



China: On the March to Virtual Conflict

American Public University System

American Military University

Department of Security and Global Studies

Charles Town, WV 25414

<http://www.amu.apus.edu>



David A Schroeder

david.a.schroeder@navy.mil

david.a.schroeder2@us.army.mil

<https://www.intelink.gov/wiki/das>

November 2010



Topic

How can China be expected to expand its cyber and information warfare efforts against the US?

Purpose Statement

The purpose of this paper is to perform a basic examination the scope and intent of Chinese cyber and Information Warfare (IW)/Information Operations (IO) efforts and capabilities. In US doctrine, these include all “actions undertaken to affect adversary information and information systems [...] in order to affect the information-based process, whether human or automated.”

Thesis Statement

China is a state in transition, and the evolution and expansion of its cyber and IW capabilities are seen by China as an important part of that transition.

Statement of Problem/Research Question

What are the core motivations for China’s enhancement of its IW capabilities, beyond simple military modernization, and why does China view this as important?

Hypothesis

China will continue to expand and enhance its Information Warfare capabilities because such capabilities will enable it to skip a costly generation of military-industrial modernization, and will enable it to carry out effective conventional and asymmetric warfare against information-dependent states, such as the United States.

"I think that we should start to consider that regret factors associated with a cyber attack could, in fact, be in the magnitude of a weapon of mass destruction." (USCC 2007)

– General James Cartwright, USMC
Vice Chairman, Joint Chiefs of Staff

"Cyber is more important [...] right now than nuclear." (Ross 2010)

– Admiral Gary Roughead, USN
Chief of Naval Operations

Significance of the Study

While there is a good deal of speculation on Chinese motivations in the cyber realm, there is very little solid information. Verifiable information from within China is scarce, so much of the current US and Western literature is the result of a review of Chinese literature — with the worrying proposition that such literature could, itself, represent a purposeful manipulation of information!

China's cyber warfare activities have been a popular topic in the information security, defense, and intelligence media. This has overflowed into the mainstream media, with many journalists taking notice of suspected Chinese hacking attacks, and the perceived increase in such phenomena in relation to China. The notion that China is looking to expand its capabilities in these areas — and has perhaps even already been behind attacks, or incidents that may be "testing the waters" — is nothing new. However, mainstream coverage has largely looked to the externally visible activities, and not to the

core motivations. Looking to these motivations may reveal a more fundamental driving philosophy beyond simple modernization. This is where a gap in the current understanding lies.

Introduction

In order to address the question of the nature of China's IW aspirations, this study will employ a qualitative case study approach. Because these questions are somewhat subjective with respect to IW, they will rely on current doctrine, practices, and theory within IW communities. The efficacy of IW in the context of both independent variables of the hypothesis will be shown, or can be discounted.

This research aims to answer difficult questions about a society that has been historically closed, and one that closely guards its military and intelligence plans and capabilities. However, there is indeed expertise on the subjects at hand, mostly in the form of military experts, academics, and practitioners in the study of China and IO/IW.

This study would employ the purposive/judgmental or expert choice method of sampling. The pool will be limited, and will consist of literature on IO/IW, Chinese military history, current Chinese military capabilities, Chinese strategic interests, US information vulnerabilities, and similar. The sample will include literature with a differing range of research and variance in opinions to most effectively answer the question.

The key element of research is literature dealing specifically with Information Warfare, Information Operations, Information Security, and related areas. This literature may help describe any relationship between China's ostensible motivations for pursuing IW via the intersection with current broader thinking on IW topics. Such works to be consulted will

be respected anthologies of IO/IW theory, such as those compiled by various organizations such as RAND (Khalilzad et al. 1999, Arquilla et al. 1997) and the National Institute for Strategic Studies (Alberts et al. 1997), individual publications often referenced in studies of IO/IW, and government reports analyzing information vulnerabilities and cyberwarfare (Hildreth 2001).

A pattern-matching analysis will be conducted to determine the veracity of the hypothesis. Elements from literature and media reports will be compared against the variables in the hypothesis. Such an analysis will either support or disprove the linkages in China's assumed motivations for continuing to aggressively pursue the expansion of its Information Warfare capabilities. An understanding of these motivations can help shape US policy and response to any threat that may exist.

Background

China is a state in transition, and the evolution and expansion of its Information Warfare (IW) capabilities are an important part of that transition. There has been a fair amount of attention in the mainstream press to hacking incidents and alleged Chinese breaches of US computer systems. However, because of the shadowy nature of espionage and the realm known as Information Operations (IO), these incidents are often viewed as isolated, and there has not been a broad focus on China's overall efforts in this realm. The United States has comfortably and decisively held a technological edge for generations in many areas. The application and manipulation of information to military ends is no exception, and the United States has not felt particularly threatened on this front. Consequently, the

threat from China is viewed in a tactical rather than strategic sense, and has not received the attention it perhaps deserves.

Another complicating factor is that IO spans several arenas, from the purely technical to the social and psychological. The goals and missions of IO and intelligence in general, particularly against and within non-free societies, will constantly be at odds with the democratic nature of the United States and the West. Even so, the United States currently doesn't appear to acknowledge the scope of the information campaigns China has executed against it. The thought in some circles that China isn't the danger others believe it to be is apparently proof that China's long-standing information campaigns to convince Americans of just that appear to be working quite well. China's motives are strategic rather than tactical in nature; that is, they do not necessarily serve any direct or immediate specific purpose, but rather serve to create influence in its own favor over long periods of time. For this reason, many in the US see China as something of a misunderstood ally, while China simultaneously builds out its military capability.

While cyber warfare is now routinely considered in various analyses of China and other nations, the larger question of why China is so diligently pursuing this path is overlooked. China's activities in this realm are assumed to be part of a natural technological progression. However, a study of literature examining China's efforts in Information Warfare viewed against the backdrop of the importance of the Information Revolution which is sweeping the globe paints a picture of a nation looking to the information realm as a critical and key mechanism to modernize its military capabilities. Similar to how the Industrial Revolution ushered in a new era and greatly enhanced nations' abilities to wage war, the Information Revolution again could change the face of conflict. China's

motivations for expanding its cyber warfare capabilities against the United States may transcend that of simple technological evolution, and warrant a deeper examination. Why, then, can China be expected to expand its Information Warfare capabilities, particularly with respect to the United States?

Theoretical Framework

Learning about the internal motivations of the leadership of a nation, particularly in a military context, is more difficult in a closed society than it is in the open democracies and the relatively transparent governments of the West. Thus, any objective studies of the state of Information Warfare (IW) philosophy and strategy in China are limited by this inherent secrecy. Still, as the Chinese military works to create a global reach and as China's academics and theoreticians increasingly participate in the world community, clues about China's aims in this realm have begun to reveal themselves.

The gap in the literature in the study of the question of China's motivations is largely due to the disconnect between the dependent factor of the general state of China's Information Operations (IO)/Information Warfare (IW) capabilities, and the independent factor of whether the Information Revolution's impact on military operations represent a Revolution in Military Affairs (RMA). If the impact of information on military operations constitutes such a dramatic change — akin to, e.g., the RMA associated with the Industrial Revolution — then China's view of the benefits of bolstering its information capabilities is further supported.

Thus, any study of this question must strive to bridge the gap between modern thought on Information Warfare and its impact on military operations, and China's motivations with

respect to the same. Another consideration relates not only to the actual impact of Information Warfare on military operations, but China's *belief* with respect to this impact, even if it ultimately ends up being incorrect. The belief can still explain motivations for following a particular course of action. Because consideration for the total information realm is still relatively new to military affairs, this is still a learning experience for all involved (Toffler 1997).

Another gap relates to the independent factor of whether Information Warfare capabilities enable asymmetric capabilities against militaries or societies more dependent on information technologies. While literature exists addressing the potential application of asymmetric information attacks by small guerilla groups or transnational terrorist organizations, there is a lack of literature addressing such attacks executed by a traditional nation-state with fixed infrastructure. A guerilla organization may be able to execute information attacks without any substantial fear of retaliation. A nation-state, such as China, could be subject to retaliation, via both conventional military and information channels. As such, the relationship between asymmetric application of IW by a traditional state actor and the potential for retaliation in kind, mitigating or terminating such an attack, deserves further study.

Analysis

The study of this area in the United States is still largely limited to military think tanks and research institutes scouring obscure publications for Chinese thinking on Information Warfare. The information that is available comes from the writings of Chinese military leaders and scholars. It reveals a picture of a China that is fascinated with the notion of

Information Warfare — not only because of the prospect of better managing military operations or disabling foes dependent upon information technologies during a warfare situation, but because the Information Revolution may represent what is referred to in Western parlance as a Revolution in Military Affairs (RMA).

This revolution could represent as great an impact on military operations as the Industrial Revolution — perhaps more so. The US Army War College's Strategic Studies Institute encapsulates these findings in one simple thought: to China's leadership, it could mean a pathway to modernization that would obviate the need for costly and time-consuming interim modernization. In his study of China's information warfare strategy, Yoshihara (2001) delves into China's expanding interest in this realm. Chinese military leadership closely monitored recent high-technology conflicts, particularly the NATO action in Kosovo and the US actions in the Middle East.

“IW offers opportunities to win wars without the traditional clash of arms” (Yoshihara 2001). Indeed, China appears to be focused on the notion of such asymmetric warfare. Yoshihara (2001) goes on to explore the current state of Chinese IW and IO philosophy. The focus of Chinese theoreticians appears squarely focused on the possibility of IW offering China a decisive option to defeat a superior adversary by crippling its command and control capabilities. Moreover, Yoshihara (2001) notes that some Chinese military scholars consider the notion of victory without conventional battle; not only via disabling information-based attacks in the electronic realm, but even via more subtle psychological operations (PSYOP) designed to alter and shape an adversary's thinking.

Part of China's motivations for the intense focus on the information realm stems from China's fascination with recent conflicts driven by information. China witnessed the decisive US tactical victory in the Persian Gulf War, and wondered how such practice could be applied by its own military. In a recent Joint Forces Staff College monograph on Information Operations, Armistead explores this aspect of China's interest (2004). Again, the analysis is based on the writings of Chinese military scholars and academics. What is reflected is a strikingly modern interpretation of IO capabilities, viewed through the lens of traditional Chinese military philosophy. China is cognizant of the fact that it, too, will be subject to information-based attacks as it becomes more dependent on information-based systems. Armistead notes that China's focus is again on building a high technology war-fighting machine, with the prospect of skipping costly interim steps to modernize its military capabilities (2004). While it is acknowledged that Chinese IW capabilities are comparatively primitive at present, the United States is also much more vulnerable to information-based attack.

This is a cornerstone to the Chinese philosophy of asymmetric warfare previously discussed by Yoshihara. However, current Chinese military thinking on IW appears to contain a significant mirroring of US thought and doctrine. It remains to be seen whether these principles can be usefully applied in the Chinese military framework. Interestingly, Armistead notes that not only should the United States be aware of — and make preparations for — China's advances in this realm, but so should China's smaller neighbors, such as Taiwan, South Korea, and Japan (2001). Pervasive in the Chinese writing on IW is the notion of shaping the environment to facilitate military objectives; critically, the Chinese “view information warfare as a tool to counter the overwhelming

military superiority of the United States” (Armistead 2001). It is this thought process that summarizes China’s core motivations and thinking on IW.

The analysis of Chinese IW strategy has not stopped at the borders of military campuses and research institutes. The most recent Report to Congress of the US-China Economic and Security Review Commission finds that China’s emphasis on Information Warfare capabilities stems from their intensive “search for asymmetric capabilities to leverage against US vulnerabilities” and “represents a serious form of irregular warfare preparation” (USCC 2007). This strategy appears directed at obtaining capabilities that can deter or defeat the US in a limited engagement. One common theme in Chinese scenarios is a potential conflict over Taiwan.

China’s Information Warfare strategy with respect to the United States is indeed two pronged: in addition to the focus on technical activities, China has invested a great deal of effort to manipulate world opinion to cast itself and its activities in a positive light (USCC 2007). This, too, requires a patient and deliberate control of information, again serving to place China at an advantage in any potential conflict with the United States. The manipulation of perception via psychological operations and propaganda is a key component of Chinese strategy to placate an adversary into a false sense of security.

The report further notes that China’s “weapons acquisitions and training are guided by an overall strategy of preparation to win ‘informationized wars’”, here referring to the notion of conflict which is defined by a heavy reliance on information systems. Indeed, China’s military modernization plans seem squarely rooted in the idea of informationized war, in which China believes it could achieve the upper hand against the United States.

Between a building the capability to render a crippling blow to information-dependent US forces and the careful manipulation of world and US opinion, China is positioning itself to obtain what it believes will be the upper hand in any future conflict with the US, particularly with regard to Taiwan (USCC 2007).

In recent years, US literature on this topic has even begun monitoring “mainstream” Chinese military journals and textbooks. In a 2007 RAND report on Chinese strategy to deny US forces the ability to respond, Cliff notes that China appears to be mulling a first strike strategy, in which an initial Chinese attack takes the US by surprise, and disables or greatly deteriorates US forces’ ability to respond, leaving China free to pursue other aims — namely, a campaign against Taiwan. As one Chinese military expert put it, such an asymmetric information-based attack would render US military forces “blind,” “deaf,” and “paralyzed” (Cliff 2007). Direct, large scale attacks against US computer and information systems, either via disabling electromagnetic weapons or hacking, would be a part of this attack strategy.

China appears to be exploring its capabilities in the information realm. In early 2010, two incidents occurred which “demonstrated that China has the ability to substantially manipulate data flows on the Internet.” (USCC 2010) In March 2010, Chinese firewall policies appeared to cause a significant number of users within the United States to be denied access, or informed of restrictions. This appeared to be due to a deliberate or unintentional misconfiguration of a Domain Name Service (DNS) server in China. (USCC 2010) In April 2010, a more serious situation was observed. For about 18 minutes, China rerouted about 15% of all Internet traffic to servers within China, including traffic destined for US government (.gov) and US military (.mil) hosts and

networks. (USCC 2010) This was accomplished due to the way a core internet protocol known as Border Gateway Protocol (BGP) functions; while it cannot be proved to be intentional, it shows that China has the technological capability to significantly alter the flow of Internet traffic.

Again shifting to the social realm of Information Warfare, Cliff observes that the Chinese also believe the will of the American public can be shifted against pursuing a conflict with China by a combination of attacks designed to sway public opinion in favor of avoiding conflict, against the backdrop of a wave of devastating surprise attacks that would cripple US command and control (Cliff 2007). The asymmetry is important in Chinese strategy, as one Chinese expert believes China facing the US in a conventional conflict would be akin to “throwing an egg against a rock.” Thus, gaining the advantage using the information realm is viewed as a cornerstone in Chinese thinking in this area.

Defense

The effectiveness of CNO for intelligence and espionage operations has been demonstrated. For example, a malware network known as “GhostNet” was analyzed by the Information Warfare Monitor, and found to have an extensive operational reach. The research team found nearly 1,300 compromised hosts in 103 countries. These malware was controlled via servers based at a commercial ISP in China, and had full, realtime access to all data stored on each infected system. Peripherals such as local cameras and microphones could also be activated without the user's knowledge. Importantly, many of the infected hosts belong to officials in various governmental organizations and NGOs.

GhostNet demonstrates the reach and practicality of cyber operations for espionage and intelligence collection activities. (SecDevGroup 2009)

Historically, US CNO activities have been distributed through joint elements, such as Joint Task Force-Global Network Operations (JTF-GNO), Joint Task Force-Computer Network Defense (JTF-CND), and Joint Functional Component Command-Network Warfare (JFCC-NW). (Kenyon 2010) A foreign computer intrusion in 2008, likely from China, spurred further consolidation of offensive and defensive cyber capabilities. (Gertz 2010) In 2009, a new subunified combatant command was created, known as US Cyber Command (USCYBERCOM), which combined all cyber operations under one organization. USCYBERCOM is colocated with the National Security Agency (NSA) at Ft Meade, MD, and its commander is dual-hatted as Director, NSA. USCYBERCOM is now responsible for all computer network attack, defense, and exploitation activities. (Kenyon 2010)

Various US exercises conducted by “Red Teams” acting as enemy hackers have demonstrated vulnerabilities in US military and commercial information systems. (Adams 2001) Senior defense officials have described cyberspace as “the new domain of warfare”, with Deputy Defense Secretary William J. Lynn saying, “Information technology provides us with critical advantages in all of our warfighting domains so we need to protect cyberspace to enable those advantages.” (Pellerin 2010) Secretary of Defense Robert Gates warned that cyber attacks pose a "huge future threat and there is a considerable current threat", and that the US must respond in a coordinated fashion to defend both military and civilian networks with shared capabilities concentrated in NSA and USCYBERCOM. (AFP 2010) This worries civil liberties groups and privacy

activists, but the concern is that the resources of NSA and USCYBERCOM cannot be replicated for domestic affairs: “there isn't enough money, there isn't enough time and there isn't enough human talent.” (AFP 2010)

The US plans to defend information assets using a layered strategy, which “automatically deploy defenses to counter intrusions in real time. Part sensor, part sentry, part sharpshooter, these active defense systems represent a fundamental shift in the U.S. approach to network defense,” along with “multiple layers of defense that give us better assurance of capturing malware before it gets to us.” (Pellerin 2010) This is what is generally known in computer security as “defense in depth”, a practice in which there are multiple layers of protection, the defeat of any one of which doesn't result in a compromise.

Conclusion

The common theme in most analyses of the question of why China will continue to expand its Information Warfare capabilities against the US appears to be the notion of asymmetry acting as a distinct Chinese advantage in any such conflict. But why do Chinese strategists so easily embrace this asymmetric approach? A further examination of the literature reveals clues, and they lie in Sun Tzu's philosophy of victory by scaring the enemy into submission without battle, and Mao's concept of “people's war”, in which an inferior force exploits advantages to successfully engage and defeat a superior adversary. Because of this belief system, China is likely to continue to make significant investments in the expansion of its information warfare capabilities.

* * *

References

Alberts, David S., and Daniel S. Papp, eds. 1997. *The Information Age: An Anthology on Its Impact and Consequences*. Washington, DC: Office of the Assistant Secretary of Defense Command and Control Research Program (CCRP). http://www.dodccrp.org/files/Alberts_Anthology_I.pdf (accessed November 12, 2010).

AFP. 2010. US faces 'huge' cyber threat in the future: Gates. *AFP*, November 16. http://news.yahoo.com/s/afp/20101116/pl_afp/usinternetcybermilitary (accessed November 23, 2010).

Armistead, Leigh, editor. 2004. Recent Information Operation Campaigns. In *Information Operations: Warfare and the Hard Reality of Soft Power*. 91-116. Norfolk, VA: National Defense University. <http://www.iwar.org.uk/iwar/resources/jiopc/io-textbook.pdf> (accessed November 12, 2010).

Arquilla, John, and David Ronfeldt, eds. 1997. Foreword in *In Athena's Camp - Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND Corporation. http://rand.org/pubs/monograph_reports/MR880/ (accessed November 12, 2010).

Chaisson, K. 2007. "China Report Looks at 'Informationization'." *Journal of Electronic Defense* Vol. 30 Issue 7: 20. Online database *EBSCO Host*. <http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=25657991&site=ehost-live> (accessed November 12, 2010).

Cliff, Roger, Mark Burles, Michael S. Chase, Derek Eaton, and Kevin L. Pollpeter. 2007. *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the*

United States. Santa Monica, CA: RAND Corporation.
<http://rand.org/pubs/monographs/MG524/> (accessed November 12, 2010).

Gertz, Bill. 2010. 2008 intrusion of networks spurred combined units. *Washington Times*, June 3. <http://www.washingtontimes.com/news/2010/jun/3/2008-intrusion-of-networks-spurred-combined-units/> (accessed November 23, 2010).

Hildreth, Steven A. 2001. *Cyberwarfare*. CRS Report for Congress, June 19. Washington, DC: Library of Congress Congressional Research Service (CRS). <http://www.fas.org/irp/crs/RL30735.pdf> (accessed November 12, 2010).

Kenyon, Henry. 2010. Cyber Command grew from 12 years of work: How lessons learned allowed new command to form. *Government Computer News*, October 4. <http://gcn.com/Articles/2010/10/04/Operational-Lessons-Paved-The-Way-For-Cyber-Command.aspx> (accessed November 23, 2010).

Khalilzad, Zalmay, John P. White, and Andrew W. Marshall, eds. 1999. *The Changing Role of Information Warfare*. Santa Monica, CA: RAND Corporation. http://rand.org/pubs/monograph_reports/MR1016/ (accessed November 12, 2010).

Perellin, Cheryl. 2010. Lynn: Cyberspace is the New Domain of Warfare. *Defense News*, October 18. <http://www.defense.gov/news/newsarticle.aspx?id=61310> (accessed November 23, 2010).

Ross, Adam. 2010. Navy's World Class Cyber Command. *Nextgov*, April 9. http://cybersecurityreport.nextgov.com/2010/04/navys_world_class_cyber_command.php (accessed November 18, 2010).

SecDevGroup. 2009. Tracking Ghostnet. *Information Warfare Monitor*, March 29. <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network> (accessed November 23, 2010).

Toffler, Alvin and Heidi Toffler. 1997. Foreword in *In Athena's Camp - Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt. Santa Monica, CA: RAND Corporation. http://rand.org/pubs/monograph_reports/MR880/ (accessed November 12, 2010).

USCC. 2007. 2007 Report to Congress of the US-China Economic and Security Review Commission. US-China Economic and Security Review Commission, October 29. http://www.uscc.gov/annual_report/2007/report_to_congress.pdf (accessed November 17, 2010).

USCC. 2010. 2010 Report to Congress of the US-China Economic and Security Review Commission. US-China Economic and Security Review Commission, November 17. http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf (accessed November 18, 2010).

Yang, Richard H., and James C. Mulvenon. 1999. *People's Liberation Army in the Information Age*. Santa Monica, CA: RAND Corporation. http://rand.org/pubs/conf_proceedings/CF145/ (accessed November 12, 2010).

Yoshihara, Toshi. 2001. *Chinese information warfare: a phantom menace or emerging threat?* Strategic Studies Institute. Carlisle Barracks, PA: US Army War College.