Talks. The reduction of military tension between China and the United States and the establishment of some mutual predictability in their military planning is an agreed aim of both countries.[17] The negative impact on this goal of the asymmetry of power between the United States and China has not been comprehensively analyzed. Above all, there is a structural dilemma. States expect negotiations to result in reciprocal obligations, and in many cases these are unconsciously conceived as being equal or symmetrical in some way. For example, arms control agreements between the USSR and the United States were premised on strategic equivalence in which each side would adjust its forces in different ways judged to produce an overall, mutually acceptable outcome. The two sides accepted differences in numbers of particular strategic nuclear systems (land, sea or air) as long as the total number of warheads was equivalent and key strategic concerns of the other side were addressed. However, states do not have any agreed understanding of strategic equivalence or strategic stability in the cyber age. There is little understanding of how strategic stability might be achieved between adversary pairs so visibly separated by a large, military cyber asymmetry.

As foreshadowed by Joseph Nye and Bill Owens in 1996,[18] there is not even wide acceptance of a fundamental reality that cyber warfare capabilities affect strategic nuclear warning time, classic notions of deterrence, and second strike capability. Fortunately, there is a private view in some senior U.S. military circles that the United States should abandon pre-emptive (first strike) aspects of its cyber war doctrines, and move to a doctrine of strategic stability in cyberspace. In cyberspace, such a doctrine may be the closest we can get to the doctrine of strategic parity, which in the Cold War was one of the primary concepts underpinning the reduction of the risks of nuclear war.

China is seriously planning for cyber warfare operations against the United States, and possibly more so than it is preparing for naval or air combat operations.

A landmark 2011 study from the Carnegie-Tsinghua Center for Global Policy on China's reactions to the most recent U.S. nuclear posture review canvassed the new importance placed by China's leaders on the concept of strategic stability.[19] The report advocated the opening of dialogue with China on what strategic stability between it and the United States might mean. While the report noted that Chinese sources see this as the main characteristic of the military relationship between the United States and China, there is no direct mention of the impact of cyber weapons on Chinese or American views of their relationship.

The United States does appear to have a choice: maintain its doctrine of information dominance and cyber pre-emption, thereby threatening many of the diplomatic gains in U.S.-China relations of the last 15 years, or begin talking to China about what a new posture of "mutual" security in cyber space would like. The task will be massively difficult, given the high sensitivity of the issues and the highly compartmentalized character of expertise on cyber warfare issues as they affect strategic stability. This engagement would not be about counting missiles that can be photographed from space or making technical assessments of missile range and readiness levels. This would be about finding confidence-building measures at a political level that can accommodate the complexities not just of cyber warfare, but also of the broader China-U.S. strategic relationship. The linkage made by senior U.S. officials between China's cyber espionage and the entire fabric of U.S. economic and industrial competitiveness imposes an even bigger burden on that relationship than that imposed by linking a country's human rights policies and American preparedness to conduct normal diplomatic relations. The cyber asymmetry is causing something akin to a cosmic disturbance in bilateral diplomacy, for which officials on both sides have few responses. While cybersecurity might be one of a long list of bilateral issues, a case could be made that it has morphed into an overarching fundamental reality in the past decade. The core diplomatic challenge of the bilateral relationship is how to manage persistent asymmetries in cyber military power between China and the United States because it so fundamentally affects the main security interest of both sides.

Several commentators have observed that China's massive use of cyber espionage against foreign cyber assets, civil infrastructure, and military technologies may be related to its relative weakness. One point often not canvassed is the incentives that China would need to see on the table for it to even consider some abatement of its current activities. The even tougher question is what would abatement look like in an environment where China's rivals are not showing any interest in curtailing their own espionage, and there is interest in maintaining doctrines of pre-emptive cyber-strike and "information superiority." In March 2014, U.S. Defense Secretary Chuck Hagel, said in remarks at the National Security Agency that "outside of government networks," the United States would exercise restraint in cyber space, and was urging other states to do the same.[20] But this does not address the cyber power asymmetries between China and the United States.

The 2013 U.S.-China working group on cyber security, now suspended after recent U.S. indictments of five Chinese uniformed personnel for industrial espionage, was a useful start. Yet the working group came after a decade of confrontation in cyber space, and probably incorporates the wrong people to address the two countries' asymmetries of cyber power. The 2012 agreement between Russia and the United States that added a cyber warning component in their bilateral nuclear risk reduction center is a useful precedent, but its value is weakened in the China case because of the approximate parity of the nuclear arsenals of both sides. The U.S.-Russia agreement is premised on recognition of the direct link between cyber war capability and strategic nuclear stability. Similarly, to make progress in the U.S.-China case, both sides need to recognize that the military cyber domain is not independent or a discrete component of military power. Cyber power has redefined military power, and China is very weak. How can the United States ease this security dilemma for China? How can China come to accept that its actions, though defensible in many ways, discourage the United States from cooperative behavior on military aspects of cyberspace?

There is only one answer. Both countries have to agree on a shared concept of sufficiency of defense in cyber space; they have to agree on how cyber capability affects strategic nuclear capability and conventional force readiness; and they have to commit to measures of mutual restraint in civil and military uses of cyberspace. That is a huge and protracted agenda. But in the absence of this vision as the end point, any bilateral cyber dialogue, including by well-meaning NGOs and research institutes, will be fruitless. Refusal to commit to such a vision by both sides or by just one of them—which means acceptance of the belief that strategic superiority is achievable and meaningful for nuclear-armed countries—would negate 40 or 50 years of progress in security thinking, and may undermine everything that we achieved in our understanding of strategic self-sufficiency and mutual security.

Continuing reliance on expectations of reciprocity and of equivalence may be not only misplaced but a threat to peace. This may be more relevant to the strategic approach of China than that of the United States, but heavy reliance by either state on an assumption of strategic equivalence of cyber military power and a demand for a resulting policy reciprocity will become a serious threat to mutual security. For Chinese leaders, the cyber military capability of the United States, attended by its dozens of cyber allies, has irreversibly and fundamentally transformed pre-existing assumptions of strategic stability and China's security, because this has enhanced the United States' global military and economic pre-eminence.

Disclaimer: This article represents the views of the author and not necessarily those of the EastWest Institute.

NOTES

[1] Austin and Gady, "Cyber Détente between the United States and China: Shaping the Agenda".

[2] See for example, Magnus Hjortda, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", Journal of Strategic Security, Volume IV, Issue 2, 2011, pp. 1-24. Annual reports by the United States Department of Defense to Congress on military developments in China offer useful and balanced comments on some aspects of China's military cyber capability but do not address China's sense of cyber insecurity as a dominating reality of its military planning. For some treatment of this issue,see Greg Austin, Cyber Policy in China, Polity, 2014 (forthcoming), chapter five.

[3] Desmond Ball, "China's Cyber Warfare Capabilities", Security Challenges, Vol. 7, No. 2 (Winter 2011), pp. 81-103, p. 101.

[4] "The U.S. Navy's Vision for Information Dominance", May 2010, p.1, http://www.insaonline.org/assets/files/NavyInformationDominanceVision-May2010.pdf.

[5] This phrase was coined by Charles Krauthammer, "The Unipolar Moment", Foreign Affairs, Vol. 70, No. 1, America and the World (1990/1991), pp. 23-33.

[6] He wrote: "The center of world power is the unchallenged superpower, the United States, attended by its Western Allies" (p. 23).

[7] United States. Office of the National Counter Intelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011", October 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[8] Ibid. p. 4.

[9] A senior Russian official told me that Russia views China as less trustworthy in cyberspace than the United States.

[10] This point needs considerable analysis beyond the scope of this paper since the way alliances play out in cyberspace is very different from traditional patterns. At one very simple level for example, sharing of information with allies is much less common than it is for conventional military capabilities and plans.

[11] Healy 2010 but replayed in the authoritative CSSA report "Addressing Instability in cyberspace", 2010.

[12] For arguments on similar themes, see the briefing by Oxford Analytica, "China Will Speed Up Military Cyber Development", November 14, 2012.

[13] "A preliminary level has been achieved in interoperability among command and control systems, combat forces, and support systems, making order transmission, intelligence distribution, command and guidance more efficient and rapid. Strategic planning, leadership and management of informationization have been strengthened, and relevant laws, regulations, standards, policies and systems further improved. A range of measures, such as assembly training and long-distance education, have been taken to disseminate knowledge on information and skills in applying it. Notable achievements have been made in the training of commanding officers for joint operations, management personnel for informationization, personnel specialized in information technology, and personnel for the operation and maintenance of new equipment. The complement of new-mode and high-caliber military personnel who can meet the needs of informationization has been steadily enlarged."

[14] One diagnostic indicator cited by two sources was United States' superiority in space-based assets, which they regarded as absolutely central to effective cyber operations at the strategic level of war.

[15] This was the conclusion of a 2011 study by the Chinese Academy of Sciences, Information Science and Technology in China: A Roadmap to 2050. The study also registered broad agreement, though in visible disappointment, with a set of IT competitiveness rankings by The Economist that placed China 50th in global terms, out of 66 countries surveyed. See Li Guojie (ed.), Information Science and Technology in China: A Roadmap to 2050, Chinese Academy of Social Sciences, Science Press, Beijing, Springer, 2011, pp. 20-21. A similar view can be found in the World Economic Forum's 2014 Network Readiness Index (NRI), which had China sitting at 61st in world rankings for its use of information technologies to advance its national competitiveness and its citizens' lives. China had slipped from 36th in the 2011 rankings. The NRI gives only a partial picture of China in cyber world but it mirrors quite critical sentiment within the country about its weak position relative to others. The United States, Japan, Singapore, Taiwan, South Korea and Malaysia are all ahead of China in the 2014 NRI. See World Economic Forum, The Global Information Technology Report 2014, April 2014, http://www.weforum.org/reports/global-information-technology-report-2014. See also Austin, Cyber Policy in China, chapter four.

[16] Chinamil.com, "PLA Cyberspace Strategic Intelligence Research Center founded", 30 June 2014. http://eng.chinamil.com.cn/news-channels/china-military-news/2014-06/30/content_6025789.htm

[17] There are sound reasons for this originating in policy and academic analysis. On the scholarly side, as outlined so aptly by Jack Snyder and Barry Posen in their 1984 books, The Ideology of the Offensive and The Sources of Military Doctrine, a state with offensive doctrines, and an institutional disposition to offense, is more likely to miscalculate in favor of a decision for war than states with defensive postures and an institutional disposition to defense.

NOTES

[18] As observed in a famous 1996 article in Foreign Affairs by Professor Joe Nye and Admiral William Owens, "The information technologies driving America's emerging military capabilities may change classic deterrence theory." Joseph F. Nye Jr and William A. Owens, "America's Information Edge", Foreign Affairs, 1996 (March/April), http://www.foreignaffairs.com/articles/51840/joseph-s-nye-jr-and-william-a-owens/americas-information-edge.

[19] Lora Saalman, "China and the U.S. Nuclear Posture Review", Carnegie-Tshinghua Center, Carnegie Endowment for International Peace, Beijing, Feb 2011, See http://carnegieendowment.org/files/china_posture_review.pdf/.

[20] Jim Michaels, "Hagel encourages 'restraint' in cyber warfare", USA Today, 28 March 2914, http://www.defensenews.com/article/20140328/C4ISR-NET07/303280032/Hagel-encourages-restraint-cyber-warfare.