Countering Chinese Cyber Operations:

Opportunities and Challenges for U.S. Interests

Mark A. Stokes and L.C. Russell Hsiao

October 29, 2012

PROJECT 2049 INSTITUTE

Mark A. Stokes is the Executive Director of the Project 2049 Institute. A twenty-year U.S. Air Force veteran, Mr. Stokes served as Team Chief and Senior Country Director for the People's Republic of China, Taiwan, and Mongolia in the Office of the Assistant Secretary of Defense for International Security Affairs. He also was Assistant Air Attaché at the U.S. Embassy, Beijing and served as a signals intelligence officer at Clark AB, Philippines and West Berlin, Germany. Prior to co-founding Project 2049, he was Vice President and Taiwan Country Manager for Raytheon International. He has served as Executive Vice President of Laifu Trading Company, a subsidiary of the Rehfeldt Group; and a member of the Board of Governors of the American Chamber of Commerce in Taiwan. He holds a BA from Texas A&M University and graduate degrees in International Relations and Asian Studies from Boston University and the Naval Postgraduate School. He has working proficiency in Mandarin.

L.C. Russell Hsiao is a Senior Research Fellow at the Project 2049 Institute. He was the Editor of China Brief at The Jamestown Foundation from October 2007-July 2011. Previously, he served as a Special Associate/Program Officer in the International Cooperation Department at the Taiwan Foundation for Democracy in Taipei, and a Researcher at The Heritage Foundation. Mr. Hsiao graduated from the American University's School of International Service and the University Honors Program. He is a member of the Young Leaders' Program of the Honolulu-based think tank Pacific Forum CSIS. Mr. Hsiao is proficient in Mandarin.

Cover image source: Csrc.nist.gov

About the Project 2049 Institute

The Project 2049 Institute seeks to guide decision makers toward a more secure Asia by the century's mid-point. The organization fills a gap in the public policy realm through forward-looking, region-specific research on alternative security and policy solutions. Its interdisciplinary approach draws on rigorous analysis of socioeconomic, governance, military, environmental, technological and political trends, and input from key players in the region, with an eye toward educating the public and informing policy debate.

www.project2049.net

Introduction

Computer networks are the main arteries of cyber operations. Information and communications technology enable and enhance the capabilities of actors to engage in the cyber realm. Modern societies and governments increasingly rely on cyber-based information systems in order to process, coordinate, and manage critical processes necessary to function. Yet due to the highly automated and interconnected nature of economic transactions and the protection of critical infrastructure, the cyber domain is emerging as a new dimension in conflicts of the future. Therefore, the capability inherent in the exploitation of computer network operations (CNO) represents a significant evolutionary stage in both civil and military affairs. In the case of the People's Republic of China (China), driven by political insecurities and a quest for total information awareness, the Chinese Communist Party (CCP), state authorities, and the Chinese People's Liberation Army (PLA) are allegedly waging a coordinated CNO campaign against a broad range of international targets.

Chinese cyber espionage poses an advanced persistent threat to U.S. national and economic security. Groups operating from PRC territory are believed to be waging a coordinated cyber espionage campaign targeting U.S. government, industrial, and think tank computer networks. A dozen of these groups have been identified and linked with the PLA, and others connected with universities and information security enterprises.[1] The largest and most active of these groups may operate from Beijing and Shanghai.[2]

Few, if any, U.S. organizations that work on China issues have escaped intrusions.[3] Targets include U.S. government networks, defense industry, high-technology and energy companies, think tanks and other nongovernmental organizations, media outlets, and academic institutions. Characterized by methods of encrypting exfiltrated data, attempts to gain control and access to U.S. computer systems rely in large part upon socially engineered email messages that may seem authentic targeting organizations and individuals of interest. Emails usually include an attachment, image or hyperlink, which, when opened, installs a remote access tool (RAT) that enables an operator to gain access and control of the recipient's computer. Operators may also use other techniques in which a computer of a targeted individual is compromised after accessing an infected website.[4]

While there are many cases, attributing responsibility to a specific Chinese-entity is a difficult task. However, the PLA General Staff Department (GSD) Third Department is likely a leading authority for cyber surveillance. In the absence of officially verified evidence, this informed hypothesis is based on an assessment of the department's

traditional core competency in signals intelligence, its high performance computing and encryption/decryption technical capabilities, and status as China's largest employer of well-trained linguists.[5] Roughly analogous to the U.S. National Security Agency (NSA), the Third Department manages one of the largest intelligence collection and information security infrastructures in the world. Accepting as premise that the capabilities of the Third Department may be an indicator of its possible mission: How may the Third Department be organized and equipped to command and control a coordinated CNO infrastructure? And from a U.S. standpoint: What means are available to counter an integrated cyber espionage campaign?

This assessment posits that the GSD Third Department command authorities manage a complex cyber reconnaissance infrastructure that exploits vulnerable computer networks around the world, while also ensuring the integrity of classified networks within China. Based on a thorough evaluation of available data, this infrastructure may center upon the Third Department's Beijing North Computing Center (BNCC). While the command relationships between these known and other unknown entities remain unclear, the PLA's CNO infrastructure also relies on a handful of Third Department managed information security bases that serve as a platform for cooperation with academia and cybersecurity companies. Operational Third Department entities, such as the Third Department Second Bureau in Shanghai, also appear to play a prominent role within a broader CNO network, alongside technical reconnaissance bureaus (TRBs) under military regions.

This assessment concludes with a brief discussion of policies that could best mitigate challenges posed by Chinese cyber espionage. Countering a coordinated cyber reconnaissance campaign requires reducing the value of information through thoughtful deception, enhanced counterintelligence, greater cooperation with international partners such as Taiwan, and imposing costs through effective deterrence.

Background

The PRC government views *informatization* of Chinese society as a means to ensure sustained economic growth, compete globally in the information technology realm, and ensure national security.[6] Informatization relies on information security systems that can support economic restructuring and national security. In the information age, information security can be viewed within the broadest context as ensuring CCP legitimacy, enhancing the party-state's ability to consolidate power, defending national networks against internal and external threats, and supporting economic development. Therefore, security of the party and state requires mastery of the global cyber sphere.[7]

Party and state leaders oversee an expansive but fragmented cyber operations policy infrastructure. The State Informatization Leading Group (SILG), consisting of senior representatives of the CCP Central Committee Politburo, State Council, and PLA, establishes national informatization policies.[8] With cyber security an important facet of informatization, the SILG's Network and Information Security Working Group [网络与信息安全组] has advised senior leaders on CNO policy.[9]

From a military perspective, Chinese PLA authors view cyber operations as a basis of modern warfare. Chinese CNO often is placed in the context of information security, or "network attack and defense," based on the premise that "without understanding how to attack, one will not know how to defend."[10] The GSD Third Department manages China's largest network for surveillance of foreign computer-controlled communications and computer networks themselves. The GSD Third Department enjoys a traditional core competency in signals intelligence (SIGINT), high performance computing, and encryption/decryption technical capabilities. The Third Department also is China's largest employer of well-trained linguists.

Cyber reconnaissance, or computer network exploitation (CNE) in the U.S. lexicon, represents the cutting edge of SIGINT and there are indicators that point to the Third Department serving as a national executive agent for CNE.[11] The Third Department has direct authority over 12 operational bureaus, a computing center, and three research institutes.[12] Bureau-level leaders have grades equivalent to that of an Army division commander, and oversee between six and 14 subordinate sites or offices [*chu*; 处]. The Third Department's 12 operational bureaus mostly likely report to the Headquarters Department. The operational bureaus are separate and distinct from TRBs under the PLA's seven Military Regions, and the three Services: Air Force, Navy, and Second Artillery.[13]

On behalf of the State Council's Ministry of Science and Technology, National Crypto Management Center, State Secrecy Bureau, Ministry of Public Security, and Ministry of State Security, the GSD Third Department also has administrative oversight of at least three information security engineering bases located in Shanghai, Beijing, and Tianjin.[14]

The Third Department's National Information Security Engineering Technology Center (NISEC) was established in Shanghai in 2001 and is directed by Senior Colonel Wen Zhonghui [文仲慧]. Born in 1954, NISEC Director Senior Colonel Wen is a cryptologic specialist who rose through the ranks of the GSD 58th Research Institute. He sits on the 863 Program Information Security Expert Working Group (863-917 Program, which funded establishment of the Great Firewall of China security system), and two information security standardization committees (WG-3 and WG-7).[15]


Sr. Col. Wen Zhonghui
Source: Web.nuist.edu.cn

Established in 2005 and directed by Major General Yuan Jianjun [袁建军], the engineering center's Beijing base is known as the National Research Center for Information Technology Security. Major General Yuan, director of the National Research Center for Information Technology Security, was formerly head of the PLA Information Security Evaluation and Certification Center (a Third Department Third Bureau-affiliated entity).[16]

Central authorities approved the establishment of a third base in Tianjin in 2009, which specializes in cryptographic keying material, systems integration, and computer network attack technology.[17] Collocated with these engineering centers are National Information Security Industrial Bases [国家信息安全产业基地], with additional industrial bases located in Wuhan and Chengdu.[18]

In addition to ensuring adherence to national information security standardization guidelines and training a new generation of cyber operations specialists, national information security bases appear to function as clusters that leverage academic and entrepreneurial talents of host cities. For example, Sichuan University's Institute of Information Security supports the Chengdu information security base and Shanghai Jiaotong University's School of Information Security supports the Shanghai base.

Within the Third Department, responsibilities for cyber reconnaissance remain opaque. Successful reconnaissance depends on cryptologic skills, stealth, automated scanning of targeted network vulnerabilities, data fusion and storage, and counter-reconnaissance technology.[19] While a number of PLA and other governmental entities likely share CNO responsibilities, at least two GSD Third Department organizations may be cognizant of groups responsible for cyber espionage. In particular, BNCC appears to have the technological capacity to manage a coordinated cyber operations network. The

Third Department Second Bureau in Shanghai is a representative example of a group possibly charged with collection and exploitation operations.

Beijing North Computing Center


Sr. Col. Geng Xiaohe
Source: Pku.edu.cn

Among PLA entities surveyed in this study, the GSD Third Department BNCC appears most capable of cyber reconnaissance architecture design, technology development, systems engineering, and acquisition. BNCC is located adjacent to Beijing University and the Central Party School in the city's northwestern Jiaoziying [哨子营] suburb. At least 10 subordinate divisions appear responsible for design and development of computer network defense, attack, and exploitation systems. One of China's earliest organizations engaged in high performance computing, BNCC leaders are equivalent in grade to an army division commander or Third Department bureau director.

BNCC, which is also referred to as the GSD 418th Research Institute, has a military cover designation of the 61539 Unit (previously was the 57370 Unit). BNCC may also be known as the Beijing North Commercial College [北京北方商业学院].[20] Senior BNCC authorities include Senior Colonel Geng Xiaohe [耿孝和] and Jia Yinghe [贾颖禾], and former BNCC Director Zhu Zhaoming [朱兆明] remains active in cyber community. Geng Xiaohe and Jia Yinghe both have served as senior advisors to the State Council Informatization Office's Information Security Working Group, and are also committee members of national-level computing associations. BNCC Chief of Staff and division directors include Fu Shengxin, [伏圣信], Li Xiaohui [李晓惠], Yao Jingsong [姚京松], Kong Tiesheng [孔铁生], Ma Hang [马航], and Yang Baoming [杨宝明].[21]


Jia Yinghe
Source: Media.ccidnet.com

Specific BNCC responsibilities are shrouded by a thick veil of secrecy. Initial indications of a role in cyber operations emerged in 2000, when Falungong authorities accused BNCC of launching denial-of-service attacks against the organization's mail servers.[22] Facility construction projects underway since 2006 indicate a significant growth in its scope of operations.[23] China's

leading cybersecurity experts, including BNCC Deputy Director Jia Yinghe, have highlighted the need for active defense involving intrusions of and attacks against enemy systems.[24] BNCC likely plays a leading role in command and control network management, code breaking, advanced malware development and acquisition, data storage, and vulnerability assessment. BNCC officers have experience in computer network attack and defense [网络攻防], network intrusion monitoring and control, and information collection. BNCC software source code has been made available to enterprises for commercialization. In addition to developing one of China's first stealthy RATs, BNCC fielded China's most advanced network intrusion detection system for analyzing threats and assessing vulnerabilities, including those associated with operating systems such as Android.[25] BNCC's active defense software was certified in tests involving attacks against target networks.[26] Its risk assessment function includes analysis of command and control systems. Supercomputing is required to crack advanced encryption systems. BNCC's advanced computing networks servers appear sufficient to handle vast databases containing collected electronic communications and files, including recorded phone calls, radio chatter, private emails, internet search records, passwords, password-protected computer files, as well as an abundance of personal data on individuals of interest.

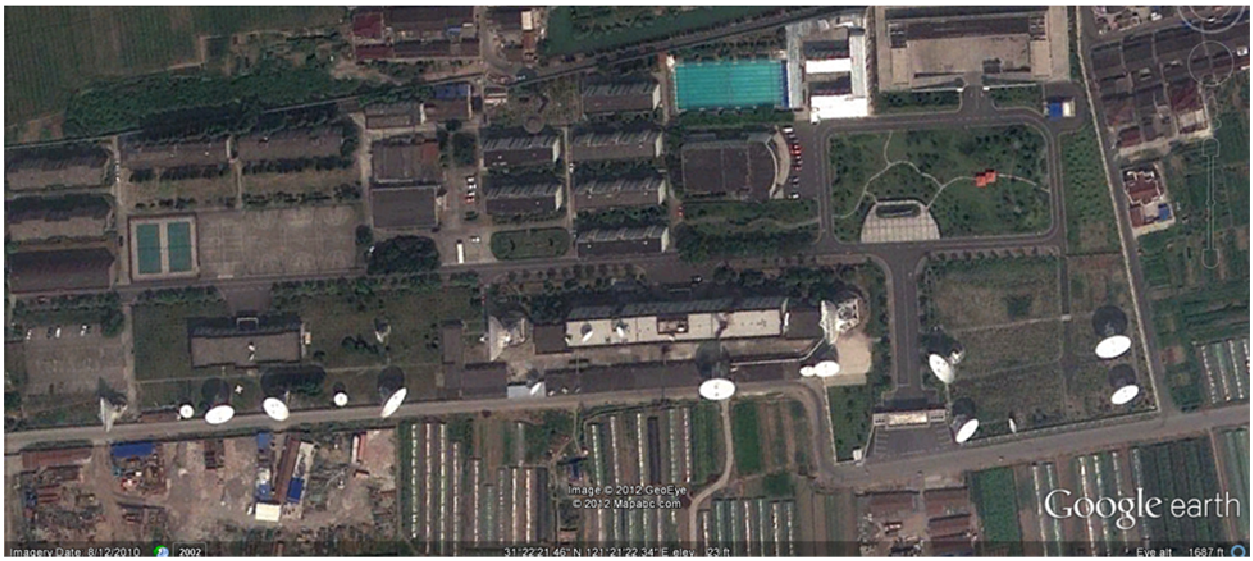
BNCC maintains a close relationship with a number of organizations within China's broader CNO community. In addition to formal positions within China's parallel and high performance computing community, BNCC senior engineers serve as advisors to the State Council Informatization Office, specifically the Information Security Working Group. Basic and developmental research support on high performance computing is carried out by the Third Department 56th Research Institute in Wuxi and National University of Defense Technology (NUDT) in Changsha. BNCC divisions rely on at least a dozen cybersecurity companies for day to day work. BNCC-affiliated companies also support information security engineering bases in Beijing, Shanghai, and Tianjin.[27]

GSD Third Department Second Bureau

While BNCC appears to be a central CNO authority, other GSD Third Department entities may manage routine exploitation of vulnerabilities in U.S. computer networks. The GSD Third Department Second Bureau is an illustrative example.[28] Responsible for collection operations against U.S. communications and computer networks, most Second Bureau elements are situated in Shanghai City. The Second Bureau command compound is located in Shanghai's northeastern Gaoqiao district. The First Division is collocated with Second Bureau headquarters, and appears responsible for analysis. Four of the eight identified divisions under the Second Bureau are located in Shanghai's northern Baoshan District. At least two of these divisions appear to operate from a

Third Department Second Bureau satellite ground station in Baoshan District's Caijiaying village. Other elements probably under command of the Second Bureau are located in Sichuan Province and on Hainan Island.[29]

PROBABLE THIRD DEPARTMENT SECOND BUREAU SATELLITE GROUND STATION
SHANGHAI BAOSHAN DISTRICT



The Second Bureau maintains relationships with a range of entities in the greater Shanghai area. The Second Bureau leverages access to the Shanghai City's internet monitoring center (dubbed the Shanghai 005 Center), which is managed by China Telecom.[30] It maintains facilities in the vicinity of submarine cable landing stations on Chongming Island and in Shanghai's southern Nanhui District.[31] Senior officers, both retired and active, maintain academic affiliations with the Shanghai Association of International Strategic Studies and the Shanghai Strategy Association.[32] The Second Bureau managed the establishment of the Third Department's information security engineering base in Shanghai.[33] Based on the number of technical studies jointly produced by representatives from both organizations, the Second Bureau also enjoys a cooperative working relationship with Shanghai Jiaotong University's School of Information Security Engineering.[34]

Other Third Department elements in the Shanghai area include the Third Department 12th Bureau command (61486 Unit); and the Third Bureau's Third Division (61587 Unit). As a side note, members of the Third Department Third Bureau's Third Division have conducted studies on cyber warfare, including analysis of weaknesses in Android operating systems and NTLM authentication protocols. Members of the Third Division have carried out joint studies with Shanghai Jiaotong University's Department of Computer Science and Engineering.[35]

In short, the GSD Third Department command authorities manage a complex infrastructure that exploits vulnerable computer networks around the world. Responsible for ensuring PLA freedom of action in cyberspace, BNCC appears to play a central role in coordinating cyber reconnaissance operations among a range of players, software engineering, and data storage. In addition to the Third Department's Second Bureau in Shanghai, other PLA organizations are also positioned to exploit foreign computer networks.

While appearing to exercise executive authority, the GSD Third Department does not enjoy a monopoly over cyber espionage. TRBs subordinate to military regions, the Air Force, Navy, and Second Artillery also may collect against foreign targets of interest. For example, one source with a record of reliable reporting on cyber issues has highlighted operations traced back to the Shenyang Military Region TRB. Public security bureaus at city and provincial levels also have computer monitoring groups, as does the Ministry of State Security. The Third Department First Bureau (61786 Unit) manages an information security research center [信息安全研究中心] that is most likely focused on cryptography, and the Seventh Bureau has published a number of studies on cyber operations. The Third Department Third Bureau oversees several cyber security functions, such as certification of public keying material.[36]

Concluding Comments

Cyber espionage and potential disruption of critical U.S. computer networks have emerged as a significant national security challenge. In his May 2011 *International Strategy for Cyberspace,* President Obama declared that the United States will work with partners to "encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate." In response, the U.S. national security community is adopting a multifaceted approach to address the cybersecurity challenge, including through strengthened awareness, deterrence, greater investment into counterintelligence, and international partnerships. Defenses require a combination of measures. Counterintelligence tools include both disruption and deception, which offset the inherent asymmetric advantages that the attacking side enjoys.[37]

Deception as Defense

Passive or defensive network operations alone are inadequate to defend sensitive data. Offensive operations are core to counter-cyber espionage doctrine.[38] An initial approach to defending against Chinese cyber surveillance is deception and perception management.[39] Viewing cybersecurity as a major national security problem, the White

House established the Comprehensive National Cybersecurity Initiative (CNCI) that includes a government-wide cyber counterintelligence plan and developing enduring deterrence strategies and programs.[40] Programs also involve forensic examination of networks to identify, disrupt, neutralize, penetrate, or exploit Chinese cyber reconnaissance activities. With the Federal Bureau of Investigation (FBI) as lead for cyber counterintelligence operations, a key aspect of the CNCI includes proactive disruption of Chinese exploitation of U.S. computer networks.[41] Presumably as part of the CNCI, U.S. Cyber Command (CYBERCOM) has implemented a cyber deception program, with care taken to avoid "blowback" that affects U.S. society.[42] Deception and disinformation has also been recommended as a defensive tool for U.S. corporations and non-profit enterprises.[43]

Cyber deception likely would be effective due to PLA tendency for stovepiping and an ingrained cognitive bias regarding the United States and its intentions. Deception as a defense complicates an attacker's ability to plan and execute operations.[44] Necessary tools allow cyber intruders to retrieve material that is manipulated before release. Honeypots, or the creation of false networks, are one form of deception.[45] However, more sophisticated forms of data manipulation creates challenges for PLA collectors and analysts, and increases workload with minimal investment of resources for the U.S. side. The Pentagon's Defense Advanced Research Projects Agency (DARPA) has invested in research and development on "fog computing,"[46] a scalable and automated architecture for detecting intruders and offering decoy products rather than legitimate information.[47] DARPA also is investing in a next generation national cyber range to be managed by Johns Hopkins Applied Physics Laboratory.[48] As a final note, cyber defenses could benefit from greater investment into traditional human intelligence work and open source exploitation. Individuals with direct access to party-state information security policies and GSD Third Department cyber reconnaissance activities may provide valuable support for technical operations.[49]

International Cyber Code of Conduct

Another approach to cyber-defense is engaging PRC civilian and military authorities on the International Code of Conduct for Information Security, an initiative that Chinese and Russian representatives proposed in September 2011.[50] While Chinese expression of interest in an international code of conduct is a positive move, the proposal fails to strengthen international cross-border law enforcement. Article 3 only supports international collaboration in the case of a threat to its power base by dissident political extremists or terrorists. The proposed code promotes national censorship policies, while at the same time promoting the freedom to search, acquire, and disseminate information. Furthermore, the proposed code of conduct makes no reference to cyber espionage.[51] While challenges exist in developing a common set of

interests, most important would be a focus on managing non-state actors engaged in cyber-related criminal activities. Worth noting is Beijing's claim that non-state actors are responsible for cyber reconnaissance activities launched from Chinese territory.[52]

An Asian Cyber Defense Alliance?

While developing an international code of conduct presents challenges, greater collaboration with allies and coalition partners in the Asia-Pacific region may be warranted. The Republic of China (Taiwan) is the most obvious candidate for co-development of techniques best suited for the challenges emanating from the PRC.[53] Taiwan was the first and most intense target of CCP-sponsored cyber espionage.[54] For instance, in spite of the thaw in tensions between China and Taiwan over the past four years, Taiwan's intelligence chief – National Security Bureau director Tsai Der-sheng [蔡得胜] – recently revealed at a legislative hearing that Chinese hackers have been launching attacks on Taiwan-based websites, exfiltrating more than 26,000 pieces of information over the past seven years. Moreover, the NSB has been the target of more than 1 million cyber-attacks in the first half of this year alone.[55]

According to Chuang Ming-hsiung, section chief at the Taiwan Criminal Investigation Bureau's High-Technology Crime Prevention Center: "Before China releases a virus to the United States, it will test it on Taiwan. That's why Taiwan has a faster response rate than the United States."[56] Furthermore, cyber defenders on Taiwan are assisted by a shared cultural heritage with China, helping them to better decipher a Chinese attacker's strategic culture and way of thinking.[57] The October 2007 agreement on information technology signed by senior representatives of Taiwan MND and US DoD is a solid foundation upon which to deepen and broaden the bilateral relationship and beyond.[58] As part of Taiwan's own efforts to strengthen its cyber-defense capabilities against China, the Taiwanese government is reportedly increasing its spending on cyber-defenses by expanding the Communication Electronics and Information Bureau (CEIB) and creating a facility for conducting simulated cyberwarfare.[59]

Forceful Response?

The PLA's ambitious cyber operations also warrant consideration of appropriate responses to hostile attacks intended to neutralize U.S. command and control and critical infrastructure. Most important would be the determination of what types of computer network attacks would constitute an act of war, and whether or not kinetic responses would be appropriate. As National Security Agency Director and CYBERCOM Commander General Keith Alexander noted in a recent Congressional testimony: "I can assure you that, in appropriate circumstances and on order from the National Command

Authority, we can back up the department's assertion that any actor threatening a crippling cyber attack against the United States would be taking a grave risk."[60]

Cyberspace is a critical domain for national security and computer network operations are essential tools for ensuring future operational effectiveness. Governments throughout the world are taking active steps to strengthen cybersecurity. In the case of the PRC, the existing data suggests that BNCC may be the leading agent responsible for planning, coordinating, integrating, and synchronizing PLA computer network operations, including defense of classified networks, exploitation of foreign networks, and possibly denying an adversary access to his networks. Roughly analogous to the U.S. CYBERCOM, BNCC ensures PLA freedom of action in cyberspace. Information security engineering bases in Shanghai, Beijing, and Tianjin serve as windows to the broader academic and commercial cybersecurity community. The Third Department Second Bureau is an illustrative example of a front end collection entity that may exploit the network managed by BNCC and information security bases.

In order to mitigate the challenges posed by Chinese cyber espionage and countering a coordinated cyber reconnaissance campaign require reducing the value of information through thoughtful deception, enhanced counterintelligence, greater cooperation with international partners such as Taiwan, and imposing costs through effective deterrence. The U.S. appears to be taking the Chinese cyber challenge seriously and dedicating resources into countermeasures. As noted above, deception and technological defenses are two viable investments that could be augmented with an expanded dialogue on a cyber code of conduct. Greater consideration of appropriate and measured deterrent options and potential forceful responses are warranted as well.

---

[1] Siobhan Gorman, "U.S. Homes In on China Spying," *Wall Street Journal*, December 13, 2011, at http://online.wsj.com/article/SB10001424052970204336104577094690893528130.html.

[2] David Barboza, "Hacking Inquiry Puts China's Elite in New Light," *New York Times*, February 21, 2010, at http://www.nytimes.com/2010/02/22/technology/22cyber.html?_r=2&; Michael Riley and Dune Lawrence, "Hackers Linked to China's Army Seen from EU to D.C.," *Bloomberg*, July 26, 2012, at http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html; Siobhan Gorman, "U.S. Homes In on China Spying," *Wall Street Journal*, December 13, 2011, at http://online.wsj.com/article/SB10001424052970204336104577094690893528130.html; and Bill Gertz, "White House Hack Attack," *The Washington Free Beacon*, September 30, 2012, at http://freebeacon.com/white-house-hack-attack/. Command and control servers have also been traced to Chengdu, Guangzhou, and Hebei province. LUCKYCAT Redux: Inside an APT Campaign with Multiple Targets in India and Japan, Trend Micro Research Paper, Forward-Looking Threat Research Team, 2012, at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf.

[3] Jim Wolf, "U.S.Cyber Warrior Accuses China of Targeting Pentagon," September 27, 2012, at http://www.reuters.com/article/2012/09/28/usa-cybersecurity-china-idUSL1E8KRL0E20120928.

[4] Among various sources, see Robert O'Harrow Jr., "In Cyberattacks, Hacking Humans Is Highly Effective Way To Access Systems," *Washington Post*, September 27, 2012, at http://www.washingtonpost.com/investigations/in-cyberattacks-hacking-humans-is-highly-effective-way-to-access-systems/2012/09/26/2da66866-ddab-11e1-8e43-4a3c4375504a_story.html; Crouching Tiger, Hidden Dragon, Stolen Data (London, Context Information Security, 2012), at http://www.contextis.com/news/articles/targetedattacks/Targeted_Attacks_Whitepaper.pdf.; and Ellen Messmer, "Spear-Phishers Lie In Wait At 'Watering Hole' Websites," Network World, October 9, 2012, at http://www.networkworld.com/news/2012/100912-spearphishing-watering-holes-263156.html.

[5] See James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in *Beyond the Strait: PLA Missions Other Than Taiwan*, eds. Roy Kamphausen, David Lai, and Andrew Scobell, Strategic Studies Institute, U.S. Army War College, April 2009, p. 274; and Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Northrop Grumman Corporation Information Systems Sector Report for the U.S.-China Economic and Security Review Commission, at http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf. For an excellent review of Chinese cyber operations, see Desmond Ball, "China's Cyber Warfare Capabilities," Security Challenges (Australia), Vol. 7, No. 2 (Winter 2011), pp. 81-103, at http://www.securitychallenges.org.au/ArticlePages/vol7no2Ball.html.

[6] "China Maps Out Informatization Development Strategy," May 11, 2006, PRC Embassy in Washington DC, at http://www.china-embassy.org/eng/xw/t251756.htm.

[7] See Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Northrop Grumman Report Prepared for the U.S.-China Economic and Security Review Commission, March 7, 2012, at http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf; and *Annual Report to Congress on Military and Security Developments Involving the People's Republic of China* (Wash DC: Department of Defense, 2012), at http://www.defense.gov/pubs/pdfs/2012_CMPR_Final.pdf.

[8] As of October 2012, members of the State Informatization Leading Group include Wen Jiabao, Li Keqiang, Liu Yunshan, Zeng Peiyan, Zhou Yongkang, and Guo Boxiong. The leading group is assisted by an Advisory Committee for State Informatization (ACSI). The State Council Informatization Office (SCITO; 国务院信息化工作办公室) is responsible for day to day tasks. Among various sources, see Advisory Committee for State Informatization website, at http://www.acsi.gov.cn/en/. The 863-917 Program has served as an extra-budgetary source of funding for cyber technology development, and is best known for the developing the National Information Security Management System [国家信息安全管理系统], also known as the 005 Engineering project (aka, the Great Firewall of China).

[9] See Jimmy Goodrich, "Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy," in Jon Lindsay (ed.), *China and Cybersecurity: Political, Economic, and Strategic Dimensions* (University of California, San Diego Workshop Report, April 2012). The working group has included Li Keqiang, Zhang Dejiang, Liu Yunshan, Ling Jihua, Meng Jianzhu, and Chen Bingde.

[10] For the concept of "without understanding how to attack, one will not know how to defend" [不懂进攻就不会防守], see Qiu Junbo [邱俊波] and Hu Zewen [胡泽文], "The Incredible Abilities of Hacker MM: Chengdu Area Universities' Cyber Defense and Attack Competition" ['黑客MM'实力不俗 成都高校举办网络攻防大赛], *Sichuan Morning News,* April 25, 2005, http://news.qq.com/a/20050425/001504.htm. Also see a 2007 news article published on Chengdu's University of Electronic Science and Technology of China website at http://news.cduestc.cn/news/xykj/ShowArticle.asp?ArticleID=5030. Also see You Ming and Zhou Xiyuan, "Analysis of Attack and Defense Mechanisms in Information Network War" [信息网络对抗机制的攻防分析], *Network Security Technology and Application*, December 6, 2004, at http://tech.ccidnet.com/art/1101/20041206/185771_1.html.

[11] See, for example, "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, March 29, 2009, at http://www.nartv.org/mirror/ghostnet.pdf. SIGINT consists of communications intelligence (COMINT) and electronic intelligence (ELINT). The latter involves collection, analysis, and storing of radar emissions. While Third Department has the COMINT portfolio, the GSD Fourth Department likely is responsible for ELINT. See Ian Easton and Mark Stokes, *China's Electronic Intelligence Satellite Developments: Implications for U.S. Air and Naval Operations* (Arlington, VA: Project 2049 Institute, 23 February 2011).

[12] Eight of the 12 bureau headquarters are clustered in Beijing. Two others are based in Shanghai, one in Qingdao, and one in Wuhan. See Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 2049 Occasional Paper*, November 11, 2011, at http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.

[13] See James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in *Beyond the Strait: PLA Missions Other Than Taiwan*, eds. Roy Kamphausen, David Lai, and Andrew Scobell, Strategic Studies Institute, U.S. Army War College, April 2009, p. 274; and Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Northrop Grumman Corporation Information Systems Sector Report for the U.S.-China Economic and Security Review Commission, at http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf. For an excellent review of Chinese cyber operations, see Desmond Ball, "China's Cyber Warfare Capabilities," Security Challenges (Australia), Vol. 7, No. 2 (Winter 2011), pp. 81-103, at http://www.securitychallenges.org.au/ArticlePages/vol7no2Ball.html.

[14] See "Construction Completed on National Information Security Engineering Technology Center Website" [国家信息安全工程技术中心网站完工], Beijing Lan Bo Synergy Technology Co. Ltd. [北京蓝博融智科技有限 公司], September 22, 2008, at http://www.librich.com/news_view.asp?viewid=51; furthermore, Beijing Guowei Xin'an Network Technology Company [北京国卫信安网络技术有限公司] works closely with Third Department First Bureau in supporting the project. See "Yin Chuan-xi" [尹传喜], at http://www.ushi.cn/p/2991; and "Cooperation Partners," China Cuslink Co., Ltd. [北京中海通科技有限公司], at http://www.cuslink.cn/Partners.aspx.

[15] Among various sources, see "Wen Zhonghui," Nanjing University of Science and Technology website, at http://web2.nuist.edu.cn:8081/JRY/toArticle.action?id=1153. For an official NISEC overview, see the

National Information Security Engineering Technology Center website [国家信息安全工程技术研究中心] at http://www.nisec.cn/.

[16] The National Research Center for Information Technology Security is located adjacent to GSD Third Department Seventh Bureau command headquarters on Nongda Road in northern Beijing suburb of Shangdi. Li Jingchun [李京春] is the center's Chief Engineer and has spoken publicly on cyber warfare issues [see "网络特攻"，谁主沉浮？]. Gong Yafeng [宫亚峰], who has been linked with the Third Department's 61062 Unit, serves as Deputy Chief Engineer. For further background, see The National Research Center for Information Technology Security [国家信息技术安全研究中心] website at http://www.isra.org.cn/.

[17] "Tianjin National Information Security Engineering Center" [天津国家信息安全工程技术研究中心], Center website, at http://www.nisib.cn/News_4.aspx.

[18] Among various sources, see "Construction Completed on National Information Security Engineering Technology Center Website" [国家信息安全工程技术中心网站完工], Beijing Lan Bo Synergy Technology Co. Ltd. [北京蓝博融智科技有限 公司], September 22, 2008. Sichuan University houses an Information Security and Network Attack/Defense Research Lab [四川大学信息安全及网络攻防研究室].

[19] Le Chang, "On Computer Network Reconnaissance" [关注计算机网络侦察], *PLA Daily*, June 12, 2002, at http://www.pladaily.com.cn/gb/pladaily/2002/06/12/20020612001037.html. Also see Wang Yongjie, Xian Ming, Wang Guoyu, and Xiao Nangping, "A Data Fusion Algorithm of Computer Network Reconnaissance" [种计算机网络侦察的数据融合算法], *Computer Engineering*, March 2005. Also see Zhu Wei, "Research on Remote Internal Network Infiltration" [远程内网的渗透和信息密取技术研究], Shanghai Jiaotong University thesis, September 1, 2006.

[20] BNCC may also be known as the Beijing North Commercial College [北京北方商业学院], which is assigned IP addresses in the range of 202.205.240.0 - 202.205.243.255.

[21] Other prominent PLA authorities on cyber issues include: Shen Changxiang [沈昌祥] from the PLA Navy; retired Third Department computer engineering export Jin Yilian [金怡濂]; Cui Shukun [崔书昆] from the Third Department; Song Jianping [宋建平] from the Third Department Technology Exchange Center; Third Department cryptographic specialist Yuan Wengong [袁文恭]; Ji Zengrui [吉增瑞] from the GSD 56th Research Institute; Zhao Zhansheng [赵战生]; Chen Zuoning [陈佐宁] from the 56th Research Institute; Chen Huaping [陈华平] from the GSD Third Department; Huang Minqiang [黄民强] from the Third Department First Bureau; Third Department and Central Committee cryptographic expert Zhou Zhongyi [周仲义]; Wei Zhengyao [魏正耀] from the 58th Research Institute, Lu Haimin [吕海民]; Dai Hao [戴浩] with the GSD 61st Research Institute;. Xiao Jinghua [肖京华] from the Third Department Third Bureau; and retired BNCC cryptographic specialist Nan Xianghao [南相浩].

[22] See "Falun Gong Mailboxes Attacked," Minghui.org, April 28, 2000, at http://en.minghui.org/html/articles/2000/4/28/8378.html#.UI6ApMXEZ_Q. The attacks started on April 24. Most of the attackers used the servers of 263.net, 163.net and 371.net. The article notes that the organizations involved in the attacks included the "Internet Security System Lab of the Beijing North Computing Center (seal.bncc.edu.cn)," "Department of Computer Science of Beijing North Commercial College," "Shangdu information center," and "Zhengzhou data communication branch bureau of

Zhengzhou city, Henan Province 450052." "Shangdu" may be a misspelling of Shangdi, where BNCC registers its IP addresses.

[23] One source asserts that BNCC is expanding to a group army-level institute [军职]. Another source claims that BNCC is no longer subordinate to the GSD Third Department.

[24] See Gao Lihua, "Information Security: The Solution Lies in the "Core"?" [信息安全：出路在于"中国芯"？], *Computer World*, November 22, 2002, at http://tech.sina.com.cn/it/e/2002-11-22/1329151576.shtml. Other sources available upon request.

[25] Systems developed and fielded by BNCC are licensed by or compete with private enterprises, such as Venus Technologies. Among various sources, see http://product.it168.com/ProductCompare_p199458_101684_s0515.shtml. The NETMAN covert remote access software was awarded a PLA technology award in 1999. See Zhu Chunyan, "Helping to Control Own Networks: Beijing North Computing Center Produces NETMAN Network Management System"［帮助你管好自己的网络 北方计算中心推出网络管理系统 NetMan], *Computer World Journal*, 1995 (Issue 47). NETMAN, which was certified in 1995, has become a common remote access tool that is advertised as capable of stealthy network penetration. BNCC also was responsible for SAFEmate [网络安全伴侣], a network attack and defense project sponsored by the State Council Informatization Office and certified in 1997. BNCC also co-developed the NISDetector network monitoring and early warning system, ISExplorer intrusion detection system, and the DSC-200 software package that cleans electronic fingerprints. In addition to developing NetGet information collection software (see http://www.netget.com.cn/), BNCC engineers have also conducted R&D on rootkit technology.

[26] [杀毒软件"杀"气渐微 微点主动防御强者自强], *Xinhua News Agency*, September 27, 2008, at http://news.xinhuanet.com/internet/2008-09/27/content_10120722.htm.

[27] Sources can be made available upon request.

[28] The Third Department Second Bureau was formerly the 57322 Unit. Former Second Bureau leader Lu Peng [吕蓬] now serves as Deputy Director of the Shanghai Institute for International Strategic Studies. Former Second Bureau Political Commissar Qiu Zuping [邱祖平] appears to have been transferred to the PLA Air Defense Command Academy in the 2010/2011 timeframe.

[29] More specifically, the Sichuan site has a military cover designation of Unit 61357 and is located in Minzhu City's Zundao Village. The facility was damaged during the Sichuan earthquake in 2008. The old MUCD was 57332.

[30] See "Regarding GSD Third Department Requirements for Our Company's Communication Channels" [关于总参三部二局需使用我公司通信管道的请示], China Telecom Marketing Department Announcement, March 20, 2009.

[31] These landing sites are high volume entry points for internet traffic to and from China. The Chongming facility may be subordinate to the 61161 Unit (possibly the Second Bureau's Third Office). As a side note, a GSD Fourth Department brigade (61251 Unit) oversees an element in the Nichangzhen area, and possibly on Chongming Island.

[32] The former is not to be confused with its affiliate, the Shanghai Institute of International Strategic Studies [SIIS; 上海国际问题研究院]. Zhou Jianping is a senior officer from the Second Bureau's First Office who has an affiliation the Shanghai Association of International Strategic Studies [SAISS; 上海国际战略问题研究会] and the Shanghai Strategy Association [上海战略研究会]. Former Second Bureau leader Lu Peng [吕蓬] serves as SAISS Deputy Director.

[33] A construction company listed the Second Bureau as the contracting organization for construction of the Engineering Center's six-story building in Pudong. The same company also won the bid for construction of the Second Bureau's new general headquarters building in 2007. See "Notice of Unit and Project Management" [报名单位及项目经理信息], Changzhou Project Bidding Center Website, at http://www.czzbb.net/czzb/YW_Info/YW_ZiGeYS/BaoMingInfo.aspx?YW_RowID=41726&BiaoDuanBH=CZS20091202901&enterprise_id=70362377-3. A Shanghai company refers to the Information Security Engineering Technology Center as a Third Department window for international cooperation, and was awarded a contract for a malicious network attack behavior lab [网络恶意攻击行为研究实验室].

[34] A senior State Council Informatization Advisory Committee [国家信息化专家咨询委员会] member, He Dequan [何德全], directs the Jiaotong University School of Information Security Engineering. The school is collocated with the Third Department's National Information Security Engineering Technology Research Center. See "School of Information Security Engineering at Shanghai Jiao Tong University," School of Information Security Engineering website, at http://infosec.sjtu.edu.cn/infosec/en/introduction/intro1.html. For an example of joint research, see Jiang Weixin, Xue Zhi, and Chen Yiqun, "Design of a Collaborative Intrusion Monitoring System Architecture" [协同式入侵监视系统的体系结构设计], *Computer Applications and Software*, June 2007.

[35] See Chen Yiqiang, "Brief Analysis of Android System Security" [简析Android系统的安全性能], *Information Systems Engineering*, 2011(9), at http://d.wanfangdata.com.cn/periodical_xxxtgc201109035.aspx. The 61587 Unit also maintains a presence in Ningbo City. As of 2011, Jin Ying [金鹰] commanded the Third Bureau Third Division (61587 Unit). He likely replaced Shi Yuanjie [石元杰]. Senior Colonel Zhang Fangxin [张方新] has been Political Commissar since at least 2008. Deputy Commander Li Genquan [李根权] previously commanded a Third Department Third Bureau collection site in Hangzhou (61791 Unit). Another Deputy Commander is Shi Tongnian [施彤年].

[36] The PLA Secrecy Committee Technical Security Research Institute [解放军保密委员会技术安全研究所] is the 61600 Unit, which is most likely Third Department.

[37] *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (Wash DC: 2011), at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

[38] Among various references, see James M. Olson, "Ten Commandments of Cyber Counterintelligence: A Never-Ending Necessity," *Studies in Intelligence* (Central Intelligence Agency Center for the Study of Intelligence), June 27, 2008, at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/fall_winter_2001/article08.html.

[39] Neil C. Rowe, "Deception in Defense of Computer Systems from Cyber-Attack," L. Janczewski, & A. Colarik (eds.), *Cyber Warfare and Cyber Terrorism*, pp. 97-104, at http://faculty.nps.edu/ncrowe/wardefdec.htm.

[40] *The Comprehensive National Cybersecurity Initiative* (Wash DC: Executive Office of the President, 2010), at http://www.cyber.st.dhs.gov/docs/CNCI-Cybersecurity.pdf.

[41] "National Cybersecurity Center Policy Capture." Available from: http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf

[42] Bill Gertz, "Pentagon Deception," *Washington Times*, September 14, 2011, at http://www.washingtontimes.com/news/2011/sep/14/inside-the-ring-860333104/?page=all.

[43] *Employing Disinformation Security™ to Protect Corporate Networks with NetBait™*, NetBait, June 2003, at http://www.infosecwriters.com/text_resources/pdf/NetBait_disinfo_wp.pdf.

[44] For an excellent overview on deception in cyber defense operations, see Neil C. Rowe, "Deception in Defense of Computer Systems from Cyber-Attack," L. Janczewski, & A. Colarik (eds.), *Cyber Warfare and Cyber Terrorism*, pp. 97-104, at http://faculty.nps.edu/ncrowe/wardefdec.htm.

[45] Fred Cohen, "The Use of Deception Techniques: Honeypots and Decoys," *Handbook of Information Security*, V3 (Hoboken: Wiley and Sons, 2006), p. 646, at http://all.net/journal/deception/Deception_Techniques_.pdf

[46] Noah Shachtman, "Feds Look to Fight Leaks With 'Fog of Disinformation'," *Wired*, July 3, 2012, at http://www.wired.com/dangerroom/2012/07/fog-computing/.

[47] Dan "Rags" Ragsdale, Scalable Cyber Deception, DARPA Cyber Colloquium, Arlington, VA, November 7, 2011, at http://www.dtic.mil/dtic/tr/fulltext/u2/a551951.pdf; and "Anomaly Detection At Multiple Scales (ADAMS)," Allure Security Technology Inc, study sponsored by Sponsored by the Defense Advanced Research Projects Agency (DOD), November 9, 2011, at http://dsearch.dtic.mil/search?q=cache:FsgWcwTFmzAJ:www.dtic.mil/dtic/tr/fulltext/u2/a552461.pdf+%22Allure+Security%22&site=tr_all&client=dticol_frontend&proxystylesheet=dticol_frontend&ie=UTF-8&access=p&oe=UTF-8.

[48] "APL Receives $24.7 Million to Build Prototype Cyber Range," Johns Hopkins University Applied Physics Laboratory website, January 21, 2010, at http://www.jhuapl.edu/newscenter/pressreleases/2010/100121.asp.

[49] Edward Wong, "Official Suspected of Spying for U.S. Said to Be Held in China," *New York Times*, June 1, 2012, at http://www.nytimes.com/2012/06/02/world/asia/china-is-said-to-detain-official-spying-for-united-states.html?_r=0.

[50] "China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations," Chinese Ministry of Foreign Affairs, September 13, 2011, at http://nz.chineseembassy.org/eng/zgyw/t858978.htm.

[51] Jeffrey Carr, "4 Problems with China and Russia's International Code of Conduct for Information Security," Digital Dao: Evolving Hostilities in the Global Cyber Commons, September 22, 2011, at http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html.

[52] Camino Kavanagh with Matthew Carrieri, Cyber Dialogue 2012 Briefs: Thinking Strategically About Cyber Security, second annual Cyber Dialogue forum on March 18-19, 2012 in Toronto, Canada, at http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012briefs/brief-4.pdf.

[53] Chung Chen-fang, "Experts Say Taiwan is China's Primary Target" [专家说台湾是中国网络攻击优先目标], *Voice of America*, May 15, 2012, at http://www.voacantonese.com/articleprintview/1149438.html.

[54] Mark Stokes and L.C. Russell Hsiao, "Taiwan's Role in Air-Sea Battle," *AsiaEye*, April 16, 2012, at http://blog.project2049.net/2012/04/taiwans-role-in-air-sea-battle.html.

[55] Joseph Yeh, "Chinese cyber-attacks worse than feared: NSB," *China Post*, September 28, 2012, at http://www.chinapost.com.tw/business/company-focus/2012/09/28/355801/Chinese-cyber-attacks.htm.

[56] Wu Tsen-Hsi, "Taiwan's Cyber Defense Honed By Frequent Attacks," *Epoch Times*, May 21, 2012, at http://www.theepochtimes.com/n2/china-news/taiwans-cyber-defense-honed-by-frequent-attacks-240544.html.

[57] Wu, "Taiwan's Cyber Defense Honed By Frequent Attacks."

[58] See "Taiwan Economic and Cultural Representative Office (TECRO) and American Institute in Taiwan (AIT) Information and Communication Technologies (ICT) Forum Terms of Reference," October 31, 2007, at http://www.ait.org.tw/en/tecro-agreement/108.pdf.

[59] Kevin Kwang, "Taiwan ups cyberwar prep," ZDNet, September 3, 2012, at http://www.zdnet.com/taiwan-ups-cyberwar-prep-7000003603/.

[60] Zachary Fryer-Biggs, "U.S. Military Goes on Cyber Offensive," *Defense News*, March 24, 2012, at http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive.